СПбГУТ)))

Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М. А. Бонч-Бруевича

12TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2023

Международная научно-техническая и научно-методическая конференция
«Актуальные проблемы инфотелекоммуникаций в науке и образовании»

АПИНО ICAIT

2023

СБОРНИК НАУЧНЫХ СТАТЕЙ

APINO.SPBGUT.RU

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

технологии бесконечности

КОМПАНИЯ Т8

Компания «Т8»
t8.ru

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ
ИНФОРМАЦИЯ
КОСМОС

ТУЗС

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

Научный журнал
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
И ТЕЛЕКОММУНИКАЦИИ
ijitt.ru

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. И. Макаренко; сост. В. С. Елагин, Е. А. Аникевич. СПб. : СПбГУТ, 2023. Т. 1. 1030 с.

В научных статьях участников конференции исследуются состояние и перспективы развития мирового и отечественного уровня IT и телекоммуникаций. Предлагаются методы и модели совершенствования научно-методического обеспечения отрасли связи и массовых коммуникаций.

Предназначено научным работникам, аспирантам и студентам старших курсов телекоммуникационных и политехнических вузов, инженерно-техническому персоналу и специалистам отрасли связи.

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 15.05.2023.
Вышло в свет 31.05.2023. Формат 60×90 1/8.
Уст. печ. л. 64,38. Заказ № 096-ИТТ-2023.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ISBN 978-5-89160-292-2

СОДЕРЖАНИЕ

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

УДК 35.075
ГРНТИ 81.01.00

БЕЗОПАСНЫЙ ГОРОД – ПРАКТИКА И ИННОВАЦИОННЫЕ РЕШЕНИЯ В ИНТЕРЕСАХ ГОРОЖАН

И. А. Лобацкий

Санкт-Петербургское государственное казенное учреждение «Городской мониторинговый центр»

Для обеспечения безопасной среды жизнедеятельности Санкт-Петербурга была создана государственная информационная система «Аппаратно-программный комплекс «Безопасный город», в состав которого вошли системы обеспечения безопасности и отраслевые системы. Некоторые из этих систем представлены в данной статье.

«Безопасный город», автоматизированные системы, видеонаблюдение, безопасность, мониторинг.

В Санкт-Петербурге проживает более 5 млн жителей, а его площадь составляет полторы тысячи квадратных километров. В городе каждый день проводятся разные по масштабу мероприятия. Для управления городом такого масштаба и обеспечения безопасности населения в Санкт-Петербурге создана и успешно функционирует государственная информационная система «Аппаратно-программный комплекс «Безопасный город» (далее – АПК БГ). При этом, среди российских регионов Санкт-Петербург уже не первый год является лидером по созданию развитию и внедрению элементов «Безопасного города».

В настоящее время в состав АПК БГ входят 11 автоматизированных систем: такие как 112, видеонаблюдение, 004, контроль автотранспорта, КСОМБ и другие.

Все эти системы, обеспечивающие безопасность, а также более 20 отраслевых систем – объединяет в едином окне система «Прогнозирование и поддержка принятия управленческих решений» или кратко ППППУР.

Вот некоторые из них.

Городской центр видеонаблюдения (ГЦВН)

В настоящее время системой видеонаблюдения охвачены все 18 районов города, это более **76** тысяч камер, в их числе **около 10 000** интегрированных камер сторонних систем видеонаблюдения. С учетом плановой работы по развитию данной системы до конца 2023 года количество камер должно возрасти **до 90** тысяч.

ГЦВН как современная система постоянного мониторинга способна не только выявлять правонарушения, но и способствовать их раскрытию правоохранительными органами, для которых АПК БГ стал незаменимым инструментом как в борьбе с преступностью, так и обеспечения общественного порядка. Об эффективности данной системы можно судить и по отчетным показателям ГУ МВД, так в 2022 году с использованием ГЦВН было выявлено **1700** и раскрыто **около 2000** преступлений.

Во исполнение решений Комиссии по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности Санкт-Петербурга и решений Межведомственной комиссии по профилактике правонарушений в Санкт-Петербурге в 2019 году Комитетом по информатизации и связи (далее – Комитет) совместно с Комитетом по строительству обеспечено внесение изменений в Региональные методические документы «РМД 11-22-2013». С учетом внесенных изменений в «Руководстве по проектной подготовке капитального строительства в Санкт-Петербурге» (далее – Руководство) предусмотрены рекомендации застройщикам объектов жилищного комплекса обеспечивать оснащение таких объектов системами безопасности (в том числе системами видеонаблюдения) на стадии их проектирования и строительства с последующей интеграцией указанных систем в АПК БГ, а также наделение Комитета полномочиями на выдачу соответствующих технических условий на основании запросов застройщиков (технических заказчиков).

Таким образом, при поступлении от застройщиков запросов на выдачу технических условий на оснащение новых объектов жилищного комплекса Санкт-Петербурга системами видеонаблюдения могут быть предусмотрены мероприятия по их интеграции с городской системой видеонаблюдения.

Комитетом, в рамках реализации комплексного инфраструктурного проекта «Умный двор», осуществляется модернизация домофонной инфраструктуры парадных многоквартирных домов и размещения на входах в парадные не просто видеодомофонов, а современных устройств мониторинга (далее – УМ). Благодаря реализации проекта «Умный двор», ГСВН позволяет контролировать безопасность и в спальных районах города. В соответствии с проектом осуществляется установка современных запорно-переговорных устройств (домофонов), оснащенных видеокамерами высокого разрешения, технологической сетью Wi-Fi, каналами передачи данных

и средствами аналитики. При этом необходимо отметить, что Комитет не занимается непосредственной установкой таких устройств, а получает видеопоток по сервисной модели, при этом работы по установке и согласованию с собственниками жилья возложены на подрядчика.

В настоящее время размещено более 36 тысячи таких устройств. Следует отметить, что по информации органов внутренних дел раскрываемость квартирных краж посредством УМ составляет порядка 90 %, что само по себе отражает уровень высокой эффективности данного сегмента.

Комплексная система обеспечения мониторинга безопасности (КСОМБ)

Для комплексного мониторинга безопасности объектов социальной инфраструктуры Санкт-Петербурга используется автоматизированная система «Комплексная система обеспечения мониторинга безопасности».

В соответствии с законодательством Санкт-Петербурга «О дооснащении комплексными системами обеспечения безопасности объектов социальной инфраструктуры Санкт-Петербурга» СПб ГКУ «ГМЦ» осуществляется мониторинг сигналов о срабатывании средств охранной сигнализации, средств тревожной сигнализации, средств автоматической пожарной сигнализации и оповещения, средств контроля загазованности, установленных на объектах социальной инфраструктуры Санкт-Петербурга (далее – ОСИ), с последующей их передачей в соответствующие структуры для реагирования (ГУ МЧС, ГУ МВД, Петербург Газ).

В АПК БГ поступают сигналы от 6433 объектов от пожарной, тревожной и охранной сигнализаций и систем контроля загазованности (информация представлена на слайде). Все поступающие извещения сначала анализируются для исключения ложных вызовов. После этого извещения, которые требуют реагирования экстренных служб, передаются в дежурную часть через службу «112». Такой алгоритм минимизирует передачу заявок по ложным срабатываниям в дежурные службы.

На настоящее время в адресном перечне объектов социальной инфраструктуры Санкт-Петербурга учтено 7 393 объекта. При дооснащении комплексными системами обеспечения безопасности ОСИ запрашивают и получают в СПб ГКУ «ГМЦ» технические условия.

Инновационные проекты.

Возможности АПК БГ не ограничиваются только поиском злоумышленников.

Городской мониторинговый центр разрабатывает проекты для обеспечения комфортного проживания граждан и поддержания на высоком уровне городского имиджа в глазах гостей города. В качестве примера одного из них, можно назвать совместно разработанный с администрациями райо-

нов, Комитетом территориального развития, Комитетом по природопользованию охране окружающей среды – план по противодействию несанкционированным свалкам отходов (далее – НСО) с помощью автоматизированной системы «Городской центр видеонаблюдения».

Так, на первом этапе планируется реализовать пилотный проект во Фрунзенском районе Санкт-Петербурга. Он предусматривает размещение средств городской системы видеонаблюдения на объектах НСО для круглосуточного контроля и фиксации государственных регистрационных знаков транспортных средств (далее – ГРЗ), появившихся на территории объектов с автоматической передачей данных о факте срабатывания сигнализации, включая фото распознанного ГРЗ нарушителя в систему ППППУР. При положительной реализации пилотного проекта он будет реализован на всей территории города.

В настоящее время в городе зафиксировано порядка 237 объектов НСО.

Не менее остро стоит вопрос своевременного вывоза мусора. В рамках исполнения поручения Губернатора Санкт-Петербурга в городе внедрена платформа видеонаблюдения и мониторинга (далее – Платформа) вывоза твердых коммунальных отходов (далее – ТКО), на базе которой реализован пилотный проект с использованием городской системы видеонаблюдения.

Комитетом доработаны: государственная информационная система «Объекты городской среды» и Портал «Наш Санкт-Петербург», в которых все места накопления ТКО нанесены на карту. С помощью нейронной сети обработка видео позволяет выявить нарушения в сфере контроля обращения с ТКО: «Контейнер пуст», «Контейнер переполнен», «Обнаружен мелкий мусор», «Зафиксирован мусоровоз». Таким образом определен механизм для решения городских задач в этой сфере, а при условии развития функционала Платформы предполагается в перспективе – обучение нейронных сетей для увеличения точности фиксации событий.

Нейронные сети помогают принимать разумные решения с ограниченным участием человека. Они могут изучать и моделировать отношения между нелинейными и сложными входными и выходными данными. Например, нейронные сети могут выполнять задачи в области контроля качества изображения средств видеонаблюдения: «Проблема с цветопередачей/поврежденный снимок», «Поворот в стену», «Помеха в виде зеленой кроны», «Помеха в виде веток деревьев», «Расфокусировка», «Неверная сцена обзора» и т. д. Важным для городского хозяйства является распространение нейросетей в области контроля благоустройства территории («Не очищена пешеходная зона», «Дорожное покрытие на очищено от снега», «Повреждение асфальтобетонного покрытия», «Наличие граффити», «Стертая дорожная разметка», «Обнаружен объект не характерный для дворовой территории»), детектирования огня («Обнаружено возгорание»), детектирование

дыма («Обнаружено задымление»). В области безопасности нейросетевой детектор объектов для контроля периметра («Обнаружен человек», «Обнаружен легковой транспорт», «Обнаружен грузовой транспорт» и т. п.).

Еще одной серьезной проблемой в городе является парковка автотранспорта в неположенных местах. Подавляющая часть автомобилей размещается во дворах жилых домов, иногда на зелёных газонах и площадках отдыха. Это обстоятельство, прежде всего, ухудшает условия проживания горожан. Автомобили оставляют также на проезжей части улиц. А это затрудняет городское движение, становится одной из причин дорожно-транспортных происшествий. Подобные «стоянки» занимают огромные площади городской территории, портят внешний облик городов.

Для решения данной проблемы Санкт-Петербургским государственным казённым учреждением «Городской центр управлением парковками Санкт-Петербурга» (далее – Учреждение) проведена работа по поиску необходимого программного обеспечения для тестирования обработки видеопотоков с видеокамер ГЦВН, а также анализ видеопотоков перспективных видеокамер для фиксации административных правонарушений за нарушения требований, предписанных дорожными знаками или разметкой проезжей части дороги и запрещающими остановку или стоянку транспортных средств. Реализация данного проекта позволит оказать существенное влияние на недобросовестных водителей автотранспортных средств.

Ещё один проекта Комитета – «Умные остановки». В планах 2023 года оснащение видеокамерами 200 остановок общественного транспорта (автобусные, троллейбусные уличные павильоны остановки транспорта). Это способствует профилактике правонарушений как в повседневной жизни, так и при проведении массовых мероприятий и акций, в ходе которых существует повышенный риск актов вандализма, краж, нанесения вреда здоровью. Наличие видеокамер на павильонах позволит скорректировать движение тех или иных маршрутов, тем самым снизив время ожидания и сохранить целостность павильонов, что является немаловажным фактором в связи с погодными условиями Санкт-Петербурга.

Акустическая смарт система «распределенного» звука

Данная всесезонная акустическая система – это технологичное решение, возникшее из задачи развивать региональную автоматизированную систему централизованного оповещения населения в случае чрезвычайных ситуациях. Заложенные на этапе проектирования возможности, с учетом перспективы, позволили посредством звукоусилительного оборудования не только передавать сигналы и речевые сообщения, но и транслировать высококачественный художественный контент, музыкальные и иные творческие программы. Таким образом помимо своей целевой задачи, в том числе используется для повышения уровня комфорта жителей и гостей города при

проведения массовых городских мероприятий, в числе которых шоу «Поющие мосты», предполагает – безупречный звук, отражающий величие и глубину классической музыки, а также резкое снижение громкости за границами системы.

Система эксплуатируется круглый год, имеет удаленное управление, функцию раздельной подачи контента на разные участки, а также выделенный канал связи с Городским мониторинговым центром для обеспечения информирования населения при проведении массовых мероприятий или возникновении чрезвычайных ситуаций.

В этом году цифровой комплекс был интегрирован в саду Смольного собора и Сквере финансистов. В планах Администрации города оборудовать смарт-системой до 30 самых значимых и посещаемых мест города. Развитие умных систем и их интеграция в едином контуре городского пространства – первоочередная задача цифровой трансформации города.

Проекты реализуются при поддержке Администрации Губернатора Санкт-Петербурга, Комитета по информатизации и связи, Комитета по печати и взаимодействию со средствами массовой информации Санкт-Петербурга.

Автоматизированная система «Прогнозирование и поддержка принятия управленческих решений» (ППППУР)

Система «Прогнозирование и поддержка принятия управленческих решений» объединяет в едином окне практически все системы, входящие в АПК БГ, в том числе и отраслевые. Ежедневно в ППППУР поступает информация (извещения) о более 5 тысячах происшествий. По каждому из них формируется карточка, а местоположение происшествия автоматически отображается на карте. В зависимости от типа происшествия в системе заложен алгоритм, благодаря которому к месту происшествия привязываются те или иные объекты, которые могут быть использованы при реагировании.

В системе ППППУР собрана информация практически обо всех объектах города:

- группировка ближайших видеокамер, с возможностью оперативного выбора камер и просмотра видео онлайн и из архива. Сейчас в городе более 76 тысяч камер, в том числе до 20 тысяч камер с видеоаналитикой;
- объекты социальной и транспортной инфраструктуры;
- потенциально-опасные объекты;
- места проведения массовых мероприятий;
- ограничения движения транспорта и ордера Государственной административно-технической инспекции;
- схемы теплосетей с подробной информацией;

•информация о домах, отключенных от электро-, газа-, водо- и теплоснабжения.

По каждому объекту можно увидеть подробную информацию: год постройки, информацию о собственнике, количество проживающих и т. д.

В режиме онлайн отображается геопозиционирование уборочной техники, общественного наземного и водного транспорта.

Ход реагирования фиксируется в протоколе.

Комитет по информатизации и связи является единым центром компетенций по созданию и развитию государственных информационных систем. Благодаря этому все разрабатываемые системы являются унифицированными, за счет чего достигается адаптивность к созданию новых слоев в ППППУР.

Пользователями ППППУР являются **до** 600 человек: руководство города, в том числе Губернатор, МЧС, правоохранительные органы, дежурные службы Администрации Губернатора, районов, а также исполнительных органов государственной власти (комитеты и подведомственные учреждения).

Еще до пандемии Городской мониторинговый центр планировал реализовать в ППППУР эпидемиологическую карту. Вместе с тем, уже сейчас имеются научные доказательства о зависимости здоровья от качества воздуха. В ППППУР уже реализована эпидемиологическая карта города, а до конца года будет реализована экологическая карта с отображением данных о качестве воздуха и карта здоровья населения.

Для развития Единой государственной системы предупреждения и ликвидации чрезвычайных происшествий внедрено геопозиционировании машин экстренных служб. Будет создана мобильная версия ППППУР.

Система ППППУР сейчас это центр (мозг) фиксации, анализа и решения задач по пресечению угроз в режиме многозадачности, позволяющий сократить риски, связанные с «человеческим фактором» такие как необъективность информации о событии, несвоевременное получение и анализ ситуации, неэффективный алгоритм оповещения заинтересованных ведомств и других.

В ежегодном планировании Комитета особое внимание уделяется развитию АПК БГ как неотъемлемому фактору обеспечения безопасной среды жизнедеятельности Санкт-Петербурга.

Список используемых источников

1. Постановление Правительства Санкт-Петербурга от 17.05.2007 года № 550 «О Комиссии по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности Санкт-Петербурга».

2. Постановление Правительства Санкт-Петербурга от 07.09.2007 года № 129 «О межведомственной комиссии по профилактике правонарушений в Санкт-Петербурге».

3. Постановление Правительства Санкт-Петербурга от 25.08.2016 года № 759 «О государственной информационной системе Санкт-Петербурга «Аппаратно-программный комплекс «Безопасный город».

4. Руководство по проектной подготовке капитального строительства в Санкт-Петербурге (РМД 11-22-2013 Санкт-Петербург).

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 654.927.2
ГРНТИ 49.46.01

КРАТКИЙ ОБЗОР ПОДВОДНОЙ БЕСПРОВОДНОЙ АКУСТИЧЕСКОЙ СВЯЗИ

С. С. Абрамов, Е. С. Абрамова, И. И. Павлов, М. С. Павлова

Сибирский государственный университет телекоммуникаций и информатики

В статье на основе произведенного анализа и обзора научных работ в области беспроводной подводной акустической связи представлена краткая история об образовании подводной акустической связи и её развитие. Рассмотрен вопрос о том, как изменялась скорость передачи и дальность передачи в подводной акустической связи. Также для решения проблемы подводного акустического канала было обсуждено и предложено несколько схем модуляции.

подводная беспроводная связь, подводная акустическая связь, скорость передачи данных, подводные акустические датчики.

В настоящее время подводная беспроводная связь реализуется через системы связи, основанные на акустических волнах, и электромагнитных волнах, которые в свою очередь реализуются на радиочастотных волнах и оптических волнах.

Подводная акустическая связь, которая рассматривается как наиболее популярный метод в подводной беспроводной связи, впервые в 1490 году, когда Леонардо да Винчи предложил использовать акустические средства для обнаружения кораблей, катеров и всевозможных лодок на расстоянии. Он использовал трубку, вставленную в воду, чтобы определять сосуды на слух. Подводные акустические методы продолжали использоваться в течение длительного времени, вплоть до конца 1800-х годов. В связи с неизбежной потребностью в средствах связи как во время первой мировой войны, так и во время второй мировой войны система подводной акустиче-

ской связи достигла желаемой осуществимости и, таким образом, стала известной технологией, так как применялась практически ко всем аспектам подводных беспроводных сетей датчиков [1].

Первое устройство подводной акустической связи было создано в США с использованием однополосной амплитудной модуляции с подавлением несущей, которая имеет диапазон несущих частот от 8 до 15 кГц, с основным диапазоном передачи голоса и фильтрами формирования импульсов. В результате принятый сигнал был плохого качества, что требовало способности человеческого уха и мозга распознавать и понимать искаженную речь. Значительное увеличение скорости передачи данных и функционального диапазона было отмечено с прогрессом в области цифровой передаче данных в 1960 году. Производительность была повышена с использованием многопутевых подходов. Чтобы обеспечить более эффективную подводную акустическую связь, было проведено множество исследований, которые в конечном итоге привели к разработке передовых методов оценки канала и различных алгоритмических конструкций в течение длительного периода. В 1995 году была предложена система подводной акустической беспроводной связи со скоростью передачи данных 40 Кбит/с. Система подводной акустической беспроводной связи с частотой 8 Кбит/с была усовершенствована для глубины 20 м и горизонтального расстояния 13 км в 1996 году. Интересно, что более высокоскоростная система подводной акустической беспроводной связи была предложена в 2005, который достигает скорости передачи данных 125 Кбит/с, используя метод 32 квадратурной амплитудной модуляции с частотой ошибок символов 10^{-4}. Более того, была доказана другая система подводной акустической беспроводной связи, которая имеет скорость передачи данных 60 Кбит/с, использующая 32 QAM, который может поддерживать связь на глубине 100 м и на расстоянии 3 км по горизонтали. Чтобы достичь больших скоростей передачи данных без необходимости сложных вычислений, многие исследователи использовали мультиплексирование с ортогональным частотным разделением широко используется в подводной акустической связи. Наряду с исследованиями, которые были проведены на подводной акустической беспроводной системы связи как в экспериментальном, так и в теоретическом направлениях, акустические модемы различных конструкций, которые могут быть использованы для подводных применений, были выпущены на рынок и были коммерчески доступны [2]. Несмотря на удивительный технический прогресс, подводная акустическая связь не достигла эффективных коммуникационных показателей из-за различных препятствий. Наиболее важными препятствиями, ограничивающими эффективную связь подводных акустических коммуникаций, является отсутствие каких-либо подобных типов подводных звуковых каналов, из-за особенностей подводной среды, где это крайне важно и сложно. Другими словами, система, которая работает

в одном месте (например, мелководье), может не работать в другом месте (таком как глубоководный океан) [1]. В настоящее время исследования физического уровня подводной акустической связи достигли определенной степени развития. Многие морские эксперименты доказали такую связь на расстоянии десятков километров или даже дальше и скорость передачи до десятков килобит в секунду или даже больше [3, 4, 5]. Последнее представляет собой значительное развитие на ранней стадии в несколько десятков бит в секунду.

Также была продемонстрирована передача видео на акустической основе. Наиболее значительным достоинством подводной акустической связи является ее огромная дальность контакта, которая может достигать десятков километров, учитывая огромную ширину океана и сильное ослабляющее воздействие соленой воды на другие каналы передачи, такие как оптическая волна и радиочастотная волна. В то время как системы подводной акустической беспроводной связи способны предоставлять приложения для командования и управления из-за большой дальности передачи, которую они доказали, их скорость передачи данных недостаточна для мультимедийных приложений под водой [1]. Чтобы сократить время и частотную дисперсию подводных акустических каналов была использована новая схема передачи, получившая название неортогонального множественного доступа с обратным временем (*the time-reversed non orthogonal multiple access* (TR-NOMA). В зависимости от разницы во времени прибытия (*the time difference of arrival* (TDOA) был предложен алгоритм локализации для сетей подводных акустических датчиков [6]. Для решения проблем подводного акустического канала было обсуждено и предложено несколько схем модуляции. Была предложена схема для решения проблемы избыточной энергии в мультиплексировании с ортогональным частотным разделением по уникальному слову (*the unique word orthogonal frequency division multiplexing* (UW-OFDM), и эта схема показала свое превосходство с точки зрения частоты битовых ошибок. Была предложена схема, называемая X-преобразования синхронной индексной модуляцией во временной области OFDM. В нескольких исследованиях [7, 8, 9, 10, 11] были предложены различные типы пространственной модуляции и показано улучшение частоты битовых ошибок. Также, чтобы улучшить частоту битовых ошибок подводного акустического канала и повысить энергоэффективность, были предложены различные типы псевдослучайного мультиплексирования обучающей последовательности шума с ортогональным частотным разделением. Далее была оценена производительность обучающей кодированной индексной модуляции с расширенным спектром (*the deep learning coded index modulation-spread spectrum* (DL-CIMSS), которая была предложена [12], над моделированием и измеренными подводными акустическими каналами. Результаты моделирования показывают способность предложенной схемы увеличивать

скорость передачи подводных акустических данных при значительном повышении энергоэффективности и низком уровне системных ошибок в битах и символах.

Заключение

В то время как акустический подход является наиболее распространенным подходом для получения подводной беспроводной связи, он имеет определенные внутренние технологические ограничения. Во-первых, скорость передачи данных по акустической линии связи довольно низкая (в пределах Кбит/с), поскольку частоты подводных звуковых волн варьируются от десятков Герц до сотен килогерц. Во-вторых, из-за низкой скорости передачи акустической волны в воде (для чистой воды она составляет около 1500 м/с при 20 градусах Цельсия) акустическая линия связи подвергается экстремальной задержке контакта (обычно в секундах). Поэтому он не может поддерживать приложения, которые включают обмен большими объемами данных в режиме реального времени. В-третьих, акустические приемопередатчики обычно большие, дорогие и потребляют много энергии. Они являются дорогостоящими для крупномасштабных подводных беспроводных сетей датчиков устройств.

Список используемых источников

1. Truax B. Acoustic communication. Greenwood Publishing Group, 2001.
2. Клоков А.В. Беспроводная оптическая связь – Мифы и реальность // Технология и средства связи. 2000. № 6. С. 12–13.
3. Stojanovic M. IEEE J. Ocean. Eng., 1996, 21, 125–136, doi: 10.1109/48.486787.
4. Ochi H., Watanabe Y., Shimura T., Basic Study of Underwater Acoustic Communication Using 32Quadrature Amplitude Modulation // JPN J. Appl. Phys., 2005, 44, 4689, doi: 10.1143/jjap.44.4689.
5. Song H., Hodgkiss W. Efficient use of bandwidth for underwater acoustic communication // Acoust J., Soc. Am., 2013, 134, 905-908, doi: 10.1121/1.4812762.
6. Абрамова Е. С., Павлова М. С., Абрамов С. С., Павлов И. И., Хан В. А. Принципы организации подводной оптической связи // Современные проблемы телекоммуникаций. Материалы Международной научно-технической конференции. Новосибирск, 2020. С. 445–448.
7. Qasem Z.A.H., Esmaiel H., Sun H., Qi J., Wang J., Deep Learning-Based Spread-Spectrum FGSM for Underwater Communication // Sensors, 2020, 20, 6134, doi: 10.3390/s20216134.
8. Junejo N.U.R., Esmaiel H., Sun H., Qasem Z.A.H., Wang J. Pilot-Based Adaptive Channel Estimation for Underwater Spatial Modulation Technologies // Symmetry, 2019, 11, 711, doi: 10.3390/sym11050711.
9. Hussein H., Esmaiel H., Jiang D. Fully generalised spatial modulation technique for underwater communication // Electron. Lett., 2018, 54, 907-909, doi: 10.1049/el.2018.0948.
10. Qasem Z.A.H., Esmaiel H., Sun H., Wang J., Miao Y. and Anwar S. Enhanced Fully Generalized Spatial Modulation for the Internet of Underwater Things // Sensors, 2019, 19, 1519, doi: 10.3390/s19071519.

11. Esmaiel H., Qasem Z.A., Sun H., Wang J., Rehman Junejo N.U. Underwater Image Transmission Using Spatial Modulation Unequal Error Protection for Internet of Underwater Things // Sensors, 2019, 19, 5271, doi: 10.3390/s19235271.

12. Qasem Z.A.H., Leftah H.A., Sun H., Qi J., Wang J., Esmaiel H. Deep learning-based code indexed modulation for autonomous underwater vehicles systems // Veh. Commun, 2021, 28, 100314, doi: 10.1016/j.vehcom.2020.100314.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ УЯЗВИМОСТИ ИНТЕРФЕЙСА ICONTROL REST API И УЯЗВИМОСТИ КОНСОЛИ ВЕБ-АДМИНИСТРИРОВАНИЯ МЕЖСЕТЕВОГО ЭКРАНА SOPHOS

Е. А. Абрамова, А. О. Горячкина, П. О. Федоров, В. С. Филёва, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье приведено описание ряда уязвимостей, связанных с работой информационных систем. В данной статье применялся анализ уязвимостей и атак, выполненный при помощи эксплуатации данных уязвимостей. Приведены примеры атак, выполненных с помощью эксплуатации данных уязвимостей. В статье так же описаны меры противодействия данным уязвимостям. На основании описанного в данной статье можно сделать вывод, что к наиболее распространенным причинам возникновения уязвимостей, как правило, относят: ошибки при проектировании и использовании программного обеспечения; несанкционированное внедрение и последующее использование ПО; внедрение вредоносного ПО; человеческий фактор. Своевременное реагирование на появление определенных уязвимостей и следование рекомендациям по их устранению способствуют поддержанию общего уровня информационной безопасности на должном уровне.

информационная безопасность; уязвимость, кибератака, информационная система, мониторинг.

Широкое распространение информационных систем во многих сферах жизнедеятельности и достаточно высокий коэффициент доверия к ним с пользовательской стороны дают повод задумываться о рисках, связанных с таким обильным использованием информационных систем [1]. Достаточно важным аспектом является взаимодействие узлов на сетевом уровне,

распределенных информационных систем, а также разрозненных информационных систем. В рамках данного взаимодействия по сети осуществляется передача данных, к примеру идентификационных атрибутов, и управляющих команд [2].

У множества пользователей появилась потенциальная возможность взаимодействовать с информационными системами, обрабатывающими и хранящими данные, в том числе конфиденциальные стратегически важные, среди этих пользователь неизбежно найдутся и злоумышленники. Как правило для взаимодействия с информационными системами злоумышленники эксплуатируют уязвимости системы или – это присущие объекту информатизации свойства, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные особенностями процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, а также условиями эксплуатации. Своевременный мониторинг сведений о появлении новых уязвимостей, может существенно повысить общий уровень информационной безопасности информационной системы [3].

В результате мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках от 11 мая 2022 года была опубликована информация об обнаруженных трех новых критических уязвимостях, получивших регистрационные номера CVE-2022-1388, CVE-2022-1040 и CVE-2022-28613 [3].

Уязвимость интерфейса iControl REST API средств защиты приложений BIG-IP CVE-2022-1388 или BDU:2022-02849 которая связана с фактом отсутствия проверки подлинности для функции, являющейся критически важной [4]. Эта уязвимость относится к классу уязвимости кода и имеет высокий уровень опасности. Эксплуатация данной уязвимости дает возможность нарушителю, действующему удаленно, выполнять различные произвольные команды, удалять или изменять файлы [5].

Уязвимость консоли веб-администрирования межсетевого экрана Sophos CVE-2022-1040 или BDU:2022-02850 связана с возможностью обхода аутентификации. Это позволяет злоумышленнику, изменив значение параметра, используемого для ссылки на объект, обойти авторизацию и получить доступ к ресурсам системы. Это прямой результат того, что приложение принимает пользовательский ввод, чтобы вернуть объект, не проводя при этом проверки авторизации. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код [6].

Уязвимость реализации протокола HCI Modbus TCP программируемых логических контроллеров Hitachi Energy RTU500 серии CMU CVE-2022-

28613 или BDU:2022-02848 связана с недостаточной проверкой вводимых данных. Эксплуатация данной уязвимости дает возможность нарушителю, действующему удаленно, вызвать перезагрузку устройства.

С помощью описанных выше уязвимостей был проведен ряд известных и официально задокументированных атак. 9 мая 2022 года российский видео-хостинг Rutube подвергся целевой компьютерной атаке. Информация об указанном инциденте размещена в официальном Telegram-канале Rutube (*t.me/rutube*) [7, 8].

По информации Telegram-канала (*t.me/NeKaspersky*) поражено более 75 % баз данных и инфраструктуры основной версии и 90 % резервных копий и кластеров для восстановления [9]. Администрация ресурса заявила, что инцидент локализован, в настоящее время ведутся работы по восстановлению инфраструктуры видеоотдачи, а вся информация будет восстановлена [10].

10 мая 2022 года в социальной сети Twitter (*twitter.com/sudormrf6/status*/1523651595770032128) опубликованы данные, якобы похищенные в результате взлома видео-хостинга.

В Telegram-канале (*t.me/readovkanews*) размещена информация о несанкционированном изменении телевизионных программ ряда провайдеров цифрового телевидения (таких, как МТС, НТВ-Плюс, Ростелеком и Яндекс) [11].

В Telegram-канале (*t.me/itarmyofukraine*2022) в период с 8 по 9 мая 2022 года координировались DDoS-атаки на следующие Интернет-ресурсы:

- Единая государственная автоматизированная информационная система учета объема производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции (ЕГАИС);
- сайты средств массовой информации (новостные порталы и сайты Интернет-телевидения);
- Интернет-ресурсы Минобороны России;
- Интернет-ресурсы, связанные с общественным движением «Бессмертный полк»;
- электронные банки документов периода Великой Отечественной войны;
- Интернет-магазины и другие Интернет-ресурсы, использующие символику специальной военной операции России на Украине.

С начала дня 11 мая 2022 года координируются атаки на Интернет-ресурсы российских сервисов для совместной работы, планирования задач и email-рассылок «Notisend» и «Weeek».

Эксплуатирования данных уязвимостей может привести к нарушению конфиденциальности информации, расположенной в различных информационных ресурсах [12]. К примеру, в социальной сети

Twitter (*https://twitter.com/Anonymous*_23_00/*status*/13432738459557891) размещены данные (порядка 188 Мб) Федеральной службы государственной статистики России. В ходе подтверждения полученной информации установлено, что опубликованные данные, наиболее вероятно, получены из открытых источников [13].

В социальной сети Twitter (*twitter.com/Ksecureteamlab/status*/1524230571580342272) опубликованы документы (порядка 1,5 Гб) компании ООО «СТРОИТЕЛЬНАЯ КОМПАНИЯ «ТРОН» [14]. Отмечается, что указанная компания реализует инфраструктурные проекты в телекоммуникационной индустрии, работает в сфере инженерно-технических средств охраны промышленных объектов, обеспечивает объекты системами электроснабжения.

В Telegram-канале (*t.me/dataleak*) размещена информация о публикации в открытом доступе данных пользователей СМИ «Главный якутский портал» (*ykt.ru*/). Отмечается, что данные включают порядка 1 млн записей, содержащих следующие поля описания: имя, телефон, адрес эл. почты, дата рождения, пол, логин, хешированный (SHA1) пароль, IP-адрес, идентификаторы соц. сетей (*Facebook*, ВКонтакте, Одноклассники, *Instagram*) [15].

В качестве меры противодействия для уязвимости CVE-2022-1388 можно привести установку обновлений из доверительных источников. В связи со сложившейся ситуацией и введением санкций против Российской Федерации рекомендуется производить установку обновления программного обеспечения только после полноценной оценки всех сопутствующих рисков. В качестве компенсирующих мер можно выделить

- блокировку доступа к iControl REST через личный IP-адрес;
- изменение TCP-портов 443 и 8443, которые используются по умолчанию;
- блокировку доступа к iControl REST через интерфейс управления;
- изменение конфигурации BIG-IP httpd. Если текущий оператор включения уже содержит конфигурацию, отличную от none, необходимо добавить следующую конфигурацию в конец текущей конфигурации в пределах существующих символов двойных кавычек.

В качестве меры противодействия для уязвимости CVE-2022-1388 можно привести установку обновлений из доверительных источников, предварительно оценив сопутствующие установке риски. Как компенсирующие меры можно выделить:

- запрет доступа к интерфейсам администрирования путем отключения неиспользуемых служб в ACL;
- изменение портов, используемых службами по умолчания (TCP-порт 8443);
- отключение доступа к пользовательскому порталу и веб-интерфейсу администрирования из общедоступных сетей (Интернет);

- использование виртуальных частных сетей для организации удаленного доступа (VPN).

Для противодействия уязвимости CVE-2022-28613 необходимо выполнить следующие компенсирующие меры:

- использовать средства межсетевого экранирования;
- сегментировать сеть с целью ограничения доступа к оборудованию из других подсетей;
- ограничить подключения персональных компьютеров к сетям общего пользования (Интернет);
- отключить функцию HCI Modbus TCP, если она не используется.

Важно отметить, что сами по себе уязвимости информационной безопасности не опасны. Они лишь открывают возможности для осуществления угроз ИБ. К наиболее распространенным причинам возникновения уязвимостей, как правило, относят: ошибки при проектировании и использовании программного обеспечения; несанкционированное внедрение и последующее использование ПО; внедрение вредоносного ПО; человеческий фактор. Своевременное реагирование на появление определенных уязвимостей и следование рекомендациям по их устранению способствуют поддержанию общего уровня информационной безопасности на должном уровне [18].

Список используемых источников

1. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36–40.

2. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика "РИ-2018" : материалы конференции. СПб., 2018. С. 570–571.

3. Волкогонов В. Н., Гельфанд А. М., Пестов И. Е., Поляничева А. В. Программное обеспечение мониторинга сети организации на основе системы zabbix // Свидетельство о регистрации программы для ЭВМ 2020617706 ; заявитель и правообладатель СПбГУТ. – № 2020616735 ; заявл. 29.06.2020 ; опубл. 10.07.2020.

4. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. Т. 1. С. 329–334.

5. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. N 3 (88). С. 38–46.

6. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. N 1. С. 47–58.

7. Красов А. В., Левин М. В., Фостач Е. С. Проблемы обеспечения безопасности облачных вычислений // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 520–522.

8. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 3. С. 26–32.

9. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. N 1. С. 70–76.

10. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. N 11. С. 39–47.

11. Виткова Л. А., Иванов А. И., Сергеева И. Ю. Исследование и разработка методик оценки рисков облачных ресурсов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 1. С. 152–155.

12. Виткова Л. А., Глущенко А. А., Сахаров Д. В., Чмутов М. В. Выбор оптимального метода оценки эффективности перехода к облачной архитектуре // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 168–171.

13. Виткова Л. А., Иванов А. И. Обзор актуальных угроз и методов защиты в сфере облачных вычислений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 179–182.

14. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации // Инновационные технологии, экономика и менеджмент в промышленности. XII международная научная конференция : сб. науч. ст. Волгоград, НПП Медпромдеталь, 2021. С. 203–204.

15. Миняев А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29–33.

16. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества : сб. науч. ст. по итогам круглого стола со всероссийским и международным участием. Москва, 2021. С. 113–115.

17. Пестов И. Е., Алехин Р. В., Руденко С. А., Федоров П. О. Исследование воздействия ddos-атаки на виртуальную машину при наличии и отсутствии технологии firewall // Теория и практика обеспечения информационной безопасности : сб. науч. тр. по материалам всероссийской научно-теоретической конференции. 2021. С. 263–269.

18. Пестов И. Е. Методика противодействия угрозам нарушения информационной безопасности инстансов и облачной инфраструктуры, основан на описании атак

и методов противодействия им, используя теории графов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 742–746.

УДК 004.7
ГРНТИ 49.39.29

ТЕНДЕНЦИИ РАЗВИТИЯ И БЕЗОПАСНОСТЬ IP-ТЕЛЕФОНИИ

Е. А. Абрамова, А. В. Красов, А. В. Поляничева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цифровая эпоха создала культуру, в которой все доступно по требованию. Это то, что предприятия испытывают растущую потребность в экономичных коммуникационных решениях, которые могут поддерживать мобильность предприятия. Именно здесь появляются системы VoIP. Эта технология позволяет пользователям внедрять гибкие системы связи. VoIP базируется на IP и использует Интернет, которая наследует все уязвимости. Для этого необходимо качественно защищать каждый ресурс в сети. Рассматривая конкретно телефонное оборудование существует также ряд угроз, а именно перехват звонков, представление нелегитимными пользователями, подмена номера и многое другое.

АТС, IP-телефония, инфраструктура, атака.

Введение

По мере своего развития IP-телефония из дополнительной услуги превращается в базовый сервис, который необходим любым организациям и компаниям, для того чтобы оптимизировать работу сотрудников. По мере совершенствования появилась возможность использовать данную технологию каждому. В настоящих условиях IP-телефония является основой для развития и формирования инструментов по обработке и передаче мультимедийного трафика. Для безопасной передачи трафика требуется комплексный подход, который может минимизировать количество возможных угроз.

Тенденции развития и безопасность

IP-телефония – это телефонная связь, работающая по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор

номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям.

В пятилетней перспективе, по прогнозам аналитической компании «ТМТ Консалтинг» CAGR (совокупный среднегодовой темп роста) за период 2022–2026 гг. составит 12,2 %. Объем рынка в 2026 году достигнет 31,5 млрд руб., количество компаний-клиентов приблизится к 618 тысячам.

Объем российского рынка виртуальных АТС в 2021 году (рис. 1) достиг 17,7 млрд рублей, увеличившись на 30,8 % в сравнении с 2021-м. Причем динамика выросла – в 2020 году темпы роста измерялась 23,3 %. Об этом свидетельствуют данные аналитической компании «ТМТ Консалтинг» [1].

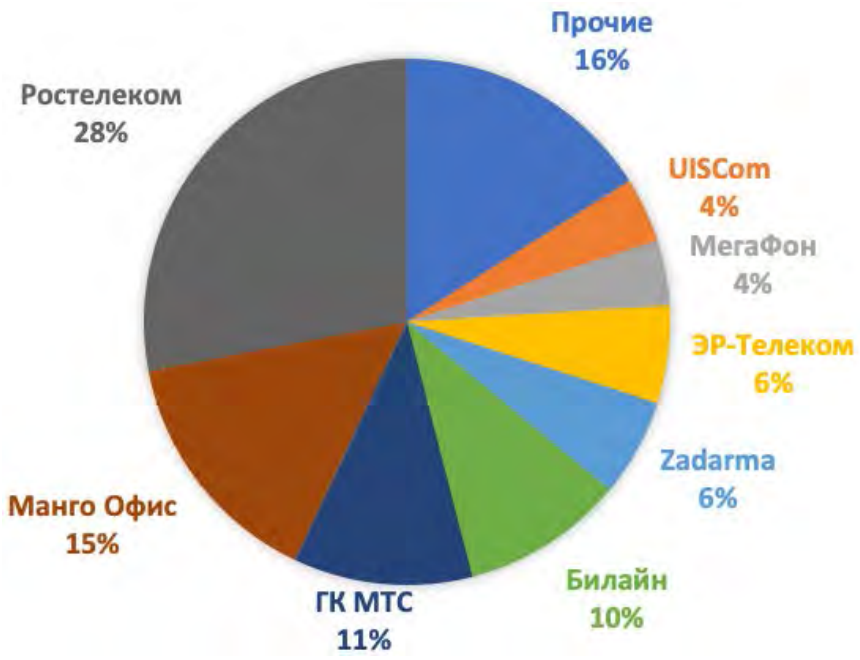


Рис. 1. Структура рынка ВАТС по числу компаний клиентов за 2021 год

Из-за экономии средств, а также функциональности системы VoIP- телефонии могут возникнуть проблемы безопасности. Предприятия должны знать, что их телефонная система устойчива к угрозам безопасности.

Ни одна телефонная система не является пуленепробиваемой.

Существует достаточное количество угроз и атак, которые могут влиять на функциональность работы любых систем [2].

Виды атак и взломов:

- подбор паролей – путем перебора всевозможных комбинаций;
- DOS – отказ в обслуживании, а именно высокая нагрузка на сеть передачи оцифрованных голосовых данных приводит к существенному искажению и даже пропаданию части сообщений, поэтому одна из атак на IP-телефонию может заключаться в посылке на сервер IP- телефонии большого числа «шумовых» пакетов;

• мошенничество со звонками, этот вид мошенничества еще называется «вишинг». Злоумышленник звонит по телефону и пытается побудить жертву к какому-либо действию. Он может притвориться сотрудником реальной компании, чтобы вызвать доверие;

• прослушивание VoIP вызовов.

Для обеспечения безопасности предлагаются некоторые советы, которые могут помочь противостоять атакам:

• отказ от стандартных паролей доступа на устройства: нельзя использовать лёгкие пароли admin, 123456 и другие простые сочетания букв и цифр;

• отказ от использования на рабочих компьютерах и смартфонах сомнительных софтфонов;

• настройка в Личном кабинете VoIP-провайдера доступ к авторизации с конкретного IP-адреса;

• постоянное обновление ПО.

Основными способами решения проблем взлома являются:

• установка сложных паролей – это одно из самых очевидных решениий проблемы, которое заключается в установке на учетные записи SIP сложных для взлома паролей;

• создание «белого списка» IP-адресов – это ограничение IP-адресов, с которых будет разрешена авторизация SIP-телефонов и софтфонов;

• регулярные проверки системы на предмет попыток взлома, контроль параметров – организация системы мониторинга состояния системы позволит улучшить качество IP-телефонии и отметить типовые для данной конфигурации параметры;

• уведомление о попытках звонков на «странные» номера – это полезное уведомление, которое в случае попытки дозвонится на подозрительные внешние линии, немедленно сообщит об этом администратору;

• использование средств аутентификации всех абонентов инфраструктуры IP-телефонии.

Все эти советы и способы помогут обеспечить и уже обеспечивают безопасное использование средствами связи, конкретно VoIP [3].

На мировом рынке VoIP наблюдался экспоненциальный рост за последние 20 лет. Благодаря постоянным технологическим усовершенствованиям, государственной поддержке и внедрению бизнеса отрасль не показывает никаких признаков замедления. Даже с учетом неопределенности, вызванной пандемией, рост удаленной работы приведет к росту индустрии VoIP в ближайшие годы. На самом деле, кажется, что он движется быстрее, чем когда-либо, с точки зрения использования, доли рынка и доходов.

Поскольку сегодня все больше компаний полагаются на поставщиков услуг VoIP для своих основных коммуникаций, важно следить за тенденци-

ями отрасли VoIP, чтобы увидеть, использует ли ваша компания эту технологию в полной мере (рис. 2). Предприятия, независимо от размера и масштаба, могут воспользоваться этими изменениями в отрасли в ближайшие годы и максимизировать свои инвестиции в эту технологию.

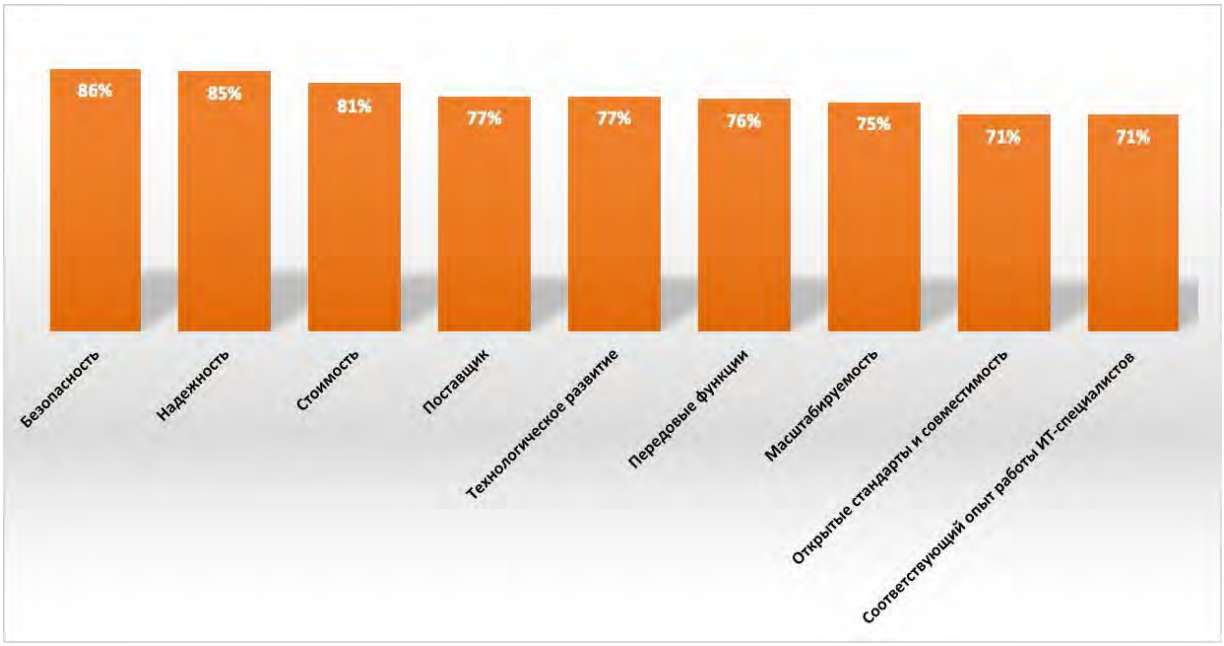


Рис. 2. Тенденции развития

Рассматривая конкретное оборудование, Mizu Softswitch – это настраиваемая серверная система VoIP общего назначения, предназначенная для операционных систем Windows, сочетающая в себе простоту использования, доступность с высокой стабильностью и пропускной способностью, что делает ее одним из выборов для корпоративных поставщиков услуг VoIP, операторов, а также для компаний малого бизнеса.

VoIP-сервер Mizu основан на открытых стандартах SIP и имеет все общие протоколы связи, встроенные для обеспечения совместимости с широким спектром устройств [4].

VoIP-сервер по умолчанию безопасен. Некоторые из методов, используемых для защиты данных клиентов:

- ограничитель скорости;
- встроенный динамический брандмауэр и черные списки – предотвращение DOS-атак на уровне адреса/ сеанса / пользователя;
- гибкая надежная аутентификация;
- поддержка шифрования (TLS, SRTP, пользовательское туннелирование VoIP на основе RSA).

При использовании всех перечисленных методов клиенты могут производить звонки, не беспокоясь о том, что они могут быть прослушаны злоумышленниками. Для передачи самих голосовых данных используется RTP.

Этот протокол реализует распознавание типа трафика, нумерацию последовательности пакетов, работу с метками времени и контроль передачи. Для сравнения ниже приведены графики звонков в незашифрованном виде, а также при правильной настройке SIP-клиентов и сервера можно зашифровать передачу голоса (рис. 3–4).

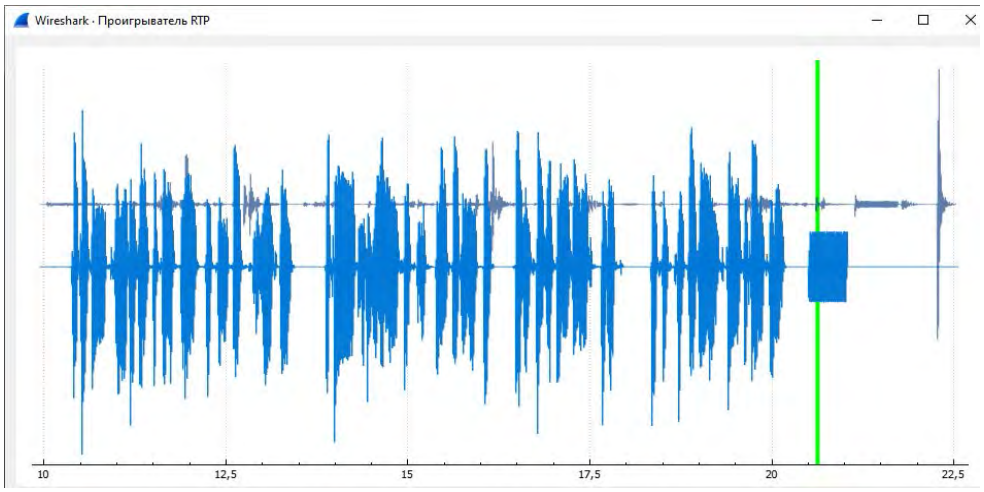


Рис. 3. График незашифрованного звонка

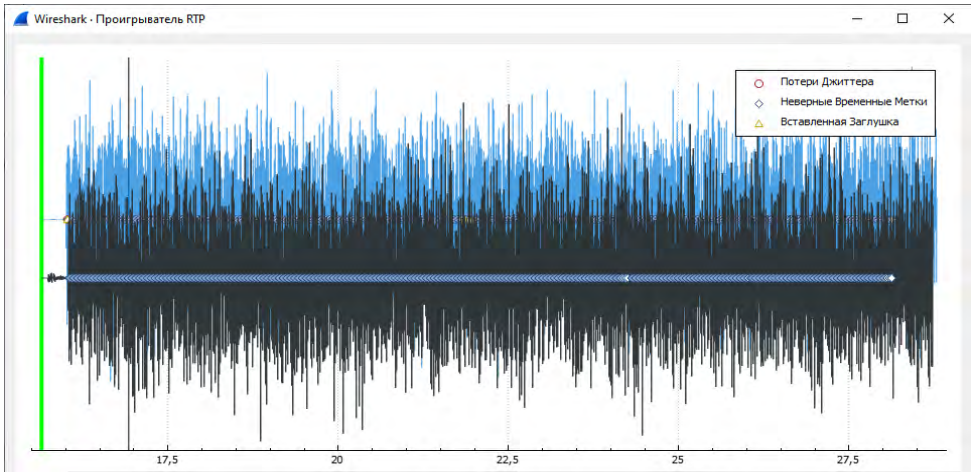


Рис. 4. График зашифрованного звонка

Безопасность остается неотъемлемой частью системы, поэтому необходимо отслеживать все возможные угрозы, которые появляются каждый день, а также

- контролировать количество и направления звонков, проходящих через АТС;
- шифрование;
- при необходимости подключения удаленных сотрудников использовать AAA, с помощью которого можно будет аутентифицировать их.

При проведении анализа были выявлены конкретные достоинства и недостатки IP-телефонии (табл. 1):

ТАБЛИЦА 1. Достоинства и недостатки IP-телефонии

Достоинства	Недостатки
Нет необходимости поддерживать две сети	Отсутствие гарантии доставки пакетов в определенном порядке
Снижение затрат, более экономичное решение, чем использование услуг проводной телефонной связи в аналогичном масштабе	Невозможность набора экстренного вызова, в случае сбоя или отключения электричества
Оптимизированная инфраструктура	Не всегда дешевое решение в контексте закупки оборудования
Масштабируемость	Риск взлома
Мобильность	Сложность первоначальной настройки

Вывод

Преимущества IP-телефонной связи неоспоримы. Анализ перспектив развития отрасли показал, что в будущем все развитые компании будут использовать именно эту технологию. Она в полной мере может сократить телефонные счета, а также есть возможность использовать ее за пределами офиса.

Угроз безопасности, с которыми могут встретиться пользователи VoIP-телефонии, немало. Данная технология наследует угрозы сети, на базе которой она работает, существует ряд угроз, непосредственно связанный с VoIP-оборудованием. Злоумышленники постоянно ищут все новые уязвимости для реализации различного рода угроз. Поэтому для того, чтобы связь была не только надежной, но и безопасной, необходимо позаботиться о нейтрализации возможных угроз и защищать соответственно само оборудование и сеть, в которой оно работает.

Список используемых источников

1. УАТС – офисные АТС (рынок России) // TAdviser [Электронный ресурс]. 11 марта 2022. URL: https://www.tadviser.ru/index.php/Статья:УАТС_-_офисные_АТС_(рынок_России) (дата обращения: 24.01.2023).

2. Безопасность АТС и системы связи // 3CX [Электронный ресурс]. URL: https://www.3cx.ru/3cxacademy/advanced/security-with-3cx-phone-system/ (дата обращения: 24.01.2023).

3. Обеспечение безопасности в сетях VoIP // АВАНТАЖ маркет телеком [Электронный ресурс]. 4 ноября 2019. URL: https://market-telecom.ru/blog/danger-voip (дата обращения 24.01.2023).

4. Mizutech Professional VoIP solutions [Электронный ресурс] URL: https://www.mizu-voip.com (дата обращения 26.02.2023).

УДК 004.896
ГРНТИ 50.43.19

ПРОГНОЗИРОВАНИЕ ВРЕМЕНИ ДОСТАВКИ СООБЩЕНИЙ БОЛЬШОГО ОБЪЕМА В СЕТИ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

В. С. Авраменко, И. А. Лукин

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С.М. Буденного

В статье предлагается подход к реализации функции прогнозирования времени доставки сообщений большого объема в сетях передачи на основе рекуррентных нейронных сетей долгой краткосрочной памяти. В результате работы искусственной нейронной сети формируются прогнозные значения времени доставки сообщений. По результатам прогнозирования при необходимости вырабатываются управляющие воздействия для обеспечения своевременной доставки сообщений.

сеть передачи данных, сообщение, своевременность, нейронные сети, прогнозирование.

Современный этап развития автоматизированных систем характеризуется существенным ростом объемов хранимой, обрабатываемой и передаваемой информации. С другой стороны, в некоторых системах повышаются требования к своевременности доставки сообщений. В условиях априорной неопределенности информации о состоянии сети и внешних негативных воздействиях, неоднородности сети (наличия в составе телекоммуникационного оборудования и каналов различного типа), низкой связности сети, наличия в сети «узких» участков (каналов с низкой пропускной способностью) задача гарантированной (с высокими требования к своевременности и достоверности) доставки сообщений большого объема становится сложной [1].

Применение приоритезации, динамической маршрутизации и других средств и способов позволяет использовать возможности сети для повышения своевременности доставки сообщений в сети в целом, но не гарантирует доведение сообщения большого объема (например, файла объемом несколько Гигабайт) в требуемые сроки конкретному абоненту.

В связи с этим возникает необходимость решения задачи прогнозного контроля времени доставки сообщения большого объема, заключающегося в прогнозировании времени доставки и сравнении результатов прогноза с требуемым значением.

При положительных результатах предварительного прогнозного контроля сообщение отправляется, при отрицательных – в автоматизированной системе принимается решение на реконфигурацию сети, вырабатываются соответствующие управляющие воздействия, выполняются мероприятия как технического, так и организационного характера.

В ходе доставки сообщения также может выполняться текущий прогнозный контроль времени доставки сообщения оставшейся части сообщения. В случае формирования отрицательного прогноза оперативно принимаются меры по обеспечению своевременной доставки сообщений (принудительно минимизируется незначимый трафик, организуются параллельные маршруты передачи данных и т. д.).

Существующие статистические подходы к прогнозированию (оценке) времени доставки сообщений ориентированы на прогнозирование времени пакетов, коротких сообщений. При их использовании для прогнозирования времени доставки больших файлов в условиях высокой степени априорной неопределенности характеристик сети ошибка прогнозирования в абсолютных значениях может достигать недопустимых значений.

Одним из путей повышения точности прогнозирования значения времени доставки сообщений большого объема в сложных сетях передачи данных в условиях априорной неопределенности информации о состоянии сети и внешних негативных воздействий является использование искусственных нейронных сетей (ИНС), а именно – рекуррентных нейронных сетей (РНС) долгой краткосрочной памяти (LSTM– *Long short-term memory*) [2].

В качестве прогнозной величины может использоваться время доставки сообщений (при передаче файлов фиксированного объема) или скорость передачи сообщений. Во втором случае прогнозное значение времени доставки вычисляется по результатам прогнозирования скорости доставки. Структура LSTM сети для времени доставки сообщения x представлена на рис. 1 (см. ниже).

На рис. 1: x_t – последовательность значений времени доставки; h_{prev} – результат, получившийся на выходе предыдущей ячейки; h_{pred} – результат прогноза для следующей ячейки; h – результат прогноза; c_{prev} – дополнительный выход предыдущей ячейки; *con* – конкатенация; *sig*, *tan* – функции активации, сигмоида и тангенсоида соответственно.

Для прогнозирования времени доставки сообщений большого объема была создана сеть LSTM из 32 слоев. Для обучения ИНС использовался набор данных (датасет), содержащий сведения об объеме файлов и затраченном времени на их передачу.

Подготовка данных включала в себя несколько этапов: очистка данных (проверка на повторяющиеся значения и на наличие пропусков), выявление выбросов и аномалий, приведение типов данных, визуализация, нормализация и кодирование. Для выявления аномалий использовался метод

на основе интерквантильного размаха, для нормализации данных – Z – масштабирование. Для подготовки данных и создания нейросети применялись инструменты языка программирования Python и библиотеки pandas, sklearn и matplotlib.

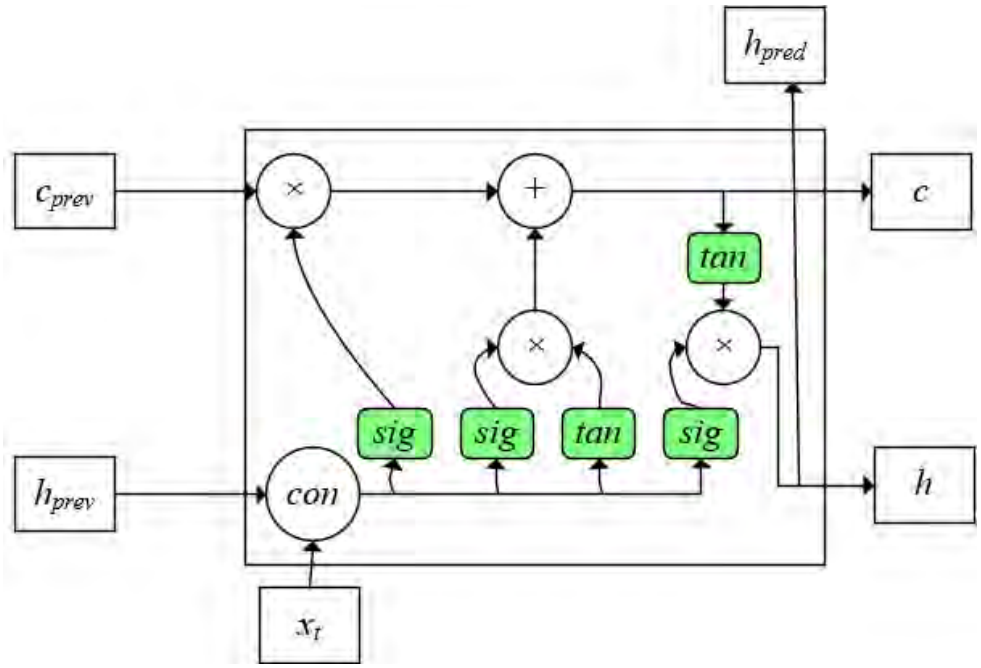


Рис. 1. Структура LSTM сети для прогнозирования времени доставки сообщения

На выходе ИНС формировалось прогнозное значение времени доставки сообщения с заданным прогнозным периодом. Результаты тестирования ИНС показали достаточно высокую точность прогнозирования по сравнению со статистическими методами, в частности – по сравнению с методом скользящего среднего.

Программное средство прогнозирования времени доставки сообщений большого объема целесообразно включить в состав программного обеспечения АРМ администратора сети передачи данных.

В качестве исходных данных для прогнозирования может быть использована уже имеющаяся в системе регистрации и учета автоматизированной системы информация об объеме переданных файлов и времени их передачи.

Таким образом, реализация функции прогнозирования времени доставки сообщений большого объема в сети передачи данных создает дополнительные возможности администратору сети для обеспечения своевременной доставки сообщений большого объема за счет появления запаса времени для принятия решения на проведение необходимых мероприятий упреждающего характера и их выполнение.

Список используемых источников

1. Авраменко В .С., Ахметзянов А. А., Бабич Б. И. Анализ проблемы гарантированного доведения информации в сети передачи данных специального назначения // Юбилейная XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26-28 октября 2022 г. : материалы конференции. Часть I. СПб. : СПОИСУ, 2022. С. 62–64.
2. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб. : Питер, 2018. 480 с.

УДК 004.056.53
ГРНТИ 81.93.29

РАЗРАБОТКА МЕТОДА ПРОТИВОДЕЙСТВИЯ АТАКАМ НСД В ПАМЯТИ ПРИЛОЖЕНИЯ

Р. И. Агаев, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Тема несанкционированного доступа к памяти приложения является одной из наиболее актуальных в области информационной безопасности. Несанкционированный доступ к памяти может привести к утечке конфиденциальной информации, изменению данных, нарушению целостности системы и другим опасным последствиям. Для решения этой проблемы представлен метод предотвращения несанкционированного доступа к памяти приложения при помощи шифрования XOR и обфускации программного кода.

память приложения, исключающее ИЛИ, XOR, обфускация, несанкционированный доступ.

С развитием информационных технологий, растет количество информации, которую необходимо защитить в компьютерных системах. Одним из наиболее распространенных методов атак на систему является «несанкционированный доступ к памяти приложения». Несмотря на то, что этот вид атак широко известен, он по-прежнему остается одним из наиболее опасных и труднодиагностируемых.

Несанкционированный доступ к памяти приложения – это ситуация, когда злоумышленники получают доступ к памяти приложения без разрешения. Это может произойти, если приложение не было достаточно защищено от этого типа атак [1].

Память приложения – это область памяти, которая используется для хранения информации, необходимой для работы приложения. Она может

содержать конфиденциальные данные, такие как идентификаторы пользователей, пароли и другую чувствительную информацию. Если злоумышленники получат доступ к этой памяти, они могут украсть данные, что может привести к утечке личной информации, финансовой информации и других важных данных [1].

Меры по защите памяти могут быть разнообразными, но не все могут обеспечить гарантированную защиту и использоваться на любых системах. В большинстве организаций сотрудники работают на слабопроизводительных компьютерах и не имеют знаний криптографии, навыков извлечения данных из памяти приложения. Одним из способов защиты от несанкционированного доступа к памяти является использование операции XOR, которая слабо влияет на производительность системы.

XOR (исключающее ИЛИ) – это бинарная операция, которая используется для битового сравнения двух чисел. Результат операции XOR будет равен 1, только если биты обоих чисел различны; в противном случае результат будет равен 0. Например, если мы выполним операцию XOR между числами 1010 и 1100, то получим результат 0110 [2, 3].

Использование операции XOR для защиты памяти заключается в том, что мы применяем XOR к данным, которые храним в памяти, и ключу (также представленному в виде битовой последовательности). В результате получается новая битовая последовательность, которая представляет собой зашифрованные данные. Для расшифровки данных необходимо применить операцию XOR к зашифрованным данным и ключу. Если ключ известен только авторизованному пользователю или приложению, то это обеспечивает защиту от несанкционированного доступа к данным.

Пример использования шифрования XOR:

Исходный текст: "HELLO WORLD".

Ключ: "ABCDEF".

Шифрование: "H"⊕"A", "E"⊕"B", "L"⊕"C", "L"⊕"D", "O"⊕"E", " "⊕"F", "W"⊕"A", "O"⊕"B", "R"⊕"C", "L"⊕"D", "D"⊕"E".

Шифрованный текст: "5B22474F27464E4D514C".

Дешифрование: "5B22474F27464E4D514C" ^ "ABCDEF" = "HELLO WORLD".

Преимущества шифрования XOR [4]:

- Простота реализации и использования шифрования;
- Быстрота шифрования и дешифрования информации;
- Высокая степень защиты информации при использовании достаточно длинных ключей.

Недостатки шифрования XOR [4]:

- Отсутствие защиты от атак методом частотного анализа при использовании коротких ключей;
- Необходимость обмена ключами между отправителем и получателем.

Данная операция может быть исследована в исходном коде и на основе этого предприняты шаги для достижения целей злоумышленника. Для решения этой проблемы разработчики могут использовать технику обфускации, которая внесет изменения в исходный код, не сказываясь на его функциональности. Обфускация представляет собой процесс трансформирования исходного кода с целью затруднения его чтения, понимания и тестирования [5].

Обфускация исходного кода является процессом, в который входят различные методы, такие как [4, 6]:

- Замена наименований переменных, функций и классов на бесполезные символы.
- Изменение порядка инструкций, что делает код менее прозрачным и сложным для отладки.
- Вставка случайных и бесполезных инструкций.
- Изменение формы исходного кода таким образом, чтобы он был менее узнаваемым для злоумышленников.
- Удаление комментариев и лишних пробелов в исходном коде.

Эти методы могут использоваться как отдельно, так и в комбинации друг с другом. Они заключаются в изменении структуры исходного кода, чтобы его идентификация и понимание стало более сложным. Обфускация делает код менее читабельным для злоумышленников, что труднее сделать внедренный код вируса и выполнить его вредные функции. Также, это способствует тому, что обычный пользователь не сможет изменить программный код. На рис. 1 изображен исходный код без обфускации.

```
Game_Data.data.money = Game_Data.saveData.money;
Game_Data.data.coins = Game_Data.saveData.coins;
Game_Data.data.avatarID = Game_Data.saveData.avatarID;
Game_Data.data.playerName = Game_Data.saveData.playerName;
Game_Data.data.openedCases = Game_Data.saveData.openedCases;
Game_Data.data.XP = Game_Data.saveData.XP;
```

Рис. 1. Часть исходного кода программы

На рис. 2 изображен обфусцированный код.

Рис. 2. Часть обфусцированного кода программы

Данный процесс выгоден для компаний и разработчиков, которые разрабатывают продукты с закрытым исходным кодом. Это может применяться в таких сферах, как финансы, телекоммуникации, промышленность и т. д.

Обфускация кода не обеспечивает полной безопасности, но при совместном использовании с методами шифрования, может повысить уровень защиты конфиденциальной информации от малоквалифицированных пользователей или поможет усложнить несанкционированное получение данных более опытным злоумышленникам.

Список используемых источников

1. Зимин А. Е. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): VI Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017. Т. 2. С. 343–348.

2. Куклин А. Е. Шифрование и дешифрование текстовых файлов методом xor-шифрования // Материалы Международной студенческой научной конференции «Студенческий научный форум 2021». 2021. N 7. С. 70–72.

3. Гарг Сатиш Кумар Криптография с использованием Xor Cipher // Исследовательский журнал науки и технологий. 2017. С. 25.

4. Ивченкова Ю. С., Савкин М. К. Виды и способы обфускации // Наука, техника и образование. 2016. N. 2 (6). С. 60–66.

5. Алексеев Д. М. Иваненко К. Н., Убирайло В. Н. Обфускация программного кода // Сборник статей международной научно-практической конференции «Новая наука: история становления, современное состояние, перспективы развития» (Челябинск, 3 октября 2016 г.). В 2 ч. Уфа: МЦИИ ОМЕГА САЙНС, 2016. Ч. 1. С. 3-4.

6. Пласковицкий В. Л. Обфускация кода. Вещественные и мнимые методы // Материалы научно-практической конференции с международным участием «Неделя науки СПбГПУ» (Санкт-Петербург, 03-07 декабря 2013 г.). Санкт-Петербург; 2014. С. 314–316.

Статья представлена научным руководителем, заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 535.14
ГРНТИ 49.46.29

ИССЛЕДОВАНИЕ ФЛУКТУАЦИЙ ПОЛЯРИЗАЦИИ И ФАЗЫ ОПТИЧЕСКОГО ИЗЛУЧЕНИЯ ПОД ДЕЙСТВИЕМ АТМОСФЕРНЫХ ТУРБУЛЕНТНОСТЕЙ В СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ В СВОБОДНОМ ПРОСТРАНСТВЕ

Ю. А. Адам, Д. А. Каргина, А. С. Колесник, Б. А. Наседкин

Национальный исследовательский университет ИТМО

Реализация безопасного обмена информацией между легитимными участниками является приоритетной задачей квантовых коммуникаций. В рамках данного вопроса системы квантового распределения ключа на непрерывных переменных являются перспективными для использования в открытом пространстве вследствие малых габаритов приемного узла и низкой себестоимости. Они могут быть легко интегрированы в мобильные компактные терминалы, а также подвижные устройства, в том числе беспилотный транспорт и летающие дроны.

квантовое распределение ключа, протокол на непрерывных переменных, флуктуация поляризации, флуктуация фазы, алгоритм компенсаций флуктуаций.

Квантовое распределение ключа (КРК) – новый подход к обеспечению безопасного обмена данными между пользователями, стойкость которого обеспечивается законами квантовой физики, что делает невозможным взлом данных систем с теоретической точки зрения. В свою очередь системы КРК можно разделить на дискретные переменные (ДП) [1] и непрерывные переменные (НП) [2]. Первые подразумевают кодирование информации о ключе в однофотонные состояния оптического излучения (поляризации, фазы, времени) и предполагают использование в системах дорогостоящих и сложных в эксплуатации детекторов одиночных фотонов. В свою очередь формирование информации о ключе в системах на НП реализуется с помощью квадратур электромагнитного поля, что позволяет использовать в таких системах методы когерентного детектирования, что существенно снижает стоимость и габариты таких систем. Особенно привлекательным сценарием использования систем КРКНП является открытое пространство, которое станет неотъемлемой частью будущих квантовых сетей в рамках решения задачи «последней мили» [3] по доставке квантовых ключей конечным по-

требителям. Однако, при распространении по открытому пространству формирование ключа осложнено атмосферными эффектами. В частности, в настоящей работе исследовалось влияние флуктуаций поляризации и фазы под действием атмосферных эффектов и методы их компенсации в рассматриваемой системе.

Разрабатываемый в рамках данной работы экспериментальный макет системы КРКНП в открытом пространстве основан на создаваемой в Университете ИТМО системе в волоконном исполнении. Основные параметры макета представлены в таблице 1.

ТАБЛИЦА 1. Параметры макета системы КРКНП в открытом пространстве

Параметр	Значение
Протокол	Непрерывные переменные
Рабочая длина волны	1550 нм
Тип модуляции	Гауссова
Тип детектирования	Двойной гомодинный
Тип согласования	Обратный
Локальный осциллятор	На стороне отправителя
Система ввода/вывода излучения	Коллиматоры, Телескопы

Протокол на непрерывных переменных был выбран вследствие возможности использования когерентного метода детектирования при помощи балансного детектора, что позволяет имплементировать данную систему в мобильные устройства. Рабочая длина волны лазерного излучения была выбрана исходя из используемой материально технической базы исходной системы и последующей возможности интеграции в квантовые сети. Тип модуляции, детектирования и согласования были определены исходя из теоретического доказательства стойкости системы к атакам и являются наиболее оптимальными [4]. Локальный осциллятор (ЛО), необходимый для когерентного детектирования, реализован на стороне Отправителя, а не Получателя, так как последний случай является технически более сложным. В качестве оптической системы вывода/ввода излучения используется как коллиматоры, так и полноценные телескопические системы с алгоритмом пространственной подстройки. Первая система предполагает передачу на несколько десятков сантиметров для апробации основных конструктивных решений, тогда же как вторая система используется для полноценной проверки функционирования макета.

Вследствие реализации ЛО на стороне Отправителя встает вопрос об организации каналов передачи между Отправителем и Получателем: использование одного канала для совместной передачи ЛО и сигнальных

импульсов (СИ) или двух каналов для раздельной передачи. Последний вариант приведет к увеличению стоимости и габаритов конечной системы, а также повышенным требованиям к точности наводки вследствие необходимости использования дополнительной пары телескопических систем. Однако, для совместной передачи ЛО и СИ в одном канале необходимо проведение их временного и поляризационного мультиплексирования. Последнее требует использования в системе пассивного или активного контроллера поляризации, выбор которого зависит от величины флуктуации поляризации в атмосферном канале (считается, что модули Отправителя и Получателя содержат только волокно с сохранением поляризации). Для этой цели была собрана экспериментальная установка, принципиальная схема которой представлена на рис. 1.

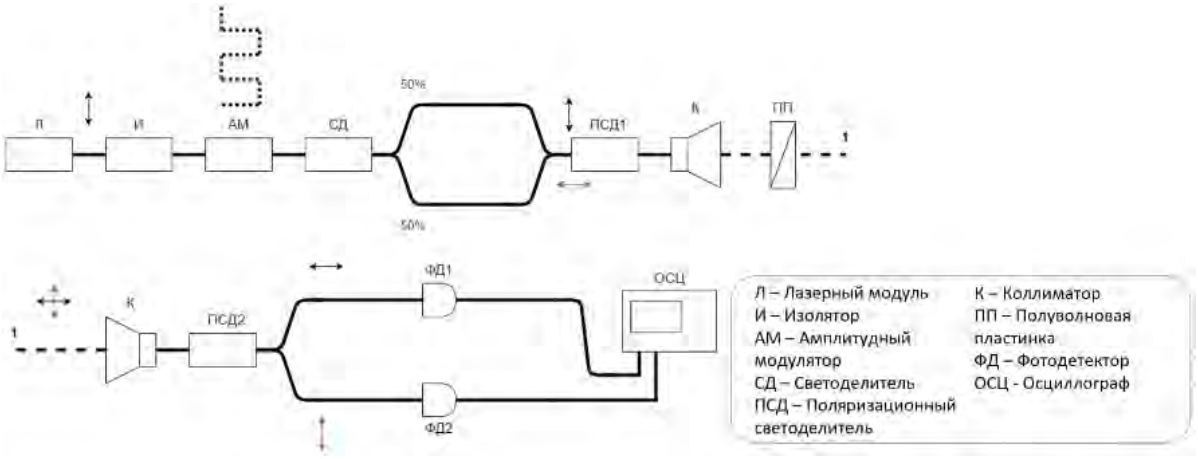


Рис. 1. Принципиальная схема экспериментальной установки по исследованию флуктуации поляризации в атмосферном канале

На стороне Отправителя линейно поляризованное лазерное излучение, проходя изолятор и амплитудный модулятор, приобретает импульсную структуру (параметры самих импульсов в данном случае несущественны). Далее излучение делится на светоделителе на два плеча, образуя таким образом ЛО и СИ. После они объединяются на поляризационном объединителе и с помощью коллиматоров направляются на сторону Получателя, при этом на объединителе происходит поворот поляризации СИ на ортогональную. Полуволновая пластинка после выходного коллиматора нужна для согласования поляризационных базисов с приемным сечением волокна на стороне Получателя. Длина атмосферного канала в данном эксперименте составила 40 см. На стороне получателя излучение аналогичным образом делится в зависимости от поляризации на плечо ЛО и СИ, после чего проводятся измерения интенсивностей пришедших импульсов.

По результатам проведенных измерений, представленных на рис. 2, где изображены измеренные напряжения на ФД1 и ФД2 при последовательном отключении каналов СИ и ЛО на ПСД1, можно сделать вывод о том, что

флуктуация поляризации в воздушном пространстве является незначительной и не влияет на работоспособность системы в течение достаточно долгого времени. Это позволяет избежать использования активного контроля поляризации на стороне получателя и существенно уменьшает стоимость и габариты приёмного модуля.

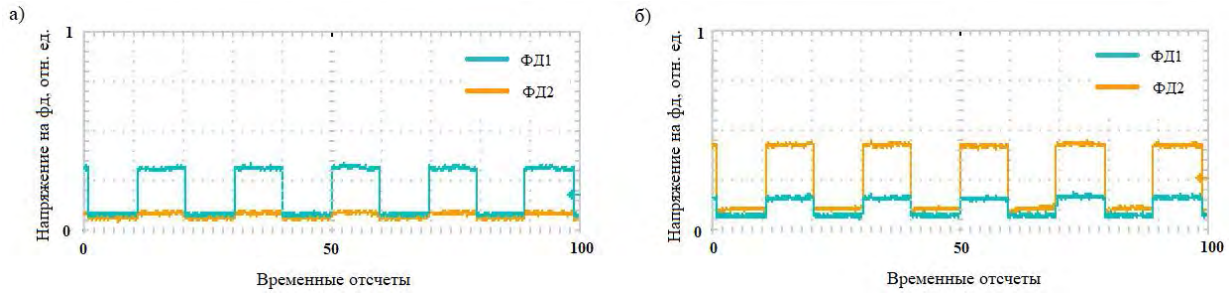


Рис. 2. Напряжение на ФД при отключенном канале СИ (а)
и отключенном канале ЛО (б) на ПСД1

Другим негативным эффектом влияния атмосферы является фазовая флуктуация, приводящая к несоответствию значений квадратур на стороне Отправителя и Получателя. Для решения данной проблемы используется специальный алгоритм компенсации фазовых флуктуаций [5]. Его идея заключается в использовании специальных опорных импульсов с заранее заданными значениями квадратур, по которым будет происходить расчет угла θ, определяющего величину фазовой флуктуации. Для проверки данного алгоритма была собрана экспериментальная установка, принципиальная схема которой изображена на рис. 3. Аналогичным образом, как и в схеме по проверке флуктуации поляризации, излучение делится на светоделителе на ЛО и СИ (по уровню мощности соответствующие опорным), однако во втором случае происходит повторная амплитудная модуляция, формирующая опорно-сигнальные импульсы (ОСИ). Важно отметить, что значения квадратур опорного импульса могут быть выбраны любыми. В нашем случае они составили $P = 1$, $Q = 0$ в относительных единицах. Также соотношение опорных импульсов к сигнальным в исследуемом случае составило 1:9. Данное значение соответствует волоконному каналу связи и в дальнейшем будет подобрано для открытого пространства. На стороне Получателя при помощи девяностоградусного гибрида двумя балансными детекторами осуществлялось измерение квадратур полученного излучения.

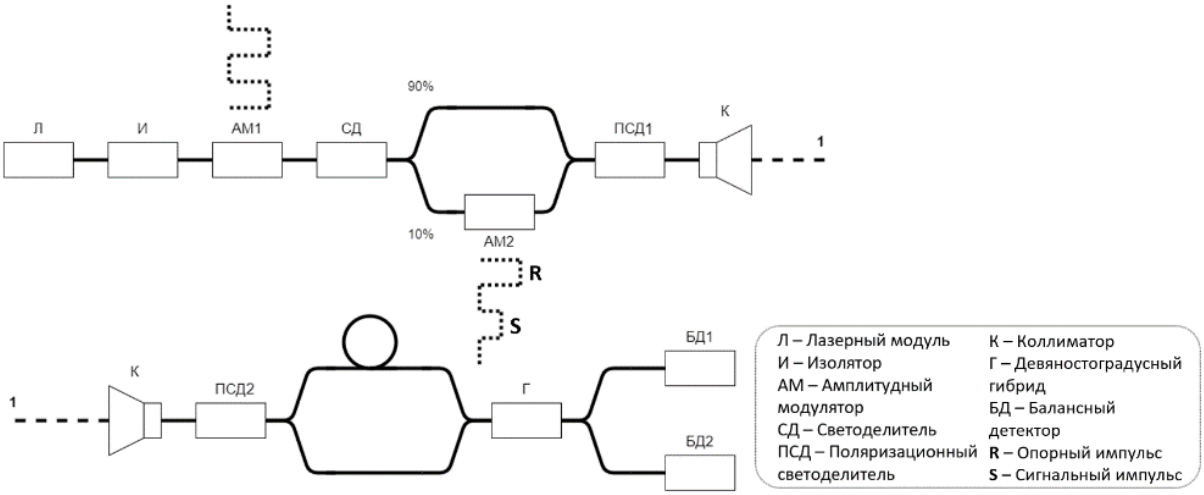


Рис. 3. Принципиальная схема экспериментальной установки по исследованию работы алгоритма компенсации фазовых флуктуаций

Полученные значения квадратур представлены на рис. 4а. Как видно по графику, значения квадратур испытывают случайный дрейф вследствие фазовых флуктуаций. Стоит помнить, что на стороне Отправителя значения всех квадратур были одинаковыми.

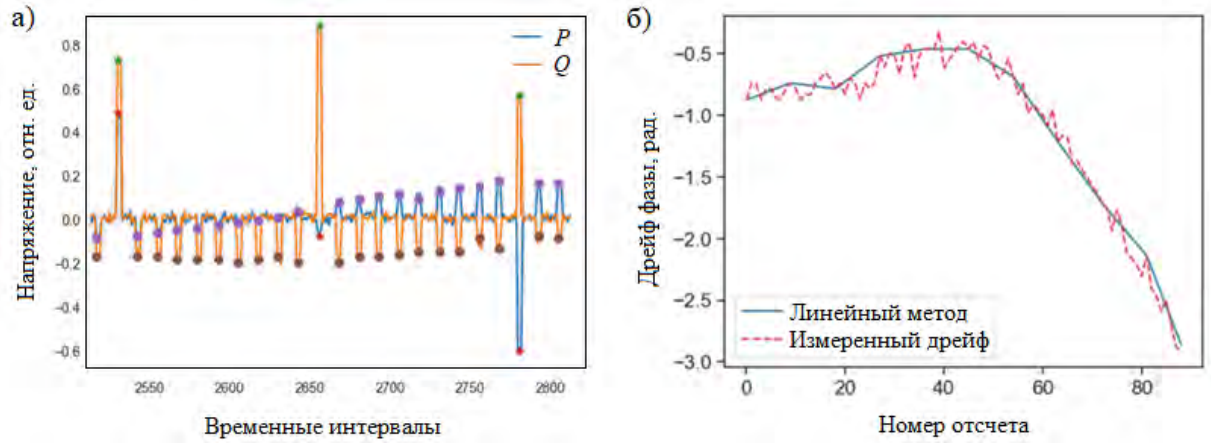


Рис. 4. Значения измеренных квадратур при неработающем алгоритме компенсации (а), измеренный угол флуктуации фазы (б)

В свою очередь на рис. 4б представлен рассчитанный с помощью приведенного алгоритма угол θ, который в дальнейшем используется Отправителем для перераспределения своей последовательности значений (как было сказано ранее, реализуется обратное согласование). Таким образом можно заключить, что данный алгоритм позволяет компенсировать изменение фазы в атмосферном канале и успешно согласовывать последовательности значений квадратур между Отправителем и Получателем.

В заключение, в рамках реализации квантового распределения ключа на непрерывных переменных в открытом пространстве были проведены экс-

перименты по изучению флуктуаций поляризации и фазы. Флуктуация поляризации не оказывает существенного влияния на работу системы, благодаря чему можно ограничиться пассивным контролем поляризации. Учет флуктуации фазы и ее компенсация производится весьма эффективно, однако с целью оптимизации необходим более точный подбор отношения количества сигнальных и опорных импульсов излучения. В ходе дальнейших работ будет произведена реализация системы на телескопических установках, осуществлена передача квантового ключа, а также проанализирована возможность различных атак.

Список используемых источников

1. Bennett C. H., Brassard G., Quantum cryptography: public key distribution and coin tossing // Proceedings of the International Conference on Computers, Systems and Signal Processing. 1984. Vol. 1. PP. 175–179.

2. Grosshans F., Grangier P. Continuous variable quantum cryptography using coherent states // Physical review letters. 2002. Vol. 88. N. 5. P. 057902.

3. Xue Y. et al. Airborne quantum key distribution: a review // Chinese Optics Letters. 2021. Vol. 19. N. 12. P. 122702.

4. Goncharov R., Vorontsova I., Kirichenko D., Filipov I., Adam I., Chistiakov V., Smirnov S., Nasedkin B., Pervushin B., Kargina D., Samsonov E., Egorov V. The Rationale for the Optimal Continuous-Variable Quantum Key Distribution Protocol // Optics. 2022. Vol. 3. N. 4. PP. 338–351.

5. Goncharov F. M., Pervushin B. E., Nasedkin B. A., Goncharov R., Yashin D. A., Gellert M. E., Sulimov D. V., Morozova P. A., Filipov I. M., Adam I. A., Chistiakov V. V., Samsonov E. O., Egorov V. I. Increase of signal to reference ratio for phase compensation in continuous-variable quantum key distribution systems // Наносистемы: Физика, химия, математика = Nanosystems: Physics, Chemistry, Mathematics. 2023. Vol. 14. N. 1. PP. 59–68.

Статья представлена научным руководителем,
доцентом НОЦ фотоники и оптоинформатики Университета ИТМО,
кандидатом физико-математических наук Э. О. Самсоновым.

УДК 004.056
ГРНТИ 81.93.29

ОБЗОР ТЕХНОЛОГИИ DATA DIODE И ЕЕ ПРИМЕНЕНИЯ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

А. Г. Александрова, В. Н. Волкогонов, Д. О. Потомако

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В условиях современного мира, где информация играет ключевую роль в различных областях, обеспечение ее безопасности является необходимым условием для успешной работы организаций. В этой связи, инструменты для обеспечения информационной безопасности становятся все более востребованными. Один из таких инструментов – Data Diode.

однонаправленная передача данных, критически важные объекты, Data Diode.

Введение

В любой организации, которая занимается обработкой какой-либо информации, рано или поздно возникает проблема недопущения утечки конфиденциальных данных. Степень актуальности этого вопроса можно определить при расчете величины ущерба, вызванного реализацией риска утечки информации. Чем выше потенциальный ущерб от утечки конфиденциальных данных, тем более жесткие меры необходимо применять для устранения потенциальных рисков. К таким мерам могут относится всевозможные организационные меры информационной безопасности, например, разработка регламентов и процедур, а также можно использовать технические меры. К техническим мерам можно отнести приобретение и установку DLP-систем, переход к концепции Zero Trust и реализацию физического отключения критически важных сегментов сети от внешних сетей и систем – «воздушный зазор» [1].

Для производственных инфраструктур, где используются автоматизированные системы управления технологическими/производственными процессами, а также для государственных компаний и компаний, работающих с данными, которые попадают под регулирование со стороны государства, изоляция защищенных сетей от обмена данными с другими сетями и сегментами особенно актуальна. Но это недостаточно эффективное и рациональное решение, так как даже таким инфраструктурам необходим обмен

данными с внешним миром, например, для получения обновлений. Решением проблемы может стать использование однонаправленной передачи данных, а именно технологии Data Diode.

Описание Data Diode

Data Diode (Диод данных) – это технология, которая используется для обеспечения безопасности данных путем односторонней передачи данных. Он позволяет передавать данные только в одном направлении и не допускает обратной передачи данных. Это обеспечивает высокую степень защиты информации и предотвращает возможность несанкционированного доступа к конфиденциальным данным. В отличие от других методов однонаправленного движения информации, большинство диодов данных физически неспособны передавать пакеты в две стороны. Он использует две отдельные физические сети – входную и выходную. Информация передается только в одном направлении – от входной сети к выходной сети (рис. 1).

Рис. 1. Принцип работы DataDiode

Data Diode обеспечивает высокую скорость передачи данных, что является важным фактором для многих организаций, которые работают с большим объемом информации. Скорость передачи данных зависит от нескольких факторов, таких как тип протокола, который используется для передачи данных, размера пакетов данных и т.д. Data Diode может работать с различ-

ными протоколами, такими как TCP, UDP, HTTP, FTP, SSH, SMTP и многими другими. Это обеспечивает универсальность и применимость технологии в различных областях [2].

Кроме того, Data Diode позволяет передавать данные в режиме реального времени. Это особенно важно для организаций, которые работают с критически важными системами и операционными процессами. Data Diode позволяет передавать данные с минимальными задержками и гарантирует своевременную доставку информации.

Data Diode имеет ряд преимуществ, которые делают его эффективным инструментом для обеспечения безопасности данных: высокий уровень безопасности, эффективность, простота использования и снижение затрат.

Data Diode находит широкое применение в различных областях, включая финансовые учреждения, правительственные организации, медицинские учреждения и т. д. Один из примеров применения Data Diode – использование его в системах управления инфраструктурой критического назначения. Например, в системах управления ядерными электростанциями или авиационными системами управления полетами, где обеспечение безопасности данных имеет высокое значение. В этих системах Data Diode используется для передачи данных в одном направлении – от источника к получателю. Это обеспечивает высокий уровень безопасности и защищает от возможных кибератак. Data Diode также может быть использован для защиты банковских данных. В этом случае Data Diode обеспечивает защиту данных при передаче между финансовыми учреждениями и защищает от возможных кибератак, направленных на получение конфиденциальной информации.

Одним из ключевых преимуществ использования Data Diode является его способность работать в различных условиях. Например, Data Diode может использоваться в системах, где есть ограничения на использование сетевых подключений. В этом случае Data Diode позволяет передавать данные между различными устройствами без необходимости подключения к сети Интернет.

Варианты реализации Data Diode

Диод данных может быть представлен как отдельное сетевое устройство или как программно-аппаратный комплекс, который предоставляет более расширенный функционал. Аппаратный вариант Data Diode реализуется путем удаления передающего компонента из устройства выходной сети и принимающего компонента из устройства входной сети. Также представлены уже готовые устройства, где один из оптоволоконных кабелей, приемники и передатчики для него отсутствуют. Еще один вариант аппаратной реализации основан на интерфейсе RS-232, но такой вид диода данных

имеет существенный недостаток, кроме линий передачи в стандарте предусмотрены и линии управления, по которым потенциально может происходить передача в запрещенном направлении [1]. В классическом исполнении корпус аппаратного диода данных включает интерфейсы для подключения к сетям источника и назначения, а также разъем для питания, но производители могут оснащать устройство дополнительными надстройками, например, индикацией или фильтрацией по IP-адресу.

Аппаратный диод способен осуществлять только однонаправленную передачу необработанных данных, например, измерений с датчиков, но для работы большинства транспортных протоколов необходимо наличие двунаправленной связи для получения сведений о доставке пакетов и другой сервисной информации. Для передачи данных с помощью транспортных протоколов требуется создание программно-аппаратного комплекса, включающего диод данных и два прокси-сервера (однонаправленный шлюз), которые будут осуществлять преобразование пакетов. Использование прокси-серверов по обе стороны диода данных позволяет реализовать гораздо больше сервисных функций: фильтрация, мониторинг, антивирусные системы [3].

Основным недостатком описанных выше реализаций Data Diode является низкая скорость передачи данных из-за небольшой пропускной способности. Увеличения скорости можно добиться за счет применения программных диодов данных – сетевых устройств, в которых ограничения на передачу информации определяются прошивкой, а не аппаратными ограничениями. Обычно программные диоды данных реализуются на базе микроядра операционной системы, которое логически разделяет сети без обратного канала передачи информации. Они обладают высокой пропускной способностью до 10 Гбит/с и поддерживают стандартные транспортные протоколы.

Сценарии применения диодов данных

Как отмечалось ранее, обычно Data Diode используется при передаче данных из незащищенной сети в защищенную. Защищенная сеть содержит и обрабатывает данные, составляющие секретную или конфиденциальную информацию, утечке которой препятствует диод данных. К типовым сценариям использования однонаправленных сетевых устройств относятся: получение обновлений для средств защиты информации, репликация баз данных, трансляция аудио или видеосигнала извне. Возможно и обратное движение данных – из защищенной сети во внешнюю. Такая схема предполагает сбор ограниченного набора информации из закрытой системы без возможности управляющего воздействия на нее. Наибольшее распространение такой сценарий получил в системах с АСУ ТП для передачи параметров от логических контроллеров, датчиков и т. д.

Существует и смешанная схема применения Data Diode. В таком случае организуются два независимых однонаправленных канала передачи информации, один для передачи в защищенную сеть, а другой для второй для передачи во внешние системы. Достоинством такого подхода является организация полноценного обмена информацией между сетями, при этом для совершения кибератаки злоумышленнику необходимо получить доступ сразу к двум отдельным каналам и обойти систему защиты каждого из них. Также допускается применение нескольких диодов данных в одном направлении, но расположенных в разных уязвимых точках. Например, между сервером данных и сегментом АСУ ТП и между сервером данных и корпоративной сетью.

Заключение

Data Diode – это эффективный инструмент для обеспечения безопасности данных, который обладает высоким уровнем безопасности, эффективностью, простотой использования и способностью работать в различных условиях. Он может использоваться в различных отраслях, таких как правительственные организации, банковский сектор, промышленность и т. д. Однако, как и любой другой инструмент для обеспечения безопасности данных, у Data Diode есть свои ограничения и недостатки, такие как высокая стоимость, ограниченность функционала и низкая гибкость. Эти недостатки могут быть устранены с помощью использования других средств обеспечения безопасности, таких как шифрование данных, системы аутентификации и т. п.

В целом, использование диода данных – это один из эффективных способов обеспечения безопасности данных, который может быть применен в различных отраслях. Однако, для достижения оптимального уровня безопасности, необходимо использовать комплексный подход и сочетать Data Diode с другими методами обеспечения информационной безопасности.

Список используемых источников

1. Новостной портал Anti-malware [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Data-Diodes (дата обращения 20.03.2023).

2. Электронный журнал Системный администратор [Электронный ресурс]. URL: https://samag.ru/archive/article/3579 (дата обращения 19.03.2023).

3. Новостной портал SecurityLab by Positive Technology [Электронный ресурс]. URL: https://www.securitylab.ru/analytics/472721.php (дата обращения 19.03.2023).

УДК 004
ГРНТИ 50.05

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ФОРМИРОВАНИЯ БЛОКЧЕЙНА С ХРАНЕНИЕМ ПРОИЗВОЛЬНЫХ ДАННЫХ

Е. А. Александрова, Д. В. Кушнир

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Блокчейн как технология становится все более популярным и востребованным направлением, что определяет необходимость его исследования, в том числе в учебном процессе. Зачастую блокчейн рассматривают как систему записей о передаче некоторых ценностей, но его применение может быть куда более широким, например, он может использоваться для размещения некоторых произвольных данных или сведений о документах. Для исследования принципов добавления данных в блокчейн реализовано приложение с возможностью работы в ОС Linux, формирующее учебный демо-блокчейн. Решение позволяет провести анализ основных свойств блокчейна при размещении произвольных данных непосредственно или с помощью универсального указателя ресурса.

блокчейн, разработка приложений, хранение данных, цифровая подпись.

Блокчейном называют технологию, с помощью которой реализуется система записей о переносе некоторых ценностей [1]. В рамках этой системы действует правило о переносе от равного к равному, то есть в самом процессе не принимает участия некоторая доверенная третья сторона. В рамках данной системы создается реестр транзакций, который является общим, децентрализованным и открытым за счет того, что копируется на большое количество узлов. Реестр транзакций работает только в режиме добавления записей [2].

Нельзя отрицать, что популярность блокчейна со временем только растет. Так, в исследовании ICT.Moscow за I полугодие 2022 года, блокчейн стал одной из наиболее обсуждаемых в различных медиа тем, причем исследователи отмечают значительный рост популярности блокчейна: за год интерес к нему вырос на 63 % [3].

Кроме того, что растет популярность блокчейна, растут и возможности его применения в повседневной жизни: так, сейчас в разработке находятся законы «О майнинге» и «О цифровых финансовых активах» [4]. Закон «О майнинге» позволяющий легализовать валюту, полученную в результате майнинга различных блокчейнов, например, через специальную площадку,

которая будет создана в России в рамках экспериментального правового режима [5].

Таким образом можно отметить, что блокчейн становится всё более востребованной технологией. Тем не менее, в большинстве случаев рассматривается классическая модель блокчейна, предполагающая, что в блокчейне хранится информация о передаче некоторых ценностей, но блокчейн можно использовать и более широко – например, позволить хранить в блоке произвольные данные.

Желание размещать в блокчейне произвольные данные может стать узким местом в производительности системы и в результирующих объемах хранящейся информации, что приведет к затруднениям в работе с системой. Традиционным решением является хранение в блоке не самих данных, а хэша этих данных. Однако, традиционные блокчейны не предназначены для хранения произвольной информации и попытки их приспособить для этой цели приводит к накладным расходам. Для решения обозначенной задачи необходимо на этапе разработки предусмотреть структуру данных для возможности размещения в блоках как необходимых данных, если они не превышают некоторого значения, так и хеша этих данных с отсылкой к реальному расположению документа, например, в виде URL (унифицированный указатель ресурса)-ссылки на этот документ. В структуре данных блока предполагается предусмотреть отдельные поля для хранения собственно текста, URL документа и хэша этого документа [6].

На сегодняшний день существует некоторое количество проектов, которые уже реализуют документооборот с помощью блокчейна, например, проект BlockSign [7].

Цифровая подпись – важная составляющая любого блокчейна, поскольку при использовании криптовалют с помощью цифровой подписи можно подтвердить владение тем, что переводится в рамках транзакции. В задаче хранения документов возникает ряд проблем, связанных с тем, что этом случае блокчейн применяется не для перевода некоторой ценности, как в криптовалютах, в которых ценность при создании привязывается к секретному ключу владельца, а для хранения произвольных данных, которые не создавались внутри самого блокчейна и исходно никак не привязаны к его функционированию. Это при водит к необходимости найти решение, которое позволило бы применять возможности цифровой подписи в блокчейне данного типа. Подробнее это будет рассмотрено дальше.

В целях исследования указанных выше возможностей блокчейна необходимо разработать приложение, которое позволит опробовать необходимый функционал хранения данных и будет включать в себя следующие функции:

- вычисление хэша для встраиваемых данных;
- генерация блока, содержащий встраиваемые данные;

- генерация цепочки блоков;
- создание распределенного реестра;
- занесение в реестр произвольных данных, как текстовых, так и целых документов;
- применение электронной подписи как для формирования записей в реестр, так и для последующей проверки;
- возможность применения электронной подписи при передаче.

Приложение реализуется на языке программирования Python, для создания графического интерфейса используется Qt Designer. Предполагается обеспечить возможность работы приложения как в ОС Windows, так и на Linux.

Реализация подобного рода блокчейна может приводить к ряду проблем, которые необходимо рассмотреть подробнее. Уделим внимание тем проблемам, которые связаны непосредственно с содержанием блоков и теми особенностями, которые возникают при использовании блокчейна для хранения некоторого произвольного текста.

Начнем с содержания основного тела блока. В классическом блокчейне в основном теле блока хранится реестр транзакций. В нашем же случае мы рассматриваем ситуацию, когда в блоке хранится произвольный текст. Как уже было указано ранее, в рамках этой системы в блоке могут храниться и URL-ссылки на документы.

В связи с этим возникает ряд проблем. Основная из них связана с тем, что, так как текст в блоке произвольный, то и длина этого текста может быть любой, из-за чего возможны проблемы с занимаемой памятью. Для решения этой проблемы предлагается ввести ограничение на текст, хранящийся непосредственно в блоках, а все, что превышает ограничение предлагается хранить вне блокчейна в виде отдельных документов. Для хранения данных в самом блоке можно предусмотреть объем равный сумме длины применяемого хеша и URL, который имеет смысл привязывать к http-запросу GET и ограничить длиной 2048 символов. В зависимости от того, какой алгоритм хэширования будет применяться – SHA-256 или ГОСТ Р 34.11-2012 – ограничение на количество символов может немного отличаться. Выделяемый в итоге объем под хранение данных объем может оказаться критичным для производительности. Для решения этой проблемы возможно применение какой-либо сервиса сокращения ссылок, благодаря чему можно существенно сократить длины используемых URL, но это приведет к зависимости от дополнительных сервисов, что может быть нежелательным.

Схема хэширования произвольного текста при размещении данных в блоке представлена на рис. 1. Еще одна возможная проблема связана с хэшированием документов в принципе, так как в блоке будет хранится URL-ссылка на документ. В этом случае предлагается следующая система: сначала хэшируются отдельно текст документа и URL-ссылка, после чего два

полученных хэша конкатенируются и для результата конкатенации вычисляется хэш, который и будет считаться хэшем документа.

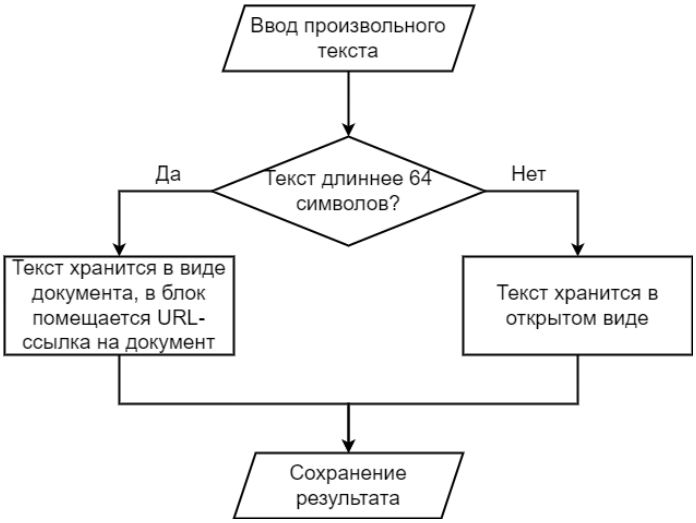


Рис. 1. Хэширование произвольного текста

Схема хэширования документа представлена на рис. 2.

Рис. 2. Хэширование документа

Кроме того, возникает ряд особенностей при использовании цифровой подписи. В классическом блокчейне цифровая подпись служит для подтверждения владения цифровым активом, но, так как в данном случае передается произвольный текст, то цифровая подпись служит для обеспечения доверия к размещаемой информации. Однако, если подпись не связана с цифровым активом, то требуется использовать внешний ресурс для снабжения участников ключами, что позволит как вносить записи, так и их проверять. Проверка понадобится как для формирования блока, так и для последующего

использования блокчейна как хранилища данных. Схема использования цифровой подписи представлена на рис. 3.

В исследовательской реализации блокчейна, нацеленного на хранение произвольных данных, реализуется и режим создания распределенного реестра с хранением данных на многих узлах. В рамках данного режима можно исследовать параллельную работу нескольких узлов, формирующих вместе распределенный реестр и совместно использующих размещаемые данные.

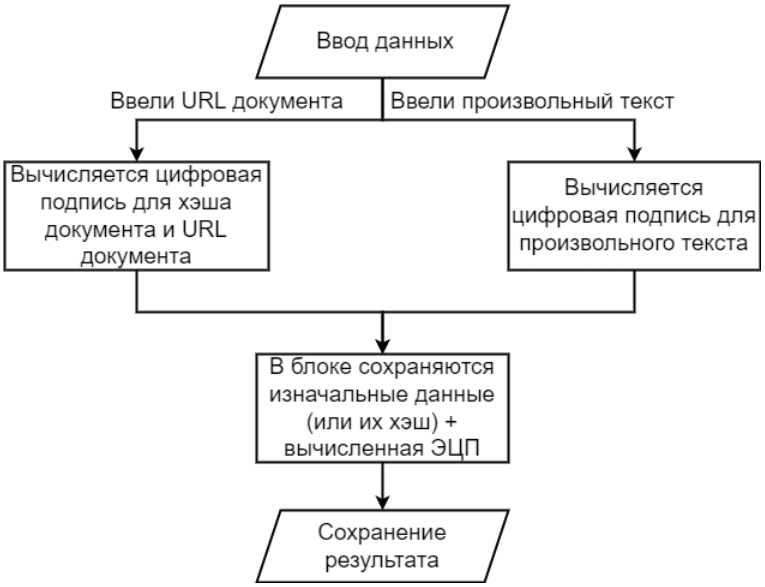


Рис. 3. Использование цифровой подписи

Таким образом, необходимость размещения произвольных данных в распределенных реестрах требует выполнения модификации структуры традиционных блокчейнов для возможности эффективного применения в реальных проектах. Варьирование размещения данных как внутри блоков, так и вне блокчейна позволяет достичь необходимой эффективности в работе систем. Проведение анализа и тестирование методов внедрения данных проводится на разрабатываемом программном обеспечении, которое реализует блокчейн со специально организованной структурой данных и формированием электронной подписи, что позволяет выявить потенциальные преимущества системы и возможные недостатки.

Список используемых источников

1. Сингхал Б., Дамеджа Г., Панда П. С. Блокчейн. Руководство для начинающих разработчиков. СПб. : БХВ-Петербург, 2019. 288 с.

2. Жданов И. Н., Федоров А. И., Балашов А. В. Введение в блокчейн 2. 0 // Научный журнал. 2017. N 10 (23). С. 39-43.

3. ИТ-медиатренды I полугодия 2022: рост упоминаний импортозамещения и переменчивость интереса к технологиям [Электронный ресурс] // ICT.Moscow URL:

https://ict.moscow/projects/mediatrends/h1-2022/?newsId=62f23664a5f7404358587da2 (дата обращения 10.01.2023).

4. Бицоева Л. Ф. Развитие законодательства о блокчейне // Аграрное и земельное право. 2020. №1 (181). С. 101–103.

5. Бурыгин И. Е., Остроумова Д. В. Влияние блокчейн на развитие экономики России // Стратегии бизнеса. – 2021. – №7. С. 213–217.

6. Blockchain Usage: List Of 20+ Blockchain Technology Use Cases [Электронный ресурс] // 101 Blockchain. URL: https://101blockchains.com/blockchain-usage/ (дата обращения 09.01.2023).

7. Block sign. Non-stop one way document solution [Электронный ресурс] // BlockSign. URL: https://blocksign.ai/intro/ (дата обращения 12.01.2023).

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ЗАЩИЩЕННОСТИ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ OPENSTACK ПРИ ЭМУЛЯЦИИ АТАКИ ВИДА DDOS НА УЗЛАХ ИНФРАСТРУКТУРЫ

Р. В. Алехин, И. Е. Пестов, Д. Н. Смирнов, П. Е. Шелкоплясова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день использование облачных технологий становится одним из самых популярных решений. Независимо от модели развертывания облачной инфраструктуры, первостепенной задачей является безопасность системы. В связи с развитием технологий, а также геополитической ситуацией растет количество атак вида доведений систем до отказа в обслуживании на российский сегмент сети. Наиболее распространенным видом такой атаки является атака Distributed Denial of Service. Важно осознавать область воздействия этого типа атаки на облачную инфраструктуру. При эмуляции атаки на узлы инфраструктуры, областью воздействия атаки станут все инстансы.

информационная безопасность, облачные технологии, облачные инфраструктуры, OpenStack, атака Distributed Denial of Service.

Целью работы является проведение анализа защищенности облачной инфраструктуры OpenStack при эмуляции атака вида DDoS на узлах инфраструктуры.

Данное исследование будет разделено на две части. В первой будет разработана принципиальная схема экспериментального теста, а во второй проведён эксперимент и проанализированы результаты.

Создание экспериментального стенда начнем с выбора программного обеспечения реализации облачной инфраструктуры.

Для решения данной задачи будем использовать свободное и открытое программное обеспечение OpenStack. Данное ПО предназначено для управления облачными вычислениями и инфраструктурой дата-центров.

Облачная платформа OpenStack – это инструмент для управления вычислительными ресурсами, который позволяет оптимизировать ресурсы, улучшать эффективность и упрощать управление инфраструктуры.

Благодаря тому, что OpenStack состоит из множества модулей, отвечающих за определенные аспекты управления вычислительными ресурсами, открывается возможность провести более тонкую настройку системы.

Так как данное программное обеспечение имеет открытый исходный код и активно развивается сообществом, открывается возможность интегрировать с другими инструментами и технологиями [1].

Данные преимущества делает OpenStack популярным выбором для многих компаний и организаций, которые хотят улучшить эффективность их вычислительных ресурсов. OpenStack обладает множеством типов развертывания, однако в данном лабораторном стенде будет использован OpenStack Multi-Node Deployment.

OpenStack Multi-Node Deployment это тип развертывания, в котором OpenStack развернут на нескольких узлах, каждый из которых выполняет различные функции, такие как контроллер, компьютер, хранилище и т. д. Этот тип развертывания является рекомендуемым для больших инфраструктур, так как он предоставляет высокую доступность, надежность, гибкость и масштабируемость [2].

В OpenStack Multi-Node Deployment некоторые компоненты устанавливаются на Control Node, а другие на Compute Node.

Control Node:

- Keystone;
- Glance;
- Horizon;
- Neutron Server;
- Nova.

Compute Node:

- Nova Compute;
- Neutron.

Control Node является основным узлом управления, отвечает за контроль всех других узлов и управление ресурсами. Compute Node используется для размещения и выполнения виртуальных машин.

Компоненты OpenStack между Control Node и Compute Node взаимодействуют друг с другом через API:

• Control Node – является основным узлом управления, который управляет всеми другими узлами и управляет ресурсами;

• Compute Node – используется для размещения и выполнения виртуальных машин. Когда пользователь запрашивает ресурсы, Control Node выполняет выбор наилучшего Compute Node для выполнения задачи и передает запрос на этот узел.

В рамках экспериментального стенда исходной операционной системой всех виртуальных машин, на которых функционирует OpenStack, была выбрана ОС Linux Ubuntu. Выбор данной операционной системы обусловлен тем, что она является бесплатной, с открытым исходным кодом, что позволяет использовать ее в рамках программы импортозамещения.

DDoS (*Distributed Denial of Service*) атака – это вид кибератаки, когда на целевой сервер или сеть направляется огромное количество запросов, что вызывает перегрузку системы и приводит к недоступности этой системы для нормальных пользователей [3]. Целью DDoS атаки может быть полная блокировка доступа к сервису, усложнение работы сервиса, понижение репутации цели.

В роли эмулятора DDoS атак выступит Cisco-TRex. Cisco TRex (*Traffic Generator and Analyzer*) это высокоэффективный программный генератор трафика, используемый в сфере сетевого тестирования и анализа. Он позволяет эмулировать поведение множества клиентских устройств, что позволяет исследователям и инженерам тестировать масштабируемость и производительность сетевых устройств, услуг и приложений [4].

Исходя из того, что Cisco TRex является генератором трафика с открытым исходным кодом, поддерживает режимы с контролем состоянием потока, является сравнительно простым и полностью масштабируемым инструментом – повлияло на выбор этого ПО в качестве эмулятора DDoS-атаки. TRex способен эмулировать большое количество сетевых устройств и генерировать высокий трафик, что позволяет проверить эффективность защиты. ПО использует многопоточный подход, чтобы симулировать большое количество трафика, подобное тому, что может быть вызвано в результате DDoS атаки. Таким образом, использование TRex в качестве эмулятора DDoS-атаки может существенно улучшить защищенность сетевой инфраструктуры.

На основе аргументов, приведенных выше, была разработана данная схема (рис. 1), включающая решения, показанные в перечне ранее.

Результатом данной работы является разработка экспериментального стенда облачной инфраструктуры. Включающая в себя решения OpenStack для развертывания облачных вычислительных ресурсов. Указана операционная система Linux Ubuntu на которой развернут OpenStack, а также определен эмулятор DDoS атаки в виде Cisco TRex, установленный контролирующем и вычислительных узлах.

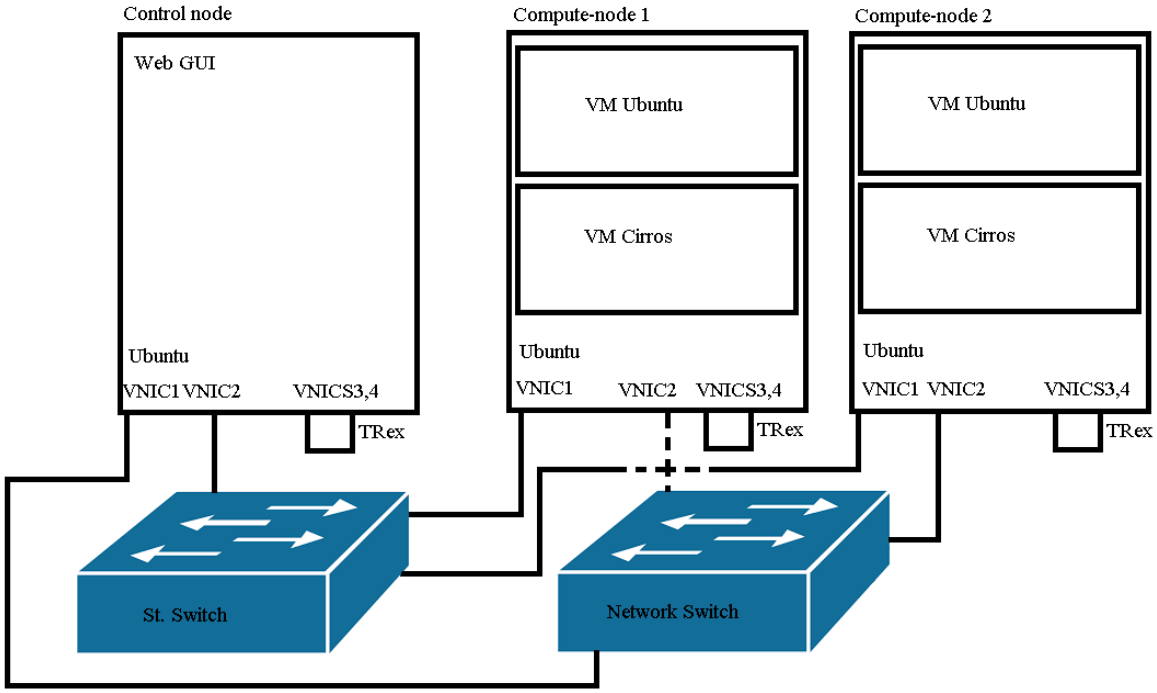


Рис. 1. Схема лабораторного стенда

Данный экспериментальный стенд позволит провести необходимый анализ инфраструктуры, ее защищенность при проведении кибератак типа DDoS, а также сделаны выводы исходя из данного исследования.

Список используемых источников

1. Jackson K., Bunch C., Sigler E. OpenStack cloud computing cookbook. Packt Publishing Ltd, 2015.

2. Luo Y. et al. Openstack security modules: A least-invasive access control framework for the cloud // 2016 IEEE 9th International conference on CLOUD computing (CLOUD). IEEE, 2016. PP. 51–58.

3. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб в 4 т. СПб. : СПбГУТ, 2019. Т. 1. С. 329–334.

4. Erlacher F., Dressler F. Testing ids using genesids: Realistic mixed traffic generation for ids evaluation // Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos. 2018. PP. 153–155.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА ЗАЩИЩЕННОЙ СИСТЕМЫ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ

К. С. Алиметов, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описана реализация ПО с графическим интерфейсом для защищённого обмена сообщениями. Основное предназначение реализуемого программного продукта - защищенная передача символьной информации и файлов. В процессе возникла необходимость решить проблемы с: корректным отображением сообщений на любых видах устройств - от персонального компьютера до смартфона; быстрой загрузкой переписки без необходимости каждый раз обновлять страницу; защитой от различных типов атак и безопасностью хранения учетных данных. Основная идея заключается в использовании: функций безопасности и низкоуровнего API для защиты от различных видов атак и криптографической подписи данных; современных способов адаптивной верстки; постоянных соединений для передачи сообщений. С этой целью было реализовано веб-приложение с гибридной версткой, фронтендом на JS и бэкэндом на Python, в котором в качестве основного способа доставки данных используются http-запросы и websocket-соединения.

информационная безопасность, разработка защищенного приложения, веб-приложение, сквозное шифрование данных, система обмена сообщениями.

Введение

Среди большого разнообразия приложений, системы для обмена мгновенными сообщениями являются теми, которые рассматривают конфиденциальность и безопасность как две важнейшие функции, поскольку данные, которыми обмениваются пользователи, часто являются частными и не предназначены для всеобщего обозрения.

Именно поэтому в процессе разработки приложений обмена сообщениями необходимо уделять должное внимание проблемам информационной безопасности пользовательских сообщений [1].

Одни методы используются для обеспечения конфиденциальности, а другие – для достижения безопасности с помощью подходящего криптографического метода [2]. Для реализации проекта используется концепция сквозного шифрования [3]. Приложение также предоставляет основные функции для обмена мгновенными сообщениями, такие как создание профиля, управление контролем доступа и поиск собеседников.

Поскольку приложение предполагает доступ через веб-интерфейс, установка программного обеспечения на компьютер каждого пользователя не требуется, и возникает необходимость в грамотной визуализации информации на экране. Для разработки веб-приложения использовалась клиент-серверная архитектура [4].

Реализация

Клиентская часть web-приложения написана с использованием HTML, CSS и JavaScript (*Vue.js*). Выбор Vue.js обусловлен высокой скоростью работы и компактным размером фрэймворка.

Механизм серверной части приложения реализован с помощью Django. Django – это свободный фреймворк для веб-приложений на языке Python, использующий шаблон проектирования MVC. Технологический стек серверной части веб-приложения: Nginx, Gunicorn, Django [5]. На рис. 1 приведен поэтапный порядок взаимодействия элементов стека.

1. Сервер Nginx, принимает и обрабатывает HTTP-запрос браузера, затем передаёт его в Application-сервер – Gunicorn.

2. Gunicorn получает данные от Nginx, разбирает их и исходя из своей конфигурации по протоколу WSGI передаёт их в Django.

3. Django обрабатывает полученные данные и возвращает результат работы обратно в Gunicorn, а он в свою очередь отдаёт результат в Nginx, который возвращает клиенту данные в JSON формате.

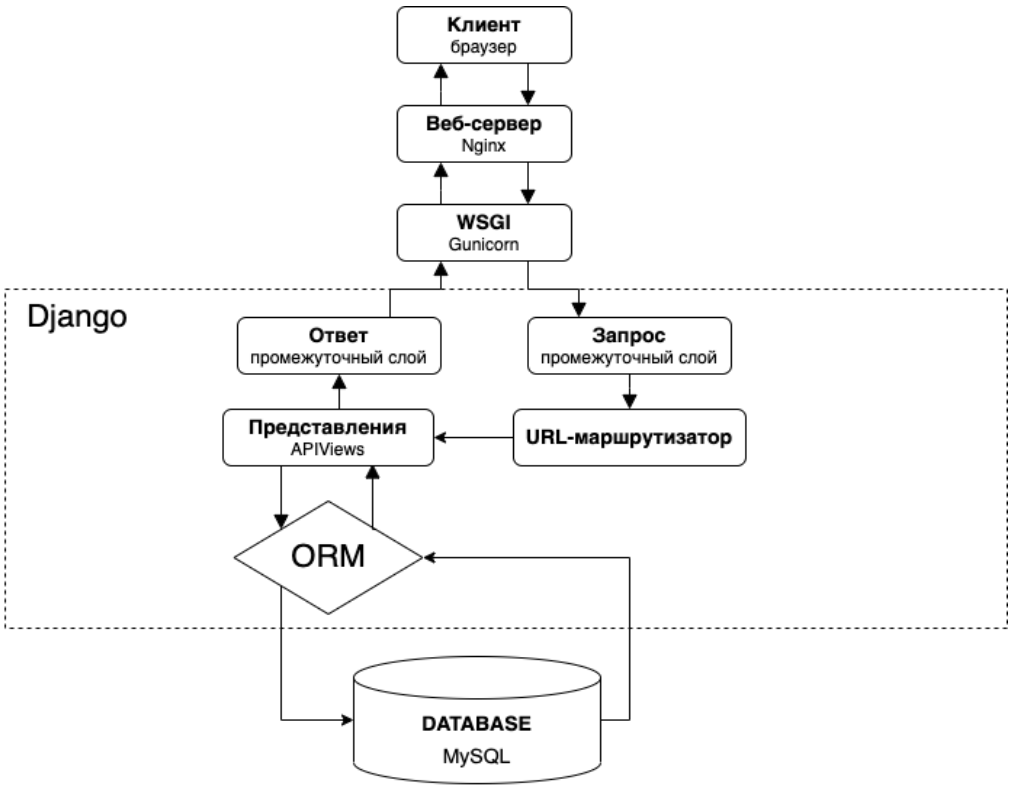


Рис. 1. Схема взаимодействия элементов стека технологий

Структура базы данных

Было решено выбрать реляционную базу данных с поддержкой языка SQL. Выбор пал на MySQL, как бесплатную СУБД с высокой скоростью обработки данных. Структура базы данных была описана с помощью Django ORM и представлена на рис. 2.

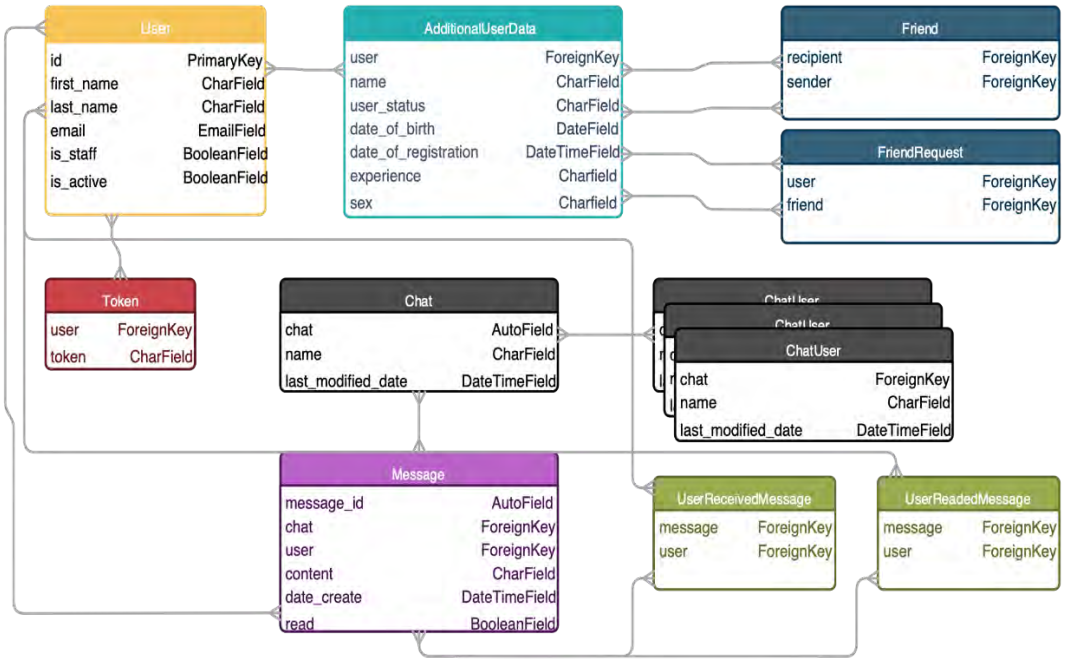


Рис. 2. Структура базы данных

Обеспечение защищенности

Django имеет методы обеспечения защиты от распространённых видов атак, включая XSS и CSRF атаки, SQL-инъекции, кликджекинг [6]. SSL/HTTPS используется на веб-сервере для шифрования всего трафика между сервером и пользователем [7]. Django позволяет настроить HOST-заголовки и принимать заголовки только от проверенных хостов.

Для защиты сообщений был выбран алгоритм РША, как один из самых надежных и распространенных алгоритмов шифрования с открытым ключом [8]. Также были использованы такие библиотеки как: Django-axes – обеспечивает защиту от атак перебором паролей; Django-two-factor-auth – добавляет поддержку двухфакторной аутентификации. Защита веб-приложения достигается постоянным мониторингом, обновлением и настройкой системы безопасности.

Заключение

Основной целью разработанной системы является безопасная передача сообщения в системе связи. Веб-приложение для безопасного обмена сооб-

щениями было разработано с использованием криптографических алгоритмов, позволяющих пользователям обмениваться зашифрованными сообщениями.

Наиболее серьезные угрозы безопасности и конфиденциальности исходят от ненадежных поставщиков сетевых услуг, поскольку все пользовательские данные находятся в пределах их досягаемости.

Таким образом, использование концепции сквозного шифрования и методов обмена ключами являются основными векторами в анализе и оценке конфиденциальности и безопасности систем мгновенного обмена сообщениями. Необходимо использовать актуальные инструменты обеспечения безопасности и механизмы мониторинга системы безопасности.

Список используемых источников

1. Попов А. А., Федорова О. В., Цветков А. Ю. Исследование современных механизмов обеспечения защиты конечных устройств под управлением ОС семейства Linux от атак с использованием rootkit // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 3. С. 36–43.

2. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т., СПб. : СПбГУТ, 2018. С. 47–51.

3. Макарова А. К., Поляничева А. В., Саматова К. А. Анализ уязвимостей оборудования передачи голосового трафика // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т., СПб. : СПбГУТ, 2022. Т. 1. С. 665–669.

4. Морозов Д. П., Слепнев А. В. Разработка автоматизированной системы проверки задач по программированию // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 4. С. 385–390.

5. Журавлев Н. Е. Взаимодействие web-сервера и web-приложения через web-socket // Мировая наука. 2019. N 12 (33). С. 143–147.

6. Ковалев Д., Ковцур М. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 // Первая миля. 2014. N 3 (42). С. 72–77.

7. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. С. 343–348.

8. Никитин В. Н., Ковцур М. М., Юркин Д. В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи // Информационно-управляющие системы. 2014. № 1 (68). С. 70–75.

Статья представлена научным руководителем, заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 654.739
ГРНТИ 49.33.29

СТАНДАРТИЗАЦИЯ И СЦЕНАРИИ ПРИМЕНЕНИЯ XURLLC В СЕТЯХ СВЯЗИ 6G

З. А. Аль-Кереа, А. С. Мутханна, Х. А. Ясир

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Три основные категории услуг, поддерживаемые 5G, – это eMBB, URLLC и mMTC. Будущие приложения указываются как утилиты URLLC, и им необходимо надежно передавать данные из одной оконечной точки в другую во время поддержки URLLC. Существуют много подходов для повышения надежности канала управления LTE, такие как подход к дублированию DCI. Вместе mMTC и URLLC, которые, по-видимому, имеют схожий будущий потенциал. Сети 5G сосредоточится на улучшенной мобильной широкополосной связи eMBB. Способность предвидеть экстремальные или частые события, масштабировать систему и внедрять дополнительные улучшения разнообразия без особых усилий, ограничения на задержку и надежность, основанные на ценности информации, также смягчаются этой перспективой, которая устраняет их все. В статье рассматривается приложения xURLLC это заключается в том, чтобы взять на себя инициативу в создании критически важных приложений для сетей 5G и 6G.

3GPP, 5G, LTE, sTTI, URLLC и Новое радио.

Введение

Долгосрочная эволюция (LTE) 3GPP (Проект партнерства 3-го поколения) будет постоянно и всесторонне улучшаться для создания новых беспроводных мобильных сетей 5G, поскольку это будет технологической революцией. Наряду с потенциалом для полностью новых радиоинтерфейсов, автономных субкадров или бесплатного доступа, это также способствует развитию бесчисленных небольших, постепенных улучшений [1]. Представленные варианты использования IMT-2020 должны удовлетворять трем ключевым требованиям. Существуют новые варианты использования, которые требуют чрезвычайно низкой задержки, чрезвычайно высокой надежности или того и другого. Одной из основных тем для будущей беспроводной сотовой связи была признана URLLC [1]. Эти варианты использования включают широкий спектр требований к сочетанию надежности и задержки, включая удаленное тактильное или тактильное управление с малой задержкой, высоконадежную беспроводную связь промышленной автоматизации с малой/средней задержкой и высоконадежные интеллектуальные сети с низкой/средней задержкой, и это лишь некоторые из них [1, 3]. Его мотивация в качестве технологии-кандидата заключается в укреплении сети LTE,

чтобы можно было достичь спецификаций IMT 2020 5G. Например, для URLLC с точки зрения надежности, низкой задержки менее 1 мс в пользовательской плоскости и потери пакетов 105 для коротких пакетов данных [3] и его рабочего элемента (WI) по сокращению задержки L2, а также технических характеристик. отчет о более коротком интервале времени передачи (TTI) и времени обработки для LTE. Эти методы допускают вышеупомянутые задержки, однако необходимы новые функции для повышения надежности при соблюдении требований к задержкам для служб URLLC. Хотя термин URLLC направлен на удовлетворение критериев надежности, а также на очень низкую задержку, орган по стандартизации 3GPP разделил проблемы надежности и задержки [1, 2]. Первоначально основное внимание при повышении производительности системы LTE уделялось факторам, связанным с задержкой, или sTTI (короткий TTI) WI. Последующий WI под названием High-Reliable Low Latency Communication был нацелен на проблемы, связанные с надежностью (HRLLC).

Стандартизация URLLC

С самого начала архитектуры системы 5G URLLC был одним из трех основных сценариев использования 5G. Rel-15, завершенный в июне 2018 г., является первым официальным выпуском для 5G в 3GPP [1]. Распределение электроэнергии и промышленная автоматизация – два основных варианта использования, которые принимает во внимание Rel-15. Ряд вариантов использования, их потребности и поддержка сетевой архитектуры для услуг URLLC были изучены рабочей группой 3GPP Service and System Aspects (SA) [4]. Кроме того, стандарты радиоуровня, которые находятся в центре нашего внимания, были установлены рабочей группой сети радиодоступа 3GPP (RAN). При задержке пользовательского уровня в 1 мс и коэффициенте блочных ошибок (BLER) 10-5 для 32 байтов цель разработки системы Rel-15 состояла в том, чтобы обеспечить надежность связи. В Rel-15 были описаны различные технические возможности для одновременного достижения целей уменьшения задержки и повышения надежности [5].

В Rel-16 3GPP работает над дополнительными улучшениями. Кроме того, он расширяет поддерживаемые услуги, включая чувствительные ко времени связи (TSC), такие как широко используемые чувствительные ко времени сети в вертикальных секторах (TSN). Намеченная цель состоит в том, чтобы достичь задержки субмс и надежности связи с BLER 10-6 [5]. Также учитываются дополнительные требования к коммуникациям, такие как:

усовершенствованная сконфигурированная передача гранта по восходящему каналу;

повышена надежность канала управления;

повторение мини-слотов для достижения высокой надежности;

расширенное дублирование уровня pdcp;

мультиплексирование внутри/между ue между различными услугами;

улучшить планирование для поддержки связи, зависящей от времени;

точная синхронизация времени между задействованными сетевыми узлами в пределах одного и того же домена синхронизации.

Проблемы и возможности

Мы рассмотрим новые проблемы и исследовательские возможности, которые использование ML привносит в xURLLC. Сложность образца, R1. Обучение модели должно происходить до того, как делать прогнозы с помощью модели ML или делать выводы. Распределение обучающих данных должно оставаться постоянным, чтобы обученная модель была действительной; в противном случае его необходимо переобучить. Время конвергенции обучения, или интервал этого непрерывного обучения, должно быть достаточно коротким по сравнению с динамикой эволюции временного канала. Количество обучающих выборок, необходимых для достижения определенного уровня точности или сложности выборки, определяется с помощью анализа сходимости обучения [6].

Еще одним вариантом является использование байесовских методов обучения, таких как регрессия гауссовского процесса (GPR), которые обеспечивают достоверность прогноза за счет дисперсии апостериорного распределения. И последнее, но не менее важное: используя искусственные выборки данных противника во время обучения, обучение противников повышает надежность в отношении нестационарных распределений данных, вызванных изменяющимися во времени каналами, ошибками и атаками [7]. Прогнозирование с учетом восприятия, или R3. При прогнозировании с опережением доступно больше ресурсов, но страдает точность. Чтобы уменьшить горизонт предсказания, следует использовать критерии восприятия. Перцептивное время реакции (BBP) водителя [8].

Случаи использования

AoI для прогнозирования в сверхнадежной связи V2V. В связи V2V необходимо обеспечить актуальность сообщений безопасности, и это можно сделать, применяя концепцию AoI [10]. Количество времени (AoI) между отправкой и получением сообщения. Хотя это зависит от предыдущего выбора распределения ресурсов и динамики канала, оценка будущей области охвата является сложной задачей. GPR можно использовать следующими способами, чтобы обойти эту проблему [10]. Сценарий, отображает хвостовое распределение несоответствия между расчетным и истинным AoI для конкретной мощности и выбора RB. Распределение хвоста становится

более четким, когда используется больше выборок. Дисперсия апостериорного распределения, уменьшающаяся по мере увеличения количества выборок, также точно описывает надежность прогноза [11, 12].

Управлять совместно разработанным URLLC

Основное приложение URLLC, управление беспроводными сетями в режиме реального времени, требует самых высоких стандартов надежности и задержки. Однако в домене управления можно повысить масштабируемость, ослабив ограничения URLLC [13]. Это зависит от определения значимости каждого пакета передачи в операциях управления с учетом таких ограничений, как минимально допустимая задержка (MAD) и максимально допустимый интервал передачи (MATI) (MAD), а также AoI. Эта схема системы конфликтует с 5G URLLC, который придает одинаковый вес всем пакетам и учитывает только ошибки беспроводной и односторонней передачи. Кроме того, стабильность является важнейшим критерием, который не учитывается в 5G URLLC, что делает (*control co-designed* (*CoCoCo*)) решающим фактором для обеспечения физической стабильности [13]. Фактически, как только устройство отклоняется от пути контролируемых состояний, продолжение связи становится неэффективным и неэффективным. Следовательно, xURLLC должен быть необходим, скажем, для предотвращения автомобильных аварий и обеспечения достижения пункта назначения [14].

Заключение

В статье представлен обзор запуска URLLC с опережением времени, который называется xURLLC. В отличие от 5G URLLC, который является восприимчивым, зависимым от радиочастот и ориентированным на передачу, xURLLC является оракулярным, свободным от радиочастот и объединяет передачу и прием. Эта версия устраняет многие элементарные ограничения URLLC, а также максимальное/ранговое предположение обстоятельств, расширяемость, интеграцию новых версий обновлений с меньшим количеством выше, а также ослабление критериев задержки и надежности в соответствии со статистикой. Делать. Цель xURLLC – стать пионером в критически важных функциях выше 5G и 6G, таких как управление на основе зрения, визуально-тактальная виртуальная реальность, флот самоопределяющихся и телепилотируемых дронов, а также другой запрос на кибер-физическое управление. xURLLC не может быть создан сам по себе. Вместо этого он должен влиять и основываться на других областях и понимании, таких как ML, non-RF и контроль. Необходимо учитывать различные области затрат, особенно в эпоху принятия решений и прогнозирования на основе данных.

Список используемых источников

1. Park J., Samarakoon S., Elgabli A., Shiri H., Abdel-Aziz M. K., Bennis M., Nishio T. Extreme URLLC: Vision, Challenges, and Key Enablers // ArXiv Computer Science. 2020. arXiv:2001.09683v1. PP. 1–7.

2. Feng D., She C., Ying K., Lai L., Hou Z., Quek T. Q.S., Li Y., Vucetic B. Toward Ultrareliable Low-Latency Communications: Typical Scenarios, Possible Solutions, and Open Issues // IEEE Vehicular Technology Magazine. 2019. Vol. 14. No. 2. PP. 94–102.

3. Chen H., Abbas R., Cheng P., Shirvanimoghaddam M., Hardjawana W., Bao W., Li Y., Vucetic B. Ultra-Reliable Low Latency Cellular Networks: Use Cases, Challenges and Approaches // IEEE Communications Magazine. 2018. Vol. 56. No. 12. PP. 119–125.

4. Bennis M., Debbah M., and Poor V. Ultra-reliable and low latency wireless communication: Tail, risk and scale // IEEE. 2018. Vol. 106. No. 10. PP. 1834–1853.

5. Eisen M. et al. Control aware radio resource allocation in low latency wireless control systems // IEEE Internet Things J. 2019. Vol. 6. No. 5. PP. 7878–7890.

6. Mahmood A. et al. Time synchronization in 5G wireless edge: Requirements and solutions for critical-MTC // IEEE Commun. Mag. Dec. 2019. Vol. 57. No. 12. PP. 45–51.

7. Park J., Samarakoon S., Bennis M., and Debbah M. Wireless network intelligence at the edge // IEEE. Nov. 2019. Vol. 107. No. 11. PP. 2204–2239.

8. Simsek M., Aijaz A., Dohler M., Sachs J., and Fettweis G. 5G-enabled tactile Internet // IEEE J. Sel. Areas Commun. 2016. Vol. 34. No. 3, PP. 460–473.

9. Aijaz A., Dohler M., Aghvami A. H., Friderikos V., and Frodigh M. Realizing the tactile Internet: Haptic communications over next generation 5G cellular networks // IEEE Wireless Commun. 2017. Vol. 24. No. 2. PP. 82–89.

10. Romano J. M. and Kuchenbecker K. J. Creating realistic virtual textures from contact acceleration data // IEEE Trans. Haptics. 2012. Vol. 5. No. 2. PP. 109–119.

11. Stanney K. M., Kennedy R. S., and Kingdon K., Virtual Environment Usage Protocols. Boca Raton. FL. USA: CRC Press. 2002. 307 p.

12. Patriciello N., Lagen S., Giupponi L., and Bojovic B. 5G new radio numerologies and their impact on the end-to-end latency // IEEE 23rd Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD). Barcelona. Spain. Sep. 2018. PP. 1–6.

13. Sachs J., Wikstrom G., Dudda T., Baldemair R., and Kittichokechai K. 5G radio network design for ultra-reliable low-latency communication // IEEE Network. Computer Science. 2 April 2018. PP. 1–2.

14. Ali R., Kim S. W., Kim B., and Park Y. Design of MAC layer resource allocation schemes for IEEE 802.11ax: Future directions // IETE Tech. 2018. Vol. 35. No. 1. PP. 28–52.

УДК 654.739
ГРНТИ 49.33.29

СЦЕНАРИИ ПРИМЕНЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ В СЕТЯХ 5G

З. А. Аль-Кереа, А. С. Мутханна, Х. А. Ясир

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Поскольку граничные вычисления обрабатывают данные на границах сети, а не сначала транспортируют их на большие расстояния, это увеличит спрос на граничные вычисления. Цель этой статьи – показать все преимущества кэширования и вычислительной периферии, доказав, что 5G должен быть в 10 раз эффективнее 4G. Также анализируется виды рабочих нагрузок, то есть когда говорим о пограничных серверах или сетевой границе. Кроме того, мы будем анализируется возможности применения Искусственного Интеллекта для граничных вычислений. Приложения с низкой задержкой теперь могут поддерживаться мобильными устройствами и пограничными серверами, когда они подключены напрямую через беспроводную сеть. Современная сетевая архитектура под названием MEC была создана для того, чтобы справиться с беспрецедентным ростом спроса на вычислительные ресурсы и возросшими ожиданиями пользователей, основанных на вычислениях. Он направлен на предоставление возможностей облачных вычислений и ИТ-услуг рядом с конечными пользователями путем перераспределения большого объема ресурсов обработки и хранения в сторону границ сети.

БПЛА, 5G, искусственный интеллект, RAN, интеллектуальные граничные вычисления.

Введение

Сложность граничных сетей будет возрастать по мере того, как сети 5G станут более специализированными и сложными, чем они есть. Необходимые инвестиции уже осуществляются, что в долгосрочной перспективе сделает периферийные сети более важными. Некоторые утверждают, что на эффективность пограничных сетей сильно влияет функциональность устройств, а функции сетей адаптируются к устройствам, которым они требуются [1]. Самоуправляемому автомобилю потребуются высокоскоростные граничные сети, главным образом потому, что факторы окружающей среды могут быстро меняться. В сети 5G обработка данных на периферии обеспечивает экономию энергии и инфраструктуры. Однако приложение определяет, где находится пограничное устройство [2].

Интегрированные пограничные мобильные сети «воздух-земля»

AGMEN имеет двухуровневую сетевую структуру, в которой мобильные пользователи, транспортные средства и оборудование RAN образуют наземную сеть. БПЛА развернуты для создания воздушной сети из нескольких БПЛА. Эта связь может включать в себя данные зондирования, а также информацию управления и координации (FANET) [3]. Воздушная сеть может выполнять определенные задачи, такие как поддержание связи в сети беспроводных датчиков, обработка данных для сетей, устойчивых к задержкам и сбоям (DTN), а затем направлять наземных пользователей для проведения мелкомасштабных миссий по зондированию или спасению, поскольку у них есть лучший диапазон обнаружения, чем у наземных пользователей, из-за их большой высоты. Свойства беспилотных летательных аппаратов и двухуровневая сетевая архитектура могут быть использованы AGMEN в своих интересах несколькими способами: беспилотные летательные аппараты могут выступать в качестве базовых станций для небольших сот, известных как беспилотные соты, за счет использования беспроводного переднего соединения, что дает группе гибкого доступа в Интернет наземных пользователей [4, 5].

Мобильное пограничное кэширование

В современных мобильных инфраструктурах управление перегруженными сетями становится критически важным, поскольку расширение данных представляет собой огромную трудность. Кроме того, растут ожидания потребителей в отношении мобильных сетей, такие как потребность в высокой скорости передачи данных и минимальной задержке [6]. Требуются новые сетевые конструкции, поскольку традиционная сетевая архитектура, ориентированная на БС, больше не может соответствовать этим целям [6]. Мобильное пограничное кэширование, впервые используя облачную платформу, МСС предлагает мощные вычислительные возможности и возможности хранения данных за счет аутсорсинга вычислений в центральном облаке. Однако у него высокое потребление пропускной способности транзитных линий и значительная задержка между мобильными устройствами и облаком, что делает его непригодным для приложений реального времени. Перемещение вычислительных процессов и содержимого ближе к конечным пользователям предлагается МЕС в качестве решения этой проблемы [7].

Проблемы и возможности

В этом разделе мы обрисовываем некоторые из наиболее важных проблем в среде МЕС. Что касается бизнес-потенциала, МЕС привел ряд из них ко многим важным участникам новой вычислительной парадигмы. Здесь

рассмотрим ключевые возможности, которые может предложить MEC [8]. Разрабатываемый дизайн сети представляет собой скоординированную пограничную мобильную сеть с поддержкой кэширования, в которой обслуживающие узлы на границе сети могут интерпретировать сигналы основной полосы частот и локально хранить файлы. Основными целями такого развивающегося дизайна сети являются снижение нагрузки на передние каналы связи и достижение высокой скорости доставки контента с малой задержкой, т. е. сквозной задержки доставки контента порядка миллисекунд [9, 10]. В результате приложения, чувствительные к задержке и учитывающие содержимое, используются в непосредственной близости от конечных пользователей. Обзор исследовательского ландшафта, включая возможности, проблемы и направления, представлен в этой статье. Сначала мы предоставим обзор архитектуры координированной пограничной мобильной сети с поддержкой кэширования, прежде чем перейти к основным технологическим препятствиям и нерешенным исследовательским вопросам, которые необходимо решить для этой архитектуры [11]. Затем представлены новые стратегии передачи на физическом уровне с поддержкой кэширования, чтобы уменьшить задержку доставки и нагрузку на передние каналы связи. Наконец, представлены перспективы будущих исследований связи с кэшированием на основе искусственного интеллекта. Многочисленные преимущества могут быть реализованы путем хранения популярного контента на границе сети с правильно скоординированными стратегиями передачи, согласно численному моделированию [12].

Отношения между граничными вычислениями и ИИ

Совершенно новая парадигма вычислений, известная как граничные вычисления, становится все более популярной в то время, когда коммуникационные технологии развиваются быстрыми темпами, а использование мобильных устройств растет [13]. Достижения в области глубокого обучения и улучшенная аппаратная архитектура привели к буму приложений искусственного интеллекта (ИИ). Границы сети генерируют миллиарды байтов данных, что предъявляет высокие требования к обработке данных и оптимизации структуры. Пограничный интеллект – это результат высокого спроса на интеграцию ИИ и граничных вычислений. В этой статье мы проводим различие между граничным интеллектом (*AI for edge*) и граничным интеллектом (*AI on edge*) (Искусственный интеллект на краю) [14].

Мобильные пограничные вычисления

В последние годы произошел сдвиг парадигмы мобильных вычислений, отход от централизованных мобильных облачных вычислений к мобильным граничным вычислениям, обусловленный концепциями Интернета вещей и связи 5G (MEC) [15]. Для поддержки ресурсоемких

и критичных к задержке приложений на мобильных устройствах с ограниченными ресурсами MEC переносит мобильные вычисления, управление сетью и хранилище на границы сети (например, на базовые станции и точки доступа). MEC обещает значительное снижение задержки и энергопотребления мобильных устройств, устраняя основные препятствия на пути реализации концепции 5G [15].

Заключение

MEC представляет собой передовую сетевую архитектуру, разработанную для удовлетворения беспрецедентно растущего спроса на вычислительные ресурсы и растущие стандарты пользовательского опыта, основанного на вычислениях. Прямое беспроводное соединение между мобильными устройствами и пограничными серверами открывает двери для поддержки приложений с чрезвычайно низкими требованиями к задержке, продлевает срок службы батареи устройства и обеспечивает высокоэффективную работу сети. В этом исследовании мы представили тщательный анализ и исследовательскую точку зрения MEC с точки зрения коммуникации. Для этого мы сначала обрисовали подходы к моделированию, используемые для важных элементов системы MEC, включая вычислительные задачи, связь и вычисления на мобильных устройствах и серверах MEC. Это упрощает описание того, насколько хорошо системы MEC работают в отношении задержки и мощности. Основываясь на системном моделировании, мы провели тщательный обзор недавних исследований по управлению ресурсами для MEC при различных системных архитектурах, в которых используются идеи разгрузки вычислений, совместного распределения радио- и вычислительных ресурсов, планирования серверов MEC, а также мульти- выбор сервера и сотрудничество. Затем были отмечены некоторые перспективные направления исследований, такие как проблемы развертывания MEC, MEC с кэш-памятью и управление мобильностью MEC, а также зеленый MEC. По каждому из этих направлений были разработаны основные исследовательские проблемы и ранние пути их решения. Наконец, мы представили многочисленные типичные сценарии использования вместе с самыми последними усилиями по стандартизации в отрасли.

Список используемых источников

1. Wang S., Zhang X., Zhang Y., Wang L., Yang J., and Wang W. A survey on mobile edge networks: Convergence of computing, caching and communications // IEEE Access. 2017. Vol. 5. PP. 6757–6779.

2. Nan C., Wenchao X., Weisen S., Yi Z., Ning L., Haibo Z., Xuemin S. Air-Ground Integrated Mobile Edge Networks: Architecture, Challenges and Opportunities // IEEE Communications Magazine. 2018. Vol. 56. No. 8. PP. 26–32.

3. Tao X., Ota K., Dong M., Qi H., and Li K. Performance guaranteed computation offloading for mobile-edge cloud computing // IEEE Commun. Lett. 2017. Vol. 6. No. 6. PP. 774–777.

4. Liu L., Chang Z., Guo X., Mao S., and Ristaniemi T. Multiobjective optimization for computation offloading in fog computing // IEEE Internet Things J. 2018. Vol. 5. No. 1. PP. 283–294.

5. Cheng N., Lu N., Zhang N., Zhang X., Shen X. S., and Mark J. W. Opportunistic WiFi offloading in vehicular environment: A game-theory approach // IEEE Trans. Intell. Transp. Syst. 2016. Vol. 17. No. 7. PP. 1944– 1955.

6. Bor-Yaliniz I. and Yanikomeroglu H. The new frontier in RAN heterogeneity: Multi-tier drone-cells // IEEE Commun. Mag. 2016. Vol. 54. No. 11. PP. 48–55.

7. Asif-Ur-Rahman M., Afsana F., Mahmud M., Kaiser M. S., Ahmed M. R., Kaiwartya O., and James-Taylor A. Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things // IEEE Internet of Things Journal. 2019. Vol. 6, No. 3. PP. 4049–4062.

8. He T., Ciftcioglu E. N., Wang S., and Chan K. S. Location privacy in mobile edge clouds: a chaff-based approach // IEEE Scientific Programming 11 Journal on Selected Areas in Communications. 2017. Vol. 35. No. 11. PP. 2625–2636.

9. Gupta A. Performance insight 360: a cloud-based quality management framework for educational institutions in India // IEEE 15th Conference on Business Informatics. 2013. PP. 139–144.

10. Rahimi M. R., Ren J., Liu C. H., Vasilakos A. V. and Venkatasubramanian N. Mobile cloud computing: A survey, state of art and future directions // Mobile Networks and Applications. 2014. Vol. 19. No. 2. PP. 133–143.

11. Chalaemwongwan N. and Kurutach W. Mobile cloud computing: A survey and propose solution framework // International Conference on Electrical Engineering/Electronics, Computer (ECTI-CON). Jun. 2016. PP. 1–4.

12. Sutton R. S. and Barto A. G. Reinforcement learning: An introduction. Cambridge, MA, USA: MIT Press. 2018. 552 p.

13. Ong H., Chavez K., and Hong A. Distributed deep Q-Learning. 2015. arXiv:1508.04186. PP. 1–8.

14. Liu D., Chen B., Yang C., and Molisch A. F. Caching at the wireless edge: design aspects, challenges, and future directions // IEEE Communications Magazine. 2016. Vol. 54. No. 9. PP. 22–28.

15. Su Z., Xu Q., Hou F., Yang Q., and Qi Q. Edge caching for layered video contents in mobile social networks // IEEE Trans Multimedia. 2017. Vol. 19. No. 10. PP. 2210–2221.

UDK 004.056
GRNTI 49.33.29

BIOMETRIC AND BEHAVIORAL AUTHENTICATION AND SOFT BIOMETRICS USING KEYSTROKE AND MOUSE DYNAMICS

Yousef Mohammed Abd Allh Alotoum

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Relying on web applications and mobile applications to store and process sensitive information, making it necessary to protect it from hackers. Behavioral biometrics such as keystroke and mouse dynamics that utilize an individual's typing and clicking rhythm can be used to enhance existing security techniques that are effective and cheap. Because of the ballistic semi-autonomous nature of typing behavior and mouse-use behavior, they are difficult to impersonate, making them useful as biometrics.

biometric authentication, keystroke dynamics, mouse dynamics, soft biometrics, continuous authentication.

It has become even more important to protect Internet networks from attackers since we rely so much on them to store and process sensitive information [2, 6]. In computer-based applications, a straightforward, inexpensive, and unobtrusive device is required for user authentication and identity [2]. The use of biometrics, such as face, fingerprints, and signatures, necessitates the use of additional equipment, raising the cost of the biometric [3]. The regular keyboard or mouse and other existing devices can be used to obtain a behavioural biometric that uses a person's typing style, making it an affordable and highly desirable method [7, 13]. The fact that this biometric is non-intrusive and may be used discreetly to improve current cyber-security systems is one of its main advantages.

Biometrics: It is a branch of science that focuses on quantitative research on population and its diversity based on measurements of the characteristics of biological organisms. Such investigations aim to classify and describe individuals and can be used to verify or identify people to protect various resources, distinguishes it from other methods that’s no need to remember the password or other items and symbols that allow access to resources, increased security (allows the use of biometric data to protect against some attacks such as phishing) and it is impossible to forget or lose it [3].

The biometric system includes three factors Something you know like a password, something you have like a certificate token or a phone number and some-

thing you are like a biometric fingerprint, an iris scan [8, 13, 14]. And must comply with seven characteristics universality, uniqueness, permanence, achievement, performance, acceptance and circumvent [1, 3].

The biometric system can be divided into two types [14]:

1. Authentication: is the process of determining whether a person is actually the one who wants to access a site [3]. Authentication [13] can be divided into two groups: Static authentication [8] the system will authenticate the user only once at the beginning of the session and continuous authentication(active) the system will monitor the user throughout an entire session to detect any change in identity during that session.

2. Identification: is the process of linking a person to an identity [3].

One of the types of biometrics is the biological biometrics [8, 13], in which people are identified through their physical characteristics such as the face and palm print. Voice There is also a third type of soft biometrics, in which physical or behavioural human characteristics are determined from the way humans are characterized, such as height, sex, and hair colour.

Keystroke dynamics KD: It is the process of analysing the way a user writes in a given part by observing keyboard input thousands of times per second in an attempt to identify the user based on their usual typing rhythm patterns, which is the study of the unique timing in an individual's writing [2, 5, 11]. Keystroke dynamics methods are language independent since the features are primarily derived from how the user uses the keyboard rather than the words, they type in a given language [6]. Spillane was the first to invent the use of keyboards to measure the dynamics of the keystrokes of individuals [14]. The first to show that keystroke dynamics can be used for authentication are Gaines, El 1980 [7, 11].

Keyboard characteristics can be extracted through the most common behavioural patterns [5], including:

1. Down-up Time: It is the time interval between a key being pressed (the duration of the key being pressed) [2, 3, 7, 13].

2. Up-Down Time: It is the time between releasing one key and pressing the next key (it is the travel time between the two keys) [13, 2, 7].

3. Down-Down Time: It is the time elapsed between pressing the first key and pressing the next key (It is often used as a substitute for Up-Down time because it is always positive).

4. Up-Up Time: It is the time between releasing two consecutive keys.

5. Release-release Time: It is the duration of the time to release the first key while pressing the second key and the duration of releasing the second button.

6. Hold-dwell time: It is the continue duration of the key press [3, 6, 7].

7. Flight Time: It is the rest time between the first key and the second key [6].

8. Trigrams: Any combination of three letters [2].

9. Tetragrams: Any combination of four letters and digraph they are two letters that have the same sound that can consist of a vowel or a consonant [2, 6, 10] (th, sh, ch).

Users are authenticated based on the way they type on the keyboard when they type a password [7]. Not only is the password itself checked to be correct, but also if the typing cadence when entering the password is correct. This process is called password hardening [13]. It is a low-cost and easy-to-implement security system because This system does not depend on other programs, it captures keystroke timing information and extracts authentication and identification features [2].

The process of evaluating and authentication of user is based on the False rejection rate (FRR), the false acceptance rate (FAR), and the Error efficiency rate (EER), if Low FRR For high security systems, it may be desirable to reduce the FAR so fewer fraudsters are identified [8, 11, 13, 17].

This leads to a higher FAR that's mean the real user may have to make more than one authentication attempt, if Low "FAR" To obtain high user acceptance and usability, it may be desirable to have a low FAR in order to increase the likelihood that the fraudster mis authenticated. The ideal situation is ERR equal 0 This means that no one can authenticate against another person's form and every user registered in the system is authenticated successfully [11].

There are studies that show that the password can be complicated using dynamic keystrokes, as it seems that the measure of complexity is related to the time it takes to move from the first key on the keyboard to the other key, and the more the location of the two keys is separated from the other, the greater the complexity of the key, for example, the distance between A-P big and between O-P small Thus, "A-P" is more complex than "O-P" [12].

Mouse dynamics MD: It is a series of movements, i.e., gestures, and each gesture is a specific and continuous physical process initiated and concluded by the user [13, 15]. The main goal of mouse tracking is to understand deeper user behaviour to infer user intentions. There is eye tracking, but mouse tracking is cheaper and better. Every mouse event that is performed on the system will be authenticated.

The field of Human-Computer Interaction is particularly interested in studying human behaviour since it can shed light on human performance. Mouse and keyboard tracking, according to previous HCI research, may give a fuller picture of user behaviour when high cognitive loads, such as decision-making and developing activities, are present [15].

Mouse characteristics [15] can be extracted through the most common behavioural patterns, including:

1. Straight style: indicates users with confident movements characterized by a pause before moving to the target location.

2. frequency pattern: can be used to infer the user's perceived difficulty, levels of risk perception, and the user's susceptibility to interacting with the system, or when hovering the mouse pointer over or under the target element or any other element that clicks on it, it also indicates doubt and difficulty in making a decision.

3. Reading style: Reading style can be divided into two different types according to behaviour Vertical reading style and horizontal reading style

4. Random pattern: It is characterized by movements without any specific intention, just playing and making random movements with or without short periods.

5. Fixed pattern: refers to the areas where users most often use the mouse cursor rest. The cursor rest areas are often on the right side of the page. This area is called the white area.

6. Guide pattern: defines the behavior of the continuous movement of the mouse cursor, acts as an exploratory role and indicates the existence of a relationship between the mouse and eye movement, and thus this pattern will give us an idea of the user's expectations. The raw mouse data consists of: events, hover, moves, mouse click.

Also, can be extracted other properties [4, 9, 13] from the mouse dynamics for authentication user: mouse clicks left or right, mouse hovers, key press time, key release time, length and number of sample movement of the mouse curve, bending and turning, speed and acceleration, elapsed time, Merge the active region where the mouse event occurs, midpoint of the active region, drag and drop: It is the transfer of the file from one place to another.

Soft biometrics: Biometric characteristics that are not sufficient to authenticate the user, such as height, gender, skin, eye, hair colour [5], and are derived from the way humans are distinguished, and these characteristics are available to all. Soft biometrics allow the refinement of the search for the real user in the database leading to a reduction in computing time for example if the capture result corresponds to a male according to the soft biometric unit, a standard biometric authentication system can limit the search field to male users without regard to females. Features discovered in soft biometrics for authentication: Determine the emotional [10] state and can be detected by 84%, determining the gender can be detected by 90%, determine handedness while typing on the keyboard one or two hands can be detected by 80%, determine If the user is left-handed or right-handed and determine the age group. Most user authentication methods focus when the user initiates the session at login time only but it is also important to authenticate the user during the session hence the term continuous authentication appears [16].

The researchers found that the sound of writing can reveal the content of writing. One of the complex methods of authentication is to integrate the fea-

tures and strength of the keystroke with the voice features [17]. This is done by extracting the features of the sound of the keystroke, as this feature reflects the biometric features of the users, after which the user is identified and authenticated. Figure 1 illustrates the user authentication mechanism based on behavioural biometrics such as keystroke and mouse dynamics, and soft measurements [4, 6].

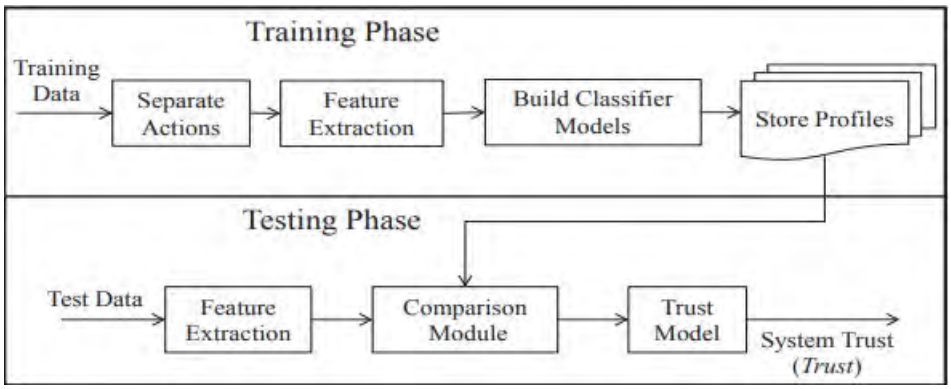


Fig. 1. User authentication mechanism based on behavioral measurements and soft

Figure 2 illustrates the user authentication lifecycle [4, 5, 10] based on keystroke dynamics and soft metrics. The user is trained based on a Support Vector algorithm [2, 4, 6, 16, 17] that is used in classification, regression, and more commonly in classification problems, for text classification such as category mapping, spam detection, sentiment analysis, image recognition, and recognition on the handwritten numbers such as postal operating services.

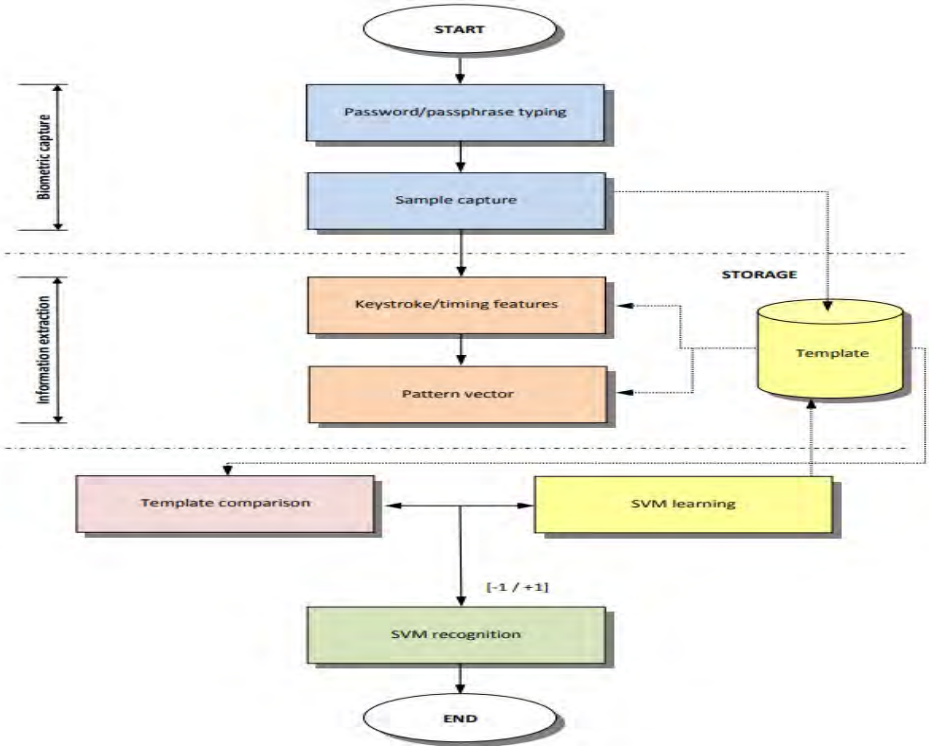


Fig. 2. Lifecycle User Authentication Behavioral and Soft Measurements

References

1. Janakiraman R., Sim T. Keystroke Dynamics in a General Setting // Lecture Notes in Computer Science, 2007. 593 p.

2. Tsimperidis I., Arampatzis A. The Keyboard Knows About You: Revealing User Characteristics via Keystroke Dynamics // International Journal of Technoethics, 2020. 51 p.

3. Kasprowski P., Borowska Z., Harezlak K. Biometric Identification Based on Keystroke Dynamics // State-of-the-Art Sensors Technology, 2022. 100 p.

4. Mondal S., Bours P. Continuous Authentication using Mouse Dynamics // International Conference of the BIOSIG Special Interest Group (BIOSIG), 2013. 124 p.

5. Zulkarnain S., Cherrier E., Rosenberger C., Mondal S., Bours P. Keystroke Dynamics Performance Enhancement with Soft Biometrics // Security and Behavior Analysis, 2015. 90 p.

6. Gaikwad J., Kulkarni B., Phadol N., Sarukte S. User Authentication using Keystroke Dynamics // Global Research and Development Journal for Engineering, 2018. 2464 p.

7. Hassan S., Selim M., Zayed Hala. User Authentication with Adaptive Keystroke Dynamics // International Journal of Computer Science Issues, 2013. 135 p.

8. Bours P. Continuous keystroke dynamics: A different perspective towards biometric evaluation // Information security technical report xxx, 2012. 43 p.

9. Mondal S., Bours P. Combining Keystroke and Mouse Dynamics for Continuous User Authentication and Identification // Security and Behavior Analysis (ISBA), 2016. 73 p.

10. Zulkarnain S., Cherrier E., Rosenberger C., Bours P. Soft Biometrics for Keystroke Dynamics: Profiling Individuals While Typing Passwords // Computers & Security, 2014. 155 p.

11. Seeger M., Bours P. How to Comprehensively Describe a Biometric Update Mechanisms for Keystroke Dynamics // Third International Workshop on Security and Communication Networks (IWSCN), 2011. 55 p.

12. Mondal S., Bours P., S. Z. Complexity Measurement of a Password for Keystroke Dynamics: Preliminary Study // Security of Information and Networks, 2013. 305 p.

13. Mondal S., Bours P. Continuous Authentication using Behavioural Biometrics // IT Professional, 2013. 15 p.

14. Banerjee S., Woodard D. Biometric Authentication and Identification using Keystroke Dynamics: A Survey // Pattern Recognition Research, 2012. 139 p.

15. Katerina T., Nicolaos P. Mouse behavioral patterns and keystroke dynamics in End-User Development: What can they tell us about users' behavioral attributes? // Computers in Human Behavior, 2018. 305 p.

16. Zulkarnain S., Cherrier E., Rosenberger C., Bours P. Soft Biometrics for Keystroke Dynamics // Image Analysis and Recognition, 2013. 19 p.

17. Zhou Q., Yang Y., Hong F., Feng Y., Guo Z. User Identification and Authentication Using Keystroke Dynamics with Acoustic Signal // Mobile Ad-Hoc and Sensor Networks, 2016. 449 p.

Статья представлена научным руководителем, заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 656.2
ГРНТИ 73.29.86

АНАЛИЗ ПРИМЕНЕНИЯ ЦИФРОВЫХ ДВОЙНИКОВ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

А. Р. Андреева, А. К. Канаев

Петербургский государственный университет путей сообщения императора Александра I

В настоящее время появляется все больше предпосылок для воплощения в жизнь концепции Индустрия 4.0 в различных отраслях экономики и повседневной жизни человека, в том числе и железнодорожный транспорт. Цифровой двойник является одним из ведущих инструментов данной трансформации. Применение цифровых двойников для различных объектов железнодорожного транспорта даст возможность оптимизировать работу данной структуры, оптимально назначать сроки службы, предотвращать неисправности, чрезвычайные ситуации и т. д.

цифровой двойник, железнодорожный транспорт, индустрия 4.0, цифровизация, моделирование.

Железнодорожный транспорт (ЖДТ) является одной из основных возможностей для путешествий, а также важной составляющей грузоперевозок во всем мире, в том числе в Российской Федерации. Рост пассажирских и грузовых перевозок дает мощный толчок к развитию, автоматизации и оптимизации железнодорожного транспорта.

Четвертая промышленная революция (Индустрия 4.0) напрямую связана с внедрением технологий, в том числе: интернет вещей, искусственный интеллект, аналитика больших данных, цифровой двойник (ЦД) и другие, которые затрагивают и сферу ЖДТ. Развитие данных технологий позволяет оперативно использовать исходные данные с реальных объектов и оперативно получать решения в различных ситуациях.

Развитие технологии цифровых двойников на ЖДТ согласуется со Стратегией развития транспортного машиностроения РФ на период до 2030 г, которая утверждена распоряжением Правительства Российской Федерации от 17 августа 2017 г. № 1756-р. В данной стратегии выделены три приоритетных области, которым ЦД позволят повысить эффективность, – это внедрение интеллектуальных систем при эксплуатации грузового подвижного состава, развитее тяжеловесного движения и развитие высокоскоростного движения [1].

Термин «цифровой двойник» в настоящее время не получил точной формулировки, в данной работе под ЦД понимается виртуальная копия фи-

зического устройства, которая обладает видом и свойствами реального аналога, моделирует внутренние процессы, технические характеристики и поведение реального объекта в условиях воздействий помех и окружающей среды, а также позволяет наблюдать прошлые состояния и прогнозировать поведение объекта в будущем.

Основные составляющие ЦД – это динамические имитационные модели и данные, своевременно отображающие состояние реального двойника. Такие данные могут быть собраны автоматически с помощью сенсорных сетей и технологии Интернет вещей (IoT), а также внесены различными работниками, например, электромеханиками, диспетчерами, дежурными по станции, машинистами и т. д. Упрощенная структурная схема реализации ЦД представлена на рис. 1 [2].

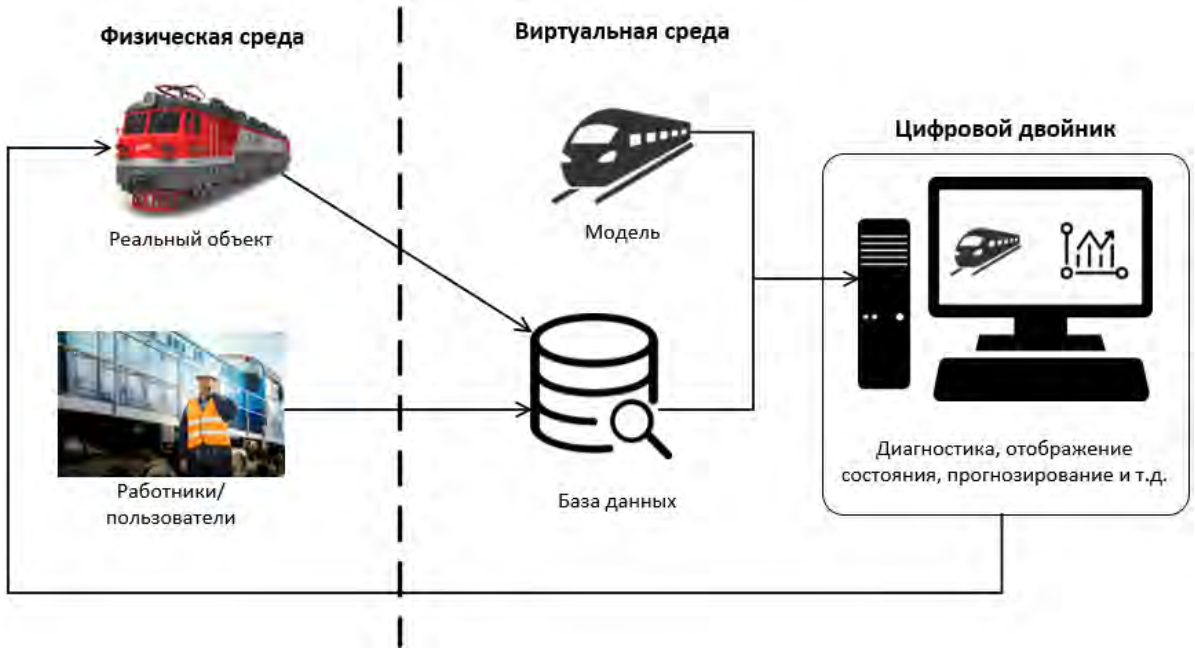


Рис. 1. Структурная схема технологии «Цифровой двойник»

Таким образом, применение ЦД на ЖДТ возможно только в случае разработанной адекватной модели различных объектов. Поэтому для реализации данной задачи необходимо рассматривать не только сам объект, но и окружающую среду и инфраструктуру. Определение поведения реального двойника в различных ситуациях и условиях невозможно без виртуального пространства, так называемого виртуального полигона для испытаний, который будет давать возможность имитировать поведение объектов.

С помощью существующих средств моделирования потенциально можно реализовать цифрового двойника динамичных объектов ЖДТ, но существует важная задача – обеспечить синхронизацию имитационной модели с реальными данными. В настоящее время большинство моделей являются асинхронными и работают при наличии уже заданного расписания.

В свою очередь, для разработки синхронной модели необходимо применение дополнительных аппаратных и/или программных средств [3].

Для реализации цифрового двойника железной дороги в целом изначально необходимо осуществить цифровизацию ЖД, в том числе: ввести контроль пути с помощью высокоскоростных поездов и железнодорожные сканеры для улучшенной диагностики и обслуживания, автоматизировать управление поездами, усовершенствовать мониторинг за персоналом, создать интеллектуальные станции, использовать тренажерные системы и систем обучения виртуальной реальности для улучшения возможностей персонала.

Важным достоинством ЦД является возможность прогнозирования изменений в различных системах ЖДТ, что дает представления о будущей производительности данных систем и составляющих, о необходимых заменах составных частей, профилактических ремонтах, а, следовательно, позволяет избежать серьезных отказов, угрожающих жизни и здоровью людей, перерывов в транспортном сообщении и крупных материальных потерь.

При строительстве новых железных дорог либо ее модернизации целесообразно сначала реализовать ее цифровой двойник, чтобы избежать рисков, которые напрямую связаны с неправильным строительством.

Железная дорогая обладает масштабным размером и сложностью и существенно отличается от заводов и фабрик, для которых чаще всего рассматриваются цифровые двойники. Также транспортная система сложна с точки зрения технологий и операций из-за участия широкого круга людей, организаций и технических решений. Для оптимизации реализации ЦД всей системы стоит использовать большое количество различных двойников, моделирующих различные подсистемы и процессы.

Ученые Бирмингемского центра железнодорожных исследований и образования (BCRRE) предлагают деление цифрового двойника железной дороги на пять слоев. Данные слои представлены на рис. 2 (см. ниже) [4].

Данное деление на уровни позволяет структурировать разработку ЦД и разделить конкретные задачи на специалистов нескольких областей науки. Взаимодействие которых увеличит эффективность внедрения и скорость разработки конкретных задач, но усложнит процесс объединения данных частей.

Создание цифровых двойников железнодорожного транспорта и инфраструктуры реально лишь при наличии мощных экономических показателей, которые могут обеспечит замену устаревшего оборудования.

Цифровой двойник железнодорожной системы позволит повысить безопасность пассажирских и грузовых перевозок, снизить затраты на ремонт, обеспечить эффективность перевозочного процесса, предвидеть серьезные отказы и исключать их, оптимально подбирать сроки эксплуатации и другое.

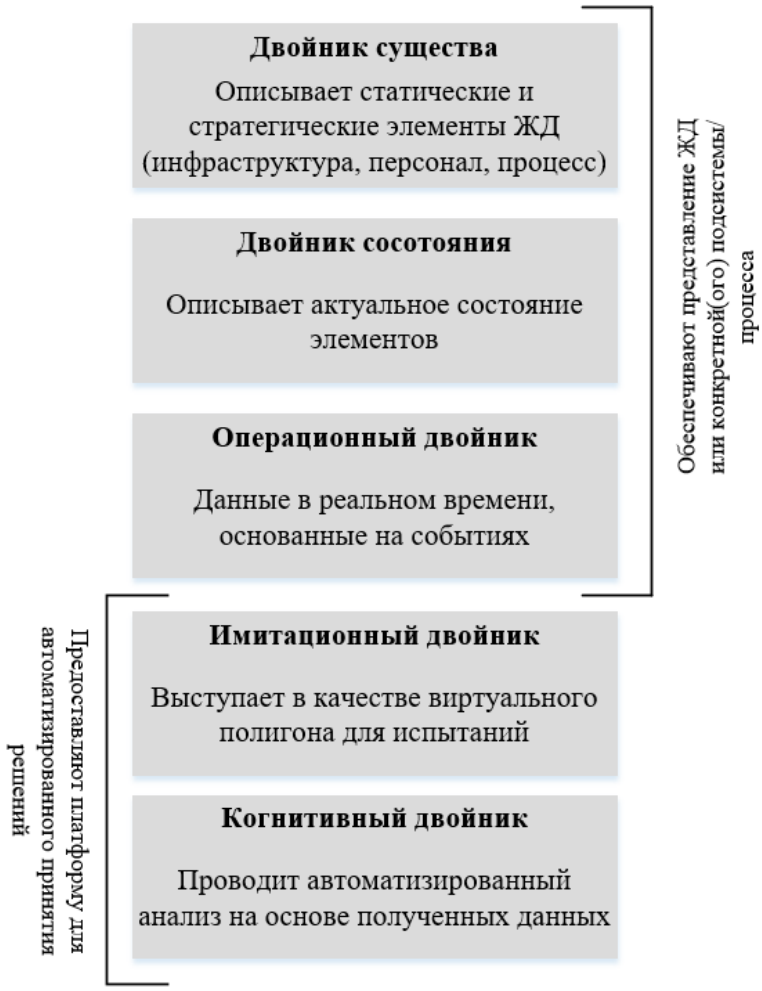


Рис. 2. Уровни цифрового двойника в соответствии с представлением BCRRE

По исследованиям компании MarketsandMarkets эксплуатация цифровых двойников вырастет в 10 раз к 2025 году. Поэтому для поддержания конкурентоспособности ЖДТ необходимо развивать данную отрасль в сторону элементов Индустрии 4.0, в том числе и цифровых двойников.

Список используемых источников

1. Шевченко Д. В. Методология построения цифровых двойников на железнодорожном транспорте // Вестник Научно-исследовательского института железнодорожного транспорта (Вестник ВНИИЖТ). 2021. Т. 80. N 2. С. 91–99.

2. Куприяновский В. П., Аленьков В. В., Климов А. А., Соколов И. А., Зажигалкин А. В. Цифровая железная дорога – ertms, bim, gis, plm и цифровые двойники // Современные информационные технологии и IT-образование. 2017. Т. 13. N 3. С. 129–166.

3. Rakhmangulov A., Mishkurov P., Kornilov S. Digital twins of railway junctions based on a simulation model // The eighth international conference transport and logistics. 2021. PP. 5–12.

4. Digital Twins and the Railway: One Framework Many Implementations [Электронный ресурс]. URL: https://www.rssb.co.uk/what-we-do/insights-and-news/blogs/digital-twins-and-the-railway-one-framework-many-implementations (дата обращения 14.02.2023).

УДК 621.3.082.1
ГРНТИ 47.01.81

ОБЗОР И СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ ДАТЧИКОВ ДАВЛЕНИЯ

А. И. Арсирий, М. С. Былина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Представлены основные типы сенсоров (датчиков) давления, нашедшие применение в различных областях техники и технологий, в электронике, главным образом, оптоэлектронике. Приведены важнейшие принципы и характеристики их работы, диапазон и спектр применения. Дана характеристика групп материалов, на основе которых реализуются функциональные свойства сенсоров давления различного уровня чувствительности, класса точности и энергопотребления, продолжительности автономной работы и т. п.

измерение давления, принципы работы, датчики давления, материалы.

Датчики давления – обязательный элемент большей части измерительных комплексов. Они входят в состав систем, служащих для осуществления автоматического контроля и управления, где необходимо знать цифровое значение давления для обеспечения бесперебойной и безопасной работы оборудования.

Существует несколько наиболее часто используемых методов измерения давления. Эти методы можно условно разделить на основные группы:

визуальный замер высоты жидкости – манометры;

метод упругой деформации – деформация упругого материала пропорциональна прикладываемому давлению;

электрические методы – изменение давления приводит к изменению электрических параметров в проводнике, полупроводнике или диэлектрике, также может быть зафиксировано косвенное изменение электромагнитных характеристик чувствительного сенсора;

оптические (волоконные) методы – основаны на изменении параметров оптического сигнала при изменении давления, фиксируемого вследствие деформационных процессов [1].

В зависимости от всех этих характеристик выделяют следующие типы датчиков:

Упругие датчики зачастую используются для измерения давления жидкости. Является прибором с упругой стенкой, представленной диафрагмой или мембраной, показатели отклонения которой определяют уровень

давления. В основном эти датчики чувствительны, особенно к резким изменениям давления, но легко сбиваются при воздействии вибраций. Мембраны выполняют из металла, полимера, стекла в форме пластин, дисков или пружин [2].

Электрические датчики устанавливаются совместно с упругими, увеличивая точность измерения и электронную фиксацию давления.

Емкостные, состоящие из параллельных пластин-конденсаторов, соединенных с металлической диафрагмой. также в конструкции есть электроды, запитанные от высокочастотного генератора.

Индуктивные, с ферромагнитным сердечником, обмотками и упругим элементом. Диапазон давления, в котором может быть использован этот датчик определяется параметрами упругого элемента.

С магнетосопротивлением – конструкция с ферромагнитным сердечником, пластиной и гибким элементов. При изменении давления, гибкий элемент перемещает ферромагнитную пластину, что приводит к изменению магнитного поля, которое в свою очередь измеряется.

Пьезоэлектрические с датчиком-кристаллом, который формирует электрический заряд в тот момент, когда воспринимает давление.

Потенциометрические оснащаются рычагом, прикрепленным к упругому датчику. При низкой чувствительности и рабочем диапазоне, они могут лучше всего подойти в качестве дешевого детектора давая грубую оценку.

Тензометрический: изменения давления определяются путем расчета колебаний сопротивления мостовой схемы Уитстона. Чувствительность датчиков сохраняется при постоянстве температуры.

Вибрационные, в них измеряются изменения резонансной частоты вибрирующих элементов, а сам датчик расположен в изолированном цилиндре под вакуумом. Такие устройства подходят для измерения стабильных величин без резких скачков и практически не подвержены воздействию температур.

Дифференциальные: измеряется разность давления, которая преобразуется в передаваемый сигнал. Используется в паре с емкостным элементом или с диафрагмой, которые и определяют чувствительность измерений.

Вакуумные или вакуумметры работают при давлении ниже атмосферного, в вакууме или при чрезвычайно низких величинах.

Тепловые, используют при работе изменение теплопроводности газовой среды вследствие изменения ее объема при градиенте давления. Такие чувствительные элементы работают только при низких давлениях.

Приборы ионизации могут быть с горячим либо с холодным катодом. В первом типе датчиков характеристики определяются электронами, полу-

чаемыми при термоэмиссии, во втором – при ионной эмиссии. Оба типа датчиков высокочувствительны и подходит для измерения дробных долей давления.

Оптические датчики давления – работают в условиях агрессивных сред, перепада температур, а также при воздействии электромагнитных полей. Поэтому устройства фотоники, обладающие резонансными свойствами, широко используются в сенсорной фотонике. Оптические датчики подразделяются на волоконно-оптические и оптоэлектронные. [3]

Волоконно-оптические датчики давления являются наиболее точными, температуростабильными. Рабочие характеристики определяются по изменению оптических – амплитуде, поляризации, интенсивности потока фотонов, проходящих по оптическому волноводу.

Оптоэлектронные датчики состоят из многослойных прозрачных структур, через которые пропускают свет. Один из прозрачных слоев может изменять свои параметры в зависимости от давления среды.

Принцип действия волоконных датчиков давления, применяемых в настоящее время основаны на эффектах резонанса, реализуемых в следующих устройствах:

– интерферометр Фабри-Перо;
– резонатор на модах шепчущей галереи;
– петлевой и узловой резонаторы.

Конструкции сразу нескольких оптических датчиков изготавливаемых из оптоволокна весьма схожи, например, р*езонатор на модах шепчущей галереи, петлевой и узловой оптические резонаторы* представляют подобие кольцевого резонатора. Преимуществом первой конструкции является их чрезвычайно высокая добротность – она может достигать 10^{10} [4], а второй – идеальное сочетание с другими элементами волоконной оптики и механическая гибкость [5]. Отличительными особенностями конструкций является путь моды. Материалом для производства волоконной части датчиков является диэлектрик – кварцевое стекло и полиметилметакрилат.

Конструкция *использующая интерферометр Фабри-Перо* изготавливается из кварцевого волокна, которое имеет сферическое углубление на торце, этот конец играет также роль одного из зеркал интерферометра, и кварцевой пластиной, являющейся гибкой мембраной и второго зеркала интерферометра. Изменение кривизны пластинки приводит к изменению резонансной частоты интерферометра за счет спектрального сдвига. Варьируя кривизну углубления и толщину пластинки, можно изменять диапазон измерений. Тот же принцип интерферометра при малых перемещениях примеряется и в оптоэлектрических датчиках [6].

На основании обзора современных источников ниже приведена сравнительная характеристика основных типов датчиков давления (табл. 1).

ТАБЛИЦА 1. Сравнительная характеристика датчиков давления

Тип элемента	Диапазон давления, МПа	Чувствительность, МПа	Преимущество	Недостатки
Трубка Бурдона	0,1…700	0,03	Экономичны	Статические измерения; Низкая точность
Диафрагмы	0,1…2,2	0,01	Высокая точность	Очень дорогой
Емкостные	$2{,}5\cdot10^{5}$ – 70	0,07	Для измерения низких давлений и вакуума	Емкостные пластины могут слипаться в процессе эксплуатации
Индуктивные	$2{,}5\cdot10^{4}$ – 70	0,35	Высокая чувствительность	Более грубые по сравнению с датчиками магнетосопротивления
Магнетосопротивления	2, $5\cdot10^{4}$ – 70	0,35	Высокая чувствительность	Требуют наличия внешнего источника переменного тока
Пьезоэлектрические	0,021…100	0,1	Очень быстрое время отклика	Подвергается влиянию высоких температур и статических сил
Потенциометрические	0,03…70	0,07–0,35	Маленькие размеры	Маленькая чувствительность
Измерения натяжения	0…$1{,}4\cdot10^{3}$	1,4–3,5	Высокая чувствительность	Медленные; Слабый сигнал
Теплопроводности	$0{,}4\cdot10^{3}$ – $1{,}3\cdot10^{-3}$	$6\cdot10^{-13}$	Способны измерять вакуум	Измерения линейны только на низких давлениях
Ионизации	$1{,}3\cdot10^{-13}$ – 10^{-8}	10^{-13} – 10^{-16}	Могут измерять глубокий и сверхглубокий вакуум	Ограничены фотоэлектрическим эффектом

Тип элемента	Диапазон давления, МПа	Чувствительность, МПа	Преимущество	Недостатки
Вибрации	0,0035…0,3	10^{-5}	Очень точные; Термостабильны	Определяют низки и средние давления
Оптические	$1{,}3 \cdot 10^{-13}$ – 10	10^{-8}	Термо- и электростабильны, просты в работе. Высокая чувствительность	Необходимость сложной калибровки

Список использованных источников

1. Козлов В. Л. Оптоэлектронные датчики : конспект лекций по одноименному спецкурсу для студ. спец. G 31 04 02 «Радиофизика». Мн. : Белгосуниверситет, 2005. 116 с.

2. Лукьянов Г. Н. Сенсоры и датчики физических величин. СПб. : Университет ИТМО, 2020. 57 с.

3. Сидоров А. И. Сенсорная фотоника : учеб. пособие. СПб. : Университет ИТМО, 2019. 96 с.

4. Ioppolo T., Ötügen M. V. Pressure tuning of whispering gallery mode resonators // J. Opt. Soc. Am. B. 2007. V. 24. PP. 2721–2726.

5. Nguyen N. Q., Gupta N. Power modulation-based fiber-optic loop-sensor having a dual measurement range // J. Appl. Phys. 2009. V. 106. 033502.

6. Фрайден Дж. Современные датчики. Справочник : пер с англ. М. : Техносфера, 2005. 587 с.

УДК 512.742.72
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКИХ ОПЕРАЦИЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ НА ПРОТОКОЛ ДИФФА-ХЕЛЛМАНА С ЦЕЛЬЮ ПОВЫШЕНИЯ НАДЕЖНОСТИ КЛЮЧЕЙ В СЕТЯХ VPN

А. М. Ахапкина, С. П. Способ

Белорусский государственных университет информатики и радиоэлектроники

В сетях VPN для вычисления открытого и закрытого ключей используется алгоритм Диффа-Хеллмана. Однако метод обратного логарифмирования позволяет заранее

вычислить все пары ключей. Применение метода, базируемого на математических операциях на эллиптических кривых, не позволяет заранее вычислить все n-битные пары ключей и, таким образом, позволяет увеличить уровень надежности при использовании более коротких ключей.

VPN, Диффи-Хеллман, эллиптические кривые, алгоритм, математические операции.

Одной из актуальных проблем беспроводных сетей в настоящее время является защита информации. Беспроводные сети представляют серьезную угрозу для пользователей, поскольку злоумышленники, подключенные к тем же сетям, могут использовать различные методы для отслеживания веб-трафика и даже захвата учетных записей на сайтах. В связи с чем широкое применение получили виртуальные частные сети (рис. 1), представляемые туннелями между двумя и более узлами в интернете, позволяющие им получать доступ друг к другу.

Рис. 1. Схема организации VPN

Взаимодействие между компьютерами базируется на следующей алгоритме:

1) установка соединения между VPN-узлами;

2) шифрование пакета с конфиденциальными данными;

3) помещение зашифрованных пакетов в поле данных незашифрованных пакетов;

4) достижение пакетов узла, где происходит извлечение и дешифрация зашифрованных пакетов.

Наибольший интерес алгоритма представляет этап установки соединения, включающая в себя идентификацию, аутентификацию и авторизацию. Преимущественно установка и шифрование соединение в VPN осуществляется по протоколу IPSec (*Internet Protocol Security*), осуществляемые по следующему алгоритму:

1) настройка одинаковой конфигурации VPN-узлов (протоколы шифрования и технологии обеспечения целостности);

2) идентификация узлов для достоверности отправки в нужном направлении;

3) принятие решение об используемых алгоритмах шифрования;

4) создание закрытого и общего ключей;

В рассматриваемом методе особое внимание уделяется созданию ключей, вычисляемых по алгоритму Диффа-Хеллмана (табл. 1) [1], где 1) генерация общего параметра; 2) создание открытого и закрытого ключа; 3) обмен открытым ключом и nonce-числом; 4) вычисление общего секретного ключа; 5) формирование ключа (заданного формата); 6) обмен данными.

ТАБЛИЦА 1. Алгоритм Диффа-Хеллмана для генерации закрытого и общего ключей

Этап	VPN-клиент (узел)	VPN-сервер (узел)
1	Общий параметр: g	
2	A = случайное число $a = g^A$	B = случайное число $b = g^B$
3	$\{a, nonce_a\} \rightarrow$ $\leftarrow \{b, nonce_b\}$	
4	$S = b^A = (g^B)^A$	$S = a^B = (g^A)^B$
5	$K = HKDF(S, nonce_a, nonce_b)$	$K = HKDF(S, nonce_a, nonce_b)$
6	$\leftarrow E(K, данные) \rightarrow$	

Отличительная черта вычисления ключей по данному алгоритму заключается в возведение чисел в степень, выбираемые браузером из подмножества простых числе. Применение обратного логарифмирования, например, алгоритма «общего метода решета числового поля» (*general number field sieve*, GNFS), позволяет заранее вычислить все n-битный пары ключей для заданных простых чисел [2].

Для решение данной проблемы я предлагаю применить алгоритм Диффа-Хеллмана на эллиптический кривых, основанный на особенностях математических операций над точками, расположенных на данной кривой. В рассматриваемом методе вычисление общего и закрытого ключей по протоколу Диффа-Хеллмана на эллиптических кривых реализуется по следующему алгоритму (табл. 2).

ТАБЛИЦА 2. Алгоритм Диффа-Хеллмана на эллиптических кривых для генерации общего ключа

Этап	VPN-клиент (узел)	VPN-сервер (узел)
1	Общая точка: G_{xy}	
2	A = *случайное число* $a_{xy} = A \times G_{xy}$	B = *случайное число* $b_{xy} = B \times G_{xy}$
3	$\{a_{xy}, nonce_a\} \rightarrow$ $\leftarrow \{b_{xy}, nonce_b\}$	
4	$K_{xy} = A \times b_{xy} = A \times B \times G_{xy}$	$K_{xy} = B \times a_{xy} = B \times A \times G_{xy}$
5	$K = HKDF(K_x, nonce_a, nonce_b)$	$K = HKDF(K_x, nonce_a, nonce_b)$
6	$\leftarrow E(K, данные) \rightarrow$	

В таблице наглядно представляется процесс создания закрытых ключей, осуществляемых путем умножения точки эллиптической кривой Gxy на случайно выбранное секретное целое число. Предлагаемый способ позволяет максимизировать количество возможных закрытых, а как следствие, и открытых ключей, основываясь на особенностях математических операций на эллиптической кривой.

Данная методика реализуется умножения точки G_{xy} на целое число A эквивалентное сумме A точек: $A \times G_{xy} = \sum_1^A Gxy$. Прибавление точки G_{xy} к самой себе геометрически эквивалентно построению касательной в этой точке и отражению точки ее пересечения с эллиптической кривой относительно оси X:

Рис. 2. Математическая операция «умножения» на эллиптической кривой

Метод, базируемый на математических операциях на эллиптических кривых, не позволяет заранее вычислить все n-битный пары ключей для заданных простых чисел, поскольку для вычисление закрытого ключа $A = a_{xy}/G_{xy}$ необходимо выполнить операцию деления над двумя точками

на эллиптической кривой, где можно производить только сложение и вычитание. Для решения предыдущего уравнения понадобится алгоритм, который эффективно выполняет деление, используя лишь сложение и вычитание. Однако ни один из известных в настоящее время классических алгоритмов на это не способен [3].

Таким образом, предлагаемый способ позволяет увеличить уровень надежности при использовании более коротких ключей, однако время вычисления увеличивается.

Список используемых источников

1. Пастухов Д., Пастухов Ю., Синица П. Шифрование данных на базе эллиптических кривых : учеб.-метод. пособие. Новополоцк : ПГУ. 2016. 72 с.

2. Кормишина В. Эллиптические кривые в криптографии: автореф // ПенГУ, 2017. С. 4–7.

3. Ярмолик В., Занкович А. Криптосистемы на основе эллиптических кривых // БГУИР, 2007. С. 4–6.

Статья представлена научным руководителем, заместитель начальника факультета по учебной и научной работе БГУИР, кандидатом технических наук, доцентом Л. Л. Утиным.

УДК 004.056
ГРНТИ 20.53.19

ПРИМЕНЕНИЕ СТЕГАНОГРАФИИ В РЕДАКТОРЕ ИГРОВЫХ УРОВНЕЙ

К. А. Ахрамеева, П. П. Бурдин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются возможности вложения информации в объекты игрового окружения с помощью редактора уровней Valve Hammer Editor. Описываются доступные в редакторе инструменты модифицирования игровых уровней и анализируется возможность их применения в контексте стеганографии. Приводятся практические примеры возможных реализаций вложения информации в игровой уровень.

стеганография, вложение информации, редактор уровней, компьютерные игры.

Для обеспечения защищенного обмена информацией зачастую важна не только невозможность ее прочтения посторонними, но и сокрытие самого

факта обмена информацией. Достигается это при помощи методов стеганографии, путем вложения дополнительной информации в не вызывающий подозрений покрывающий объект. В цифровой стеганографии покрывающими объектами выступают цифровые объекты, например, неподвижные изображения, видео, аудиосигналы, печатный текст [1]. Информацию всех перечисленных видов – визуальную, звуковую, текстовую – содержат в себе компьютерные игры, поэтому использование стеганографии в этом контексте вызывает интерес.

Произвести вложение дополнительной информации в компьютерные игры возможно различными способами, например, в игровые механики или повествовательные элементы игры [2], отталкиваясь от жанра [3], или же скрыть информацию в объектах игровых сохранений [4]. В частности, в качестве среды передачи скрываемого сообщения допустимо использование игрового уровня (карты).

Игровой уровень является частью файлов ресурсов игры или представляет собой отдельный файл. При этом в некоторых жанрах игр неотъемлемой частью является возможность редактирования игрового уровня, например, в жанре игр «песочница» (англ. “*sandbox*”) [3]. В других случаях реализовать такую возможность позволяет редактор уровней. Он может быть, как частью игры, так и отдельным программным обеспечением.

Возможности вложения информации с помощью редактора уровней зависят от конкретного такого инструмента. В качестве примера подходит редактор уровней Valve Hammer Editor, который был разработан компанией Valve и предназначен для игровых движков GoldSrc, Source и Source 2. Способы вложения информации обусловлены и самой игрой, для которой предназначаются редактированные уровни, поэтому разбор возможностей редактора целесообразно сделать на основе популярной игры Counter-Strike: Global Offensive.

Компания Valve разработала Steam – онлайн-сервис цифрового распространения компьютерных игр и программ [5]. С помощью него пользователь способен покупать игры, а также получить и сам редактор уровней. Сервисом предоставляется возможность распространения игровых уровней посредством системы внутреннего хранилища и внешних веб-страниц «Мастерская Steam» (англ. “*Steam Workshop*”) [6].

После установки редактора следует убедиться в его работоспособности путем создания тестовой карты – интерфейс редактора при ее создании продемонстрирован на рис. 1. Последующий просмотр созданного уровня в игре проиллюстрирован на рис. 2.

Valve Hammer Editor использует проприетарный формат файлов Valve Map Format, практически полностью документированный [7]. Такие файлы содержат исходный код игрового уровня, структура которого воспринимается человеком без нужды в реверс-инжиниринге.

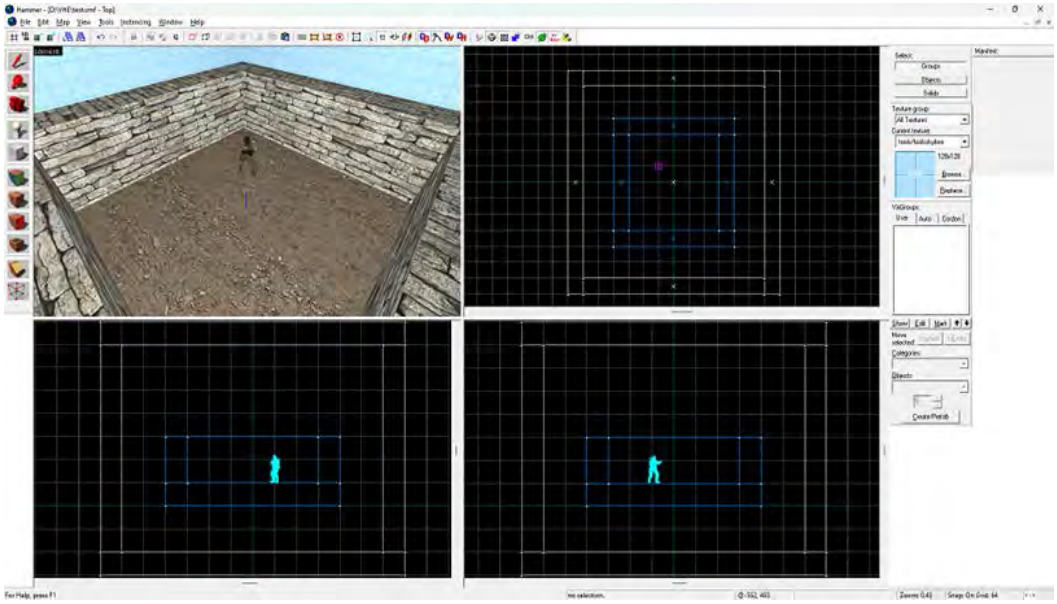


Рис. 1. Интерфейс Valve Hammer Editor при создании тестовой карты

Рис. 2. Вид тестовой карты в игре

Однако файлы данного формата, как и полагается файлам исходного кода, должны быть скомпилированы. В результате компиляции, которая выполняется с помощью редактора, создается конечный файл игровой карты с расширением bsp, который способен запускаться в игре. Но содержимое файла уже не может с легкостью восприниматься человеком.

В редакторе доступно множество инструментов для разработки игровых уровней [8]. Основными для решения этой задачи являются инструменты для создания и редактирования геометрических примитивов, инструменты для наложения текстур.

Так, дополнительное сообщение может содержаться в геометрической форме размещенных объектов или в их взаимном расположении. Еще одним фактором служат текстуры – вложенная информация интерпретируется, например, в зависимости от их цвета, яркости и других параметров, или помещается непосредственно на сами текстуры, например, в виде надписей. На рис. 3 представлен возможный вариант такого вложения.

Рис. 3. Вложение информации на основе ступенек

Перед игроком размещено шесть рядов ступенек, каждый из которых состоит из восьми ступенек в высоту. И присутствует два вида текстур, более светлая означает двоичную «1», а темная – двоичный «0». Самая верхняя ступень соответствует старшему двоичному разряду, а нижняя ступень – младшему. Просматривая каждый ряд ступенек таким образом слева направо, извлекается следующий набор двоичных данных: «01010011 01000101 01000011 01010010 01000101 01010100», что соответствует слову SECRET в кодировке ASCII.

Очевидно, что ряды ступенек могут располагаться в разных местах карты. При этом каждому отдельному символу не обязательно должны соответствовать именно ступеньки, как в этом примере, а допустимо использование различных комбинаций объектов игрового окружения.

На рис. 4 представлен еще один пример использования текстур для вложения информации, но уже с нанесением текста на них. На игровом уровне размещены 6 ящиков, на каждый из которых нанесены текстуры с названиями разных овощей. Если прочитать первую букву каждой такой надписи, следуя сверху вниз и слева направо, то они складываются в слово SECRET. Разумеется, способы вложения и извлечения информации в данном случае могут быть более изощренными.

Рис. 4. Вложение информации на основе надписей на коробках

Также следует учитывать возможности игрового движка, доступ к которым предоставляется редактором уровней. Например, движок предусматривает разрушаемость объектов. Так, очевидный способ заключается в расположении на игровой карте разрушаемой стены, за которой содержится дополнительная информация. Пример возможной реализации такого вложения проиллюстрирован на рис. 5.

Рис. 5. Вид карты до разрушения стены (сверху) и после ее разрушения (снизу)

Однако надежность такого метода не велика, ведь игрокам достаточно, например, включить режим прохода сквозь стены, вследствие чего раскроется вложенная информация, даже без знания игроком о необходимости разрушения стены для получения этой информации. В разных игровых движках и в разных играх могут присутствовать более удачные механики для вложения информации. Сервисы для распространения игровых уровней позволяют обмениваться картами с дополнительной информацией, по аналогии с тем, как хостинги изображений позволяют обмениваться изображениями со вложенной информацией.

Таким образом, редактор игровых уровней обладает потенциалом для разработки стеганографических систем. В дальнейшем предполагается как значительно усложнять и сочетать упомянутые методы вложения, так и разрабатывать другие способы погружения информации.

Список используемых источников

1. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки. Часть 1. Цифровая стеганография / Под общей редакцией профессора В. И. Коржика. СПб. : СПбГУТ, 2016. 226 с. ISBN 978-5-89160-125-3.

2. Ахрамеева К. А., Герлинг Е. Ю., Ковцур М. М., Куликов И. А. Использование стеганографии в компьютерных играх // Телекоммуникации. 2020. N 10. С. 22–26.

3. Ахрамеева К. А., Герлинг Е. Ю., Куликов И. А. Обзор жанров компьютерных игр для создания стеганографических систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 67–72.

4. Куликов И. А., Ахрамеева К. А. Обзор способов скрытия информации в файлах и объектах игровых сохранений с учетом содержимого с помощью стеганографии // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 10. С. 101–104.

5. Steam, The Ultimate Online Game Platform. URL: https://store.steampowered.com/about/ (дата обращения 19.01.2023).

6. Руководство по мастерской Steam (документация Steamworks). URL: https://partner.steamgames.com/doc/features/workshop/implementation?l=russian (дата обращения 19.01.2023).

7. Valve Map Format – Valve Developer Community. URL: https://developer.valvesoftware.com/wiki/Valve_Map_Format (дата обращения 20.01.2023).

8. Hammer Map Tools Toolbar – Valve Developer Community. URL: https://developer.valvesoftware.com/wiki/Hammer_Map_Tools_Toolbar (дата обращения 20.01.2023).

УДК 621.397
ГРНТИ 49.33.35

КОНТРОЛЬ ЦЕЛОСТНОСТИ ИЗОБРАЖЕНИЯ С ПОМОЩЬЮ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

К. А. Ахрамеева, Е. Ю. Герлинг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире все больше и больше информации передается по каналам связи, таким как сеть Интернет. Таким образом передаются, например, медицинские снимки, схемы, топографический карты. Для таких изображений актуальна проблема контроля целостности (неизменности) при передаче. Для решения этой проблемы в данной работе предлагается использовать цифровые водяные знаки.

цифровой водяной знак, точная аутентификация, целостность, алгоритм вложения.

В настоящее время по различным каналам связи, как по общедоступным, так и по частным, передается самая разнообразная информация. Для большей части информации допустимы некоторые искажения, но часть данных должна быть передана в неизменном виде. К таким данным можно отнести медицинские снимки, схемы, топографические карты. Не всегда можно гарантировать, что канал передачи данных не добавит ошибок и искажений в передаваемую информацию, но можно контролировать целостность после передачи данных по каналам связи.

В данной работе для контроля целостности данных предлагается использовать цифровые водяные знаки (далее ЦВЗ).

ЦВЗ позволяют погрузить дополнительную информацию в объект (в настоящей работе в качестве объекта используются изображения) таким образом, чтобы данную информацию нельзя было удалить из объекта. Главное свойство ЦВЗ – это неудаляемость погруженной информации без значительного ухудшения качества исходного объекта.

Также рассматривается контроль целостности передаваемого сообщения (аутентификация объекта), поскольку стоит задача обнаружить малейшие изменения данных злоумышленниками или от случайных искажений.

Перед передачей отправитель помещает ЦВЗ в передаваемое изображение. Контроль целостности проводится на принимающей стороне путем извлечения ЦВЗ из полученного изображения. Если ЦВЗ извлечено верно, значит само изображение передано без искажений (по крайней мере существенных), если ЦВЗ извлечь не удалось, то изображение содержит искажения, сделавшие его непригодным для дальнейшего использования.

Существует два типа аутентификации: точная и селективная [1].

При точной аутентификации искажение даже одного бита проверяемого файла приведет невозможности извлечения ЦВЗ.

При селективной аутентификации ЦВЗ может быть извлечено при незначительных искажениях изображения, но при сильных искажениях извлечение будет невозможным.

В данной работе рассматривается точная аутентификация.

Один из методов вложения и извлечения ЦВЗ в изображения формата Jpeg представлен на рис. 1 и рис. 2 [1].

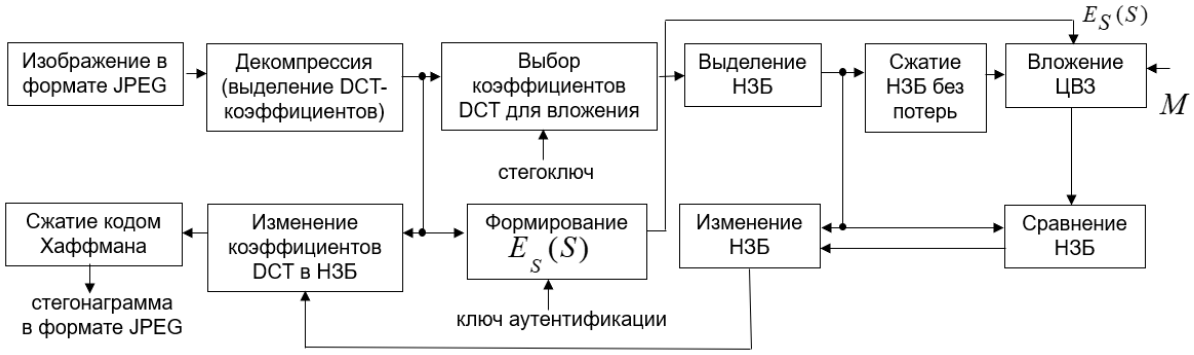


Рис. 1. Алгоритм вложения ЦВЗ

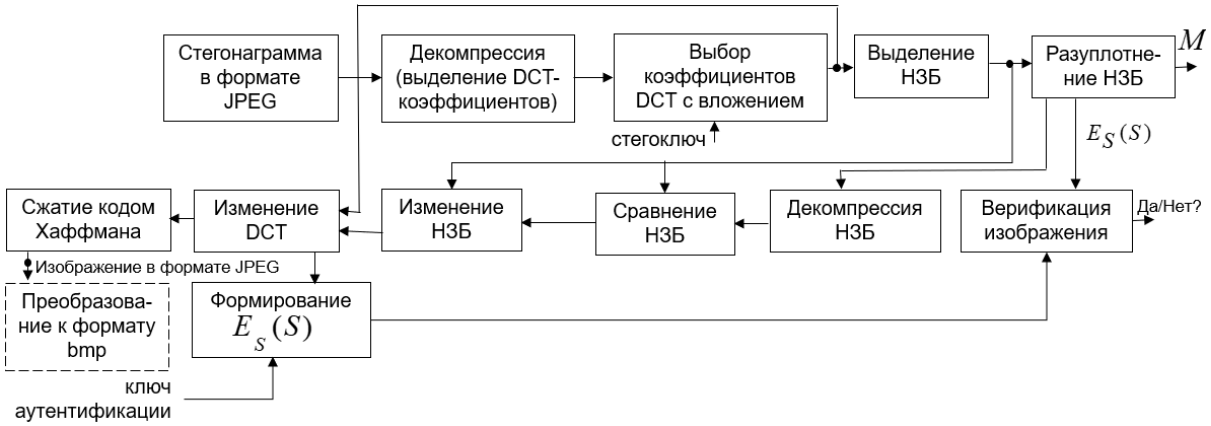


Рис. 2. Алгоритм извлечения ЦВЗ

Условные обозначения, применяемые на рис. 1 и рис. 2: DCT-коэффициенты – коэффициенты дискретно-косинусного преобразования, НЗБ – наименее значащие биты, M – сообщение, $E_s(S)$ – аутентификатор.

Проверим возможность использования ЦВЗ для контроля целостности передаваемых изображений. На рис. 3 представлен пример исходного изображения, которое используется в эксперименте.

Рис. 3. Исходное изображение

В исходное изображение производится вложение ЦВЗ, позволяющего произвести точную аутентификацию для контроля целостности. Результат вложения – изображения с ЦВЗ – показан на рис. 4.

Рис. 4. Изображение с ЦВЗ

Сравнивая рис. 3 и рис. 4 легко заметить, что найти отличия в изображениях невооруженным взглядом невозможно. При необходимости из изображения на рис. 4 можно извлечь вложенный ЦВЗ, что означает, что изображение не было повреждено. Сам рисунок после извлечения возвращается к исходному виду, как на рис. 3.

Изменим всего 1 пиксель в исследуемом изображении с ЦВЗ (см. рис. 5).

Рис. 5. Изображение с ЦВЗ с измененным пикселем

Сравнивая рис. 3 и 5 найти отличия между ними без дополнительной обработки невозможно. Ничто не указывает на то, что изображение на рис. 5 было повреждено. При этом, если извлечение ЦВЗ из изображения с рис. 5 невозможно, что указывает на отсутствие целостности изображения.

Из проведенного эксперимента видно, что использование ЦВЗ с точной аутентификации позволяет определять целостность изображения после передачи по каналам связи. Точная аутентификация позволяет убедиться в том, что изображение не подвергалось искажениям.

Список используемых источников

1. Коржик В. И., Красов А. В. Цифровая стеганография : учеб. пособие. М. : КноРус, 2023. 324 с. ISBN 978-5-406-10970-0.

2. Жувикин А. Г., Коржик В. И. Использование метода 3-битного квантования для алгоритма селективной аутентификации изображений, устойчивого к JPEG сжатию // Труды учебных заведений связи. 2016. Т. 2. N 1. С. 52–57.

3. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. N S7. С. 27–29.

4. Korzhik V., Zhuvikin A., and Morales-Luna G. Selective image authentication tolerant to JPEG compression // 6th International Conference on Information, Intelligence, Systems and Applications. 2015. PP. 06–08.

5. Lee M. H., Korzhik V. I., Morales-Luna G., Lusse S., Kurbatov E. Image authentication based on modular embedding // IEICE Transactions 89-D. 2006. N 4. PP. 1498–1506.

6. Zivic N. Robust Image Authentication in the Presence of Noise. Springer International Publishing, 2015. 187 p.

УДК 004.822
ГРНТИ 20.53.19

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ВЛОЖЕНИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯ ПРИ ПОМОЩИ GAN-СИСТЕМ

К. А. Ахрамеева, Г. В. Жиляков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей работе представлен результат анализа вложения текстовой информации в цветные изображения при помощи искусственного интеллекта, а также извлечение секретной информации из полученного изображения при помощи ИИ. В начале программа запрашивает путь, к цветному изображению, в которое необходимо поместить сообщение, затем текст сообщения. Программа, разработанная для вложения дополнительной информации, самостоятельно определяет пиксели для осуществления вложения, при обеспечении оптимальной защиты от атак, наилучшего качества стегообъекта, вложенной информации, а также приемлемого качества для извлечения вложенной информации. Используя несколько алгоритмов, по итогу, программа выдает готовое изображение с секретным сообщением. Для извлечения сообщения, необходимо указать только путь к изображению. Реализация данного метода вложения при помощи искусственного интеллекта повышает качество полученного изображения, повышает устойчивость полученных изображений к примитивным методам стегоанализа, и методам стегоанализа на основе ИИ.

генеративно-состязательные сети; стеганография; машинное обучение; GAN-системы.

Быстрое развитие сетевых технологий показывает, что сохранить сообщения в тайне не всегда удается за счет быстрого роста мощностей компьютеров. Иногда, проще скрыть сам факт существования сообщения в каком-либо другом объекте [1, 2, 3].

Стеганография на основе искусственного интеллекта (ИИ) – это направление стеганографии, которое использует алгоритмы ИИ для сокрытия информации в цифровых носителях. Идея заключается в использовании алгоритмов машинного обучения для создания новых стеганографических методов, которые являются более безопасными, гибкими и эффективными, чем традиционные стеганографические методы.

В данной работе представлена модель генеративно-состязательная сети для сокрытия произвольного битового вектора в обложке. Предлагаемая архитектура, показанная на рис. 1, состоит из трех модулей:

1. Кодировщик, который берет изображение обложки и тензор данных, или сообщение, и создает стеганографическое изображение.

2. Декодер, который берет стеганографическое изображение и пытается восстановить тензор данных.

3. Критик, который оценивает качество обложки и стеганографических изображений.

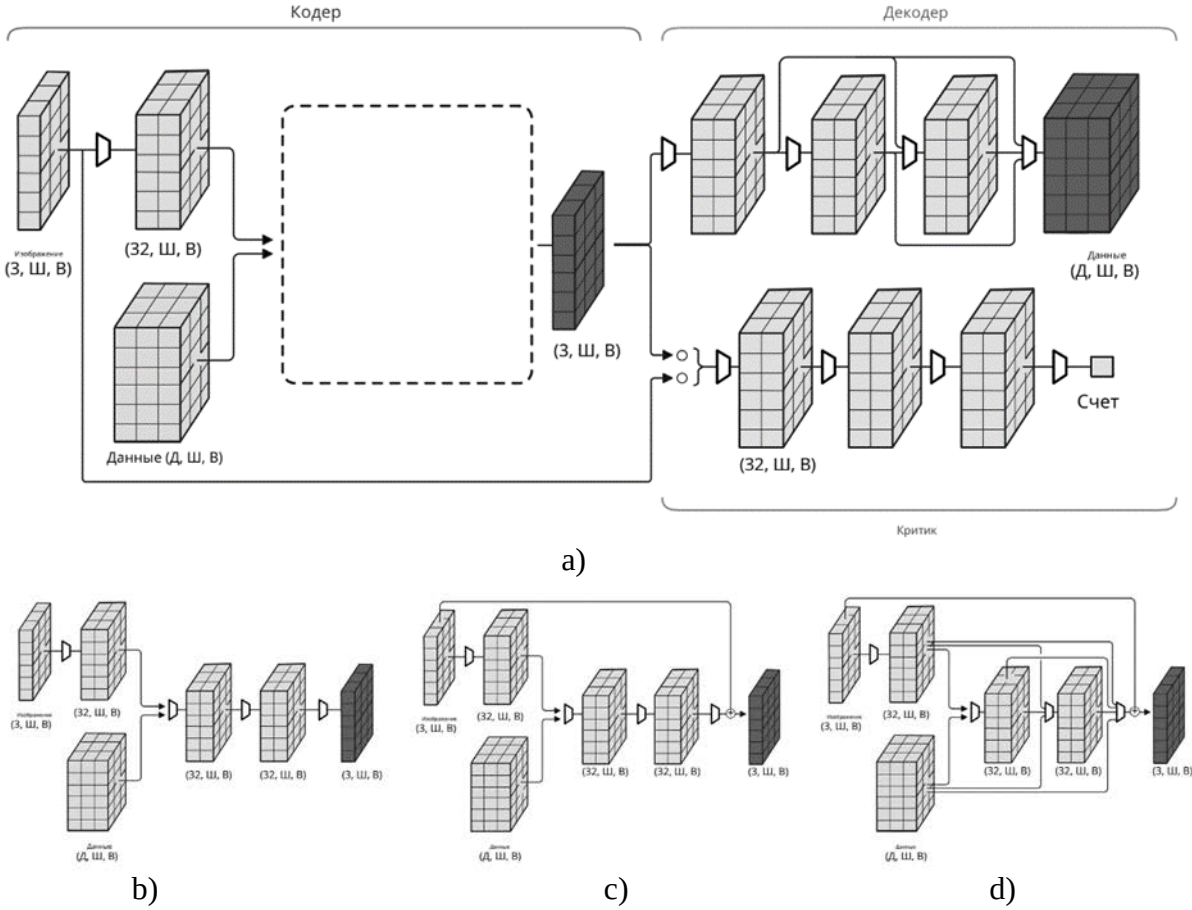


Рис. 3. Архитектура модели с кодировщиком, декодером и критиком. Пустой прямоугольник, представляющий кодировщик, может быть любым из следующих: (b) базовый кодировщик, (c) остаточный кодировщик и (d) плотный кодировщик. Трапеции представляют сверточные блоки, слияние двух или более стрелок представляет операции конкатенации, а фигурная скобка представляет операцию пакетной обработки

Кодер: Сеть кодера (encoder) берет изображение C и сообщение $M \in \{0,1\}^{D \times W \times H}$. Тогда как, M представляет собой бинарный тензор данных формы $D \times W \times H$, где D – количество битов, которые будут скрыты в каждом пикселе изображения обложки.

Ниже представлено три варианта архитектуры кодировщика с различными схемами подключения. Все варианты начинаются с применяя следующие две операции:

1. Обработка изображения C при помощи сверточного блока для получения тензора a получаемый следующим образом:

$$a = Conv_{3\to 32}(C).$$

2. Конкатенация сообщения M с тензором a, чтобы затем обработать результат свёрточным блоком для получения тензора b:

$$b = Conv_{32+D\to 32}\big(Cat(a, M)\big).$$

В итоге, последовательно применяя два сверточных блока к тензору b и генерируется стеганографическое изображение, как показано на рис. 2b. Описать это можно следующим образом:

$$E_b(C, M) = Conv_{32\to 3}\big(Conv_{32\to 32}(b)\big).$$

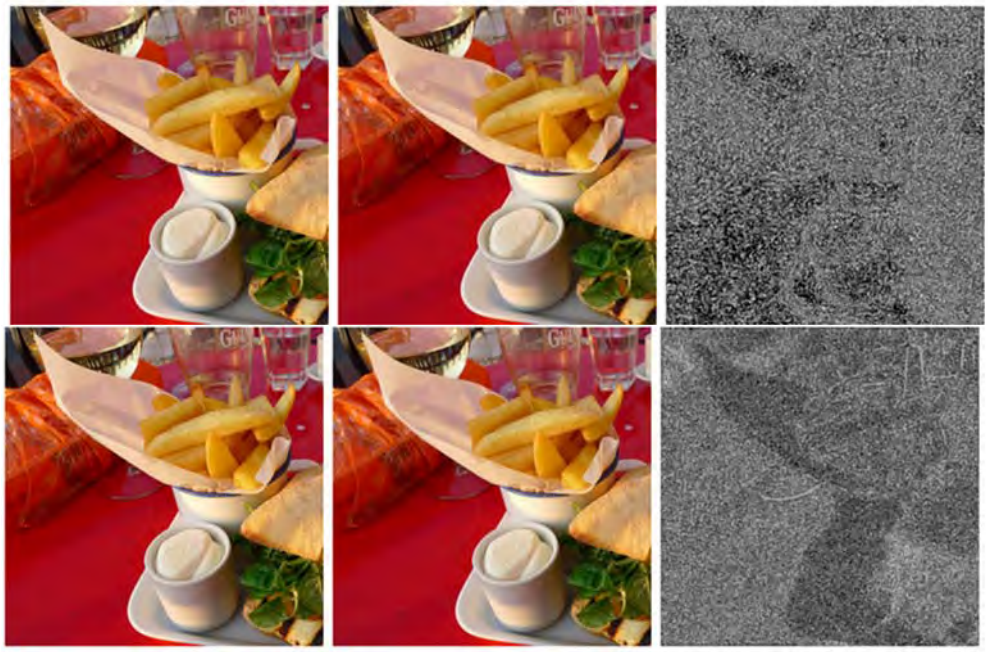


Рис. 2. Случайно выбранная пара обложки (слева) и стеганографического (справа) изображения и различия между ними. В верхней строке показан результат простого алгоритма стеганографии с наименьшими значащими битами (Джонсон и К. Катценбайссер, 1999 г.), а в нижней строке показан вывод из SteganoGAN с 4,4 бит\пиксель

Этот подход аналогичен тому, что был описан в работе [4], так как стеганографическое изображение – это просто результат последнего блока свертки.

В данной работе было показано, что использование остаточных связей улучшает стабильность и сходимость модели [5], поэтому предполагается, что его использование улучшит качество стеганографического изображения. С этой целью был модифицирован базовый кодировщик, добавив изображение C на свой выход, чтобы кодировщик научился создавать остаточное изображение, как показано на рис. 2b. Описать это можно следующим образом:

$$E_r(C, M) = C + E_b(C, M).$$

В данном варианте вводятся дополнительные соединения между сверточными блоками, чтобы карты признаков, сгенерированные более ранними блоками, были объединены с картами признаков, сгенерированными более поздними блоками, как показано на рис. 2d. Этот шаблон был разработан на основе работы DenseNet [6], которая, как было показано, поощряет повторное использование функций и смягчает проблему исчезающего градиента. Поэтому было установлено, что использование плотных соединений улучшит скорость встраивания.

$$\{c = Conv_{64+D\to 32}\left(Cat(a, b, M)\right) d =$$
$$= Conv_{96+D\to 3}\left(Cat(a, b, c, M)\right) E_d(C, M) = C + d$$

Наконец, результатом каждого варианта является стеганографическое изображение. $S = E_{(b,r,d)}(C, M)$ с тем же разрешением и глубиной, что и изображение *C*.

Декодер: сеть декодера принимает стеганографическое изображение *C,* производится кодировщиком. Формально, это можно выразить так:

$$\{a = Conv_{3\to 32}(S) b = Conv_{32\to 32}(a) c =$$
$$= Conv_{64\to 32}(Cat(a, b))\ D(S) = Conv_{96\to D}(Cat(a, b, c))$$

Декодер производит $M = D_d(S)$; другими словами, он пытается восстановить тензор данных *M*.

Критик: чтобы обеспечить обратную связь о производительности кодировщика и создать более реалистичные изображения, был введен состязательный критик. Критическая сеть состоит из трех сверточных блоков, за которыми следует сверточный слой с одним выходным каналом. Чтобы получить скалярную оценку, применяется адаптивный средний пул к выходу сверточного слоя.

$$\{a = Conv_{32\to 32}(Conv_{32\to 32}(Conv_{3\to 32}(S)))\ C(S) = Mean(Conv_{32\to 1}(a))$$

Использование разных наборов данных дают различные результаты. В таблице 1 (см. ниже), представленной ниже, продемонстрированы результаты обучения сети на данных Div2k и COCO.

Методы стеганографии на основе генеративно-состязательных сетей также обычно оцениваются по их способности избегать обнаружения инструментами стегоанализа. В этом разделе представлены эксперименты с двумя алгоритмами стеганографического анализа с открытым исходным кодом и способность модели генерировать необнаруживаемые стеганографические изображения.

ТАБЛИЦА 1. Относительные показатели полезной нагрузки и качества изображения для каждого набора данных и варианта модели. Вариант плотной модели обеспечивает наилучшую производительность по всем показателям почти во всех экспериментах

Dataset	D	Accuracy			RS-BPP			PSNR			SSIM		
		Basic	Resid.	Dense	Basic	Resid.	Dense	Basic	Resid.	Dense	Basic	Resid.	Dense
Div2K	1	0.95	0.99	1.00	0.91	0.99	0.99	24.52	41.68	41.60	0.70	0.96	0.95
	2	0.91	0.98	0.99	1.65	1.92	1.96	24.62	38.25	39.62	0.67	0.90	0.92
	3	0.82	0.92	0.94	1.92	2.52	2.63	25.03	36.67	36.52	0.69	0.85	0.85
	4	0.75	0.82	0.82	1.98	2.52	2.53	24.45	37.86	37.49	0.69	0.88	0.88
	5	0.69	0.74	0.75	1.86	2.39	2.50	24.90	39.45	38.65	0.70	0.90	0.90
	6	0.67	0.69	0.70	2.04	2.32	2.44	24.72	39.53	38.94	0.70	0.91	0.90
COCO	1	0.98	0.99	0.99	0.96	0.99	0.99	31.21	41.71	42.09	0.87	0.98	0.98
	2	0.97	0.99	0.99	1.88	1.97	1.97	32.56	39.00	39.08	0.86	0.96	0.95
	3	0.94	0.97	0.98	2.67	2.85	2.87	30.16	37.38	36.93	0.83	0.93	0.92
	4	0.87	0.95	0.95	2.99	3.60	3.61	31.12	36.98	36.94	0.83	0.92	0.92
	5	0.84	0.90	0.92	3.43	3.99	4.24	29.73	36.69	36.61	0.80	0.90	0.91
	6	0.78	0.84	0.87	3.34	4.07	4.40	31.42	36.75	36.33	0.84	0.89	0.88

В работе при оценке полученных моделей использовались методы статического анализа с открытым исходным кодом, а также методы с нейронным стегоанализом. За счет того, что модель обучается на своих же созданных моделях, она совершенствуется и демонстрирует гибкость и устойчивость ко всем моделям стегоанализа, которые использовались в работе.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Основы криптографии : учебное пособие. Санкт-Петербург, 2017. 312 с. ISBN 978-5-89160-097-3.

2. Герасимович А. С., Коржик В. И., Старостин В. С. Исследования бесключевой криптосистемы Дина-Голдсмита // Труды учебных заведений связи. 2017. Т. 3. N 3. С. 43–50.

3. Korzhik V. I., Starostin V. S., Kabardov M. M., Gerasimovich A. M., Yakovlev V. A., Zhuvikin A. G. Information theoretically secure key sharing protocol executing with noiseless public channels // Математические вопросы криптографии. 2021. Т. 12. N 3. С. 125–141.

4. Kawaguchi E., Maeta M., Noda H., and Nozaki K. A model of digital contents access control system using steganographic information hiding scheme // In Proc. of the 18th Conf. on Information Modelling and Knowledge Bases. 2007. PP. 50–61. ISBN 978-1-58603-710-9.

5. Holub V. and Fridrich J. Designing steganographic distortion using directional filters. 2012. 12. doi: 10.1109/ WIFS.2012.6412655.

6. Huang K. Q. Densely connected convolutional networks // IEEE Conf. on Computer Vision and Pattern Recognition (CVPR). 2017. PP. 2261–2269.

УДК 004.89
ГРНТИ 28.23.37

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА ГЕТЕРОГЕННОГО ТРАФИКА

В. Н. Бабич, К. Э. Есалов, А. И. Козлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Возможность с высокой точностью классифицировать трафик по типам – аудио, текст и так далее и принадлежности к социальной сети, например, Facebook, Telegram, YouTube, является важной характеристикой для работы технологии Deep Packet Inspection. В статье сравниваются различные способы классификации гетерогенного трафика – с помощью моделей машинного обучения и нейронных сетей.

анализ, трафик, классификация, машинное обучение, нейронные сети.

Введение

Анализ трафика с последующей его классификацией является важной задачей в связи с необходимостью распределения ресурсов сети для обеспечения надлежащего качества обслуживания всех типов трафика. Другими словами, для корректной работы различных приложений сеть должна знать о требованиях, на основе которых будет выделять необходимый ресурс.

Постоянно растущие требования к конфиденциальности пользователя и шифрованию данных создают основную проблему для анализа. Нельзя упускать также факт возросшего разнообразия трафика, заставляющего выделять все больше и больше отдельных классов со своими требованиями к сети.

1. *Выбор метода решения проблемы*

Для решения описанной проблемы был выбран статистический подход с опорой на модели искусственного интеллекта, который основывается на гипотезе о том, что у каждого приложения существуют свои статистические особенности, позволяющие произвести однозначную в большинстве случаев идентификацию [2].

Реализация выбранного решения предполагает сбор массива данных и его предобработку, выбор группы моделей искусственного интеллекта (ИИ) и обучение с последующим сравнением результатов.

2. Эксперимент

2.1 Массив данных (dataset)

Для подтверждения гипотезы были выбраны первоначальные классы, которые после обучения искусственным интеллектом должны однозначно выделяться из всего потока трафика. Были выбраны такие приложения, как:

- Youtube.
- Facebook.
- Telegram.

Следует учесть, что один из классов, мы разбили на подклассы в виде голосового трафика и текстового (трафика передачи данных), предполагая в будущем выделения подклассов у всех приложений при получении в первоначальном исследовании хороших результатов.

Собранные данных нуждались в обработке и фильтрации. Основываясь на данных о сетевых протоколах и исследований по схожей теме, из массива данных остались только полезные для обучения признаки и добавились новые, такие как разница между временем прихода соседних пакетов. Последним действием в настоящем пункте стала разметка массива.

2.2 *Обучение ИИ*

Машинное обучение (*Machine Learning*; ML) – это способ обучать компьютеры без программирования и явных инструкций, используя только шаблоны и логические выводы. Для анализа полученного трафика были использованы несколько моделей классификации машинного обучения: метод *k*-ближайших соседей (*KNeighborsClassifie*r) и «катбуст» (*CatBoostClassifier*).

В процессе эксперимента метод *k*-ближайших соседей показал лучший результат при количестве соседей, равном 5 (табл. 1, см. ниже в п. 3). Также в качестве метрики оценки модели использовалась минимальная квадратичная ошибка (*MeanSquaredError*; MSE), которая вычисляется по формуле:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \overline{y_i})^2.$$

Следующая модель работает на основе градиентного бустинга и называется CatBoost (от c*ategorical boosting*). Исходя из названия основным преимуществом выступает возможность работы с категориальными данными без необходимости использования one-hot кодирования или других методов предобработки. Концептуально модель является ансамблем деревьев решений, выстроенных последовательно. При этом каждое отдельное дерево решений показывает плохой результат, но их объединение позволяет сильно уменьшить ошибку. Наилучший результат занесен в таблицу 1 (см. ниже в п. 3).

Однако хорошие результаты моделей сохраняются только при работе с малым количеством классов, поэтому для возможности в будущем продолжать исследования, добавляя новые данные, необходимо обратиться к нейронным сетям, которые гораздо лучше справляются с узкими задачами мульти-классификации [3].

Нейронные сети представляют собой компьютерные системы, которые имитируют работу человеческого мозга. Они состоят из множества связанных между собой нейронов, каждый из которых выполняет простейшие операции с входными данными и передает результат следующему нейрону. Нейронные сети используются для решения задач классификации, анализа данных, распознавания образов, и многих других. Они обучаются на основе опыта и корректируют свои веса и соединения, чтобы достичь наилучшей производительности в конкретной задаче.

В данном случае нейронные сети были использованы для классификации гетерогенного трафика. Использовались две архитектуры нейронных сетей – полносвязный перцептрон и модель долгой краткосрочной памяти.

Полносвязный перцептрон – это один из видов искусственной нейронной сети, состоящий из входного и выходного слоя, полностью связанных скрытым. Каждый нейрон следующего слоя связан с каждым нейронами предыдущего, что позволяет моделировать сложные нелинейные зависимости между данными.

Для обучения модели используется метод обратного распространения ошибки. Его цель – вычислить частные производные $\partial C/\partial w$ и $\partial C/\partial b$ функции стоимости C для каждого веса w и смещения b сети. Как уже упоминалось, построенная архитектура вмещала в себя 3 слоя (входной, скрытый и выходной). Последний слой состоит из 4 нейронов, каждый из которых соответствует метке класса.

Для оценки работы модели использовалась ошибка для многоклассовой классификации categoricalcrossentropy. Она показывает вероятность принадлежности к классу (2).

$$f(s)_i = \frac{e^{s_i}}{\sum_j e^{s_j}},$$
$$CE\big(t; f(s)\big) = -\sum_i t_i \log(f(s)_i). \quad (1)$$

Помимо этого, использовалась метрика точность (*Accuracy*), которая показывает число верно угаданных меток с помощью матрицы ошибок (*Confusion matrix*).

В результате обучения нейронной сети получались следующие значения точности – 0,9849 и ошиб-ки – 0,1816. Для наглядности изменение ошибки с течением эпох представлено в виде графика (рис. 1).

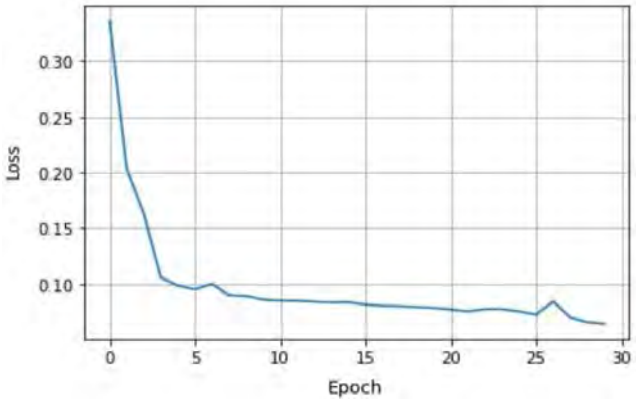


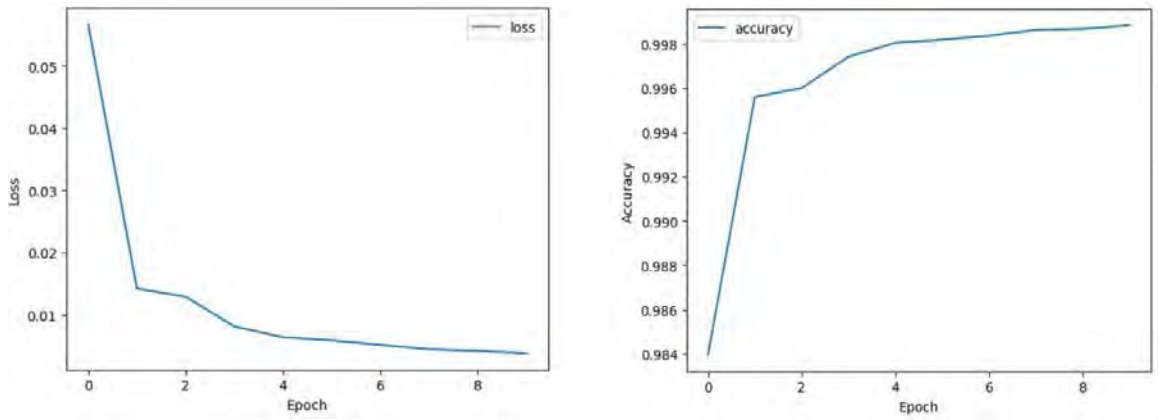
Рис. 1. График ошибки модели полносвязного перцептрона на протяжении 30 эпох обучения

Следующая модель нейронной сети – долгая краткосрочная память (LSTM). Долгая краткосрочная память (*Long short-term memory*; LSTM) – особая разновидность архитектуры рекуррентных нейронных сетей, способная к обучению долговременным зависимостям, то есть запоминанию информации на долгий период времени.

В этом случае структура имеет более сложное строение. В ней имеются несколько типов слоев:

- LSTM – осуществляет идею запоминания определенного количества ранее полученной информации;
- Dropout – уменьшает вероятность переобучения;
- Dense – реализует распределение весов в процессе обучения.

Оценка нейронной сети осуществлялась с аналогичными метриками: categoricalcrossentropy и accuracy. В результате значения ошибки – 0,0038 и точности – 0,9988. Зависимости этих величин от кол-ва эпох показаны на рис. 2.



а) б)

Рис. 2. График зависимости: а) ошибки; б) точности от количества эпох обучения модели LSTM

3. Результаты

Результаты работы наглядно изобразить в виде сводной таблицы.

ТАБЛИЦА 1. Результаты используемых в эксперименте моделей ИИ

Модели машинного обучения/Нейронные сети			
Название	Результат (accuracy)	Основной параметр	Значения
KNeighborsClassifier	0,9919	Количество соседей	5
CatBoostClassifier	0,9950	Скорость обучения	0,1
Perceptron	0,9849	Количество нейронов	44
		Количество слоев	3
LSTM	**0,9988**	Размер массива LSTM слоя	20 × 60

Вывод

Для задачи классификации 4-х видов приложений статистический подход на основе ИИ показал впечатляющие результаты. Исходя из этого можно сделать вывод о том, что расшифровка для идентификации часто необязательно, т. к. существуют косвенные статистические признаки поведения каждого приложения, позволяющие провести однозначную идентификацию.

Эта статья является первым этапом исследования методов анализа и классификации трафика. В дальнейшем предполагается взять гораздо больше приложений (потенциальных классов), а также проверить результативность работы ИИ при появлении различных видов VPN-трафика.

Список используемых источников

1. Christopher Olah. Understanding LSTM Networks [Электронный ресурс]. URL: http://colah.github.io/posts/2015-08-Understanding-LSTMs

2. Crotti M., Dusi M., Gringoli F., Salgarelli L. Traffic classification through simple statistical fingerprinting // ACM SIGCOMM Comput Commun Rev. 37 (1). 2007. PP. 5–16.

3. Tal Shapira, Yuval Shavitt. A Generic Representation for Encrypted Traffic Classification and Applications Identification // IEEE Transactions on Network and Service Management. 2021. PP. 1218–1232;

4. Michael A. Nielsen. Neural Network and Deep Learning. URL: http://neuralnetworksanddeeplearning.com/chap2.html

Статья представлена доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056
ГРНТИ 19.31

ИССЛЕДОВАНИЕ СПОСОБОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ SIEM-СИСТЕМЫ В КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ

И. Н. Бабков, З. А. Федорова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы выбора оптимального способа контроля состояния информационной безопасности для организаций на основе сравнения. Приводится обзор существующих мер по обеспечению информационной безопасности в условиях импортозамещения. Приведена карта отечественных и зарубежных решений SIEM-систем.

информационная безопасность, информационные системы, защита информации, SIEM-системы, DLP-системы, политика информационной безопасности.

В настоящее время количество кибератак на информационные ресурсы организаций продолжает стремительно расти. В целях поддержания их нормального функционирования необходимо осуществлять эффективный контроль и оперативное реагирование на возникающие события и инциденты информационной безопасности (ИБ) [1].

Основным документом организации является политика информационной безопасности (ПИБ), которая описывает технические и программные средства, используемые для обеспечения защиты информации (ЗИ), и регламентирует действия сотрудников по обеспечению безопасности.

Состояние ИБ в организации может контролироваться разными способами, как вручную, так и автоматизировано, через анализ журналов аудита, сбор данных из подсистем комплексной системы защиты информации (КСЗИ), системы предотвращения утечки данных (DLP-системы), системы управления информацией и событиями в безопасности (SIEM-системы) и др.

Вышеприведенные способы подробно рассматривались в статье «Сравнение способов контроля состояния информационной безопасности на предприятии» [2]. Сравнительный анализ показал, что наиболее приемлемым подходом для большинства организаций является внедрение SIEM-системы.

В отличие от других способов контроля SIEM-система способна в автоматизированном режиме осуществлять сбор данных из отдельных модулей КСЗИ (журналов операционных систем, систем управления базами данных, антивирусных средств, межсетевых экранов, систем обнаружения вторжений и др.), интегрироваться с ПИБ и является доступной для организаций с разным бюджетом.

Отличительной особенностью SIEM-системы является обеспечение управления событиями безопасности посредством осуществления функций сбора, анализа, обработки и хранения информации в режиме реального времени («до того, как ситуация станет критической») или за прошлые периоды, с целью выявления и расследования отклонений, а также проверки соответствия систем управления ИБ существующим нормам и требованиям, в том числе ПИБ организации [3]. Эффективность работы SIEM-системы в организации зависит от подключения достаточного количества источников событий, правильно настроенных правил корреляции и выстроенного процесса обработки, реагирования и устранения инцидентов ИБ [4].

Сегодня на рынке средств ЗИ представлен широкий ряд SIEM-систем, которые отличаются друг от друга функциональными возможностями и архитектурой: особенностями построения интерфейса, производительностью обработки событий ИБ и технологиями выявления зависимостей между ними, показателями состояния и др.

На текущий момент в большинстве организаций используются SIEM-системы зарубежного производства, поскольку на момент покупки и внедрения на рынке было мало российских решений, которые удовлетворяли бы требованиям пользователей. В результате изменения геополитической ситуации многие российские организации стали активно изучать возможности перехода на отечественное программное обеспечение (ПО), остро встал вопрос об импортозамещении. Этому способствует Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», устанавливающий запрет на использование с 1 января 2025 года средств защиты информации из недружественных стран [5].

Карта российского рынка ИБ в части SIEM-систем на конец 2022 года [6] представлена на рис. 1 (см. ниже).

Среди отечественных систем следует отметить SIEM-системы KOMRAD Enterprise SIEM, разработчиком которой является НПО «Эшелон» и MaxPatrol SIEM от Positive Technologies. Зарубежные системы представлены в России с ограничениями – приостановлена техподдержка, отсутствует возможность скачивать новые версии ПО или заблокирована работа оборудования и проходящий через него трафик.

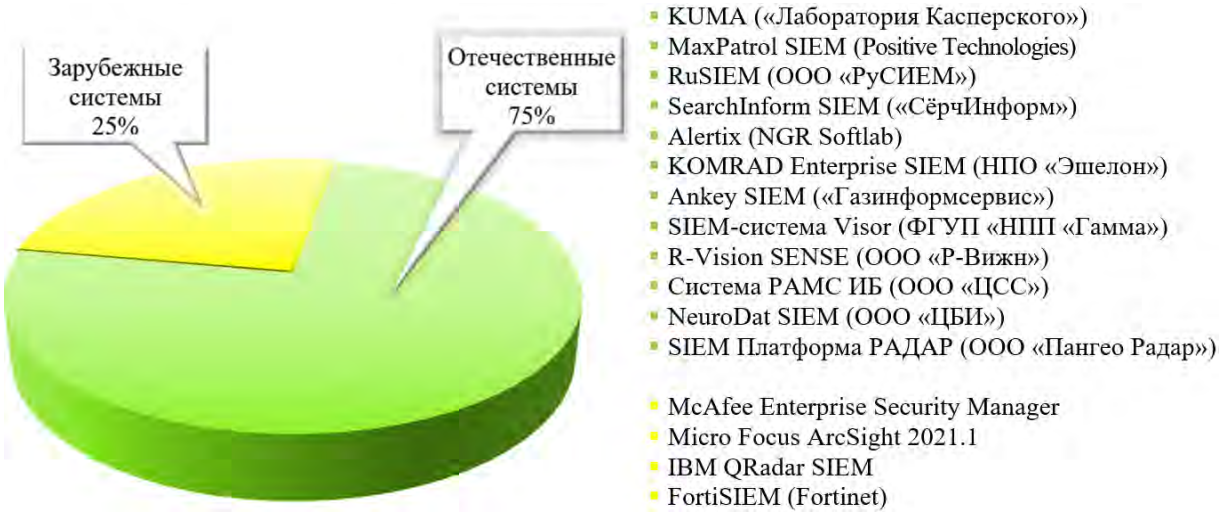


Рис. 1. Карта российского рынка ИБ в части SIEM-систем

При выборе SIEM-системы следует учитывать требования организации, ее политику информационной безопасности и ограничения, наложенные существующим законодательством, в особенности для организаций из сфер, относящихся к критической информационной инфраструктуре (КИИ) Российской Федерации. Чем критичнее система, тем в большей степени должны учитываться требования импортозамещения.

При выборе SIEM-системы важным инструментом является сравнение решений, основанное на методе экспертного анализа. Для повышения эффективности использования SIEM-системы в организации, необходимо:

Во-первых, прежде всего провести инвентаризацию комплексной системы защиты информации в организации и разработать техническое задание на внедрение SIEM-системы с учетом имеющейся информационной инфраструктуры.

Во-вторых, выбор SIEM-системы осуществлять в соответствии с принадлежностью организации к определенной сфере деятельности, принятой в организации политики информационной безопасности и имеющейся КСЗИ.

В-третьих, при внедрении, если возникла необходимость, провести модернизацию либо комплексной системы защиты информации, либо отдельных модулей в SIEM-системе.

Таким образом, основная цель – обеспечить, при всех ограничениях ПИБ, наиболее эффективный контроль состояния ИБ организации, во-многом зависит от эффективности функционирования SIEM-системы.

В случае правильного выбора и внедрения SIEM-системы, корректного интегрирования ее со всеми компонентами КСЗИ, организация может существенно повысить эффективность контроля информационной безопасности.

Список используемых источников

1. Бабков И. Н., Казаков Н. И., Карельский П. В., Миняев А. А. Определение показателей эффективности систем мониторинга и корреляции событий информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2022. Т. 1. С. 125–129.

2. Бабков И. Н., Федорова З. А. Сравнение способов контроля состояния информационной безопасности на предприятии // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей; материалы конф. СПб. : СПбГУТ, 2023. Т. 1. С. 433–437.

3. Кузнецова А. Д., Сахаров Д. В. Обзор состояния исследований информационной безопасности и применение SIEM-систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. Т. 1. С. 626–631.

4. Котенко И. В., Саенко И. Б., Захарченко Р. И., Величко Д. В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации // Журнал «Вопросы кибербезопасности» 2023. N 1. С. 13–27.

5. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/47796 (дата обращения 15.03.2023).

6. Спецпроект: SIEM. Сравнение решений класса SIEM // Журнал «Information Security / Информационная безопасность». 2022. N 4. С. 28–31.

УДК 621.396.4
ГРНТИ 50.37.03

СПЕЦИФИКА СОВРЕМЕННЫХ ТРЕБОВАНИЙ К НАДЕЖНОСТИ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ, РЕАЛИЗУЮЩИХ ОБЛАЧНЫЕ И ГРАНИЧНЫЕ ВЫЧИСЛЕНИЯ

В. А. Бабошин[1], С. Б. Ногин[2], В. А. Цыванюк[3]

[1]Военный институт (железнодорожных войск и военных сообщений) Военной академии материально-технического обеспечения им. генерала армии А. В. Хрулева

[2]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

[3]Научно-исследовательский центр связи ВУНЦ ВМФ «Военно-морская академия»

Рассмотрены и систематизированы специфические требования к надежности современных стационарных и мобильных центров обработки данных, реализующих облач-

ные и граничные вычисления. Данные требования затрагивают как общие аспекты технической готовности объектов такого класса, так и аспекты безотказности, ремонтопригодности и уровня технического обслуживания их программно-аппаратных средств. Выполнение рассмотренных требований позволит обеспечить безусловную надежность функционирования центров обработки данных, ориентированных на реализацию облачных и граничных вычислений.

надежность, центр обработки данных, облачные и граничные вычисления, требования, ремонтопригодность, техническое обслуживание.

Современные стационарные, мобильные и модульные центры обработки данных (ЦОД), как объекты IT-инфраструктуры крупных промышленных и хозяйствующих субъектов, а также, как важнейшие компоненты подсистемы управления киберфизическими системами, характеризуются структурной и функциональной сложностью, многогранностью их архитектур и нетривиальными условиями контроля их работоспособности, что предопределяет особые требования к их надежности [1, 2].

Особое значение требования к надежности объектов такого класса приобретают сейчас, когда в мире определились и приняты инженерным IT-сообществом некие функциональные границы, очерчивающие роль, место и архитектуру взаимосвязи стационарных, мобильных и модульных ЦОД в рамках больших георасределенных сетей центров обработки данных. Эти границы определяют для различных типов ЦОД – стационарных, мобильных или модульных, подходы к вычислению значений параметров надежности, характеризующих состояние их элементов и их функциональные возможности. Причем для различных типов ЦОД их функциональная сложность, а значит, и требуемая степень надежности, обусловлены различным уровнем пользователей и разнообразием реализуемых функций, таких как обработка, хранение и выдача по запросу информации в интересах должностных лиц органов и пунктов управления. Принято считать, что взаимосвязь различных типов ЦОД и соответствие их взаимных функций с точки зрения современных технологий вычислений и хранения данных, определяется в мировой практике понятиями «облачные», «туманные» и «граничные» вычисления [3, 4, 5].

Под, так называемыми, облачными вычислениями (*Cloud Computing*) принято понимать реализацию функций вычислений и хранения данных, традиционно осуществляемых крупными, зачастую главными корпоративными, либо центральными государственными стационарными ЦОД. Под, так называемыми, туманными вычислениями (*Fog Computing*), принято понимать процедуры хранения и обработки данных, осуществляемые на региональных стационарных ЦОД или в региональной локальной сети, подключенной к сети Интернет и состоящей из небольших региональных стационарных ЦОД и оконечных терминалов пользователей.

Однако наиболее актуальны в современных условиях мобильные (модульные, «чемоданные») масштабируемые ЦОД, предназначенные для, так называемых, граничных (периферийный) вычислений и хранения данных «рядом с пользователем» (*Edge Computing*). При реализации технологии Edge Computing добивались преимущества перед облачными и туманными вычислениями – осуществить «вынос» вычислительных мощностей и ресурсов хранения данных как можно ближе, вплотную к местам работы пользователей [3, 4, 5]. В наших исследованиях предпринята попытка проанализировать специфику современных требований к надежности ЦОД, реализующих именно облачные и граничные вычисления, т. е., особенности предъявляемых требований по надежности к стационарным и мобильным ЦОД. В этой связи будем ориентироваться на традиционный подход к формулировке понятия «надежность», как к собирательному свойству, количественно либо качественно характеризующему готовность ЦОД к работе и учитывающему влияние на данное свойство ЦОД различных эксплуатационных факторов, в частности: безотказности, ремонтопригодности и уровня технического обеспечения [6].

Предъявляемые требования по надежности стационарных и мобильных ЦОД, реализующих соответственно, облачные и граничные вычисления, могут быть интерпретированы и проиллюстрированы с различных точек зрения, в виде численных значений параметров и показателей, количественно, например: с точки зрения готовности ЦОД к работе могут быть определены требования: к процентному соотношению времени безотказной работы в течение всего срока эксплуатации стационарного или мобильного ЦОД, к интенсивности (частоте, количеству в единицу времени) аварий, сбоев, коллизий или к длительности интервала простоя в работе стационарного или мобильного ЦОД, что существенно влияет на оперативность и доступность результатов облачных и граничных вычислений для пользователей; с точки зрения безотказности могут быть рассмотрены и введены количественные требования, характеризующие среднее время между аппаратными авариями, отказами и программными сбоями или коллизиями, а также временные требования, задающие диапазон значений по продолжительности безотказной работы; с точки зрения ремонтопригодности элементов стационарного или мобильного ЦОД могут быть введены требования, описывающее допустимые пределы восстановления элементов ЦОД, а значит, и процедур облачных или граничных вычислений после аварий: требования к среднему времени до восстановления и требования, собственно, к времени восстановления; с точки зрения требований к техническому обеспечению могут быть установлены допустимые границы времени запаздывания материально-технического обеспечения или, например, оборотного времени поставки запчастей для ремонта и восстановления элементов стационарного или мобильного ЦОД [6, 7].

Некоторая специфика проявляется также в требованиях к общему уровню надежности объектов такого класса, когда, в интересах гарантированно бесперебойного обеспечения облачных или граничных вычислений, могут быть заранее определены допустимые границы для: объема и номенклатуры используемых программно-аппаратных средств облачных и граничных вычислений в составе элементов стационарного или мобильного ЦОД, уровня их надежности и их взаимосвязи и взаимозависимости в общей схеме обеспечения надежности комплекса программно-аппаратных средств ЦОД; степени мастерства (квалификации) штатных сотрудников стационарного или мобильного ЦОД, эффективности организации их работы, иногда говорят – задаются допустимые границы (требуемый уровень) надежности действий персонала ЦОД; регламента, механизмов, режимов, организационных форм и иных параметров технической эксплуатации стационарных или мобильных ЦОД, реализующих, соответственно, облачные или граничные вычисления; уровня целесообразности ранжирования и степени рациональности распределения задач, решаемых стационарными или мобильными ЦОД, между программно-аппаратными средствами облачных или граничных вычислений и штатными сотрудниками (персоналом) ЦОД; степени использования различных видов применяемых алгоритмов параллельных, последовательных или иных типовых (аналоговых, цифровых, словесных, реляционных, смысловых) облачных и граничных вычислений и различных способов резервного копирования данных, применяемых на стационарных или мобильных ЦОД.

Помимо этого, необходимо, чтобы выполнялся ряд специфических требований, ориентированных на облачные и граничные сервисы. Объективная необходимость обязательного выполнения этих требований обусловлена потребностью предусмотреть и нейтрализовать возможные проблемы в обеспечении надежности предоставления облачных и граничных сервисов привилегированным клиентам и пользователям из силовых структур (например, военным и специалистам оборонно-промышленного комплекса), поскольку: потеря информации в «облаке» – на стационарном ЦОД, или «на границе» – на мобильном ЦОД, означает фактическую невозможность ее восстановления; очень многое зависит от надежности оператора (хостинг-провайдера, предоставляющего облачные или граничные сервисы), надежностных характеристик его оборудования; важным отрицательным аспектом обеспечения надежности является возможная потеря контроля над ситуацией, например, когда потребитель воспользовался облачными или граничными сервисами внешнего провайдера, взаимодействующего с «нашими» корпоративными стационарными или мобильными ЦОД, вероятные аварии, сбои и отказы «перемещаются» из «нашего» ЦОД в центр обработки данных провайдера.

Именно поэтому для реализации надежного выполнения особо ответственных функций облачных и граничных вычислений на стационарных и мобильных ЦОД должны быть предусмотрены независимые, альтернативные (резервные) аппаратные и программные средства.

Таким образом, детально рассмотрены и систематизированы специфические требования к надежности современных стационарных и мобильных центров обработки данных, реализующих облачные и граничные вычисления. Данные требования затрагивают как общие аспекты технической готовности объектов такого класса, так и аспекты безотказности, ремонтопригодности и уровня технического обслуживания их программно-аппаратных средств. Выполнение рассмотренных требований позволит обеспечить безусловную надежность функционирования центров обработки данных, ориентированных на реализацию облачных и граничных вычислений.

Список используемых источников

1. Докучаев В. А., Кальфа А. А., Маклачкова В. В. Архитектура центров обработки данных / Под ред. профессора В. А. Докучаева. М. : Горячая линия-Телеком, 2020. 240 с.

2. Михайличенко А. В., Паращук И. Б. Архитектура системы проактивного контроля технической надежности мобильных центров обработки данных // I-methods. Т. 14, N 2. 2022. С. 1–15.

3. Дмитриев К. А. Discover the Edge: современные решения для задач будущего // ИнформКурьер-Связь. 2019. N 3. С. 58–59.

4. Хрисанфова Е. Ф. Облачные, туманные и граничные вычисления: отличия и перспективы развития технологи. (2019) [Электронный ресурс]. URL: https://rb.ru/story/edge-computing/ (дата обращения 08.12.2022).

5. Броницкий Т. Л., Вишневский К. О., Гохберг Л. М. и др. Развитие отдельных высокотехнологичных направлений. Белая книга. М.: Национальный исследовательский университет «Высшая школа экономики», 2022. 188 с.

6. Андреев А. В., Яковлев В. В., Короткая Т. Ю. Теоретические основы надежности технических систем : учебное пособие. СПб. : Изд-во Политехн. ун-та, 2018. 164 с.

7. Крюкова Е. С., Ткаченко В. В., Михайличенко А. В., Паращук И. Б. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. N 5. С. 86–95.

УДК 004.428.2
ГРНТИ 50.41.25

БЛОКЧЕЙН-ОРАКУЛЫ, КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ КОНВЕРТАЦИИ В КРОСС-ЧЕЙН ПРОЦЕССАХ

В. Н. Бакатов, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Активное развитие современных технологий, в частности, технологии блокчейн, приводит к развитию новых способов для интеграции систем между собой. Наиболее необходимым и популярным инструментом для обеспечения взаимодействия между различными блокчейн-сетями являются мосты или конверторы. Данные программные решения позволяют проводить процесс обмена токенов из одной блокчейн-сети на одноименные токены в другой без потери исходного количества. Этот механизм позволяет обеспечить не только равнозначность токенов в разных сетях, но и бесшовное взаимодействие систем. Дальнейшее развитие подобных решений позволяет проводить более сложные операции, чем перевод токенов из одной сети в другую. Однако, вопрос доверия в подобных программных решениях является критическим, поскольку они являются централизованными. В работе рассматривается возможность применения оракулов, как ключевого механизма, позволяющего обеспечить безопасность и доверие к системам обеспечения взаимодействия в рамках кросс-чейна.

блокчейн, оракул, TON, Ethereum, смарт-контракт, bridge.

Чаще всего блокчейн-сети спроектированы таким образом, что они являются изолированными системами со своим набором правил, консенсусами и ограничениями. Под этим подразумевается, что такие системы ограничены в нативных решениях в области взаимодействия с реальным миром и не могут самостоятельно запрашивать и получать информацию у различных внешних источников. В связи с этим разработчики децентрализованных приложений столкнулись с необходимостью получать внешние данные для корректной работы приложений и сервисов. Единственным решением для поставки подобной информации является внедрение оракулов.

Оракул – это программное обеспечение, являющееся связующим звеном между смарт-контрактами и внешним миром, которое поставляет данные в блокчейн-сеть. Стоит отметить, что сам по себе оракул не является источником данных, а одним из слоев, который запрашивает, проверяет и аутентифицирует все показания внешних источников, а затем ретрансли-

рует эту информацию. Передаваемые данные бывают разных видов, например: информация о ценах, успешное завершение платежа или температура, измеренная датчиком.

Оракулы можно классифицировать по параметру безопасности на централизованные и децентрализованные. Централизованным называется оракул, который контролируется одним физическим или юридическим лицом, а также является единственным источником данных для смарт-контрактов. Использование только одного источника является небезопасным, поскольку эффективность работы контракта полностью зависит от данного оракула, чьи данные могут быть скомпрометированы. Потеря доступа или вмешательство мошенника будет иметь прямое влияние на смарт-контракт и его работу.

Децентрализованный оракул, контролируемый несколькими физическими или юридическими лицами, может представлять из себя сеть централизованных оракулов, которая собирает данные от нескольких источников и повышает надежность полученной информации. Такие оракулы также можно назвать оракулами консенсуса, так как они не преследует цель отказаться от необходимости доверять кому-либо, а скорее распределяют это среди множества участников, а также используют данные, подтвержденные большинством из них.

Чаще всего оракулы используются в приложениях, которые позволяют перемещать цифровые активы из одного блокчейна в другой без потери стоимости. Такое решение можно использовать для повышения эффективности работы какого-либо программного обеспечения или удобства пользования.

В данной статье произведено исследование вопроса обеспечения безопасности на примере моста ETH-TON bridge [1]. Это мост позволяет децентрализованно с помощью сети оракулов передавать монеты TON между сетью TON и сетью Ethereum. В TON нативной валютой является TON Coin, а её аналогом в сети Ethereum – TONCOIN Token, основанный на стандарте ERC20. Этот сервис представляет из себя систему из следующих компонентов:

1) основной смарт-контракт моста в TON, которые создает переводы [2];

2) управляющий мостом смарт-контракт в TON, контролируемый оракулами через мультиподпись, то есть через подписание транзакций несколькими оракулами [3];

3) сборщика подписей в TON — смарт-контракт, в котором хранятся подписи, необходимые для создания TONCOIN в других сетях [4];

4) смарт-контракт моста в сети Ethereum [5];

5) оракул — программное обеспечение, обслуживающее мост. Каждый экземпляр хранит свои открытые/закрытые пары ключей для сетей TON и Ethereum.

6) Конфигурация сети TON, содержащая информацию, необходимую для работы моста – например, текущий список оракулов и размер их доли.

Чтобы стать оракулом необходимо вложить значительное количество монет TON (долю) в управляющий смарт-контракт, указав при этом публичные ключи Ed25569 (TON) и Secp256k1 (*Ethereum*). Пока оракул не включен в конфигурацию в сети TON, его данные не будут приниматься и обрабатываться. Управляющий смарт-контракт замораживает все переданные средства на начальный период, достаточный для включения нового оракула в конфигурацию TON. Изменить конфигурацию можно только в том случае, если за него проголосуют 3/4 валидаторов сети TON. Оракулы могут вывести свои доли только после того, как в конфигурационном файле TON будет назначен другой управляющий смарт-контракт (по согласованию с сетевыми валидаторами).

Набор оракулов, подтверждающих переводы, постоянно изменяется. Во время ротации валидаторы TON извлекают информацию об оракулах и выбирают желаемые. Они генерируют предложение для нового набора оракулов и голосуют за него. Смарт-контракт моста TON обнаруживает обновление конфигурации, затем запускает процесс сбора подписей для обновления набора оракулов на стороне моста Ethereum. Как только в контракте TON будет собрано достаточное количество (*Ethereum*) подписей для нового набора, один из новых оракулов должен вызвать определенный метод и предоставить собранный набор подписей; Таким образом, обновляется оракул, установленный на стороне моста Ethereum.

Если оракул подписывает неправильные параметры перевода (например, неправильное количество монет TON), вообще не подписывает их или не участвует в процедуре ротации оракулов, это считается мошенничеством. Поскольку весь процесс подписи оракулом происходит публично в блокчейне TON, мошенническая транзакция будет видна всем и является причиной штрафа оракула. Поскольку для выполнения перевода требуется подтверждение не менее 2/3 всех оракулов, такая транзакция не будет выполнена. Имея подтверждение мошенничества, оракулы будут штрафовать провинившегося оракула при выводе ставок из смарт-контракта управления.

При переводе из TON в Ethereum используется следующий алгоритм:

1) пользователь отправляет нативные монеты TON на смарт-контракт моста TON, указывая свой Ethereum-адрес, на который он хотел бы получить аналогичные токены;

2) контракт моста TON проверяет входящее сообщение и выдает специальную транзакцию, в которой содержится вся необходимая информация;

3) каждый оракул постоянно отслеживает такие транзакции и отправляет подписанные своим приватным ключом правильные параметры перевода (сумма, адрес назначения, метаданные) в контракт сборщика подписей (накапливать такие подписи на стороне TON экономически выгоднее);

4) как только 2/3 всех оракулов представили подпись, пользователь может получить подписанные данные и отправить их в смарт-контракт Ethereum;

5) смарт-контракт Ethereum проверяет подписи, извлекает подписанные параметры перевода, создает указанное количество токенов ERC-20 TONCOIN и отправляет их на указанный адрес пользователя.

При обратном переводе из Ethereum в TON используется следующий алгоритм:

1) пользователь отправляет сообщение на смарт-контракт моста в Ethereum, сжигая при этом свои токены ERC20 TONCOIN. В сообщении пользователь указывает количество токенов для сжигания и адрес в сети TON;

2) смарт-контракт моста Ethereum генерирует специальное событие с параметрами перевода: Ethereum-адрес отправителя, TON-адрес получателя и сумма до вычета комиссии;

3) каждый оракул постоянно отслеживает события, создает сообщения с корректными данными для перевода, подписывает своим приватным ключом, а затем отправляет их управляющему смарт-контракту в сети TON;

4) после сбора минимального количества подписей (2/3 всех оракулов) управляющий контракт отправляет транзакцию на основной смарт-контракт моста для перевода монет с вычетом комиссии на адрес пользователя в сети TON.

При пользовании данным мостом пользователь будет платить комиссию, которая состоит из двух частей: фиксированная комиссия, равная 5 нативным монетам TON, и пропорциональная комиссия, равная 0,25 % от суммы перевода. Взимаемая комиссия как за входящие, так и за исходящие переводы делится на две части: 2 монеты удерживаются основным смарт-контрактом для покрытия расходов на обработку транзакции, другие 3 монеты и 0,25 % от суммы перевода накапливаются в пуле комиссий оракулов. Этот пул распределяется между оракулами во время их ротации.

Таким образом, можно сделать вывод о том, что оракулы – полезный инструмент в работе со смарт-контрактами, который значительно расширяет их потенциал. Децентрализованные оракулы помогают решить проблему обеспечения безопасности, надежности и корректности данных при работе с внешними данными.

Список используемых источников

1. ETH-TON bridge TIPs. URL: https://github.com/ton-blockchain/TIPs/issues/24 (дата обращения 18.02.2023).

2. TON Bridge. URL: https://github.com/ton-blockchain/bridge-func (дата обращения 19.02.2023)

3. TON Bridge governing contract. URL: https://github.com/ton-blockchain/bridge-func/blob/master/func/multisig-code.fc (дата обращения 22.02.2023).

4. TON Bridge signature collector contract. URL: https://github.com/ton-blockchain/bridge-func/blob/master/func/votes-collector.fc (дата обращения 18.02.2023).
5. ETH Bridge. URL: https://github.com/ton-blockchain/bridge-solidity (дата обращения 18.02.2023)
6. Mainnet BSC-TON bridge launch. URL: https://github.com/ton-blockchain/TIPs/issues/37 (дата обращения 21.02.2023)

Статья представлена доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.056.53
ГРНТИ 81.93.29

ИЗУЧЕНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ОТ АТАКИ DNS-ФАРМИНГА

А. Ю. Х. Баракат, Р. Б. Петрив

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В этой статье мы поговорим о атаке фарминга DNS и о том, как защитить от нее наши машины. После проверки методов защиты мы определим основные задачи, которые будет выполнять разработанное приложение для защиты от атак фермы, затем я собираюсь для создания приложения Java, которое сможет обнаруживать любое отравление DNS на компьютерах с Windows, и это приложение также будет исправлять или удалять любые записи DNS, добавленные вредоносным источником.

DNS, Фарминг, Веб-сайты, IP-адреса, HTTP, HTTPS.

DNS-фарминг

DNS-фарминг [1] – это тип DNS-атаки, при котором пользователи автоматически перенаправляются на фальшивую версию веб-сайта, которая часто выглядит идентичной версии настоящего веб-сайта, с целью кражи личной информации, такой как учетные данные для входа в систему, адреса электронной почты и данные кредитной карты.

Этот тип атаки обычно происходит из-за компрометации отдельного локального устройства путем заражения файла их хостов или всей локальной сети путем изменения DNS-серверов на сервер, находящийся под контролем злоумышленника, на маршрутизаторе, используемом для подключения к Интернету (рис. 1).

Хотя обнаружение изменений в файле hosts может быть простым, часто вредоносные программы, которые скомпрометировали этот файл, также добавляют измененные записи на веб-сайты распространенных антивирусных программ, чтобы пользователям было трудно их удалить.

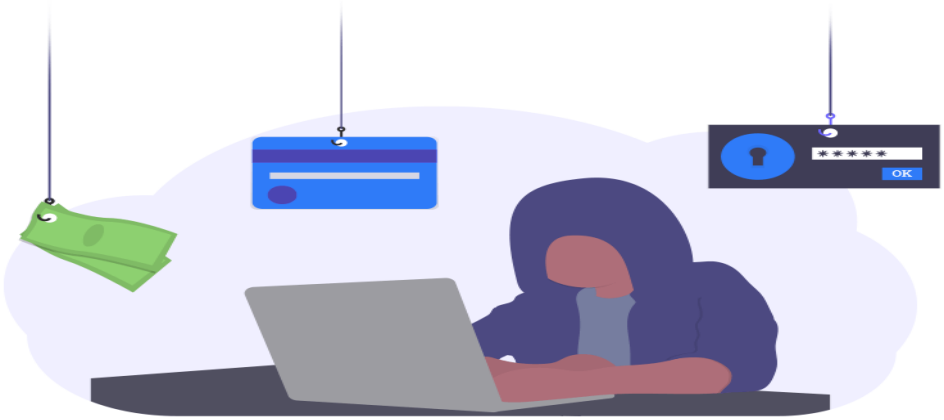


Рис. 1. Цели DNS-фарминга

Как защититься от фарминга [2]

– Выберите авторитетного интернет-провайдера (ISP). Хороший интернет-провайдер по умолчанию отфильтрует подозрительные перенаправления, гарантируя, что вы никогда не попадете на фарм-сайт.

– Используйте надежный DNS-сервер. Для большинства из нас наш DNS-сервер будет нашим интернет-провайдером. Однако можно переключиться на специализированную службу DNS, которая может обеспечить большую защиту от отравления DNS.

– Переходите только по ссылкам, начинающимся с HTTPS, а не только по HTTP. «s» означает «безопасный» и указывает, что сайт имеет действующий сертификат безопасности. Оказавшись на сайте, проверьте значок замка в адресной строке – еще один показатель того, что сайт защищен.

– Не нажимайте на ссылки и не открывайте вложения от неизвестных отправителей. Хотя вы не можете защитить себя от отравления DNS, вы можете позаботиться о том, чтобы избежать вредоносного программного обеспечения, которое делает возможным фарминг. Не нажимайте на ссылки и не открывайте вложения в любых электронных письмах или сообщениях, в которых вы не уверены.

– Проверьте URL-адреса на наличие опечаток. Фармеры иногда используют орфографические приемы, чтобы обмануть посетителей, заменяя или добавляя буквы в доменные имена. Внимательно посмотрите на URL-адрес, и, если вы заметите опечатку – избегайте ее.

– Вообще избегайте подозрительных веб-сайтов. Помимо URL-адреса, признаки, на которые следует обратить внимание, включают орфографические или грамматические ошибки, незнакомые шрифты или цвета и отсутствующий контент – например, некоторые фармеры не удосуживаются заполнить политику конфиденциальности или условия. Прежде чем отправлять какую-либо информацию, убедитесь, что все соответствует вашим ожиданиям.

– Избегайте сделок, которые кажутся слишком хорошими, чтобы быть правдой. Интернет-мошенники иногда заманивают жертв привлекательными предложениями – например, скидками намного ниже, чем у законных конкурентов. Если предложения кажутся неправдоподобными, проявите осторожность.

– Включите двухфакторную аутентификацию, где это возможно. Многие платформы предлагают двухфакторную аутентификацию, и, если она доступна, рекомендуется включить ее. Это затрудняет взлом ваших учетных записей – даже если мошенники получили ваши данные для входа в систему с помощью фарминга, они не смогут получить доступ к вашей учетной записи.

– Измените настройки вашего Wi-Fi роутера по умолчанию. Изменение стандартного пароля и использование вместо него надежного пароля для вашей частной сети поможет защитить вас от отравления DNS. Также важно поддерживать ваш маршрутизатор в актуальном состоянии. Если на вашем маршрутизаторе нет автоматических обновлений, подумайте о замене его на тот, который это делает.

– Используйте надежное решение для защиты от вредоносных программ и вирусов и регулярно обновляйте его. Например, Kaspersky Total Security защищает вас от хакеров, вирусов и вредоносных программ и работает круглосуточно и без выходных для защиты ваших устройств и данных.

Задачи для разрабатываемого специализированного приложения, которые защитят от фарм-атак

– Проанализировать данные в файле hosts (рис. 2) и убедиться, что записи IP-адресов достоверны и соответствуют легитимным ресурсам. Каждая запись должна быть проверена, и, если какая-либо из записей недействительна, со стороны приложения должно появиться предупреждающее сообщение, показывающее имя записи и уведомляющее пользователя о необходимости изменить учетные данные или заблокировать кредитную карту, которые были введены на этом веб-сайте, если для этого требуются учетные данные, затем запись будет удалена из файла hosts, наконец кэш DNS будет очищен.

– Проанализировать кеш DNS (рис. 3) в ОС и убедиться, что записи IP-адресов достоверны и соответствуют легитимным ресурсам. Должна быть

проверена каждая запись, и, если какая-либо из записей недействительна, должно появиться предупреждающее сообщение, показывающее имя записи и уведомляющее пользователя о необходимости изменить учетные данные или заблокировать кредитную карту, которые были введены на этом веб-сайте, если для этого требуются учетные данные, затем кэш DNS будет очищен.

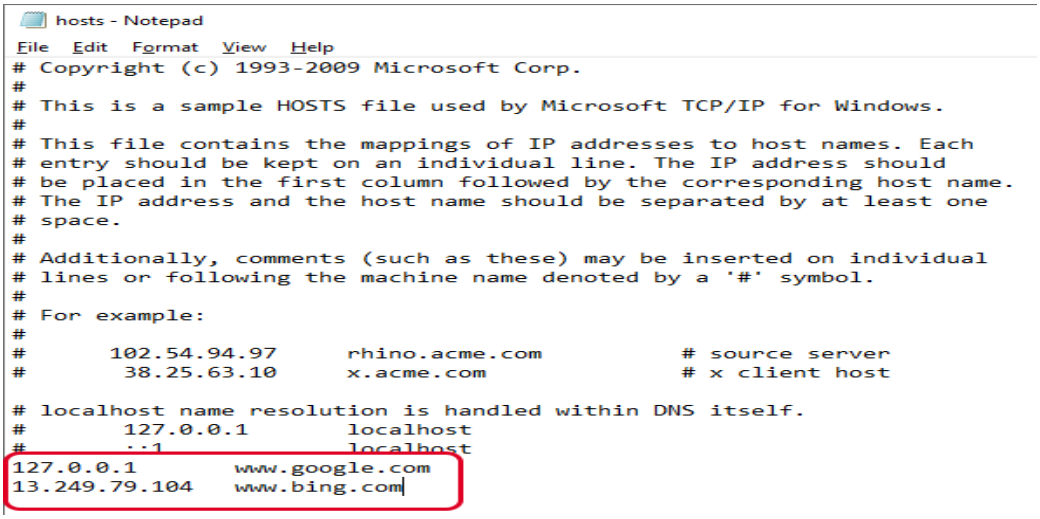


Рис. 2. Записи файла хоста

Рис. 3. Записи кеша ОС DNS

Приложение, которое мы разрабатываем для защиты от фарминга DNS, будет написано на платформе Java Standard Edition, приложение будет легким и будет работать локально на рабочих станциях Windows и серверах в домене, оно будет проверять файл hosts на устройствах домена и он проверит, что каждая запись действительна, и если это не так, она удалит эту

запись, а также проверит локальный кеш DNS и убедитесь, что каждая запись действительна, и если это не так, кеш DNS будет очищен, для все операции, выполняемые приложением, приложение будет отображать предупреждения, чтобы пользователи знали, что они использовали недействительный веб-сайт для выполнения дальнейших действий, а также будет создан журнал для критических операций, выполненных приложением.

Список используемых источников

1. Pharming. URL: https://www.whatsmydns.net/dns-security/dns-attacks/dns-pharming (дата обращения 28.04.2023).

2. What Is Pharming and How to Protect Yourself. URL: https://www.kaspersky.com/resource-center/definitions/pharming (дата обращения 03.05.2023).

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.391.883
ГРНТИ 49.01.81

ИЗМЕРЕНИЕ ПАРАМЕТРОВ ГОТОВНОСТИ ЦИФРОВЫХ КАНАЛОВ И ТРАКТОВ

К. А. Батенков[1], О. Н. Катков[2]

[1]МИРЭА – Российского технологического университета

[2]Академия Федеральной службы охраны Российской Федерации

Рассматриваются параметры качества цифровых каналов и трактов в форме времени готовности, получаемого путем сложения всех периодов готовности в интервале измерений, и времени неготовности – путем сложения всех периодов неготовности. Указываются, что элементы пути определяются географическими, а не архитектурными соображениями, и их границы не обязательно совпадают со скоростью передачи рассматриваемого сквозного пути.

сеть связи, телекоммуникационная сеть, показатель качества, цифровой тракт, сквозной путь.

Период неготовности T_u канала или тракта начинается десятью последовательными секундами с существенными ошибками SES (рис. 1) [1]. Эти десять секунд считаются частью интервала неготовности T_u. Новый период готовности T_a начинается десятью секундами без существенных ошибок (не SES). Эти десять секунд считаются частью интервала готовности T_a.

Рис. 1. Состояния готовности и неготовности однонаправленных каналов и трактов

Двунаправленный тракт находится в состоянии неготовности, если одно или оба направления находятся в состоянии неготовности (рис. 2).

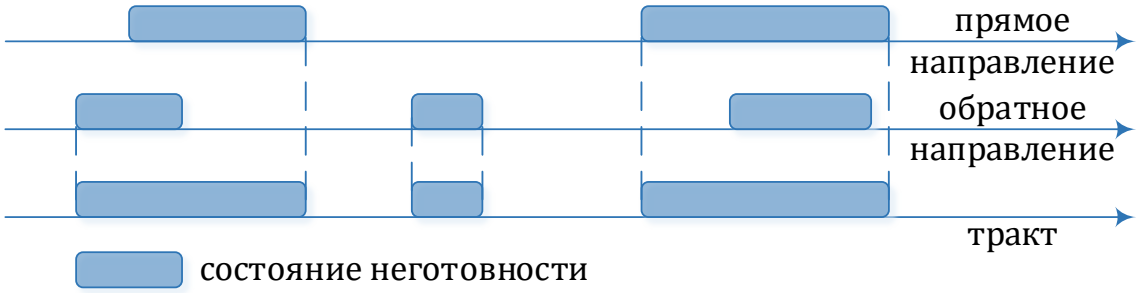


Рис. 2. Состояния готовности и неготовности двунаправленных каналов и трактов

Время готовности T_a получается путем сложения всех периодов готовности в интервале измерений, соответственно время неготовности – путем сложения всех периодов неготовности.

Коэффициент готовности (*AR – availability ratio*) – доля времени готовности канала T_a или тракта относительно всего периода измерений T [1]:

$$a = \frac{T_a}{T}.$$

Коэффициент неготовности (*UR – unavailability ratio*) – доля времени неготовности канала T_u или тракта относительно всего периода измерений T [1]:

$$u = \frac{T_u}{T}.$$

Существует естественное условие нормировки для данных коэффициентов и времен.

$$a + u = 1,$$

$$T_u + T_a = T.$$

Стандартным периодом измерений T считается интервал, соответствующий календарному году [1].

Сквозной путь (*end-to-end path*) – набор объектов, занимающихся переносом целостной информации между конечными точками пути. Сквозной путь состоит из комбинации элементов пути (*path element*).

Элемент пути (*PE – path element*) – часть сквозного пути, определяющий готовность всего пути. Элементы пути определяются географическими, а не архитектурными соображениями, и их границы не обязательно совпадают со скоростью передачи рассматриваемого сквозного пути. Например, сквозной путь со скоростью 2 Мбит/с может физически включать элементы со скоростью 140 Мбит/с на международных участках.

Классификационные признаки элементов пути (рис. 3):

– географическое расположение в сети;

– длина;

– уровень качества.

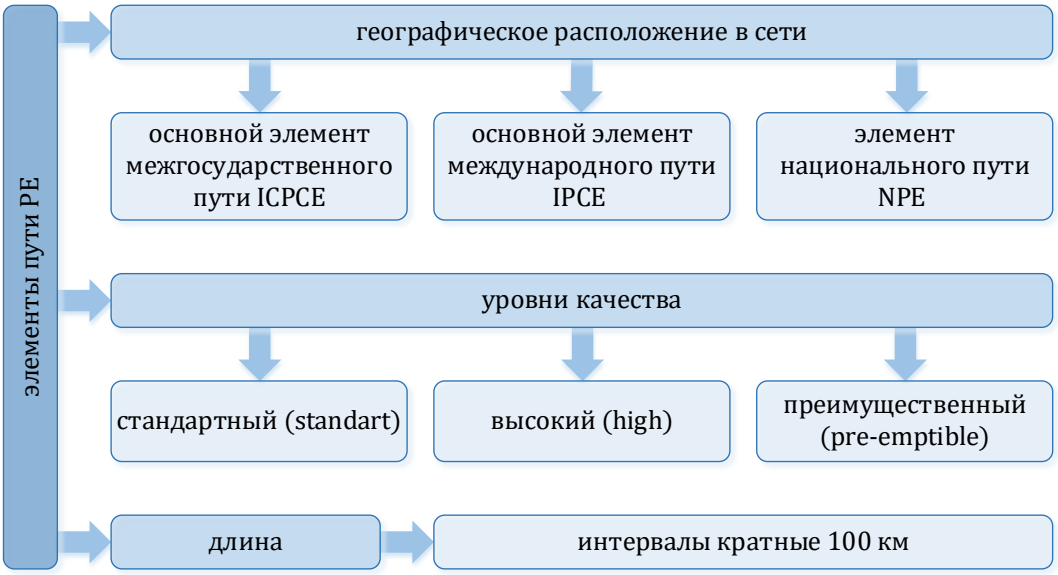


Рис. 3. Классификационные признаки элементов пути PE

Список используемых источников

1. Rec. G.827. Availability performance parameters and objectives for end-to-end international constant bit-rate digital paths. 2003–09. Geneva : ITU-T, 2003. 26 p.

2. Rec. G.826. End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections. 2002–12. Geneva : ITU-T, 2002. 34 p.

3. Rec. G.821. Error performance of an international digital connection operating at a bit rate below the primary rate and forming part of an Integrated Services Digital Network. 2002–12. Geneva : ITU-T, 2002. 18 p.

4. Нормы на электрические параметры линейных трактов магистральной и внутризоновых первичных сетей. II часть : Утв. М-вом связи РФ 08.01.1997. М. : МК-Полиграф, 1996. 168 с.

5. Rec. G.233. Recommendations concerning translating equipments. 1993. Geneva : ITU-T, 1993. 13 p.

6. Батенков К. А. К вопросу оценки надежности двухполюсных и многополюсных сетей связи // Успехи современной радиоэлектроники. 2017. С. 604.

7. Батенков К. А. Моделирование непрерывных каналов связи в форме операторов преобразования некоторых пространств // Труды СПИИРАН. 2014. N 1 (32). С. 171–198. https://doi.org/10.15622/sp.32.11.

8. Батенков А. А., Батенков К. А., Фокин А. Б. Формирование сечений телекоммуникационных сетей для анализа их устойчивости с различными мерами связности // Информатика и автоматизация. 2021. Т. 20. N 2. С. 371–406. https://doi.org/10.15622/ia.2021.20.2.5.

9. Батенков К. А. Анализ и синтез структур сетей связи методом перебора состояний // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2022. Т. 18. N 3. С. 300–315. https://doi.org/10.21638/11701/spbu10.2022.301.

10. Батенков А. А., Батенков К. А., Фокин А. Б. Анализ вероятности связности телекоммуникационной сети на основе инверсий ее состояний // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2022. N 59. С. 91–98. https://doi.org/10.17223/19988605/59/10.

УДК 004.49
ГРНТИ 50.41.27

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ БЭКДОРОВ, ОСНОВАННЫХ НА ПАССИВНОМ МОНИТОРИНГЕ КАНАЛОВ ДОСТУПА

Е. А. Батин, А. И. Катасонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире наши устройства всё чаще подвергаются атакам злоумышленников. Одним из средств, которыми пользуются хакеры является бэкдор. Бэкдор – вредоносная компьютерная программа, которая предоставляет злоумышленнику несанкционированный доступ к заражённому устройству путём использования уязвимости в системе безопасности. В данном исследовании рассматривается задача выявления класса бэкдоров, обеспечивающих интерактивный доступ на нестандартных портах, путем пассивного мониторинга канала доступа.

вирусы, бэкдоры, информационная безопасность, обнаружение вирусов.

Бэкдор – это механизм, который злоумышленник скрытно пускает в компьютерную систему для облегчения несанкционированного доступа к ней. Хотя бэкдоры могут быть установлены для доступа к различным службам, особый интерес для сетевой безопасности представляют те, кото-

рые обеспечивают интерактивный доступ. Они часто устанавливаются злоумышленниками, которые скомпрометировали систему, чтобы облегчить их последующее возвращение в систему.

Бэкдоры очень опасны в руках злоумышленников, потому что с их помощью человек, незаконно проникший в систему, получит доступ к системным настройкам, личным данным, паролям и, ко всему этому, сможет тайно запускать немалое множество вредоносного ПО, совершать различные атаки, контролировать интернет-трафик и множество других правонарушающих действий.

Бэкдоры могут быть административными и вредоносными. Административные бэкдоры – это те, которые разработчики программного обеспечения сами намеренно оставляют в программе, чтобы, в случае какого-нибудь программного сбоя или системной ошибки, они смогли быстро добраться до ядра программного кода и быстро решить проблему. Такие бэкдоры известны только разработчикам, но умелый хакер может незаметно использовать их в своих целях.

Вредоносные бэкдоры – это бэкдоры, которые устанавливаются в систему непосредственно самим преступником в своих целях и для злых умыслов при помощи вредоносных программ. В большинстве случаев, такие бэкдоры специально создаются для получения полного контроля над системой или сетью жертвы.

При совершении бэкдорных атак часто пользуются различными типами вредоносных программ [1, 2], такими как:

1. Программа вымогатель. С помощью них злоумышленник получает доступ к системе и содержащимися в ней файлам. Обычно, за возврат данных и доступа к ним, злоумышленники просят огромный выкуп;

2. Различное шпионское ПО. Через шпионское ПО злоумышленник получает конфиденциальную информацию и личные данные в тайне от владельца;

3. Троянские кони. Благодаря ним злоумышленники получают возможность администрирования целевой системы;

4. DoS-атаки. Они перегружают системы, серверы и сети мусорным трафиком, из-за чего пользователь не может получить к ним доступ;

5. Атаки с использованием криптоджекинга. Данные атаки нужны для добычи криптовалюты с помощью ресурсов жертвы.

Общая статистика атак показана на рис. 1.

С точки зрения мониторинга сети, бэкдоры часто запускаются по таким протоколам, как Telnet, Rlogin или SSH. Примером не интерактивного бэкдора может быть неавторизованный SMTP-сервер, например, для облегчения пересылки спама по электронной почте. А чем-то средним может быть

бэкдор FTP, используемый для предоставления доступа к незаконному контенту, такому как пиратское программное обеспечение, или же сервер Napster, запущенный с нарушением о политике сайта.

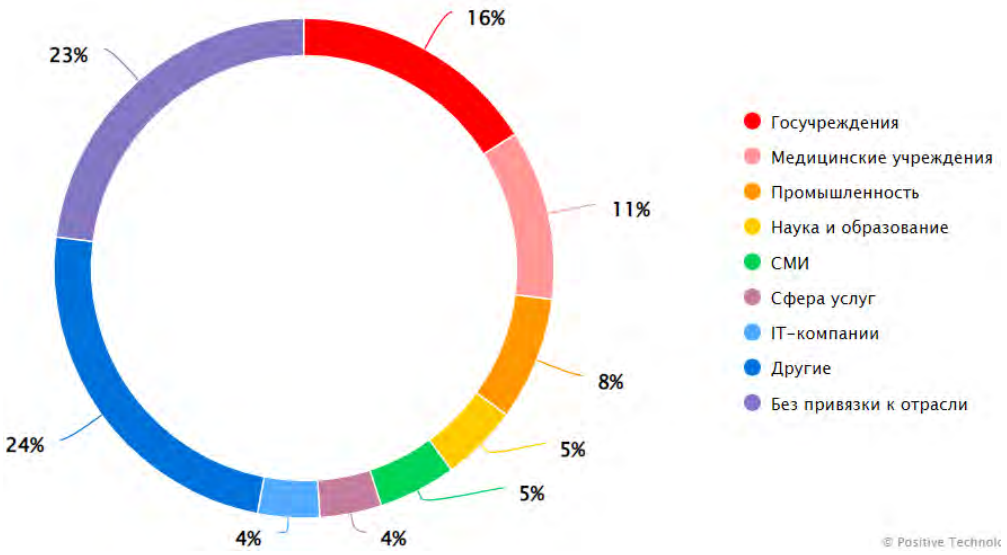


Рис. 1. Статистика бэкдорных атак за 2022 год

Бэкдоры, как таковые, достаточно сложно обнаружить. Обычно их присутствие скрывают путём запуска сервера для стандартной службы, к примеру, Telnet, на незаметном порту или же порту, связанном с другой службой.

Основной принцип обнаружения бэкдора заключается в нахождении отличительных черт, указывающих на подозрительную активность. Поскольку интерактивный трафик имеет характеристики, сильно отличающиеся от характеристик большинства машинного трафика (меньшие размеры пакетов, более длительные периоды простоя), можно эффективно обнаруживать подобный трафик.

Обнаружение несанкционированного доступа [3] становится намного сложнее, когда злоумышленник работает вместе с бэкдором и активно пытается избежать обнаружения всевозможными способами, например, неоднозначностью в потоке трафика. Однако, если вдруг злоумышленник уже заполучил доступ как удалённому, так и локальному хосту, то обнаружить бэкдор будет практически невозможно, так как злоумышленник сможет пользоваться большим количеством ухищрений, к примеру, различные скрытые каналы.

Преимущество пассивного мониторинга заключается в том, что он не нарушает работу сети. С другой стороны, активный мониторинг может усилить обнаружение, подключаясь к подозрительным бэкдорам, чтобы проверить сервер и определить его службу. Но это может дать злоумышленнику понять, что его вредоносный бэкдор обнаружили.

Обнаружение бэкдоров [4] может включать в себя:

Использование направленности соединения. При поиске нажатий клавиш мы должны учитывать только трафик, отправленный инициатором соединения. Однако, если монитор не видит установления соединения, то есть соединение является частичным, значит нет никакого способа определить, кто является фактическим инициатором. В таком случае мы должны учитывать оба потока. Если же мы отслеживаем канал доступа и заинтересованы только в обнаружении бэкдоров внутри локальной сети, то можно дополнительно использовать направленность соединения и игнорировать все исходящие потоки, даже если соединение является частичным;

Использование характеристик длины пакета. Пакеты нажатий клавиш часто очень маленькими, даже если они отправляются в линейном режиме, так как большинство команд – короткие. Исходя из этого можно исключить те соединения, в которых недостаточно маленьких пакетов и разработать метрику для измерения частоты небольших пакетов в соединении, чтобы определить, следует ли исключать то или иное соединение.

Алгоритмы обнаружения специального назначения:

SSH – защищенная оболочка шифрует передаваемый контент с помощью надежной криптографии. Она все чаще используется как для интерактивной, так и для массовой передачи трафика. Хотя в целом его внедрение представляет собой значительный шаг вперед в области интернет-безопасности, оно создает значительные трудности для обнаружения вторжений на основе контента именно потому, что делает монитор слепым к особенностям каждого подключения. Таким образом, он особенно привлекателен для использования бэкдором. Оптимальный алгоритм: ssh-sig, ssh-len. Эффективный алгоритм: ssh-sig-filter

Telnet. Протокол Telnet включает в себя довольно общий механизм согласования вариантов. Поскольку большинство сеансов Telnet начинаются с серии согласований опций, мы можем попытаться обнаружить их. Оптимальный алгоритм: telnet-sig. Эффективный алгоритм: telnet-sig-filter.

FTP – это протокол запроса/ответа, в котором запросы отправляются в виде отдельных, обычно коротких, строк ASCII-текста, а ответы имеют аналогичную структуру, но могут быть более длинными и многострочными. Некоторые FTP-запросы отправляются в ответ на активность пользователя и имеют интерактивную синхронизацию. Другие генерируются механически FTP-клиентом и поступают на близком расстоянии друг от друга. Оптимальный алгоритм: ftp-sig. Эффективный алгоритм: ftp-sig-filter.

Napster – это распределенная система, с помощью которой пользователи могут обмениваться копиями музыки, оцифрованной в формате MP3. Пользователи запускают клиент, который подключается к серверам napster.com, для публикации MP3-файлов, которые пользователь сделал общедоступными, и для поиска конкретных MP3-файлов, доступных в других

местах распределенной базы данных. Сервер перенаправляет клиента к другим клиентам, у которых доступен нужный MP3, и затем клиент устанавливает прямое соединение с источником MP3, минуя сервер на этом этапе. Обнаружение трафика Napster во многом аналогично обнаружению других бэкдоров, хотя в этом случае трафик отражает не нарушение безопасности доступа, а скорее нарушение политики. Оптимальный алгоритм: napster-sig. Эффективный алгоритм: napster-sig-filter.

Gnutella – это система, схожая по духу с Napster. Его отличительной особенностью является то, что он полностью с открытым исходным кодом, его можно использовать для обмена произвольными файлами, а не только MP3, а также у него нет централизованного компонента – клиентам Gnutella просто нужно знать имя другого клиента и они могут взаимодействовать с распределительной сетью. Следовательно, контролировать Gnutella будет сложнее для сайтов, чем Napster. Оптимальный алгоритм: gnutella-sig. Эффективный алгоритм: gnutella-sig-filter.

Проблема обнаружения бэкдоров в потоке законного сетевого трафика поначалу кажется сложной и долго реализуемой. Но поскольку интерактивный трафик имеет характеристики, сильно отличающиеся от большинства машинно-управляемых трафиков (меньшие размеры пакетов, более длительные периоды простоя), возможен эффективный поиск такого трафика. В данной статье были рассмотрены основные бэкдоры, рассмотрены их характерные особенности, а также признаки, по которым их можно обнаружить и избежать в дальнейшем.

Список используемых источников

1. Сикорски М., Хониг Э. Вскрытие покажет! Практический анализ вредоносного ПО. СПб. : Питер. 2018. 768 с.

2. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm-Телекоммуникации и Транспорт. 2018. Т. 12. N 10. С. 36–40.

3. Штеренберг С. И., Максудова Р. Р., Нефедов В. В. Анализ алгоритма работы компьютерных вирусов троянцев-вымогателей и Slingshot // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2020. N 1. С. 43–46.

4. Цветков А. Ю. анализ существующих методов атак типа переполнения буфера на операционные системы семейства microsoft // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 751–756.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004
ГРНТИ 50.41.25

СОЗДАНИЕ КОНВЕЙЕРА С АВТОМАТИЧЕСКОЙ ПРОВЕРКОЙ НА УЯЗВИМОСТИ ВЕБ-ПРИЛОЖЕНИЙ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ РЕПОЗИТОРИЯМИ ПРОГРАММНОГО КОДА GITLAB

А. В. Башмаков, П. А. Огорельцев, М. А. Скорых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа посвящена разработке решения для автоматизации проверки на уязвимости приложения. В рамках данной работы предлагается автоматизированное решение, разработанное на базе инструмента жизненного цикла DevOps GitLab, целью которого является минимизация риска возникновения уязвимостей в приложении. В работе рассматриваются особенности создания конвейера с автоматическим тестом на уязвимость, с использованием платформы для реализации жизненного цикла GitLab, а также инструмента статического анализа кода semgrep. Приведены особенности создания теста, написан шаблон для поиска сигнатуры уязвимости, создано тестовое уязвимое веб приложение, показан функционал конвейера.

уязвимости веб-приложений, GitLab, semgrep, автоматизация.

GitLab – это платформа совместной разработки проектов, включающая в себе версионное хранилище кода, инструменты для автоматической сборки, тестирования и запуска проектов, позволяющее также включать методики аудита безопасности приложений. Данная платформа имеет все необходимые инструменты для реализации DevOps практик [1].

DevOps – методология автоматизации технологических процессов разработки программного обеспечения, созданная для увеличения эффективности и скорости этих процессов. Цикл разработки обычно начинается с планировки приложения или обновления, написания кода, сборки, тестирования, выпуска, развертывания и мониторинга приложения. Также в данный цикл часто включаются практики безопасности на разных этапах. Одной из DevOps практик является CI/CD – комбинация непрерывной интеграции и непрерывного развертывания программного обеспечения. В данной статье рассматривается проверка безопасности на стадии тестирования приложения с помощью инструмента semgrep [2].

Semgrep – это утилита статического анализа программного кода с открытым исходным кодом, поддерживающая 12 языков программирования и имеющее множество уже написанных сообществом правил поиска уязвимостей [3].

Конвейер предполагает следующую последовательность действий (рис. 1):

1. Разработчики делают изменения и загружают их в версионное хранилище кода, делая запрос на слияние отсоединенной ветки в основную. Полагается, что проверку слияния производят только на работоспособность.

2. После слияния запускается автоматический тест на уязвимости, для которого было написано semgrep правило и подключен локальный тестировочный агент-сервер. По окончанию теста отмечается в каких строках кода была найдена уязвимость, либо выводится сообщение об успешном завершении теста.

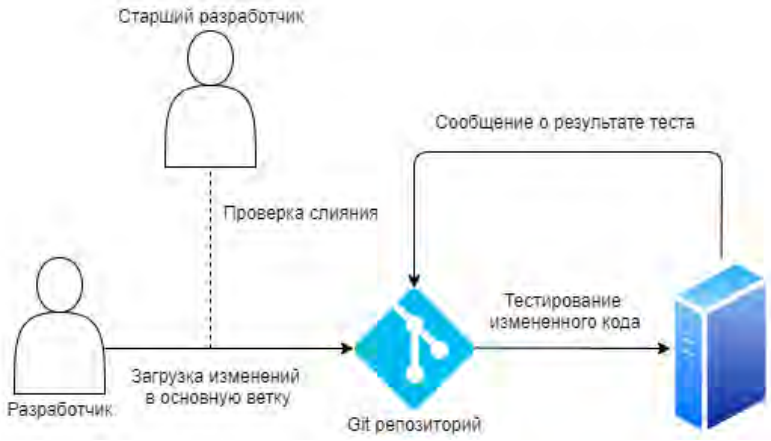


Рис. 1. Краткая схема созданного конвейера

В качестве тестового приложения была создана страница регистрации и аутентификации с умышленно оставленной уязвимостью SQL инъекции, которую в последующем необходимо будет автоматически обнаружить. Основной причиной возникновения SQL инъекций является попадание не обработанных пользовательских данных в SQL запрос. Подобные данные могут динамически изменять SQL запрос. Данная атака может привести к следующим негативным последствиям:

1. Нарушение конфиденциальности – уязвимость может привести к несанкционированному доступу к сведениям, хранящимся в базе данных SQL.

2. Обход системы аутентификации – если для проверки имен пользователей и паролей используются неверные SQL-команды, появляется возможность подключиться к системе с именем другого пользователя.

3. Обход системы авторизации – если информация об авторизации хранится в базе данных, может появиться возможность изменить эти данные путем успешной эксплуатации SQL инъекции.

4. Нарушение целостности – с помощью эксплуатации данной уязвимости можно внести изменения или удалить сведения, хранящимся в базе данных SQL.

Необходимо отметить, что по итогам исследования OWASP различные рода инъекции находились на третьем месте из десяти по популярности среди веб-приложений [4].

После написания тестового приложения был создан GitLab репозиторий с .gitlab-ci.yml файлом, в котором описывается CI/CD конфигурация. В нём можно прописать ряд стадий, в каждой из которых запустить несколько шагов. К примеру, в стадии сборки приложение будет собираться, а в стадии тестирования, при успешной сборке, приложение проверяется на работоспособность. В нашем случае (рис. 2) производится только статический анализ кода, потому стадия сборки не требуется.

```
semgrep:
  image: returntocorp/semgrep
  script: semgrep ci
  rules:
  - changes:
      - .gitlab-ci.yml
  - if: $CI_PIPELINE_SOURCE == "web"
  - if: $CI_COMMIT_BRANCH == $CI_DEFAULT_BRANCH
  variables:
    SEMGREP_RULES: >-
      s/p5nN
```

Рис. 2. CI/CD конфигурация

Основным пунктом конфигурации является SEMGREP_RULES, в которой указывается адрес написанного правила (рис. 3) на сайте semgrep.

```
rules:
  - id: sql-injection
    languages:
      - php
    severity: ERROR
    message: User data flows into this manually-constructed SQL string.
    mode: taint
    pattern-sanitizers:
      - pattern-either:
          - pattern: mysqli_real_escape_string(...)
          - pattern: real_escape_string(...)
          - pattern: $MYSQLI->real_escape_string(...)
    pattern-sources:
      - patterns:
          - pattern-either:
              - pattern: $_GET
              - pattern: $_POST
              - pattern: $_COOKIE
              - pattern: $_REQUEST
    pattern-sinks:
      - pattern-either:
          - patterns:
              - pattern: |
                  sprintf($SQLSTR, ...)
              - metavariable-regex:
                  metavariable: $SQLSTR
                  regex: .*\b(?i)(select|delete|insert|create|update|alter|drop)\b.*
          - patterns:
              - pattern: |
                  "...{$EXPR}..."
              - pattern-regex: |
                  .*\b(?i)(select|delete|insert|create|update|alter|drop)\b.*
```

Рис. 3. Правило для статического анализа

В данном правиле описываются определенные шаблоны, которые semgrep ищет в коде приложения.

После написания конфигурации CI/CD и правила semgrep конвейер уже будет работать и их можно запустить из интерфейса GitLab, но тесты будут запускаться на выделенных серверах GitLab. В данной работе был подключен локальный Ubuntu сервер с установленной на нем утилитой semgrep, а также необходимым бинарным файлом для подключения к самой платформе GitLab. После подключения сервера ему необходимо присвоить теги, а также отключить возможность использования общих агентов, при необходимости (рис. 4).

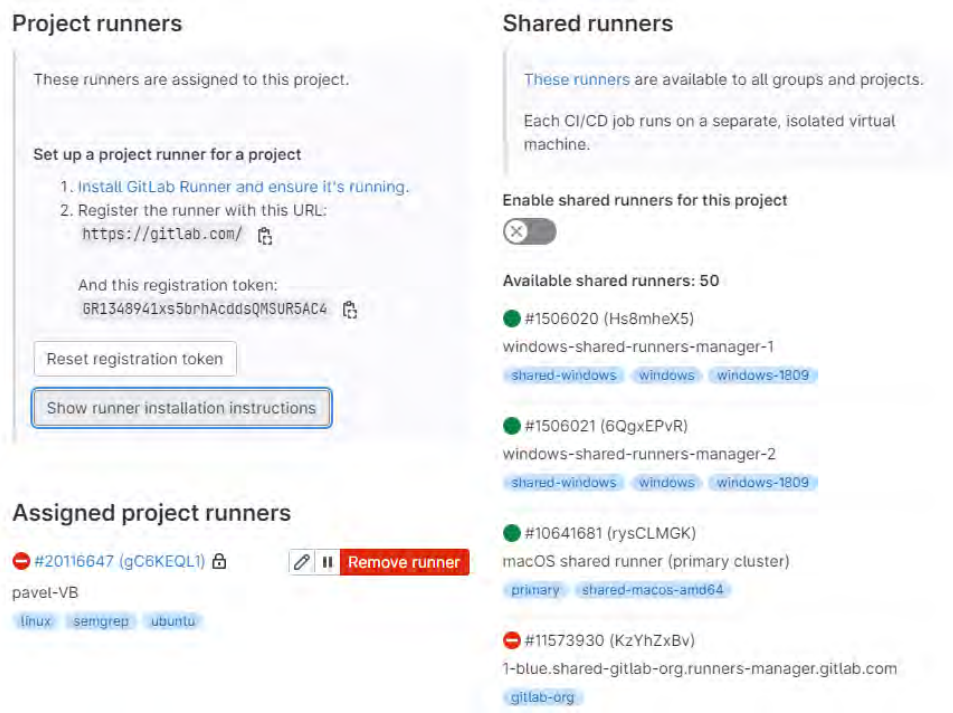


Рис. 4. Меню агентов

В рамках проведенной работы был настроен конвейер с автоматическим тестом на SQL инъекцию на базе платформы GitLab с использованием утилиты статического анализа semgrep.

Список используемых источников

1. The DevSecOps Platform | GitLab. 2023. URL: https://about.gitlab.com/ (дата обращения 01.02.2023)

2. Offerman T., Blinde R., Stettina Ch. J., Visser J. A Study of Adoption and Effects of DevOps Practices 2022. URL: https://www.researchgate.net/ publication/365486977_A_ Study_of_ Adoption_ and_Effects_of_DevOps_Practices (дата обращения 02.02.2023)

3. Semgrep repository. 2023. URL: https://github.com/returntocorp/semgrep (дата обращения 01.02.2023)

4. Johny J. H., W. Nordin A. F. B., Lahapi N. M., Leau Yu Beng. SQL Injection Prevention in Web Application: A Review // Advances in Cyber Security. 2021. PP. 568–585. URL: https://www.researchgate.net/publication/356737343 SQL Injection Prevention in Web Application A Review

УДК 004.77
ГРНТИ 49.37.29

РАЗРАБОТКА АППАРАТНОГО ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ОБРАБОТКИ ДАННЫХ СЕНСОРНОЙ СЕТИ

Л. С. Беккель, М. Э. Максименко, С. Г. Некрасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящей работе рассматривается возможность построения масштабируемой системы умный дом. Система состоит из сенсорной сети, программного комплекса для управления сетью и предоставления программный интерфейс для работы с ней и приложения, которое предоставляет данные и позволяет управлять датчиками конечному пользователю. Задача, поставленная в данной работе – создание законченной системы умный дом для домашнего использования, с возможностью последующего расширения и использованием недорогого аппаратного обеспечения. Для решения поставленной задачи разработаны прототипы датчиков на аппаратной платформе Arduino, а также программный комплекс для обработки и представления информации с датчиков.

интернет вещей, умный дом, архитектура, система интернета вещей, разработка.

Интернет вещей – это концепция, позволяющая физическим вещам, которые подключены к сети Интернет, соединяться друг с другом без участия человека (рис. 1). Цель концепции – измерение, сбор и анализ данных для лучшего обслуживания пользователей и улучшения качества продуктов. Входящая в это понятие концепция «умный дом», предполагает автоматизацию домашнего быта с помощью объединения электроприборов и бытовой техники в единую экосистему [1]. При проектировании такого решения вещей необходимо учесть четыре важнейших компонента: датчики, шлюз подключения, платформу(хаб) и приложение [2].

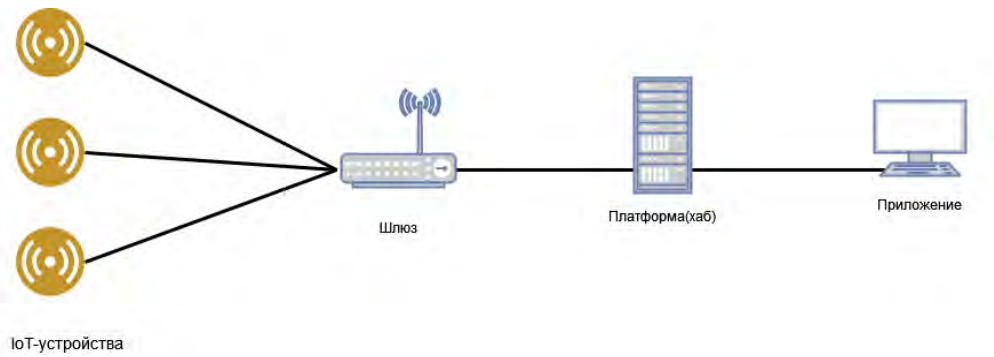


Рис. 1. Архитектура IoT системы

В качестве основы для датчиков была выбрана аппаратная платформа Arduino, на базе процессора ATmega328. В системе используется два типа датчиков: датчик влажности и температуры на базе сенсора DHT11 и датчик освещенности на базе датчика освещенности GL5528. Логика работы датчиков описывается с помощью конечного автомата на рис. 2.

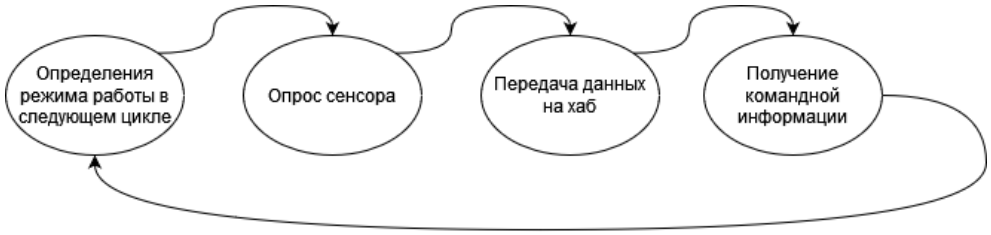


Рис. 2. Алгоритм работы датчика

Следующей задачей является выбора шлюза подключения датчиков. При выборе технологии передачи данных для сенсорной сети упор был сделан на следующие требования:

1) Низкое энергопотребление.

2) Низкая стоимость устройств и коммутационных элементов.

При проектировании рассматривались технологии IEEE 802.11 Wi-Fi, IEEE 802.15.4 ZigBee, IEEE 802.15.1 Bluetooth. Сравнение параметров этих технологий представлено в таблице 1.

ТАБЛИЦА 1. Сравнительная характеристика модулей связи

	ESP8266(802.11)	CC2530(802.15.4)	HC-06(802.15.1)
Среднее энергопотребление, мА	170	10	20
Средняя стоимость, руб.	130	180	150

Исходя из приведенных данных выбор был сделан в пользу модулей CC2530 технологии 802.15.4, поскольку они имеют самый низкий уровень потребления энергии и имеют цену сопоставимую с ценой модулей ESP8266 и HC-06.

Система предполагает автономную работу датчиков. При проектировании была произведена оценка времени автономной работы датчиков. Расчет произведен по формуле:

$$t = C\text{ак}/I\text{н},$$

где t – продолжительность автономной работы, ч; Cак – емкость аккумулятора, мА*ч; Iн – ток нагрузки, мА.

Для питания датчиков используются 4 батарейки типа AA, имеющие емкость 2000 мА*ч. За ток нагрузки возьмем суммарный ток всех элементов датчика. Токи нагрузки приведены в таблице 2.

ТАБЛИЦА 2. Токи нагрузки элементов датчиков

Элемент	Ток нагрузки, мА
Arduino Uno	24
DHT-11	0,5
GL5528	0,19
CC2530	8

Согласно формуле время автономной работы датчика освещенности составляет приблизительно 163,8 часов, а датчика температуры и влажности 162,3 часа. Таким образом датчики могу работать без необходимости замены батареи в течении 6 дней.

Хабу в данной системе отводиться роль моста, который объединяет сеть датчиков и пользовательское приложение, обеспечивая их взаимное функционирование. Для общения хаба с датчиками применяется протокол MQTT, поскольку он решает проблему безопасности, имеет механизмы отслеживания сеанса, может обеспечивать форму качества обслуживания и в то же время остается простым для реализации [3]. Хаб обрабатывает сообщения, приходящие от датчиков и записывает полученные показания в базу данных. Также он отвечает за мониторинг состояния самих датчиков (доступность по сети, уровень заряда) и может отправлять управляющие команды (отключить устройство, изменить период отправки сообщений). Со стороны приложения хаб получает команды с помощью протокола удаленного вызова процедур gRPC. Универсальный язык описания интерфейса Protocol Buffers обеспечивает простой доступ к API со стороны приложения, а механизм аутентификации с применением протокола TLS обеспечивает безопасность интерфейса.

В качестве решения в области приложения разработано web-приложение на языке Java. Приложение, взаимодействуя с хабом, предоставляет пользователю простой и понятный интерфейс взаимодействия с системой в целом. На главной странице приложения, изображенной на рис. 3, пользователь может отслеживать состояние каждого датчика, по цвету рамки определяется уровень его значения (от 1 до 10).

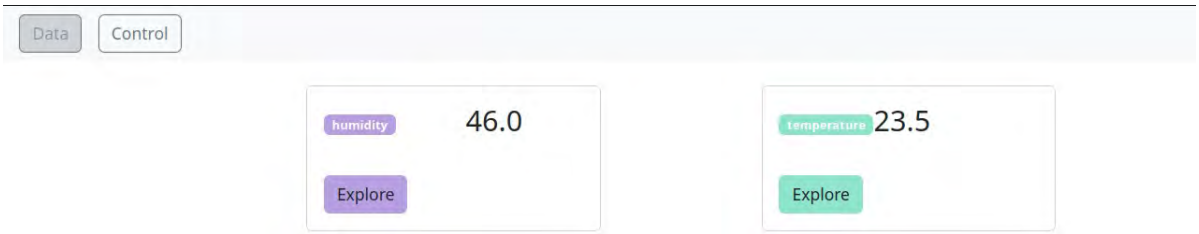


Рис. 3. Главная страница приложения

Рассматривается возможность предоставить пользователю выбирать максимальное значение самому, однако, на сегодняшний момент, это значение выбрано согласно характеристикам устройств. Позднее планируется добавить в веб-интерфейс элемент управления устройствами, в частности, включения и выключения. Сложность реализации заключается в необходимости отслеживания всех датчиков вне зависимости от их состояния, что требует больших трудозатрат на разработку логики приложения. Пользователь также может более подробно изучить состояние конкретного устройства, при клике на него. На странице устройства пользователь может запросить статистические данные за определенный временный период и получить их представление в виде графика (рис. 4). Для реализации данной функции был разработан скрипт на языке Python с применением библиотеки Matplotlib.

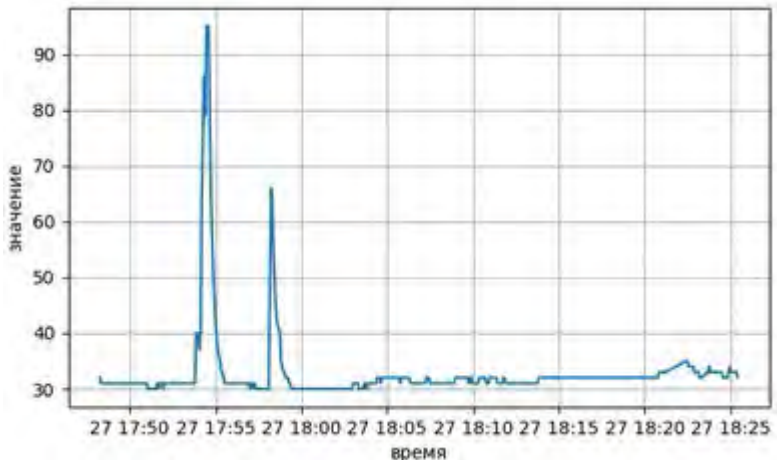


Рис. 4. График данных с датчика влажности в период с 17:49 до 18:26

Поставка и развертывание готового решения произведено с помощью системы контейнеризации Docker, что позволяет быстро развернуть программный комплекс системы на любом компьютере под управление ОС Windows или Linux.

Список используемых источников

1. Грингард С. Интернет вещей. Будущее уже здесь. М. : Альпина Паблишер, 2016. 188 с.

2. The Fundamental IoT Architecture. URL: https://www.losant.com/blog/the-fundamental-iot-architecture (дата обращения 04.03.2023).

3. Перри Ли. Архитектура интернета вещей. М. : ДМК-Пресс, 2019. 284 с.

УДК 519.237.8
ГРНТИ 27.43.51

КЛАССИФИКАЦИЯ И АНАЛИЗ СЕТЕВОГО ТРАФИКА МЕТОДАМИ КЛАСТЕРИЗАЦИИ

Т. И. Белая, А. Ю. Березин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрено решение задачи классификации сетевого IP – трафика с использованием методов кластеризации. Классификация сетевого трафика необходима для решения задач контроля и оптимизации, разделения трафика и данных, а также при принятии решений для последующей обработки. Классификация сетевого трафика используется для решения специфических задач, таких как определение приоритетов при формировании полосы пропускания для отдельных трафиков, установление правил по управлению сети, обеспечение безопасности сети. Для решения задачи классификации сетевого трафика рассматриваются алгоритмы кластерного анализа, статистические методы параметров потоков, извлекаемых из трафика, формулируются критерии выбора и условия применимости метода классификации.

кластеризация, классификация, сетевой трафик.

Методы классификации могут быть использованы для анализа сетевого трафика путем группировки схожих типов трафика в кластеры. Это позволяет выделить особенности и закономерности в поведении трафика в сети.

Рассмотрим три метода кластеризации, которые могут быть использованы для классификации сетевого трафика.

K-средних является одним из наиболее популярных методов кластеризации, который основывается на разделении объектов на *K*-групп таким образом, чтобы объекты в каждой группе были максимально схожи друг с другом и максимально различались от объектов в других группах. Алгоритм *K*-средних состоит из следующих шагов:

Пусть есть множество объектов $X = x_1, x_2, \dots, x_n$, которые необходимо разбить на k кластеров.

1. Выбрать k случайных объектов в качестве центроидов $c_1, c_2, \dots, c_k$.

2. Для каждого объекта x_i находим ближайший к нему центроид и присваиваем объекту соответствующий кластер. Обозначим множество кластеров как $\mathrm{C} = \mathrm{C}_1, \mathrm{C}_2, \dots, \mathrm{C}_\mathrm{k}$, где C_j – множество объектов, принадлежащих кластеру j [1].

3. Вычисляем новые центроиды $c_1', c_2', \dots, c_k'$ путем усреднения объектов в каждом кластере:

$$c_j^{`} = \frac{1}{|C_j|} \sum_{x_i \in C_j} x_{i,j} = 1,2 \ldots, k.$$

4. Повторять шаги 2–3 до тех пор, пока не будет достигнуто минимизация суммарного квадрата расстояний между объектами и центроидами кластеров. Эта величина называется инерцией кластеризации и вычисляется по формуле:

$$J(C) = \sum_{j=1}^{k} \sum_{x_i \in C_j} \left|\left|x_i - c_j\right|\right|^2.$$

Формула для определения расстояния между объектом x_i и центроидом c_k:

$$d(x_i, c_k) = \sqrt{(x_{i1} - c_{k1})^2 + (x_{i2} - c_{k2})^2 + \cdots + (x_{in} - c_{kn})^2},$$

где x_{i1}, x_{i2}, …, x_{in} – признаки объекта x_i, а $c_{k1}, c_{k2}, \ldots, c_{kn}$ – координаты центроида c_k[1].

DBSCAN (*Density-Based Spatial Clustering of Applications with Noise*) – метод кластеризации, который основывается на плотности точек в пространстве признаков DBSCAN может работать с любыми формами кластеров и имеет возможность определять шумовые точки, которые не относятся ни к одному из кластеров. Алгоритм основан на двух параметрах: радиусе окрестности ϵ в пределах которой должно быть минимальное количество точек $minPts$. Алгоритм DBSCAN состоит из следующих шагов:

Пусть есть множество объектов $X = x_1, x_2, \ldots, x_n$, каждый объект которого имеет d признаков (координат). Тогда можно определить расстояние между объектами с помощью евклидова расстояния:

$$dist(x_i, x_j) = \sqrt{\sum_{k=1}^{d} (x_{ik} - x_{jk})^2}.$$

Для применения алгоритма DBSCAN необходимо определить параметры ϵ и $minPts$. Алгоритм DBSCAN можно описать следующим образом:

1. Выбираем произвольную необработанную точку p из множества X.

2. Находим все точки, находящиеся в ϵ-окрестности $N_\epsilon(p)$ точки p.

3. Если число точек в ϵ-окрестности $N_\epsilon(p)$ больше или равно $minPts$, то точки в $N_\epsilon(p)$ образуют кластер C.

4. Повторяем процедуру для всех точек, которые еще не были обработаны. Если точка не может быть отнесена к какому-либо кластеру, то она считается выбросом (шумом) [2].

Иерархическая кластеризация – это метод кластерного анализа, который группирует объекты в иерархическую структуру, обычно представленную в виде дендрограммы. Существуют два типа иерархической кластеризации: агломеративная и дивизивная.

Агломеративная кластеризация начинается с того, что каждый объект представляет собой отдельный кластер, а затем объединяет ближайшие кластеры, пока все объекты не будут объединены в один кластер.

Для агломеративной кластеризации расстояние между кластерами можно определить разными способами, например [3]:

Расстояние между ближайшими объектами (*Single linkage*):

$$d_{SL}(C_i, C_j) = min_{x \in C_i, y \in C_j} d(x, y).$$

Расстояние между самыми удаленными объектами (*Complete linkage*):

$$d_{CL}(C_i, C_j) = \max_{x \in C_i, y \in C_j} d(x, y).$$

Для определения оптимальных параметров алгоритмов *K*-средних, DBSCAN, Иерархической кластеризации можно использовать меру силуэта (*Silhouette Score*) Она рассчитывается для каждого объекта как среднее значение отношения среднего расстояния между объектом и другими объектами в том же кластере к среднему расстоянию между объектом и объектами в ближайшем кластере[3].

Silhouette Score для объекта i можно рассчитать следующим образом:

$$s(i)\frac{b(i) - a(i)}{maxa(i), b(i)},$$

где $a(i)$ – среднее расстояние от объекта i до всех других объектов в том же кластере, а $b(i)$ – среднее расстояние от объекта i до всех объектов в ближайшем кластере (не считая кластер, к которому принадлежит объект i).

Общий алгоритм для применения кластеризации для классификации трафика и сравнения методов кластеризации приведен представлен на рис. 1, в качестве метрик для сравнения использовались метрики «silhouette score» коэффициент силуэта и «davies bouldin score» Индекс Дэвиса-Болдина (показатель качества кластеризации, который основан на среднем расстоянии между центроидами кластеров и мерой разброса точек внутри кластеров.), «normalized mutual info score» (NMI) используется для оценки сходства между двумя кластеризациями [4]. Эта метрика измеряет взаимную информацию между двумя кластеризациями и нормализуется таким образом, чтобы она принимала значения между 0 (когда кластеры не сходятся) и 1 (когда кластеры совпадают), где: features: матрица признаков объектов трафика, на которых будет производиться кластериза-

ция, n_clusters: количество кластеров, на которое нужно разбить данные (для KMeans и AgglomerativeClustering), eps: радиус окрестности, в пределах которой должно быть min_samples точек (для DBSCAN), min_samples: минимальное количество точек, необходимое для того, чтобы образовался кластер (для DBSCAN), pred: массив, содержащий метки кластеров для каждого объекта, silhouette_score и davies_bouldin_score, normalized_mutual_info_score метрики.

Require: features: dataset to be clustered
Ensure: cluster_metrics: dictionary containing clustering evaluation metrics
procedure CLUSTERING(features, cluster_metrics)
$kmeans \leftarrow KMeans(n\_clusters, random\_state)$
$kmeans\_pred \leftarrow kmeans.fit\_predict(features)$
$cov \leftarrow EmpiricalCovariance().fit(features)$
$kmeans\_radius \leftarrow \sqrt{1/\text{diag}(cov.covariance\_)}$
$dbscan \leftarrow DBSCAN(eps, min\_samples)$
$dbscan\_pred \leftarrow dbscan.fit\_predict(features)$
$hierarchical \leftarrow AgglomerativeClustering(n\_clusters)$
$hierarchical\_pred \leftarrow hierarchical.fit\_predict(features)$
$metrics \leftarrow [silhouette\_score, davies\_bouldin\_score]$
$cluster\_metrics \leftarrow$
for $metric \leftarrow metrics$ **do**
$kmeans\_score \leftarrow metric(features, kmeans\_pred)$
$dbscan\_score \leftarrow metric(features, dbscan\_pred)$
$hierarchical\_score \leftarrow metric(features, hierarchical\_pred)$
$cluster\_metrics[metric.name] \leftarrow$
$[kmeans\_score, dbscan\_score, hierarchical\_score]$
end for
return $cluster\_metrics$
end procedure

Рис. 1. Общий алгоритм кластеризации

Датасет на котором тестировались алгоритмы – «Hive_06082021» небольшим объемом в 55,8 Мб [5]. Датасет представляет собой дамп сетевого трафика, включающий в себя различные типы трафика, такие как DNS, HTTP, HTTPS, TCP, IP, ETHII и прочие.

В таблицах 1 и 2 представлены результаты классификации сетевого трафика использованием трех алгоритмов: к-средних, DBSCAN и иерархической кластеризации. Для каждого из этих методов были вычислили метрики, которые позволяют оценить качество кластеризации. Кроме того, на рис. 2 предоставлены визуализированные результаты метрик.

ТАБЛИЦА 1. Сравнение метрик и количество кластеров

Параметр/метрика	*K*-средних	DBSCAN	Иерархическая
Количество кластеров	25	26	12
Коэффициент силуэта	0,97469158	0,9016294	0,9084971
Индекс Дэвиса-Болдина	0,190191	0,963616	0,2561720

ТАБЛИЦА 2. Метрика NMI

NMI	Значение
К-средних – DBSCAN	0,9241941
К-средних – Иерархическая	0,9498545
DBSCAN – Иерархическая	0,9324237

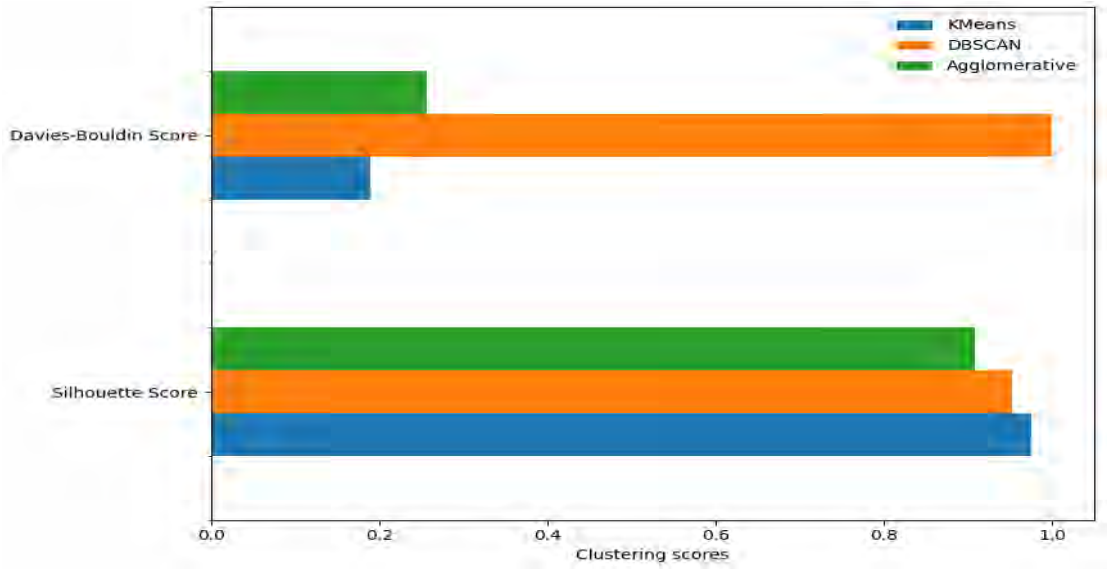


Рис. 2. График распределения метрик

Результаты анализа алгоритмов кластеризации показали, что все три метода дали сравнимые результаты по метрике силуэта, но также и наблюдались различия. Алгоритм dbscan показал лучшие результаты по метрике силуэта, но при этом создал наибольшее количество кластеров. Алгоритм иерархической кластеризации создал меньше всего кластеров, но по индексу Дэвиса-Болдина опередил *k*-средних. Алгоритм *k*-средних показал неплохие результаты по метрикам, но в среднем был менее эффективен, чем DBSCAN. Исходя из метрики NMI, можно сказать можно сделать вывод о том, что данные имеют явную структуру и что все исследуемые кластеризации показывают схожую интерпретацию этой структуры, кроме того, это говорит о том, что эти кластеризации достаточно стабильны и надежны.

Список используемых источников

1. Aggarwal C. C, Reddy C. K. Data Clustering: Algorithms and Applications editors. London : CRC Press, 2014. 617 p.
2. Alpaydin E. Introduction to Machine Learning. E. London : MIT Press, 2014. 616 p.
3. Geron A. Hands-on machine learning with scikit-learn, keras, and TensorFlow: Concepts, tools, and techniques to build intelligent systems. Sebastopol, CA : O'Reilly Media, 2019. 600 p.
4. Metrics and scoring: quantifying the quality of predictions // scikit-learn [Электронный ресурс]. URL: https://scikit-learn.org/stable/modules/model_evaluation.html (дата обращения 09.02.2023).
5. Ransomware PCAP repository // Unavarra.es [Электронный ресурс]. URL: http://dataset.tlm.unavarra.es/ransomware/ (дата обращения 09.02.2023).

УДК 65.011.56
ГРНТИ 50.41.25

РАСПРЕДЕЛЕНИЕ СЕТЕВЫХ РЕСУРСОВ В СЕТИ 5G НА ОСНОВЕ ИГРОВОГО ПОДХОДА

К. В. Белозеров[1], С. В. Кисляков[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]НТЦ АРГУС

Разделение ресурсов является важным аспектом при создании сетевых срезов, поскольку различные виды услуг могут требовать различных параметров передачи данных. Представлен метод выделения ресурсов кэш-памяти с использованием теории игр, в частности, игры в банкротство, для оптимизации распределения кэш-памяти между срезами сети пятого поколения

теория игр, слайсинг, сети 5G, управление сетью.

Технология сетевой нарезки (слайсинга)

Сетевой слайсинг – это технология в сетях 5G, которая позволяет разделить физическую инфраструктуру сети на несколько виртуальных сегментов, каждый из которых может быть оптимизирован для конкретных требований пользователей и приложений. Это позволяет предоставлять различные типы услуг, которые требуют разной скорости передачи данных, качества обслуживания, безопасности и других параметров

Распределение ресурсов между срезами является важным аспектом, поскольку различные услуги могут требовать различных ресурсов и «бороться» за них.

Архитектура сетевого слайсинга показана на рис. 1

Рис. 1. Архитектура сетевого слайсинга

Исследования по оптимизации распределения ресурсов публиковались в ряде работ. Так, в работе Ю. В. Самуйлова [1] предложен и реализован алгоритм освобождения ресурсов слайсами-нарушителями, а также предложен и реализован алгоритм распределения ресурсов на основе весов слайсов. Разработано средство имитационного моделирования механизма распределения ресурсов. В статье Ю. В. Гайдамака [2] построена математическая модель разделения ресурсов соты между двумя виртуальными операторами, которая иллюстрирует влияние параметров изоляции на метрики производительности сети.

Однако задача оптимального разделения ресурсов в сетях 5G всё ещё считается актуальной.

Теории игр

Теория игр (ТИ) – раздел прикладной математики, с помощью которого можно исследовать поведение нескольких «игроков» и принятые ими решения в условиях следования собственным интересам. ТИ находится на стыке компьютерной науки и направлена на изучение и создание алгоритмов для стратегий.

ТИ – это средство для моделирования и изучения взаимодействия между субъектами, заинтересованными «в себе» [4]. Она изучает проблемы, связанные с разработкой стратегий взаимодействия, которые позволят максимизировать благосостояние агента в случае взаимодействия нескольких агентов. В [4] выработка рекомендаций для агентов является главной задачей, решаемой при помощи ТИ. Стратегия агента – это система правил, которая определяет поведение агента на каждом ходе. Когда стратегии агентов пересекаются, образуется ситуация, в которой каждый агент получает определенный результат. Результат может быть, как положительным, так и отрицательным. Выбор стратегии основан на получении желаемого в самый короткий срок, но нельзя забывать про шаги противоположного агента, так как они тоже влияют на ситуацию в целом.

Модель игры в банкротство

Игра в банкротство – это одна из кооперативных игр, которая используется для решения проблем распределения и моделируется как кооперативная игра. Если активов банкротной [4, 5] компании недостаточно для удовлетворения всех требований кредиторов, все кредиторы могут использовать игру в банкротство для распределения активов компании. Алгоритм игры в банкротство показана на рис. 2.

Рис. 2. Алгоритм игры в банкротство

Под игрой мы будем понимать процесс, в котором участвуют две и более сторон, ведущие борьбу за реализацию своих интересов. Пусть условия игры допускают совместные действия и перераспределения выигрыша. Главная задача исследования – это оптимальное распределение благ между членами объединения. Пусть $N = \{1, 2, ..., n\}$ – это множество всех игроков в рамках рассматриваемой модели. Тогда любое непустое подмножество $S \subset N$ мы будем называть коалицией. Под характеристической функцией v будем понимать функцию, которая для каждой возможной коалиции ставит в соответствие вещественное число. Для любых двух непересекающихся коалиций $T \subset N$ и $S \subset N$ выполняется неравенство: $v(T) + v(S) \leq v(T \cup S)$. Это означает, что коалиция $T \cup S$ имеет не меньше возможностей, чем две непе-

ресекающиеся коалиции *T* и *S*, действующие в одиночку. Тогда кооперативной игрой назовём пару (*N*, *v*) и определим её решение. Чаще всего используются принципы оптимальности такие как C-ядро, NM-решение, вектор Шепли. Но мы выберем метод, который подходит для решения задачи справедливого дележа и, который гарантирует единственность решения. Этот принцип вводится аксиоматически.

Аксиомы Шепли.

Аксиома 1. Если *S* – любой носитель игры (*N*, *v*), то выполняется:

$$\sum_{i \in S} \varphi i\ [v] = v(S).$$

Аксиома 2. Для любой подстановки π и ∀i ∈ N верно:

$$\varphi_{\pi(i)}[\pi v] = \varphi_i[v].$$

Аксиома 3. Если (*N*, *v*) и (*N*, *u*) – две произвольные кооперативные игры, то:

$$\varphi_i[v + u] = \varphi_i[u] + \varphi_i[v].$$

Пусть φ – это функция, которая ставит в соответствие согласно аксиомам (1)-(3) любой игре (*N*, *v*) вектор φ(*v*). Тогда этот вектор будем называть вектором Шепли игры (*N*, *v*).

Применение ТИ для оптимизации ресурсов слайсинга

Операторы должны экономить ресурсы, так как им выгодно внедрять максимум услуг используя минимальное количество ресурсов, но для стабильной работы им необходимо иметь резерв, который они смогут использовать при сбоях работы срезов. Рассмотрим ситуацию, когда размер кэш-памяти намного меньше, чем размер требования каждого среза. Тогда срезы работают вместе, чтобы сформировать коалицию, которая определяется как подмножество игроков. Предполагая, что игроки обмениваются информацией о соответствующих требованиях (размер пространства кэша), претензии могут быть смоделированы как совместная игра. Выбор игровой характеристической функции [6], представляющей интересы, приписываемые каждому игроку в коалиционной игре, является предпосылкой формирования коалиций. Игровая характеристическая функция показана ниже.

$$u^{(d,E)}(S) = \max\{E - \sum d_i, 0\}, i \in N \backslash S,$$

где *E* – это общее количество кэш памяти, $d = (d_1, d_2, \ldots d_n)$ – требования каждого среза, *N* = {1, 2, ..., *n*} – множество всех игроков в рамках рассматриваемой модели, *S* – любой носитель игры, а *u* – характеристическая функция кооперативной игры.

После создания коалиций и формирования всех ограничений, рассчитываются значения вектора Шепли. Формула расчета значения Шепли приведена ниже.

$$\Phi(u)_i = \sum_{i \in K} \frac{(k-1)!\,(N-k)!}{N!} \big(u(K) - u(K \backslash i)\big),$$

где N – количество игроков, k – количество участников коалиции K.

Значения Шепли предназначено для более справедливого распределения результирующих выгод между участниками игры. Метод расчета значения Шепли заключается в следующем. В модели есть значение размера пространства кэша, полученного срезом. Значение Шепли [6] выбирается для получения стабильного вектора решения. При значении Шепли ресурсы кэша логически и справедливо распределяются между фрагментами, что повышает эффективность использования пространства кэша. Если срезам недостаточно памяти, т. е. происходят сбои, задержки, то выделяется дополнительное количество ресурсов, которое также распределяется, как и основное.

Результаты работы модели

Для реализации данного алгоритма был выбран язык программирования Python.

Для проведения тестов алгоритма были взяты следующие входные данные: E = 1000 и $E1$ = 1500, d = (400, 500, 700). В результате получили распределение ресурсов кэш-памяти между сетевыми срезами. Частично результаты приведены ниже на рис. 3.

В результате разработан алгоритм двухуровневого оптимального распределения кэш-памяти между сетевыми срезами сети.

```
1 Вариант
Коалиции
[0, 0, 0, 100, 300, 500, 600, 1000]

Распределение кэша
(250.0, 300.0, 450.0)

Проверка
1000

2 Вариант
Коалиции
[0, 300, 400, 600, 800, 1000, 1100, 1500]

Распределения кэша
(333.3, 383.3, 783.3)

Проверка
1500
```

Рис. 3. Результаты алгоритма

Список используемых источников

1. Агеев К. А., Сопин Э. С., Яркина Н. В., Самуйлов К. Е., Шоргин С. Я. Анализ механизмов нарезки сети с учетом гарантий для различных типов трафика // Информатика и её применение. 2020. Т. 14, N 3. С. 94–100.

2. Москалева Ф. А., Гайдамака Ю. В., Шоргин В. С. Влияние параметров изоляции на разделение ресурсов при нарезке сети // Информатика и её применение. 2020. Т. 14, N 4. С. 9–16.

3. Мухизи С., Киричек Р. В. Анализ технологии слайсинга в сетях связи пятого поколения // Информационные технологии и телекоммуникации. 2017. Т. 5. N 4. С. 57–63.

4. Parsons S., Wooldridge M. Game Theory and Decision Theory in Multi-Agent Systems // Department of Computer Science, University of Liverpool, Liverpool L69 7ZF, United Kingdom.

5. Bamdad M., Jamali S., Fotohi R. Dynamic Allocation of 5G Network Resources using Game Theory // Faculty of Computer Science and Engineering, Shahid Beheshti University, G. C. Evin, Tehran 1983969411, IRAN.

6. Zhang L., Wang G., Wang F. A Bankruptcy Game for Optimize Caching Resource Allocation in Small Cell Networks // KSII Transactions on Internet and Information Systems. 2019. Vol. 13, No. 5. PP. 2319–2337. DOI: 10.3837/tiis.2019.05.005.

УДК 004.432.2, 004.773.3
ГРНТИ 81.93.29

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ OPENSSL ДЛЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ МГНОВЕННЫХ СООБЩЕНИЙ

Д. Л. Беляев, И. Ю. Рогальников

Академия Федеральной службы охраны Российской Федерации

Статья посвящена вопросам разработки системы обмена защищёнными мгновенными сообщениями. Для обеспечения безопасности предлагается использовать возможности пакета OpenSSL в операционной системе Astra Linux, а также криптобиблиотеки PyGOST. Для установления доверия к сертификатам предложено встраивать элементы инфраструктуры открытых ключей в клиентское и серверное программное обеспечение.

сертификат открытого ключа, система обмена мгновенными сообщениями, формирование ключей.

Удовлетворению потребностей пользователей в передаче и получении сообщений и документов от других пользователей со своего рабочего места способствуют инфокоммуникационные службы электронной почты и обмена мгновенными сообщениями. Безопасность систем электронной почты может быть обеспечена средствами S/MIME или PGP. Данные средства совмещают достоинства симметричных и асимметричных криптоалгоритмов, позволяя клиентским приложениям на стороне оконечных абонентов формировать ключи, шифровать и подписывать документы. Однако они не предоставляют возможности получения мгновенных сообщений, а также возможность видеть статус присутствия абонента в сети.

Системы обмена мгновенными сообщениями в корпоративных сетях получают наибольшее предпочтение благодаря своему удобству и своевременности. Однако большинство существующих систем либо имеют неудовлетворительную криптографическую защиту, либо не имеют её вообще. Варианты защиты на основе протоколов типа SSL/TLS создают иллюзию безопасности, передавая сообщения по криптографически защищённым соединениям между клиентами и сервером, но, при этом оставляя их на сервере в открытом виде. Достаточно часто сервер вовлекается в процесс выработки криптографических ключей для защищённого обмена между абонентами, якобы для их удобства, на самом деле создавая серьёзную угрозу безопасности информации. На сегодняшний день остаётся нерешённой проблема обмена защищёнными сообщениями [1].

Разработке систем защиты на основе отечественных криптоалгоритмов, поддерживаемых сертифицированными криптопровайдерами, такими как Крипто ПРО CSP, VipNet CSP, Signal-COM CSP, сопутствуют довольно существенные сложности. Основными из них являются необходимость приобретения отдельных лицензий на сам криптопровайдер и на удостоверяющий центр, развёртывание удостоверяющего центра на основе специализированного программного обеспечения.

Более предпочтительным решением является использование отечественной операционной системы Astra Linux [2]. Встроенное в неё приложение XCA позволяет развернуть свой центр сертификации на основе российских криптоалгоритмов в соответствии с ГОСТ Р 34.10-2012 и использовать возможности пакета OpenSSL также с российскими криптографическими стандартами.

Перспективная схема обеспечения безопасности мгновенных сообщений предполагает установление защищённого взаимодействия попарно между двумя абонентами с выполнением криптографических операций как на основе симметричных, так и асимметричных алгоритмов. Исключительно клиентским программным обеспечением должны выполняться: генерация ключей, зашифрование и расшифрование, вычисление и проверка электронной подписи передаваемых сообщений. В случае развёртывания инфраструктуры открытых ключей третья доверенная сторона может привлекаться только для заверения своей электронной подписью готовых открытых ключей абонентов.

В операционной системе Astra Linux клиентская программа для отправки и получения мгновенных сообщений может использовать команду интерпретатора *Bash* следующего вида [3]:

openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out gostpkey.pem

Указанная команда позволит сгенерировать пару асимметричных ключей в соответствии с ГОСТ Р 34.10-2012, сохранив их в одном файле. Пример выполнения команды для преобразования ключевой информации

из данного файла в текстовый формат и более наглядного отображения, а также использования другими программами:

openssl pkey -in genpkey.pem -text
-----BEGIN PRIVATE KEY-----
MEYCAQAwHwYIKoUDBwEBAQEwEwYHKoUDAgIjAQYIKoUDBwEBAgIEIF+1g7ysXfJl
2Cb7+qUI1nBgJU6jz0AeqQpVegG0xZho
-----END PRIVATE KEY-----
Private key:
6898C5B4017A550AA91E40CFA34E256070D608A5FAFB26D865F25DACBC83B55F
Public key:
X:BAF1E0D416D268D423644EFAAB4111575EDFB114DBFB2D015154550E1327D8FA
Y:8C12233333555EA7C3D3A5268268977F9ED5380A4C7FE625DB002CB67C46EB8D
Parameter set: id-GostR3410-2001-CryptoPro-A-ParamSet

В представленном примере показаны сгенерированные открытый и секретный ключи, которые могут быть использованы для защиты сеансового ключа или вычисления подписи клиентом обмена мгновенными сообщениями [2]. В дальнейшем, секретный ключ должен быть зашифрован при помощи пароля и сохранён в одном файле, а открытый ключ с дополнительными сведениями о владельце ключа и его электронной подписью сохранится в другом файле в виде запроса на сертификат. Файл, содержащий запрос на сертификат передаётся в удостоверяющий центр, поддерживающий криптографические стандарты ГОСТ, и являющийся доверенным для всех участников информационного обмена.

Информационные объекты (секретные ключи и сертификаты открытых ключей), полученные с помощью пакета OpenSSL в операционной системе Astra Linux полностью совместимы с другими решениями, например, криптобиблиотекой PyGOST. Кроме того, возможности OpenSSL позволяют создать простой https-сервер, обеспечивающий проверку действенности сертификатов на основе протокола OCSP.

В настоящее время в свободном доступе существует большое количество примеров для создания чат-систем на языке Python, которые могут использоваться в качестве основы для разработки клиентских и серверных приложений, обеспечивающих передачу, приём и возможностью временного хранения мгновенных сообщений в базе данных sqlite3. При этом должен быть справочник абонентов с собственным хранилищем сертификатов открытых ключей. Установленное соединение клиентов с сервером необходимо для определения статуса абонентов и верификации сертификатов открытых ключей.

Использование функциональности пакета OpenSSL и библиотеки PyGOST позволяет разработать полноценную систему обмена защищёнными мгновенными сообщениями. Известные наборы команд операционной системы позволят использовать все преимущества инфраструктуры

открытых ключей, а добавление функций криптографической защиты в соответствии с отечественными криптографическими стандартами в клиентские приложения позволит обеспечить безопасность сообщений между абонентами.

Список используемых источников

1. Беляев Д. Л., Шорохов Е. Г. Разработка системы безопасной передачи оперативных сообщений на основе функций CryptoAPI // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2022. Т. 3. С. 427–431.

2. Справочный центр Astra Linux. URL https://wiki.astralinux.ru/ (дата обращения 01.12.2022).

3. Компьютерная безопасность: практикум. В 2 ч. Д. Л. Беляев [и др.] ; под общ. ред. Д. Л. Беляева. Орёл : Академия ФСО России, 2016. 187 с.

УДК 004.021
ГРНТИ 73.37.81

ИСПОЛЬЗОВАНИЕ ПЧЕЛИНОГО АЛГОРИТМА ДЛЯ УПРАВЛЕНИЯ РОЯМИ БПЛА ПРИ МОНИТОРИНГЕ МЕСТНОСТИ

П. Ю. Беляев[1], И. А. Зикратов[1], Т. В. Зикратова[2], Е. А. Неверов[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Военный институт (Военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия»

Рассмотрены методы управления роями беспилотных летательных аппаратов при планировании мониторинга местности. Показано, что для экономного расходования ресурсов целесообразно использовать метаэвристические алгоритмы, которые могут обеспечить достаточно хорошее решение задачи оптимизации. Авторами предложен двухэтапный алгоритм решения задачи поиска объектов на местности, основанный на пчелином алгоритме. На первом этапе осуществляется предварительный мониторинг территории и составлении карты «перспективных участков». На втором этапе агенты роя исследуют выявленные «перспективные» участки. Результаты работы могут быть полезными разработчикам алгоритмов управления самоорганизующихся групп БПЛА.

групповая робототехника; роевые алгоритмы, метаэвристические алгоритмы; пчелиный алгоритм; мониторинг; беспилотные летательные аппараты.

Беспилотные летательные аппараты (БПЛА) находят все большее применение в разведывательных и поисково-спасательных операциях, целью

которых является поиск потерявшихся (заблудившихся, потерпевших аварию и т. п.) людей или техники. Как правило это требуется в горных и/или лесистых труднодоступных местностях. Для решения таких задач разработано множество теоретических моделей организации групп (роев) роботов, и методов, направленных на совершенствование качества группового управления при патрулировании, охране и мониторинге объектов, когда требуется достижение рационального распределения группы роботов (агентов роя) в пространстве, совместной координации движения, коллективного картографирование и т. д. [1, 2, 3, 4].

В частности, для мониторинга местности в работе [5] предложен генетический алгоритм для оптимизации маршрута БПЛА при облете реперных точек. В работе [6] решена задача равномерного покрытия ограниченной территории при ее облете группой БПЛА. Авторами предлагается равномерное распределение и поиск максимально и минимально возможных расстояний между БПЛА так, чтобы они находились в зоне видимости друг друга и вся территория покрывалась бы действием датчиков без промежутков. Мониторинг местности осуществляется посредством анализа информации, получаемой от фото- видеокамер, тепловизоров, а также от других сенсоров, в зависимости от технической оснащенности летательного аппарата.

Такой подход позволяет осуществить рациональное покрытие роем БПЛА всей территории, однако он имеет ограничение, затрудняющее применение в поисковых операциях. Ограничение обусловлено требованием нахождения соседних БПЛА в зоне видимости своих сенсоров. Это означает, что все агенты роя в процессе мониторинга должны двигаться с одинаковой скоростью, независимо от характера местности, находящейся под ними. Вместе с тем известно, что задача обнаружения объектов в лесной местности гораздо сложнее, чем та же задача на открытом пространстве, и требует более тщательного, а значит длительного по времени, исследования.

Таким образом, все БПЛА группы, даже находящиеся над открытым пространством, должны выбирать одну из двух стратегий. Либо при сканировании местности сохранять постоянную скорость полета, принимая риск возрастания ошибки второго рода в задаче распознавания образов. Либо снижать скорость всех БПЛА в группе, вплоть до режима «зависание», при выполнении поиска одним или несколькими дронами над сложнодоступным участком местности, что приводит к нерациональному расходу топлива (энергии аккумулятора) у всех агентов роя, и, как следствие, появляющемуся риску отказа от исследования оставшейся части территории.

Известно, что для решения слабоструктурированных задач, в том числе задач маршрутизации, все более широкое применение находят метаэвристические алгоритмы (МА) поиска [7, 8] локальных экстремумов функции.

Одним из известных МА является пчелиный алгоритм [9], суть которого заключается в поиске «перспективных» участков «танцпола» «пчелами-разведчиками» с последующим их детальным исследованием «пчелами-фуражирами» с целью поиска максимума или минимума целевой функции.

Следуя такому подходу, представляется целесообразным осуществлять поэтапный мониторинг местности при поисково-разведывательных работах с использованием БПЛА:

1 этап – инициализация. Предварительный анализ всей территории с целью выявления на ней «перспективных» участков.

2 этап – локальная разведка. Детальное обследование выявленных локальных участков.

Первый этап реализуется всеми агентами роя, который на высокой (крейсерской) скорости сканирует местность и составляет карту «перспективных» участков. На этом этапе возможно использование менее точных, но более быстрых алгоритмов анализа видеоизображений, например, алгоритмы иммунокомпьютинга [10].

Под «перспективными» в данном случае будем понимать наиболее сложные для поиска объекта участки местности. При поиске с использованием видеокамер и тепловизоров к таким участкам относятся местность со сложным рельефом, с высокой и/или густой растительностью, городские постройки, обломки зданий и сооружений, очагами возгорания и задымления и т. п.

На втором этапе агенты роя задействованы для тщательного исследования составленной карты участков, с использованием наиболее точных алгоритмов распознавания и на рациональной для этих алгоритмов скорости полета. Для организации взаимодействия БПЛА на этом этапе могут быть использованы соответствующие алгоритмы группового управления, например, описанные в работе [11].

Например, при исследовании роем участка местности, представленного на рис. 1 (слева) БПЛА на первом этапе перемещаясь со скоростью V_1 составляют карту «перспективных» участков (рис. 1 справа), на которой обозначены квадраты (элементарные участки местности) с условно низкой (*low*) и высокой (*high*) способностью скрывать искомые объекты. Нельзя исключать и более сложной градации «перспективных» участков, например, трехуровневой – low, medium и high.

На втором этапе агенты распределяются по выявленным элементарным участкам местности (ЭУМ), и осуществляют поиск объектов. При этом скорость полета на этом этапе V_2 ($V_1 >> V_2$) выбирается оптимальной для каждого агента, в зависимости от сложности исследуемого участка местности.

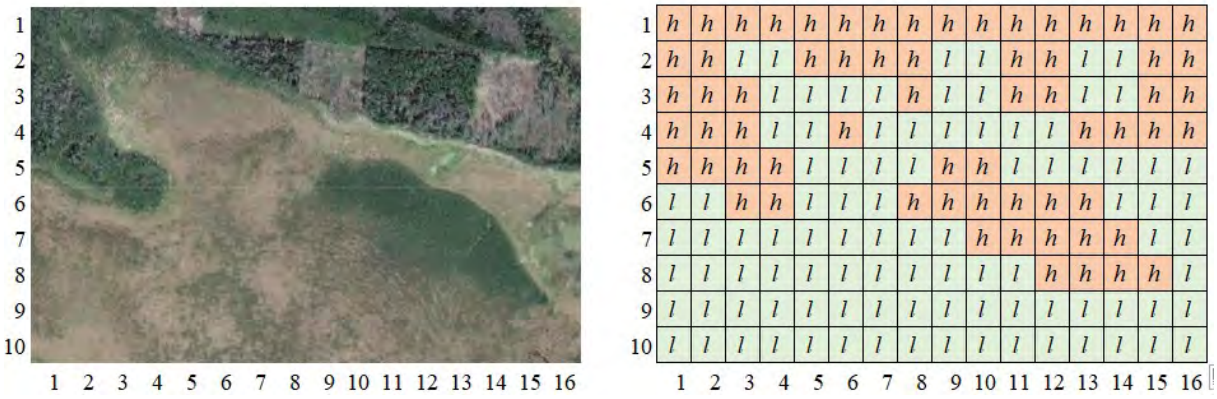


Рис. 1. Участок местности и карта «перспективных участков»

Для практического использования, предлагаемого МА необходимо решить ряд частных задач, типичных для пчелиного алгоритма.

1. Определить критерии, по которым участки местности будут классифицированы как low- или high-участки.

2. Определить параметры радиуса разведки для отдельного агента роя, и, следовательно, количество БПЛА, выделяемых на каждый участок.

3. Определить стратегию поведения для свободных (при их наличии) БПЛА.

Очевидно, что решение этих задач будет зависеть от того, как именно будут сформулированы целевая функция и ограничения задачи оптимизации. Учитывая, что обнаружение объектов на местности представляет собой вероятностную задачу, целесообразно общую постановку задачи оптимизации осуществлять методами стохастического программирования [12]. Например, можно потребовать обеспечения минимума общего времени поисковой операции при заданных показателях качества обнаружения объекта:

$$\begin{cases} M[\mathrm{C}\vec{x}] \to min \\ P\left\{\sum_j a_{ij}x_j\right\} > \alpha_i, \;\; i = \overline{1,n}, j = \overline{1,m}, \end{cases}$$

где $M[\mathrm{C}\vec{x}]$ – математическое ожидание целевой функции, которая представляет собой суммарное время исследования местности, $\vec{x} = (x_1, x_2, \dots, x_m)$ – искомый вектор, представляющий собой совокупность пространственно-временных параметров, определяющих качество обнаружения, n – количество типов ЭУМ, m – количество $high$ – участков на исследуемой территории, α_i – уровень значимости для i-го типа ЭУМ, a_{ij} – матрица случайных величин, характеризующих используемые технические средства для обнаружения объекта.

Таким образом, использование МА, в частности алгоритма пчелиного роя, позволит находить численное квазиоптимальное решение слабоструктурированных задач, к которым относятся поисково-разведочные задачи с привлечением БПЛА.

Достоинствами такого подхода являются:

- Эффективная разведка: Пчелиный алгоритм использует популяцию поисковых агентов для эффективного исследования пространства поиска. При мониторинге местности это может помочь БПЛА охватить всю интересующую область и получить необходимые данные.
- Устойчивость: Пчелиный алгоритм устойчив к изменениям в окружающей среде и может адаптироваться к меняющимся условиям. В контексте мониторинга местности это может помочь БПЛА ориентироваться в различных типах местности и погодных условиях.
- Гибкость: Пчелиный алгоритм можно использовать как для глобальной, так и для локальной оптимизации. Для мониторинга местности это означает, что БПЛА может использовать пчелиный алгоритм для определения наилучшего общего пути для покрытия местности, а также вносить коррективы в режиме реального времени для оптимизации покрытия в конкретных областях, представляющих интерес.
- Адаптивность: Пчелиный алгоритм может быть адаптирован к конкретным требованиям и ограничениям, таким как высота полета, препятствия на местности и время автономной работы. Это делает его пригодным для использования в различных сценариях мониторинга местности.

В целом, такой подход может помочь повысить эффективность и результативность мониторинга местности с беспилотного летательного аппарата, что делает его ценным инструментом для таких задач, как наблюдение, картирование и мониторинг окружающей среды.

Список используемых источников

1. Trianni V., Campo A. Fundamental collective behaviors in swarm robotics // Springer Handbook of Computational Intelligence. Springer Berlin Heidelberg, 2015. PP. 1377–139.

2. Navarro I., Matia F. An Introduction to Swarm Robotics // ISRN Robot. Artic. ID 608164. 2013. – P. 10.

3. Brambilla M., Ferrante E., Birattari M., Dorigo M. Swarm robotics: a review from the swarm engineering perspective // Swarm Intelligence. 2013. Vol. 7. PP. 1–41. DOI:10.1007/s11721-012-0075-2 3.

4. Зикратов И. А., Викснин И. И., Зикратова Т. В. Мультиагентное планирование проезда перекрестка дорог беспилотными транспортными средствами // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. N 5. С. 839–849. DOI:10.17586/2226-1494-2016-16-5-839-849.

5. Аллилуева Н. В., Руденко Э. М. Задача маршрутизации беспилотных летательных аппаратов на графе реперных точек // I-methods. 2018. Т. 10. N 1. С. 5–18.

6. Бузина Е. А., Чупров С. С., Турсуков Н. О., Беляев П. Ю., Викснин И. И. Разработка алгоритма равномерного покрытия территории группой беспилотных летательных аппаратов // Известия СПбГЭТУ «ЛЭТИ». 2022. Т. 15, N 5/6. С. 41–50.

7. Германчук М. С., Лемтюжникова Д. В., Лукьяненко В. А. Метаэвристические алгоритмы для многоагентных задач маршрутизации // Проблемы управления. 2020. N 6. С. 3–13.

8. Ульянов М. В., Фомичёв М. И. Сравнительный анализ комбинаций методы ветвей и границ с метаэвристическими алгоритмами для решения ассиметричной задачи коммивояжера // Информационные технологии. 2019. Т. 25. N 10. С. 590–595.

9. Дьякова А. С., Морозов А. В. Применение генетического, муравьиного и пчелиного алгоритмов для решения задач автоматизации курьерских служб // Научная дискуссия: вопросы технических наук. 2016. № 6 (36). С. 8–21.

10. Соломатин А. Ю., Люберт А. С., Зикратов И. А. Идентификациядвижущегося человека в системах видеонаблюдения // Научно-технический вестник информационных технологий, механики и оптики. 2014. N 4 (92). С. 124–131.

11. Зикратова Т. В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021. N 7 (3). С. 92–100. DOI: 10.31854/1813-324X-2021-7-3-92-100.

12. Юдин Д. Б. Математические методы управления в условиях неполной информации. М. : Советское радио, 1974. 400 с.

УДК 004
ГРНТИ 28.23.37, 28.23.29

ПЛАТФОРМА ДЛЯ ОБУЧЕНИЯ НЕЙРОННЫМ СЕТЯМ НА ОСНОВЕ БИНАРНОГО КЛАССИФИКАТОРА

А. Ю. Березин, М. С. Кузнецов

Санкт–Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной стаьте рассматривается платформа для практического обучения студентов нейронным сетям на основе бинарного классификатора. В современном мире нейронные сети встречаются повсеместно для использования решения различных задач, при этом они являются достаточно сложной технологией и для лучшего понимания и большей вовлеченности студентов в основы простых моделей нейронных сетей была разработана данная платформа. Одной из таких моделей являются бинарные классификаторы, на основе которых можно наглядно понять какие параметры тем или иным образом влияют на работу нейронных моделей и применять эти знания в будущем.

нейронные сети, классификатор, обучающая платформа.

Нейронная сеть – современная математическая модель, построенная по принципу организации и функционирования биологических нейронных

сетей – сетей нервных клеток живого организма. Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы. У нейронов в таких сетях есть веса нейронов [1]. Это числовые значения, которые определяют силу связи между входными сигналами и выходным сигналом нейрона. Они представляют собой параметры модели нейронной сети, которые подстраиваются в процессе обучения для оптимизации работы сети. Каждый входной сигнал умножается на соответствующий вес и суммируется, после чего применяется функция активации для получения выходного сигнала [1]. Функция активации – это математическая функция, которая определяет выходной сигнал текущего нейрона. Она необходима для того, чтобы нелинейно преобразовывать входные данные и повышать возможность моделирования сложных зависимостей между входными и выходными данными. Различные функции активации имеют свои особенности и применяются в зависимости от конкретных задач.

Обучение нейронной сети проходит с помощью алгоритма обратного распространения ошибки (*backpropagation*) [1]. Backpropagation – алгоритм обучения нейронной сети, который используется для подстройки весов между нейронными слоями на основе оценки ошибки выходных данных. Он работает путем расчета ошибки от выходного слоя сети к ее входному слою, позволяя определить оптимальные значения весов, которые минимизируют ошибку сети.

Важным фактором при работе с нейронными сетями является понимание и прогнозирование результатов модели, основанное на знаниях о влиянии различных параметров нейронной сети на ее поведение и выводы.

В первую очередь стоит обратить внимание на количество скрытых слоев нейронной сети и нейронов в них [2]. Скрытые слои (*hidden layers*) – это слои, которые находятся между первым (входным) и последним (выходным) слоями нейронной сети. Они включают множество нейронов, которые, работая вместе, могут выполнять более сложные вычисления и способны замечать множество закономерностей во входных данных. Чем больше скрытых слоев в нейронной сети, тем больше ее возможности. Однако, большее количество скрытых слоев приводит к большему использованию вычислительных ресурсов, из–за чего нейронная сеть обучается дольше.

Не менее важный параметр – скорость обучения (*learning rate*) [2]. Это параметр нейронной сети, который определяет, насколько быстро или медленно изменяются веса нейронов при обучении. Он определяет шаг изменения параметров во время каждого обновления весов, когда сеть учится на данных. Скорость обучения влияет на процесс обучения нейронной сети. Выбор неправильного значения может привести к проблеме «осцилляции». Это означает, что веса нейронной сети начинают колебаться в течение процесса обучения, что затрудняет сходимость модели. Слишком высокая скорость обучения может привести к тому, что веса нейронной сети меняются

слишком быстро, поскольку learning rate является множителем в алгоритме обратного распространения ошибки, в результате чего обучение становится почти невозможным. С другой стороны, если скорость обучения слишком низкая, нейронная сеть может сходиться к решению только в очень медленном темпе, что может увеличить время обучения.

Третий параметр – количество эпох обучения [2]. Это параметр нейронной сети, который отвечает за количество проходов полного набора данных через нейронную сеть во время обучения. Одна эпоха обучения означает, что вся обучающая выборка была использована для обновления весов нейронной сети один раз. Увеличение количества эпох обучения может повысить точность модели. Однако, также возможно, что слишком большое число эпох обучения может привести к переобучению нейронной сети – ситуации, когда модель слишком хорошо показывает себя на обучающих данных, но плохо справляется с новыми данными.

Для проверки качества работы нейронного классификатора используются различные классы задач, представленные на рис. 1, которые помогают определить, насколько хорошо сеть способна разделять данные на классы [3].

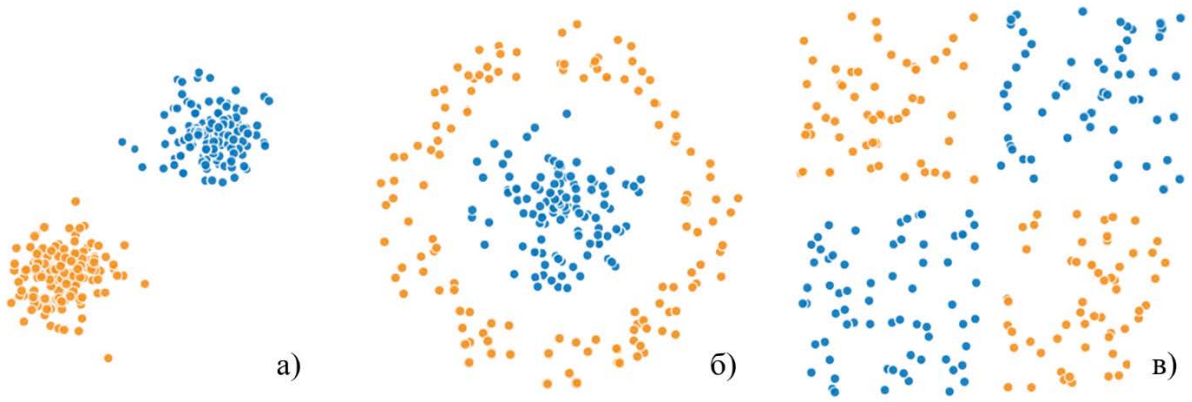


Рис. 1. Виды разделений данных: а) линейное, б) кольцевое, в) шахматное

Линейное разделение данных – это задача, в которой данные можно разделить на две категории с помощью прямой линии. Такая задача относительно проста и может быть решена даже простой нейронной сетью без скрытых слоев.

Кольцевое разделение данных – это задача, в которой данные расположены в виде двух концентрических кругов. Нейронная сеть должна научиться разделять данные на две категории по кольцу. Данная задача более сложная, и для ее решения обычно используются несколько скрытых слоев.

Шахматное разделение данных – это задача, в которой данные расположены в виде чередующихся клеток шахматной доски. Нейронная сеть

должна научиться разделять данные на две категории с помощью чередующихся прямых линий. Эта задача самая сложная из трех и требует использования нескольких скрытых слоев и большого количества нейронов.

Таким образом, пользователь сможет тестировать работу своей нейронной сети с заданными параметрами, прежде чем применять модель с этими параметрами для решения реальных задач.

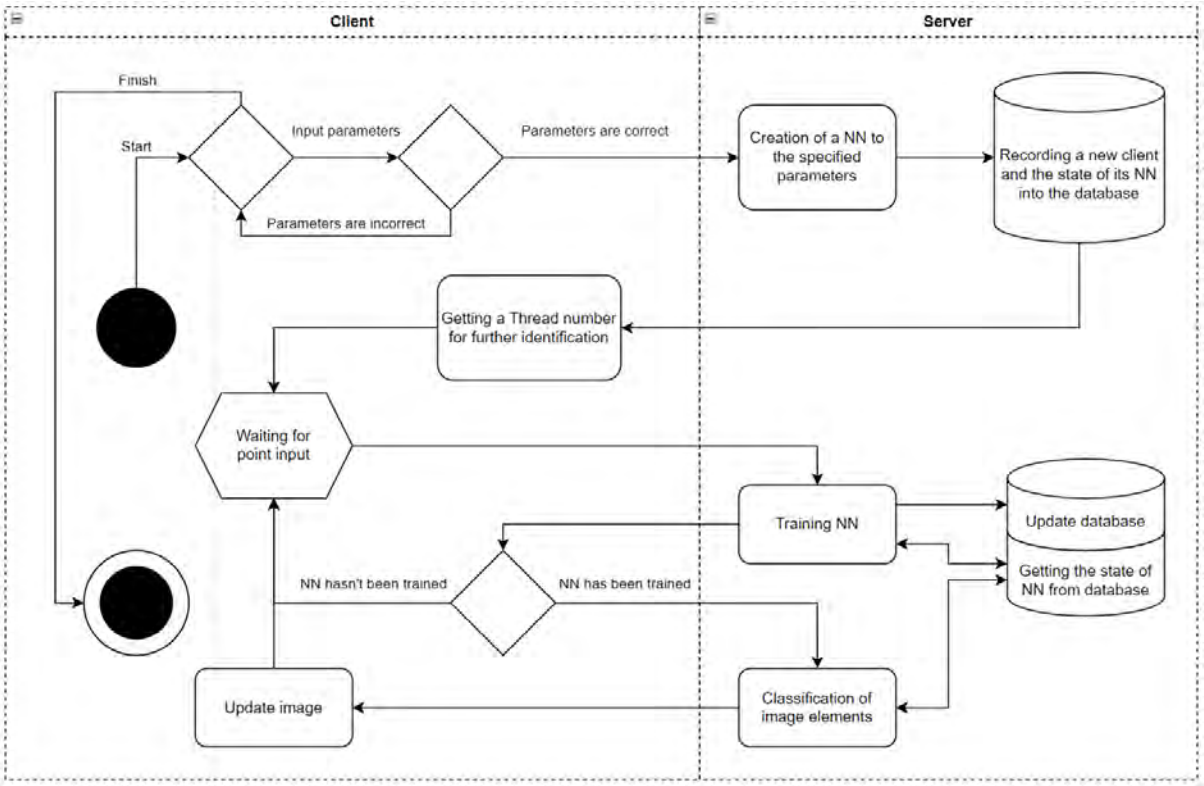


Рис. 2. Диаграмма работы приложения

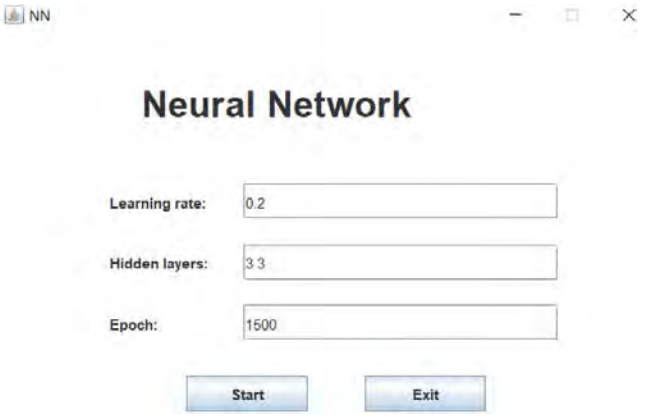


Рис. 3. Стартовое окно программы

Реализованная в программе нейросеть представляет собой полносвязный персептрон с двумя нейронами во входном и выходном слоях и сигмоидной функцией активации. Сама программа написана на языке Java и представляет собой клиент-серверное приложение с приятным и понятным пользовательским интерфейсом [4]. На рис. 2 описана схема работы программы. Сначала со стороны клиента инициализируется окно, куда вводятся три параметра: количество скрытых слоев и нейронов в них, скорость обучения и количество эпох обучения, стартовое окно программы представлено на рис. 3.

Затем эти данные отправляются на сервер, где по заданным параметрам инициализируется новая нейронная сеть, а клиенту выдается его индивидуальный номер. Под этим номером информация о нейронной сети записывается в базу данных для дальнейшей работы. Затем на стороне клиента инициализируется новое окно, куда пользователь может вводить два класса точек с помощью левой и правой клавиш мыши. Для наглядности точки разделены на желтый и розовый цвета соответственно. Когда клиент расставит все необходимые ему данные, он сможет нажать на колесико мыши и информация о расставленных точках отправится на сервер. Сервер по индивидуальному номеру клиента загрузит информацию о его нейросети из базы данных для дообучения. После прохождения указанного клиентом количества эпох обучения, сервер сообщит клиенту о завершении процесса обучения нейронной сети и затем откроет соединение на передачу информации о размеченном на классы изображении. Клиент после получения этих данных обновит изображение в окне пользователя. Затем пользователь сможет дополнять данные новыми точками при необходимости. Демонстрация разделения изображения в пользовательском окне представлена на рис. 4.

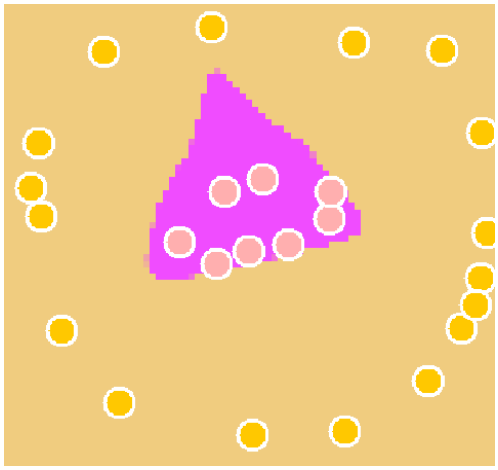


Рис. 4. Демонстрация разделения

Написанная программа поможет в развитии интереса к нейронным сетям, углублении знаний о работе нейронных моделей, понимании взаимосвязей между результатами моделей и ее основными параметрами.

Список используемых источников

1. IBM Neural Network Topic. URL: https://www.ibm.com/topics/neural–networks (дата обращения 01.02.2023).

2. Гафаров Ф. М., Галимянов А. Ф. Искусственные нейронные сети и приложения: учеб. пособие. Казань : Казанский университет, 2018. 121 с.

3. Four Types of Classification Tasks in Machine Learning. URL: https://machinelearningmastery.com/types–of–classification–in–machine–learning/ (дата обращения 01.02.2023).

4. Java documentation. URL: https://dev.java/learn/ (дата обращения 01.02.2023).

Статья представлена доцентом кафедры ПиВТ СПбГУТ, кандидатом технических наук Т. И. Белой.

УДК 004.032.26
ГРНТИ 28.23.37

АНАЛИЗ ФУНКЦИЙ ПОТЕРЬ ДЛЯ ОБУЧЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ИДЕНТИФИКАЦИИ ЛИЦ

А. А. Березкин, С. А. Васильев, Л. А. Николаева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается понятие лосс-функции относительно применения данных функций для идентификации лиц в системах транспортной безопасности. Функция потерь – это математическая функция, по которой производится расчет ошибок работы модели при сравнении полученного от модели ответа с корректным ответом. Чем выше полученное значение, тем хуже модель распознавания лиц справляется с работой. В статье приводится обзор функций потерь, применимых для обучения пайплайна по распознаванию лиц и отмечены оптимальные решения с учетом специфики работы с большим количеством лиц.

распознавание лиц, детекция лиц, вектор биометрии, функции потерь, softmax loss, margin-based loss.

В рамках проекта Алкозамок была поставлена задача разработать инструмент для идентификации водителей большегрузных транспортных средств в целях повышения безопасности дорожного движения. Для решения задачи был создан пайплайн для распознавания лиц, в основу которого легла opensource-библиотека dlib.

Пайплайн принимает на вход полученное с камеры изображение лица водителя. Результатом работы пайплайна является 128-мерный вектор лица, которое было на изображении. Полученный вектор сравнивается с теми векторами, которые есть в базе данных пайплайна. Решение о том, один и тот же человек изображен на фото из базы данных и на полученном из камеры изображении или же это разные люди, принимается на основе сравнения векторов [1].

Общая схема работы пайплайна состоит из пяти последовательных шагов: 1. Детектирования лица. 2. Определение ключевых точек. 3. Выравнивание лица на кадре. 4. Получение вектора биометрии. 5. Сравнение полученного вектора по базе данных лиц, допущенных к управлению транспортным средством.

Основной показатель качества работы пайплайна – это его точность. Требуемая точность – 95 %. Это означает, что в 95 % случаев пайплайн должен давать корректный ответ на вопрос: «Эти изображения принадлежат одному и тому же человеку, или разным людям?». Соответственно, процент

ошибок (как ложноположительных, так и ложноотрицательных ответов) должен не превышать 5 %.

В настоящий момент ключевой проблемой пайплайна является то, что точность не соответствует требуемой – пайплайн ошибается более, чем в 5 % случаев. Основным способом решения проблемы может стать дальнейшее обучение пайплайна. Для обучения необходимо применение функции потерь (лосс-функции), т. к. лосс-функции играют ключевую роль в развитии наиболее точных моделей распознавания лиц [2].

Функция потерь (лосс-функция) – это математическая функция, по которой производится расчет ошибок работы модели при сравнении полученного от модели ответа с корректным ответом. Механизм работы лосс-функции следующий: функция принимает два параметра – прогнозируемые выходные данные и истинные выходные данные. Если то, что модель прогнозирует далеко от истинного значения, то и значение функции будет высоким. Соответственно, чем выше значение функции, тем хуже работает модель. Значение функции также называют штрафом [3].

К настоящему моменту разработано множество лосс-функций, используемых для обучения систем распознавания лиц. Мей Ванг в своей работе подразделяет все лосс-функции для обучения систем распознавания лиц на три типа: функции потерь на основе евклидова расстояния (*Euclidean-distance based loss*), функции потерь на основе угла/косинусного расстояния (*Angular/cosine-margin based loss*) и функции потерь на основе Softmax loss и ее вариаций [4].

Функции потерь на основе евклидова расстояния – это метрический метод обучения, который встраивает изображения в евклидово пространство, в котором интрадисперсия уменьшается, а интервариантность увеличивается. Самые распространенные функции потерь данного типа – это Contrastive loss и Triplet loss. Contrastive loss сопоставляет пары изображений лица, а затем сближает положительные (похожие) пары и раздвигает отрицательные (непохожие) пары [4].

В отличие от Contrastive loss, которая учитывает абсолютные расстояния между совпадающими и несовпадающими парами, Triplet loss учитывает относительную разницу расстояний между ними. Для этого используются триплеты лиц, а затем минимизируется расстояние между полученным вектором и положительным образцом (лицом того же человека) и максимизируется расстояние между полученным вектором и отрицательным образцом (лицом другого человека).

Функция потерь Triplet loss выглядит следующим образом:

$$L_{Triplet} = \sum_i^N \left[||f(x_i^a) - f(x_i^p)||_2^2 - ||f(x_i^a) - f(x_i^n)||_2^2 + \alpha \right], ,$$
$$\forall (f(x_i^a), f(x_i^p), f(x_i^n)) \in T$$

где α – это область (граница) между положительной и отрицательной парами изображений, T – множество всех возможных «троек» в обучающем множестве, имеющее мощность N, $f(x)$ – embedding, сгенерированный моделью по изображению x. Метрика расстояния представляет собой квадрат евклидова расстояния.

Triplet loss используется в инструменте для распознавания лиц FaceNet, разработанном Google.

Функции потерь на основе косинусного расстояния основаны на широко используемой для задачи распознавания лиц функции потерь Softmax loss. Граница решения в Softmax loss равна $(W1 - W2)\,x + b1 - b2 = 0$, где x – полученный вектор входного изображения, Wi – веса слоя классификации и bi – свободный член в Softmax loss [4].

Функция потерь Softmax Loss после добавления Cross Entropy для вычисления штрафа имеет следующий вид:

$$L_{Softmax} = -\frac{1}{N}\sum_{i=1}^{N}\log\left(\frac{e^{W_{y_i}^T x_i + b_{y_i}}}{\sum_{j=1}^{C} e^{W_j^T x_i + b_j}}\right),$$

где y_i – индекс центроида класса, x_i – вектор признаков i-го образца, относящийся к y_i-му классу, N – размер батча, n – номер класса обучающего множества [3].

Основные современные лосс-функции базируются на нормализованной функции Softmax loss – N-Softmax, в которой применяется косинус угла между вектором, полученным в результате обработки изображения и вектором центроида класса.

Однако при больших различиях внутри класса Softmax хуже справляется с задачей, т. к. расстояние между изображениями на границах близких классов может быть меньше, чем расстояние между некоторыми изображениями одного класса. Решением данной проблемы стало добавление между этими пространствами пустой области – margin. Данное решение используют функции Large-Margin Softmax Loss [5], CosFace [6], ArcFace (*Additive Angular Margin Loss function*) [7] и другие лосс-функции.

Функции потерь на основе нормализации признаков и весов Softmax loss – модификации метода Softmax для улучшения качества его работы. В 2017 году, в дополнение к преобразованию Softmax loss в Angular/cosine-margin based loss, некоторые авторы делали попытки нормализовать признаки и веса функции Softmax loss для повышения производительности модели, что можно записать следующим образом:

$$\widehat{W} = \frac{W}{||W||}, \hat{x} = \alpha\frac{x}{||x||},$$

где α – параметр масштабирования, x – вектор изученных признаков, W – вес последнего полносвязного слоя [4].

Данное решение применяется в лосс-функциях CoCo loss, а также von MisesFisher (vMF) mixture model.

При выборе лосс-функции для пайплайна распознавания лиц можно опираться на многочисленные исследования. По данным исследования Шривастава, ArcFace показывает высокую эффективность — при обучении на наборе данных CASIA-Webface с использованием этой функции точность распознавания составила 99,35 %. Результаты, полученные в работе Шривастава подтверждают результаты создателей функции, полученные еще в 2015 году при разработке ArcFace [7]. Другие лосс-функции, принимающие участие в исследовании в порядке убывания их эффективности: Additive Margin Softmax, Angular Softmax, Marginal Loss и Cross Entropy (*Softmax*). Впрочем, стоит отметить, что все указанные функции показывают хорошие результаты [8].

Учитывая высокую эффективность применения функции потерь ArcFace, данную функцию следует рассматривать для обучения и совершенствования работы разрабатываемого пайплайна по распознаванию лиц. Если требуемая точность модели не будет достигнута в обучении модели с помощью функции ArcFace, имеет смысл рассмотреть такие решения как Additive Margin Softmax, Angular Softmax, Marginal Loss.

Список используемых источников

1. Как на самом деле работает распознавание лиц. URL: https://habr.com/ru/company/ntechlab/blog/586770/ (дата обращения 15.02.2023).

2. Zhang Xiao et al. “AdaCos: Adaptively Scaling Cosine Logits for Effectively Learning Deep Face Representations” // 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), June 2019.

3. Не царская у тебя физиономия! Функции потерь для задачи распознавания лиц. URL: https://habr.com/ru/company/ntechlab/blog/531842/ (дата обращения 15.02.2023).

4. D. Wang, Mei, and Weihong Deng. “Deep Face Recognition: A Survey” // Neurocomputing. Mar. 2021. Vol. 429. PP. 215–244.

5. Large-Margin Softmax Loss for Convolutional Neural Networks. Weiyang Liu, Yandong Wen, Zhiding Yu and Meng Yang // Proceedings of the 33rd International Conference on Machine Learning. 2016. PP. 507–516.

6. Wang, Hao, et al. “CosFace: Large Margin Cosine Loss for Deep Face Recognition” // 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, June 2018.

7. Deng, Jiankang, et al. “ArcFace: Additive Angular Margin Loss for Deep Face Recognition” // IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021.

8. Srivastava Y., Murali V., Dubey S. R. A Performance Evaluation of Loss Functions for Deep Face Recognition // In: R. V. Babu, M. Prasanna, V. P. Namboodiri (eds) Computer Vision, Pattern Recognition, Image Processing, and Graphics. NCVPRIPG 2019. Communications in Computer and Information Science. Springer, Singapore. 2020. Vol. 1249.

УДК 004.896
ГРНТИ 28.23.37

ОБЗОР РЕШЕНИЙ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ МИНИМИЗАЦИИ ЗАДЕРЖКИ В СПУТНИКОВЫХ СЕТЯХ СВЯЗИ

А. А. Березкин, Х. Ф. До, Р. В. Киричек

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Эта статья предоставляет обзор различных решений, которые используют техники искусственного интеллекта для минимизации задержек в спутниковых коммуникационных сетях. Высокая задержка, связанная с спутниковыми связями, может значительно влиять на производительность различных приложений, таких как потоковое видео в режиме реального времени и телемедицина, что приводит к плохому пользовательскому опыту. Использование ИИ в спутниковых коммуникационных сетях может помочь преодолеть эти проблемы, оптимизируя различные параметры сети, такие как выделение пропускной способности, маршрутизация и коррекция ошибок. В статье обсуждаются несколько решений на основе ИИ, в том числе техники машинного обучения и обучения с подкреплением, которые были предложены для улучшения эффективности и надежности спутниковых коммуникационных сетей. Кроме того, обсуждаются преимущества и ограничения этих решений, а также потенциальные области для будущих исследований.

сеть спутниковой связи, минимизация задержек, искусственный интеллект, прогнозирующее моделирование.

Введение

Спутниковые сети [1] растут из-за спроса на связь в удаленных районах, но задержка является основной проблемой. Она может быть вызвана различными факторами, включая атмосферные помехи и расстояние между спутником и приемником. Применение искусственного интеллекта (ИИ) [2] в спутниковых сетях может уменьшить задержку, оптимизировать маршрутизацию пакетов данных, предсказывать помехи и выделять пропускную способность. Алгоритмы машинного обучения позволяют анализировать данные и создавать предсказания о производительности сети, помогая операторам принимать решения об оптимизации её работы.

Поскольку спрос на спутниковую связь продолжает расти, необходимость в эффективных и надежных спутниковых коммуникационных сетях будет становиться все более важной. Применяя ИИ для уменьшения задержки и улучшения производительности и безопасности сети, операторы

спутников могут обеспечить высочайший уровень обслуживания своих клиентов. Это будет особенно важно, когда новые приложения, такие как автономные транспортные средства и Интернет вещей, будут требовать передачи данных в режиме реального времени с низкой задержкой.

AI-решения для минимизации задержек в сетях спутниковой связи

Спутниковые коммуникационные сети широко используются в телекоммуникациях, трансляции и авиации. Однако, задержка связи может быть вызовом, который может быть решен с помощью ИИ. Методы, такие как маршрутизация на основе машинного обучения, предиктивная модель, умное кэширование, когнитивное радио и формирование луча, могут сократить задержку при передаче данных в спутниковых сетях.

Спутниковые сети [3] имеют уникальные проблемы, такие как ограниченная пропускная способность, высокая задержка и помехи сигнала, которые могут повлиять на производительность маршрутизации данных. Алгоритмы машинного обучения [4] могут помочь решить эти проблемы, оптимизируя маршрутизацию данных в режиме реального времени. Таблица 1 показывает несколько алгоритмов маршрутизации на основе машинного обучения для минимизации задержки в спутниковых сетях.

ТАБЛИЦА 1. Некоторые алгоритмы маршрутизации, основанные на машинном обучении

№ пп	Алгоритмы	Краткое описание
1	Алгоритм маршрутизации на основе обучения с подкреплением	Этот алгоритм использует обучение с подкреплением для улучшения решений по маршрутизации на основе опыта прошлых событий.
2	Маршрутизация на основе генетического алгоритма	Этот алгоритм использует генетический алгоритм для поиска оптимального пути передачи данных через сеть.
3	Алгоритм маршрутизации на основе искусственной нейронной сети	Этот алгоритм использует нейронную сеть для изучения оптимального маршрута передачи данных на основе распознавания исторических шаблонов.

Предиктивное моделирование [5] – техника, использующая статистические и алгоритмы машинного обучения для прогнозирования будущих событий на основе исторических данных. Некоторые популярные алгоритмы:

- Алгоритм долгой краткосрочной памяти (LSTM) [6] – это тип рекуррентной нейронной сети, который может использоваться для прогнозирования будущих шаблонов трафика в сети. LSTM-сети хорошо подходят для анализа временных рядов, потому что они могут захватывать долгосрочные

зависимости в данных и могут обрабатывать последовательности переменной длины.

- Алгоритм градиентного бустинга [7] объединяет несколько слабых обучателей, чтобы создать сильного обучателя для прогнозирования будущих шаблонов трафика в сети.

Умное кэширование [8] хранит часто запрашиваемые данные ближе к пользователю, уменьшая необходимость извлечения данных из центрального сервера. Использование искусственного интеллекта для интеллектуального кэширования данных на основе поведения пользователя может уменьшить задержку в спутниковой сети.

Когнитивное радио [9] динамически настраивает параметры передачи спутника на основе условий в сети. С использованием алгоритмов искусственного интеллекта спутник может выбирать лучшую частоту и уровень мощности для минимизации задержки. Таблица 2 показывает варианты алгоритмов когнитивного радио.

Лучеобразование [10] – это техника, которая используется для фокусировки энергии передачи спутника в определенном направлении. Искусственный интеллект может использоваться для настройки направления луча на основе местоположения пользователя, оптимизируя силу сигнала и уменьшая задержку.

ТАБЛИЦА 2. Некоторые алгоритмы когнитивного радио

№ пп	Алгоритмы	Краткое описание
1	Алгоритм определения спектра	Этот алгоритм определяет доступность спектра в спутниковых сетях, чтобы уменьшить задержку.
2	Алгоритм выбора канала	Этот алгоритм выбирает оптимальные каналы для передачи данных в спутниковых сетях, чтобы уменьшить задержку.
3	Алгоритм управления мощностью	Данный алгоритм оптимизирует мощность передачи когнитивного радио, уменьшая помехи для других устройств в спутниковых сетях и повышая отношение сигнал/шум для уменьшения задержки.
4	Алгоритм динамического доступа к спектру	Этот алгоритм динамически распределяет оступный спектр для когнитивных радиостанций в спутниковых сетях.

Анализ преимуществ и недостатков различных решений

Сети спутниковой связи критически важны для различных отраслей, но задержка в них может привести к нарушениям связи, потере данных и снижению производительности. Решения на основе искусственного интеллекта могут минимизировать задержки и повысить эффективность сетей.

В таблице 3 представлен анализ преимуществ и недостатков различных решений.

ТАБЛИЦА 3. Краткий анализ преимуществ и недостатков различных решений

№ пп	Типы	Преимущества	Недостатки
1	Маршрутизация на основе машинного обучения	Машинное обучение анализирует данные и оптимизирует маршрутизацию, распознавая закономерности.	Получение достаточного количества данных для обучения алгоритмов машинного обучения в спутниковых сетях может быть сложной задачей.
2	Прогностическое моделирование	Прогностическое моделирование может прогнозировать перегрузки и планировать емкость сети, минимизируя з адержку.	Неточность прогнозов может быть вызвана недостаточностью данных для прогностического моделирования.
3	Интеллектуальное кэширование	Интеллектуальное кэширование минимизирует задержку	Ограниченный объем хранения на спутнике затрудняет интеллектуальное кэширование для редко используемых данных
4	Когнитивное радио	Когнитивное радио выбирает лучшую частоту и мощность для оптимальной силы сигнала на спутниках	Ограниченные вычислительные ресурсы на спутниках и помехи ухудшают качество сигнала
5	Лучеобразование	Лучеобразование оптимизирует силу сигнала для минимизации задержки путем направления энергии передачи для более быстрого приема и ответа.	Ограниченные вычислительные ресурсы на спутниках и помехи ухудшают качество сигнала и делают лучеобразование неэффективным.

Обсуждение проблем и перспектив развития

Использование ИИ в сетях спутниковой связи для минимизации задержек показало многообещающие результаты, но вызывает некоторые проблемы и вызовы. Доступность и качество данных являются значительными вызовами, так как производительность моделей машинного обучения сильно зависит от качества и количества данных. Качество данных может быть повреждено шумом сигнала, задержкой и ограничением пропускной способности. Получение соответствующих данных для обучения в своевременном порядке может также ограничить эффективность ИИ-решений. Высокие требования к вычислительным ресурсам являются вызовом для ИИ-решений на спутниковых системах с ограниченными ресурсами. Многие ИИ-решения требуют принятия решений в режиме реального времени, что может создавать дополнительное напряжение на сетях спутниковой связи.

Тем не менее, перспективы развития ИИ-решений в сетях спутниковой связи обещают быть многообещающими.

Заключение

Минимизация задержек в сетях спутниковой связи критична для многих приложений, таких как дистанционное зондирование, спутниковая навигация и мобильные сервисы. Использование искусственного интеллекта (ИИ) показало многообещающие результаты в снижении задержки и улучшении производительности сети. ИИ-решения в сетях спутниковой связи обещают многое, несмотря на вызовы, такие как качество и доступность данных, вычислительные ресурсы и решения в режиме реального времени. Достижения в технологии ИИ, вычислительном оборудовании и технологиях спутниковой связи, а также интеграция ИИ-решений с новыми технологиями обеспечивают перспективное будущее для минимизации задержки и улучшения производительности сетей.

Список используемых источников

1. Lu Kun, et al. "Applications and prospects of artificial intelligence in covert satellite communication: a review" // Science China Information Sciences. 2023. N 66.2. PP. 1–31.

2. Fourati Fares, and Mohamed-Slim Alouini. "Artificial intelligence for satellite communication: A review" // Intelligent and Converged Networks. 2021. N 2.3. PP. 213–243.

3. Furano Gianluca, et al. "Towards the use of artificial intelligence on the edge in space systems: Challenges and opportunities" // IEEE Aerospace and Electronic Systems Magazine. 2020. N 35.12. PP. 44–56.

4. Nayak Padmalaya, et al. "Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities" // Measurement. 2021. N 178. 108974.

5. Dissanayake Asoka, Jeremy Allnutt, and Fatim Haidara. "A prediction model that combines rain attenuation and other propagation impairments along earth-satellite paths" // IEEE Transactions on Antennas and Propagation. 1997. N 45.10 PP. 1546–1558.

6. Muthukumar Pratyush, et al. "Real-time spatiotemporal air pollution prediction with deep convolutional lstm through satellite image analysis" // Advances in Data Science and Information Engineering: Proceedings from ICDATA 2020 and IKE 2020. Springer International Publishing, 2021.

7. Cárdenas, Leticia Lemus, Juan Pablo Astudillo León, and Ahmad Mohamad Mezher. "GraTree: A gradient boosting decision tree based multimetric routing protocol for vehicular ad hoc networks" // Ad Hoc Networks. 2022. N 137. 102995.

8. Seetharam Anand. "On caching and routing in information-centric networks" // IEEE Communications Magazine. 2017. N 56.3. PP. 204–209.

9. Wang Beibei, and KJ Ray Liu. "Advances in cognitive radio networks: A survey" // IEEE Journal of selected topics in signal processing. 2010. N 5.1 PP. 5–23.

10. Lin Zhi, et al. "Secrecy-energy efficient hybrid beamforming for satellite-terrestrial integrated networks" // IEEE Transactions on Communications. 2021. N 69.9. PP. 6345–6360.

УДК 004.75
ГРНТИ 81.93.29

МОДЕЛЬ БЕЗОПАСНОСТИ ДЛЯ МЕДИЦИНСКИХ КОММЕРЧЕСКИХ УЧРЕЖДЕНИЙ

Э. В. Бирих, К. М. Богомедова, Д. В. Сахаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье была составленна модель безопасности для медицинских коммерческих предприятий, на основе модели угроз, модели нарушителя и существующих законов и указов.

информационная безопасность, модель безопасности, вирусы, утечка информации, утечка данных, Федеральная служба безопасности России (ФСБ России), Минцифры России, отдел информационной безопасности.

Введение

Одной из главных задач по защите предприятия является моделирование системы информационной безопасности. Защита на каждом предприятии выстраивается индивидуально, что является необходимым фактором для сохранения конфиденциальной информации, ее целостности и непосредственно доступности.

Учреждения здравоохранения постепенно переходят на работу с электронными носителями, если оставить данные предприятия без защиты, это влечет за собой утечку данных, уменьшение бюджета предприятия [1]. Из этого вытекают последствия и для сотрудников, и для клиентов.

Последствия ненадежной модели безопасности

Чаще всего, проблема утечек данных, объясняется на этапе внедрения вирусного ПО. Из-за плохо составленной модели безопасности, вирус легко проникает на рабочие станции сотрудников, а плохая осведомленность, помогает вирусу распространиться.

Инцидент в Ascen Clinical, привел к утечке данных около 70 000 больных. Причиной утечки стала ссылка из письма. Благодаря проникновению вредоносного ПО на одну из АРМ, злоумышленники получили все персональные данные пациентов, в том числе и номера страхования.

Самая масштабная атака 2021 г. – атака вымогателя Ryuk на сеть медучреждений UHS. Компьютеры работников не загружались, на них появилось требование о выкупе [2]. Данный инцидент помешал работе врачей,

данные пациентов оказались скомпрометированы, компании пришлось оплатить выкуп.

Модель угроз

Модель угроз является одним из важных подпунктов при составлении модели безопасности на предприятии. При составлении модели безопасности необходимо опираться на методические документы утвержденные ФСТЭК России:

- Приказ ФСТЭК России от 15 февраля 2008 г. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн.
- Приказ ФСТЭК России от 15 февраля 2008 г. Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн.
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Модель нарушителя

Существует две основные группы нарушителей:

- Внешние нарушители.
- Внутренние нарушители.

Внешний нарушитель не имеет доступа к защищаемой информации, из чего следует его неспособность воздействовать на систему по техническим канал связи, при условии хорошей защищенности предприятия.

Воздействие же внутреннего нарушителя значительно выше внутреннего, но регулируется же степень воздействия учреждением.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе осуществляет техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).
- администраторы конкретных подсистем или баз данных (категория II);
- пользователи ИСПДн (категория III);

- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн.

Информационная безопасность в бюджетных медицинских учреждениях

В каждом бюджетном медицинском учреждении обязан быть отдел информационной безопасности, также медицинским организациям запрещено использование средства защиты информации, происхождение которых из недружественных государств [3]. Все это следует из подпункта б) пункта 1 Указа Президента Российской Федерации от 01.05.2022 № 250.

Сотрудники отдела информационной безопасности отвечают за безопасную и бесперебойную работу серверного оборудования, АРМ и средств защиты (СЗИ ВИ, Межсетевой экран, система обнаружения вторжений и т. д.). Сотрудники отдела информационной безопасности обязаны быстро реагировать на попытку вторжения и предотвращать ее, обязаны проводить аудит своевременно. Разработка модели безопасности предприятия также входит в основные обязанности сотрудников отдела информационной безопасности.

Так как медицинские бюджетные учреждения обязывают создавать свой отдел безопасности, многие выходят из данной ситуации назначая готовый IT-отдел новыми обязанностями. Рассмотрим минусы и плюсы такого подхода в таблице 1.

ТАБЛИЦА 1. Перевод сотрудника

Преимущества	Недостатки
1 Экономия бюджета	1 Неэффективная работа сотрудников при обнаружении уязвимостей
2 Знания сотрудников IT-отдела помогут в решении проблем с вышедшими из строя АРМ и другими техническими средствами	2 Невозможность провести инструктаж по организации работы сотрудников, работающих с МИС, дабы избежать утечек информации
3 Разработка ПО для безопасного хранения информации	3 Некомпетентность скажется на случайной утечке данных
4 Знакомая система управления, вследствие легкое обнаружение инцидентов	4 Незнание принципов реагирования на инциденты приведет к утечке данных

Проанализировав таблицу 1 становится ясно, что при назначении сотрудника из IT-отдела на новую должность, защита будет неэффективной

из-за специализации сотрудника, даже при условии высокой защиты со стороны технической части [4]. Стоит также отметить, что для более эффективной защиты информации необходимо участие IT-отдела.

Несмотря на то, что модель безопасности на каждом учреждении составляется индивидуально, перечисленные выше требования к безопасности для всех бюджетных медицинских организаций являются одинаковыми и обязательными, а их исполнение контролируются ФСТЭК России, ФСБ, Минцифры России и Роскомнадзор.

Коммерческие медицинские организации

При разработке модели безопасности, необходимо опираться на существующие указы и законы. Для начала нужно выявить модели угроз, т. к. обеспечение безопасности данных достигается определением угроз безопасности, что сказано в части 2 статьи 19 № 152-ФЗ «О персональных данных». В модели угроз должна содержаться информация, которая следует из 17-го Приказа ФСТЭК, а именно:

- описание информационной системы предприятия;
- описание возможных угроз безопасности для учреждения;
- модель нарушителя;
- уязвимости;
- возможные способы реализации угроз;
- последствия от нарушения свойств безопасности информации.

Необходимо все тщательно проанализировать и исключить те угрозы, которые являются для предприятия нежелательными [5]. Если основываться, только на нормативные документы, то необходимо исключить все угрозы, последствиями исполнения которых является утечка данных, как работников учреждения, так и клиентов.

Выявление актуальности угрозы является одним из важных шагов для сохранения конфиденциальности предприятия (табл. 2).

ТАБЛИЦА 2. Правила отнесения угрозы к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

После формирования модели угроз и выявления потенциальной опасности, необходимо составить план о борьбе с данными угрозами [6]. Для этого нужно подобрать оборудования для защиты информационных систем

предприятия, которые прописаны в приказе ФСТЭК России от 18 февраля 2013 г. № 21.

Вывод

В исследовательской работе была изучена модель безопасности, ее составляющие, выявлены наиболее частые причины утечки информации и последствия таких утечек. Была проанализирована модель безопасности бюджетных медицинских учреждений, и составлена на ее основе, модель безопасности для коммерческих медицинских учреждений.

Список используемых источников

1. Керейтова М. Р., Малыш В. Н. Информационная безопасность в медицинских информационных системах [Электронный ресурс] // Труды международного симпозиума «Надежность и качество». Компьютерные и информационные системы: электрон. научн. журн. 2020. С. 1–2. URL: Информационная безопасность в медицинских информационных системах (дата обращения 15.02.2023).

2. Горбунов П. А., Гулиев Я. И., Михеев А. Е., Назаренко Г. И., Фохт И. А., Фохт О. А. Особенности решения проблем информационной безопасности в медицинских информационных системах [Электронный ресурс] // Врач и информационные технологии. Компьютерные и информационные науки: электрон. науч. журн. 2020. С. 37–44. URL: https://www.idmz.ru/jurnali/vrach-i-informatsionnye-tekhnologii (дата обращения 15.02.2023).

3. Ларина И. А., Михеев А. Е., Ованесян А. А. Подходы к повышению безопасности пациентов средствами мис [Электронный ресурс] // Врач и информационные технологии. Компьютерные и информационные науки: электрон. науч. журн. 2020. С. 37–44. URL: https://www.idmz.ru/jurnali/vrach-i-informatsionnye-tekhnologii (дата обращения 15.02.2023).

4. Мамедова М. Г. Информационная безопасность персональных медицинских данных в электронной среде [Электронный ресурс] // İnformasiya texnologiyaları problemləri. Безопасность, защищённость данных: электрон. научн. журн. 2020. С. 1–13 URL: https://www.the_information_security_of_personal_medical_data_in_an_electronic_environment.pdf (jpit.az) (дата обращения 15.02.2023).

5. Малышенко И. С., Бочко Е. К. Информационная безопасность в медицинских информационных системах // Научное сообщество студентов. Междисциплинарные исследования. XV студенческая всероссийская научно-практическая конференция с международным участием. Новосибирск : АНС «СибАК», 2017. N 4 (15). С. 12–18.

6. Цыбина Т. С. Информационная безопасность в медицине // Компьютерные технологии в моделировании, управлении и экономике. XIII студенческая всероссийская научно-практическая конференция с международным участием. М. : Среднерусский институт управления, 2021. С. 183–203.

УДК 004.056
ГРНТИ 81.96

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ОТКРЫТЫХ ТЕЛЕКОММУНИКАЦИОННЫХ КАНАЛАХ СВЯЗИ

Э. В. Бирих, Д. В. Сахаров, Е. В. Таров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются современные методы и алгоритмы, на которых основываются криптографические методы защиты информации при ее передаче по открытым телекоммуникационным каналам связи. Проводится анализ данных методов. В результате анализа предложены меры, способствующие повышению безопасности информации, передаваемой по открытым каналам связи.

информационная безопасность, криптография, каналы связи.

Развитие информационных технологий приводит к тому, что все больше информации передается по открытым телекоммуникационным каналам связи, которые могут быть подвержены различным атакам и угрозам безопасности. В своих работах [1, 2, 3, 4, 5] Сахаров Д. В., Бирих Э. В., Красов А. В., Ушаков И. А., Глуховский М. Д., Гаврилов А. С., Сацук Е. Н., Рябов Е. Ю. рассматривают вопрос защиты средств передачи и хранения данных (каналов, сетей и информационных систем). Но наряду с обеспечением безопасности данных средств, актуальна также проблема защиты непосредственно самой информации. Потому необходимость обеспечения защиты конфиденциальности и целостности передаваемой информации становится все более востребованной.

Самым перспективным методом защиты информации, передаваемой по открытым телекоммуникационным каналам связи, является применение криптографии. Новые перспективные исследования в области криптографической защиты информации могут позволить внедрить более эффективные методы защиты данных, что будет способствовать повышению уровня безопасности информационных систем и снижению вероятности возникновения утечек и кибератак. Цель статьи – рассмотреть недостатки современных криптографических средств защиты информации в открытых телекоммуникационных каналах связи и привести более перспективные методы.

Современные средства криптографической защиты информации, применяемые в открытых телекоммуникационных каналах связи, могут включать следующее [6, 7]:

симметричное шифрование – метод шифрования, при котором применяется один секретный ключ (AES, Blowfish, DES, и TripleDES);

асимметричное шифрование – метод шифрования, при котором применяются два ключа – публичный и секретный (RSA, ECC);

хэширование – метод криптографической защиты, который позволяет преобразовать любое сообщение фиксированной длины в строку фиксированной длины (SHA-2, SHA-3, MD5);

цифровые подписи – метод криптографической защиты, который позволяет аутентифицировать отправителя сообщения и обеспечить невозможность отказа отправителя от сообщения (DSA);

протоколы обмена ключами – методы, которые обеспечивают безопасный обмен ключами между двумя или более участниками коммуникации (*Diffie-Hellman, Elliptic Curve Diffie-Hellman*);

аутентификация – процесс проверки подлинности участников коммуникации. Наиболее распространенными методами аутентификации являются парольная аутентификация и аутентификация на основе сертификатов;

VPN (*Virtual Private Network*) – технология, которая позволяет устанавливать безопасное соединение между двумя или более участниками коммуникации через открытые телекоммуникационные каналы связи. VPN использует методы криптографической защиты для защиты передаваемой информации.

Хотя современные средства криптографической защиты информации являются эффективными, но они имеют некоторые недостатки. Можно выделить следующее:

1. Симметричное шифрование нуждается в специальном механизме для осуществления передачи ключей, также данный метод имеет слабую масштабируемость и отсутствие способов обеспечения аутентификации (установления подлинности принятой информации) и неотказуемости.

2. Асимметричное шифрование решает многие данные проблемы, но при этом увеличивается время для формирования ключей и криптограмм из-за манипуляции очень большими числами и достаточно сложными математическими преобразованиями.

3. Хэширование применяется для проверки целостности данных, но может быть уязвимым к атакам типа «столкновения» или так называемая «коллизия», когда различные данные дают одинаковый хэш.

4. Цифровые подписи могут быть скомпрометированы, если злоумышленник получит доступ к закрытому ключу.

5. Протоколы обмена ключами могут быть подвержены атакам типа «человек посередине», когда злоумышленник может перехватывать и изменять сообщения.

6. VPN может обеспечивать конфиденциальность и целостность данных, но также может быть уязвимым к атакам типа «человек посередине» и может потребовать значительных вычислительных ресурсов.

Несмотря на то, что существующие методы шифрования обеспечивают достаточно высокий уровень защиты, появляются новые технологии и методы атак, которые могут преодолеть существующие протоколы защиты. В результате чего необходимо внедрение более современных и лучших мер обеспечения безопасности информации, особенно в открытых телекоммуникационных каналах связи. Исследования в области криптографии постоянно продвигаются вперед, чтобы обеспечить максимально возможную безопасность информации. В результате чего на сегодняшний день существуют перспективные меры по обеспечению большей безопасности информации. К таким мерам относятся:

– применение квантовой криптографии: использование квантовых свойств для создания безопасных криптографических протоколов, таких как квантовое распределение ключей. Этот подход обеспечивает непревзойденную защиту от подслушивания, поскольку любая попытка прослушивания изменяет состояние квантовой системы;

– применение многофакторной аутентификации: использование нескольких способов аутентификации, таких как пароль, биометрические данные и токены доступа. Это повышает уровень безопасности, поскольку злоумышленник должен преодолеть несколько препятствий, чтобы получить доступ к информации;

– применении метода Zero Knowledge Proof: это метод доказательства, при котором пользователь может доказать свою личность или владение информацией, не раскрывая никаких конфиденциальных данных. Это уменьшает риски утечки информации и обеспечивает безопасность информации;

– применение расширенных алгоритмов шифрования: разработка более сложных алгоритмов шифрования, которые обеспечивают более высокую степень защиты информации. Это может включать использование новых математических методов или технологий, таких как искусственный интеллект;

– защита от атак с использованием машинного обучения: разработка методов, которые позволяют обнаруживать и предотвращать атаки, использующие методы машинного обучения. Это может включать использование алгоритмов машинного обучения для обнаружения необычной активности на сети, чтобы предотвратить атаки [8];

– применение технологии блокчейн (*Blockchain Cryptography*): использование блокчейн-технологий для создания криптографических протоколов, которые могут быть стойкими к атакам и обеспечивать прозрачность и безопасность передачи информации;

– применение распределенной криптографии (*Distributed Cryptography*): методы, которые позволяют использовать несколько независимых устройств для создания ключей и проведения криптографических операций. Распределенная криптография может обеспечивать высокую степень безопасности и отказоустойчивости;

– применение квантово-инспирированных алгоритмов: использование алгоритмов, основанных на принципах квантовой механики.

В результате анализа было выявлено, что несмотря на значительный прогресс в области криптографии, существуют серьезные уязвимости и ограничения, которые необходимо учитывать при проектировании систем защиты информации. Таким образом, развитие криптографии продолжает оставаться важной задачей, и для обеспечения безопасности информации в открытых телекоммуникационных каналах связи необходимо постоянно следить за новейшими разработками и совершенствовать существующие методы защиты.

Список используемых источников

1. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPv6 // Защита информации. Инсайд. 2020. N 1 (91). С. 51–57.

2. Глуховский М. Д., Сахаров Д. В. К вопросам информационной безопасности SS7 в современном мире // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 331–335.

3. Бирих Э. В., Гаврилов А. С., Сацук Е. Н. Современные проблемы обеспечения внутренней безопасности распределенной сети органов государственной власти // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 104–107.

4. Бирих Э. В., Рябов Е. Ю., Сахаров Д. В. Методология формирования модели угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. С. 103–107.

5. Бирих Э. В., Сахаров Д. В. Модель нарушителя распределенной информационно-вычислительной сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2016. С. 235–238.

6. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. Санкт-Петербург : Интермедия, 2017. – 312 с.

7. Коржик В. И., Просихин В. П. Основы криптографии: учебное пособие по специальности 210403 "Защищенные телекоммуникационные системы связи". Санкт-Петербург: Линк, 2008.

8. Семенов Р. В., Таров Е. В. Искусственный интеллект в защите информации // Молодежная научная школа кафедры «Защищенные системы связи». 2020. Т. 1, N 2 (2). С. 76–80.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ВОЗМОЖНЫХ АТАК НА МНОГОУРОВНЕВУЮ МОДЕЛЬ БЛОКЧЕЙНА

М. Э. Богомаз, Д. В. Кушнир

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Благодаря своим характеристикам технология блокчейн стремительно набирает популярность в вопросах обеспечения безопасности различных приложений и сервисов. Это приводит к необходимости углубленного исследования безопасности самого блокчейна. Поскольку блокчейн представляет собой совокупность различных технологий, необходимо отдельно рассматривать вопросы безопасности на каждом уровне его архитектуры. В исследовании проведен анализ атак на многоуровневую модель блокчейна, а также предлагаются соответствующие меры противодействия этим атакам.

блокчейн, многоуровневая модель блокчейна, атаки на блокчейн, безопасность блокчейн

Введение

Технология блокчейн появилась в 2009 году в результате работы разработчика или группы разработчиков под псевдонимом Сатоши Накамото, которые разработали первую в мире криптовалюту биткоин. Основной целью было создание децентрализованной, безопасной и прозрачной системы для одноранговых транзакций и взаимодействий. Технология блокчейн устраняет необходимость в посредниках, создавая систему без доверия, которая позволяет пользователем напрямую взаимодействовать друг с другом.

По мере того, как технология блокчейн продолжает развиваться, она становится всё более сложной для проектирования и анализа возможностей и безопасности систем на его основе. Одним из подходов, призванных обеспечить масштабируемость, гибкость и безопасность таких систем является использование многоуровневой модель блокчейна [1].

Многоуровневая модель блокчейна

Многоуровневая модель предполагает рассмотрение блокчейна как совокупности уровней, каждый из которых имеет свои уникальные характеристики и функции.

Каждый уровень многоуровневой архитектуры блокчейна может быть настроен независимо, что позволяет создавать более гибкие и эффективные системы, способные адаптироваться к различным потребностям и усло-

виям [1]. Эта модель позволяет решать проблемы масштабирования, которые часто возникают при использовании традиционных блокчейнов, так как каждый уровень может обрабатывать определенный объем транзакций и данных. Существуют различные реализации многоуровневых моделей блокчейна. В зависимости от реализации уровни системы могут изменяться или дополняться. Пример архитектуры многоуровней системы блокчейна представлен в таблице 1 (см. ниже).

Кроме того, многоуровневая архитектура блокчейна позволяет улучшить безопасность системы, так как каждый уровень может быть защищен отдельно. Это значит, что даже при атаке на один уровень, другие уровни и данные в системе будут оставаться защищенными. Однако, как и любая другая блокчейн-технология, многоуровневая архитектура блокчейна не является идеальной и подвержена некоторым угрозам безопасности и атакам.

ТАБЛИЦА 1. Многоуровневая архитектура блокчейна

Уровень	Описание
Уровень консенсуса	Поддержание целостности блокчейна
Сетевой уровень	Связь между узлами в сети блокчейна
Уровень транзакций	Создание и проверка транзакций
Уровень смарт-контрактов	Самоисполняющиеся контракты, обеспечивающие соблюдение условий соглашения
Уровень данных	Хранение и извлечение данных в блокчейне
Прикладной уровень	Пользовательский интерфейс и приложения

Атаки на многоуровневую модель блокчейна

Наиболее распространенные атаки на многоуровневую модель блокчейна можно рассмотреть по отдельным уровням, как рассмотрено далее.

Атаки на уровень консенсуса являются одной из наиболее серьезных угроз безопасности сети блокчейн. Эти атаки нацелены на фундаментальный процесс, с помощью которого узлы в сети блокчейна достигают соглашения [2]. Примерами таких атак являются:

- Атака 51 % – один участник или группа участников получает контроль над более чем 50 % вычислительной мощности в сети блокчейна;
- Атака с двойным расходованием средств – злоумышленник дважды тратит одну и ту же цифровую валюту;
- Атака Сивиллы – злоумышленник создает несколько удостоверений или узлов в сети блокчейна, чтобы получить контроль над протоколом консенсуса.

Эти атаки могут иметь серьезные последствия для целостности и безопасности сети блокчейн. Внедрение таких мер, как механизмы консенсуса «доказательство работы» (PoW) или «доказательство доли» (PoS) может помочь снизить риск этих атак. Кроме того, мониторинг сети на предмет любой подозрительной активности и быстрое реагирование на любые потенциальные атаки имеют решающее значение для обеспечения безопасности сети блокчейна.

Атаки на сетевые протоколы системы блокчейн могут поставить под угрозу безопасность сети и ее узлов. Некоторые распространенные атаки на сетевые протоколы включают в себя:

- Атака затмения – злоумышленник изолирует узел от остальной сети, окружая его вредоносными узлами [3];
- Атака распределенного отказа в обслуживании (DDoS) – огромное количество запросов или трафика на сеть, что может привести к замедлению работы сети или ее зависанию;
- Атака «человек посередине» (MitM) – перехват общения между двумя сторонами.

Для защиты от атак на сетевые протоколы блокчейна используют различные методы, такие как одноранговые сети, алгоритмы распределенного консенсуса и криптографические протоколы. Эти методы помогают обеспечить целостность и безопасность сети, усложняя злоумышленникам изоляцию узлов, контроль над большой частью сети или переполнение ее трафиком.

Атаки на протокол транзакций в блокчейне могут происходить, когда злоумышленник пытается манипулировать процессом записи транзакций. Одним из распространенных типов атак является атака «двойной траты», когда злоумышленник пытается дважды потратить одни и те же средства. Это можно сделать, создав мошенническую транзакцию и транслировав ее в сеть до того, как законная транзакция будет подтверждена. Другой тип атаки – это атака «пластичности транзакции», когда злоумышленник манипулирует данными транзакции, чтобы создать новую транзакцию с другим идентификатором транзакции. Это может вызвать путаницу и задержки в процессе подтверждения транзакции.

Чтобы предотвратить атаки такого типа, важно реализовать меры безопасности, такие как механизмы подтверждения транзакций и многофакторная аутентификация. Кроме того, некоторые блокчейны используют алгоритмы консенсуса, которые требуют определенного количества узлов для проверки транзакции, прежде чем она будет добавлена в блокчейн [4], что может помочь предотвратить атаки с двойным расходом.

Атаки на смарт-контракты являются одними из самых распространенных и разрушительных атак в сети блокчейн. Смарт-контракты используются для управления цифровыми активами и автоматизации транзакций

в блокчейне. Однако, если они не защищены должным образом или не проверены, они могут быть уязвимы для атак.

- Атака с повторным входом – контракт неоднократно вызывает сам себя до завершения предыдущего выполнения;
- Атака отравления данных – злоумышленник вставляет вредоносные данные в хранилище контракта. Это может привести к непредсказуемому поведению контракта, например, к разрешению несанкционированного доступа к активам контракта.

Для защиты от атак на уровне контрактов, можно применять следующие меры: аудит контрактов перед их размещением в блокчейне, чтобы обнаружить и исправить возможные уязвимости; использование стандартных библиотек и шаблонов контрактов, чтобы избежать написания уязвимого кода; ограничение доступа к контракту только авторизованным пользователям; использование многофакторной аутентификации для доступа к контракту; установка лимитов на средства, которые могут быть переданы через контракт, чтобы предотвратить возможные потери [5].

Атаки на уровне данных могут произойти, когда злоумышленник получает несанкционированный доступ к данным, хранимым в блокчейне, и может изменять их, удалять или дублировать. Это может привести к нарушению конфиденциальности, целостности и доступности данных. Примерами атак на уровень данных являются: атаки методом подмены, атаки методом дублирования и атаки методом отказа в обслуживании (DoS).

Для защиты от атак на уровне данных, можно применять следующие меры: использование шифрования данных при их передаче и хранении в блокчейне; ограничение доступа к данным только авторизованным пользователям; использование механизмов проверки подлинности и целостности данных, таких как цифровые подписи и хэширование; регулярные мониторинг и обновление блокчейна для обнаружения и устранения возможных уязвимостей; построение многоуровневой защиты, включающей физическую защиту узлов блокчейна, контроль доступа, мониторинг и логирование событий.

Атаки на прикладной уровень относятся к атакам на приложения конечного пользователя, которые взаимодействуют с сетью блокчейна. Одним из типов атак на протокол приложения являются фишинговые атаки, когда злоумышленники обманом заставляют пользователей раскрывать свои закрытые ключи или другую конфиденциальную информацию через поддельные веб-сайты или электронные письма, которые кажутся законными. Другая атака – это использование вредоносного кода внутри приложения, которое может украсть пользовательские данные или манипулировать ими. Кроме того, уязвимости смарт-контрактов также могут быть использованы на уровне приложений. Например, злоумышленники могут манипулировать

смарт-контрактом, чтобы получить несанкционированный доступ к средствам пользователя или вызвать неожиданное поведение в контракте.

Для защиты от атак на уровень приложений важно, чтобы пользователи использовали надежные и безопасные приложения и всегда проверяли легитимность любых запросов конфиденциальной информации. Разработчики также должны проводить тщательный аудит безопасности своих приложений и смарт-контрактов для выявления и устранения уязвимостей.

Заключение

Представление блокчейна в виде многоуровневой структуры позволяет выявить характерные уязвимости каждого уровня; определить и разработать подходы к защите на конкретном уровне. Распределение атак и методов защиты по уровням модели упрощает выполнение задач для обеспечения безопасности всей системы [6].

Потенциальные преимущества применения технологии блокчейн значительны, однако обеспечение безопасности и надежности систем на его основе требует постоянного анализа и дальнейших исследований для защиты от существующих и возникающих угроз.

Список используемых источников

1. Yujuan Wen a, Fengyuan Lu a, Yufei Liu a, Xinli Huang. Attacks and countermeasures on blockchains: A survey from layering perspective [Электронный ресурс] // Computer Networks: электрон. научн. журн. 2021. N 191. С. 1–17. URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128621001080 (дата обращения 27.01.2023).

2. Сингхал Б. Блокчейн. Руководство для начинающих разработчиков. М. : BHV-СПб, 2019. 288 с.

3. Ethan Heilman, Alison Kendler. Eclipse Attacks on Bitcoin’s Peer-to-Peer Network [Электронный ресурс] // IEEE Symposium on Security and Privacy : материалы 24 науч. конф., Остин, 10–12 августа. 2016 г. М. : USENIX Security, 2016. С. 12–29. URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf (дата обращения 28.01.2023).

4. Abhishek Guru, Bhabendu Kumar Mohanta, Hitesh Mohapatra. A Survey on Consensus Protocols and Attacks on Blockchain Technology [Электронный ресурс] // Applied Sciences : междун. научн. журн., 2023. N 13. С. 1–21. URL: https://www.mdpi.com/2076-3417/13/4/2604 (дата обращения 25.02.2023).

5. Lewis A. The Basics of Bitcoins and Blockchains. M. : Mango Publishing, 2018. 408 с.

6. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных. СПб. : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2019. 92 с.

УДК 004.054
ГРНТИ 49.34.06

АНАЛИЗ ПРИНЦИПА УСТАНОВЛЕНИЯ РЕЧЕВОГО СОЕДИНЕНИЯ В ПРИЛОЖЕНИИ WHATSAPP

Т. В. Болотов, В. Ю. Гойхман

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цель исследования – анализ трафика в приложении WhatsApp. В статье на основе эксперимента требуется определить сценарий установления соединения между клиентом и сервером с помощью использования протокола STUN. Основное внимание уделяется алгоритму работы протокола STUN и TURN-сервера. Научная новизна работы состоит в том, что в ней применены статистические методы, ранее не использовавшиеся для проведения подобных исследований. В результате в ходе экспериментов был выявлен алгоритм установления речевых соединений с помощью мессенджеров на примере приложения WhatsApp.

анализ, трафик, WhatsApp, STUN, TURN.

В настоящее время мессенджеры играют важную роль в жизни современного человека, так как через них удобно обмениваться сообщениями, но помимо этого в некоторых из них предусмотрена возможность речевого соединения. Рассмотрим эту процедуру подробнее на примере приложения WhatsApp, так как оно является одним из самых популярных на момент января 2022 года (рис. 1).

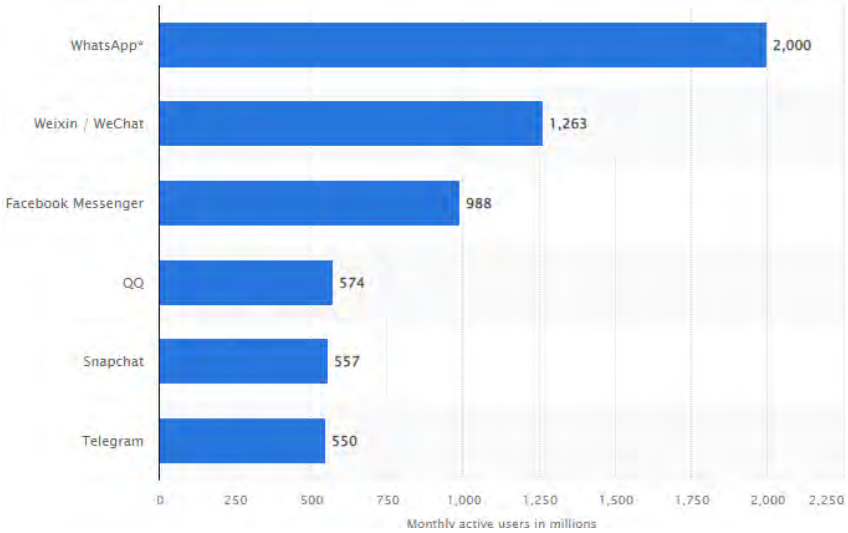


Рис. 1. Самые популярные мобильные приложения для обмена сообщениями по всему миру по состоянию на январь 2022 г., исходя из количества активных пользователей в месяц

Для проведения анализа была разработана методика захвата пакетов WhatsApp.

Рис. 2. Лабораторный стенд

Для сбора трафика использовался лабораторный стенд (рис. 2) и такие устройства, как: ноутбук Lenovo330 и iPhone 8.

В первую очередь необходимо очистить кэш устройств, чтобы не упустить пакеты, которые отправляют и получают устройства при запуске приложения. Для анализа будет использоваться программа Wireshark, поэтому она должна быть установлена на ноутбук заранее.

Затем необходимо выставить режим модема на ноутбуке и подключить к нему телефон (ноутбук тоже должен быть подключен к интернету). На этом сбор лабораторного стенда завершён.

Порядок действий в ходе сбора данных был такой:

1. Запуск приложения WhatsApp на телефоне.
2. Звонок на другое устройство.
3. Разговор 30 секунд и завершение разговора.
4. Получение и отклонение звонка от другого устройства.
5. Обмен сообщениями (одно отправленное и одно принятое).

После проделанного алгоритма необходимо остановить захват пакетов в Wireshark.

В ходе сбора данных, было получено 60 dump-файлов.

В результате анализа dump-файлов, результаты которого представлены в виде гистограмм (рис. 3), было выявлено, что наибольшей частотой встречаемости обладают пакеты длиной от 0 до 190 байт. Также при анализе интенсивности поступления пакетов было получено, что среди интенсивностей наибольшей частотой обладает интервал от 12,51 до 111,4 байт/сек.

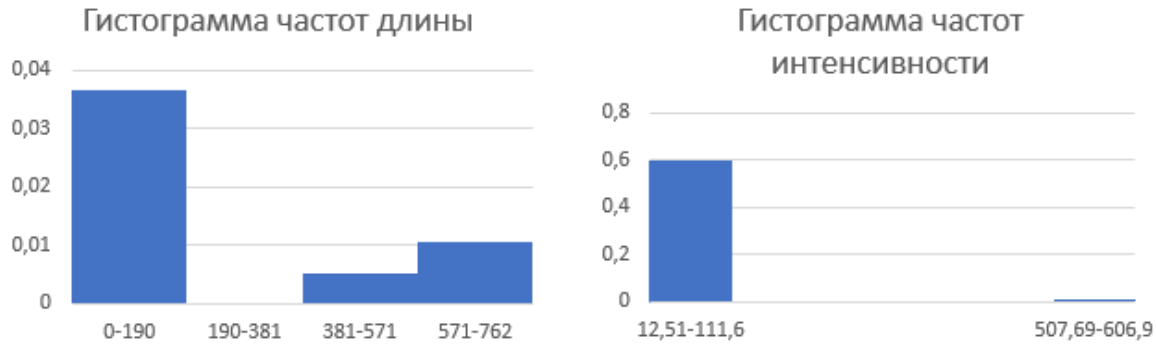


Рис. 3. Гистограммы частот длины и интенсивности

Приложение WhatsApp использует в качестве транспорта протоколы TCP и UDP (рис. 4). Основным прикладным протоколом является DNS. Также стоит упомянуть о протоколе STUN, который осуществляет корректную работу приложения, если клиент находится вне NAT.

STUN (Session Traversal Utilities for NAT) – предоставляет инструмент для работы с NAT. Он предоставляет конечной точке средства для определения IP-адреса и порта, выделенных NAT, которые соответствуют ее частному IP-адресу и порту. Он также позволяет конечной точке поддерживать активную привязку NAT [1].

Если же оба клиента находятся за NAT, то используется TURN-сервер.

TURN (*Traversal Using Relays around* NAT) – позволяет хосту управлять работой ретранслятора и обмениваться пакетами со своими одноранговыми узлами с помощью ретранслятора. TURN отличается от некоторых других протоколов управления ретрансляцией тем, что позволяет клиенту общаться с несколькими одноранговыми узлами, используя один адрес ретрансляции [2].

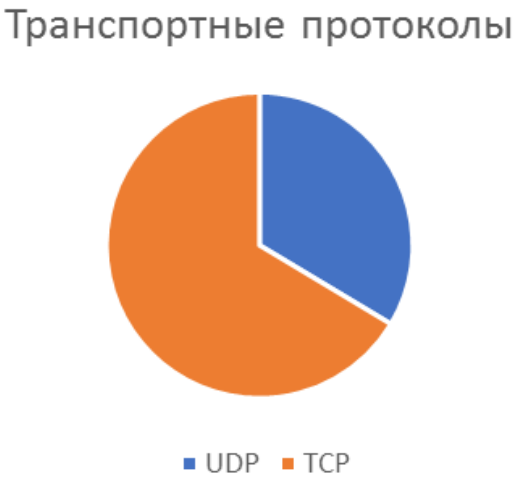


Рис. 4. Диаграмма транспортных протоколов

Главным отличием этих протоколов друг от друга является то, что STUN плохо работает с симметричным NAT'ом (и сервер и клиент находятся за NAT). Это основная причина разработки протокола TURN.

Принцип работы:

STUN: Устройством отправляется запрос к публичному IP STUN-сервера через маршрутизатор (шлюз), он, в свою очередь, перенаправляет его на STUN-сервер с внешним IP на порт 3478, а сервер отвечает устройству через маршрутизатор, сообщая, что запрос был сделан с внешнего IP-маршрутизатора с определенного порта (рис. 5).

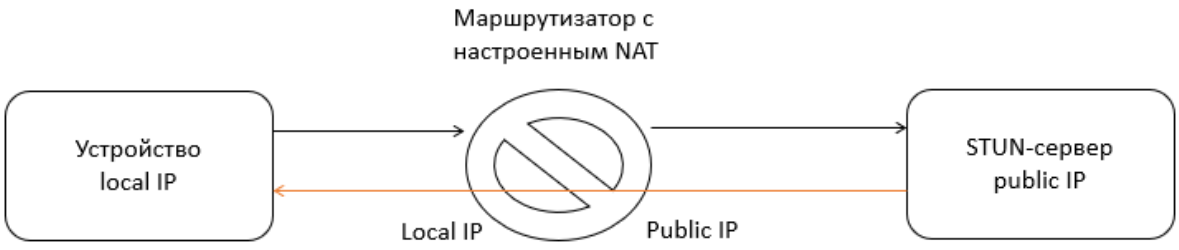


Рис. 5. Схема отправки запроса STUN-серверу и ответ

TURN: Клиент с TURN-агентом отправляет сообщение на TURN-сервер для того, чтобы обнаружить публичный IP-адрес (по аналогии

со STUN), но вместо этого TURN-сервер посылает свои IP и порт. Клиент, как только получил от TURN-сервера данные, посылает их пиру. По тому же принципу работает и с противоположной стороны. В итоге получается, что голосовой и сигнальный трафик ходит через TURN-сервер (проксирование) (рис. 6).

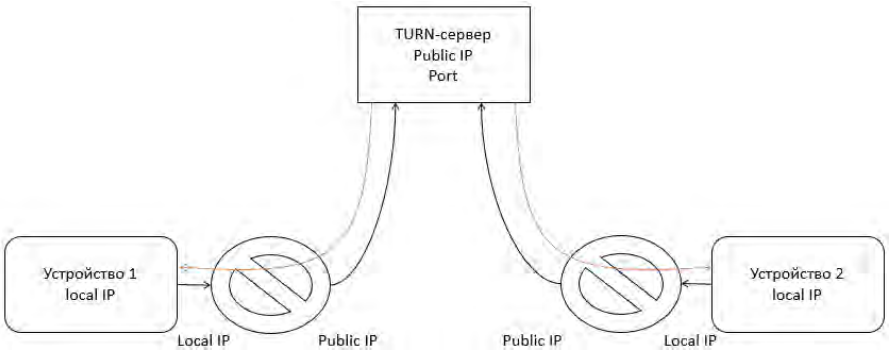


Рис. 6. Схема работы TURN

В результате исследования было выявлено 2 сценария для установления соединения. Для формирования UDP соединения используется следующий сценарий (рис. 7):

1. Присоединение к серверу.
2. Отправка пакета, содержащего binding request.
3. Получение пакета, содержащего binding response.

268 0.017702	192.168.0.106	188.243.183.166	STUN	86	Binding Request
269 0.016547	157.240.205.62	192.168.0.106	UDP	383	3478 → 62194 Len=341
270 0.001401	188.243.183.166	192.168.0.106	STUN	86	Binding Success Response
271 0.030261	188.243.183.166	192.168.0.106	STUN	86	Binding Request
272 0.004323	192.168.0.106	188.243.183.166	STUN	86	Binding Success Response
273 0.044683	192.168.0.106	188.243.183.166	UDP	147	62194 → 24832 Len=105
274 0.052510	188.243.183.166	192.168.0.106	UDP	284	24832 → 62194 Len=242
275 0.068214	192.168.0.106	188.243.183.166	UDP	227	62194 → 24832 Len=185
276 0.033206	188.243.183.166	192.168.0.106	UDP	239	24832 → 62194 Len=197
277 0.089077	192.168.0.106	188.243.183.166	UDP	261	62194 → 24832 Len=219
278 0.050752	188.243.183.166	192.168.0.106	UDP	148	24832 → 62194 Len=106
279 0.000107	188.243.183.166	192.168.0.106	UDP	67	24832 → 62194 Len=25
280 0.067173	192.168.0.106	188.243.183.166	UDP	227	62194 → 24832 Len=185
281 0.103434	192.168.0.106	188.243.183.166	UDP	233	62194 → 24832 Len=191
282 0.004510	188.243.183.166	192.168.0.106	UDP	164	24832 → 62194 Len=122
283 0.000109	188.243.183.166	192.168.0.106	UDP	187	24832 → 62194 Len=145
284 0.075334	192.168.0.106	188.243.183.166	UDP	67	62194 → 24832 Len=25
285 0.010857	192.168.0.112	239.255.255.250	SSDP	209	M-SEARCH * HTTP/1.1
286 0.094367	188.243.183.166	192.168.0.106	UDP	196	24832 → 62194 Len=154
287 0.054214	188.243.183.166	192.168.0.106	UDP	230	24832 → 62194 Len=188
288 0.137510	188.243.183.166	192.168.0.106	UDP	241	24832 → 62194 Len=199
289 0.003398	192.168.0.106	188.243.183.166	UDP	68	62194 → 24832 Len=26

Рис. 7. Установления UDP соединения

Для установления TCP соединения используется следующий сценарий (рис. 8, см. ниже):

1. Подключение к серверу.
2. Отправка пакета, содержащего allocation request.
3. Далее сервер в случае успешной регистрации присылает allocate success response с атрибутом выделенного порта на TURN-сервере, а также

XOR-MAPPED-ADDRESS – данный атрибут содержит IP и порт из отображения NAT.

4. В случае дальнейшей работой с этим TURN соединением необходимо каждый раз продлять регистрацию, отправляя refresh request. Эта процедура сделана для отбрасывания неактивный подключений.

229	0.003909	192.168.0.106	31.13.72.49	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 31.13.72.49:3478
230	0.000080	192.168.0.106	31.13.72.49	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 31.13.72.49:3478
231	0.000807	192.168.0.106	157.240.205.62	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 157.240.205.62:3478
232	0.000084	192.168.0.106	157.240.205.62	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 157.240.205.62:3478
233	0.001111	192.168.0.106	31.13.92.50	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 31.13.92.50:3478
234	0.000087	192.168.0.106	31.13.92.50	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 31.13.92.50:3478
235	0.000971	192.168.0.106	185.60.216.51	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 185.60.216.51:3478
236	0.000911	192.168.0.106	185.60.216.51	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 185.60.216.51:3478
237	0.001514	192.168.0.106	31.13.81.50	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 31.13.81.50:3478
238	0.000084	192.168.0.106	31.13.81.50	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 31.13.81.50:3478
239	0.004220	192.168.0.106	157.240.205.62	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 157.240.205.62:3478
240	0.000080	192.168.0.106	157.240.205.62	STUN	314	Allocate Request XOR-RELAYED-ADDRESS: 157.240.205.62:3478
241	0.001736	157.240.205.62	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
242	0.000107	157.240.194.55	192.168.0.106	TCP	66	5222 → 62190 [ACK] Seq=4813 Ack=2081 Win=68864 Len=0 TSval=49389308 TSecr=4284213967
243	0.000070	157.240.205.62	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
244	0.004614	31.13.72.49	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
245	0.000110	31.13.72.49	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
246	0.005174	157.240.205.62	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
247	0.000112	157.240.205.62	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
248	0.004176	192.168.0.106	157.240.205.62	UDP	88	62194 → 3478 Len=46
249	0.014064	31.13.81.50	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
250	0.000117	31.13.81.50	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
251	0.000000	31.13.92.50	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194
252	0.000000	31.13.92.50	192.168.0.106	STUN	110	Allocate Success Response XOR-MAPPED-ADDRESS: 91.238.229.242:62194

Рис. 8. Установления TCP соединения

Список используемых источников

1. RFC 5389: Session Traversal Utilities for NAT (STUN).
2. RFC 5766: Traversal Using Relays around NAT (TURN).

УДК 621.391.1
ГРНТИ 49.43.01

АНАЛИЗ ПОЛИТИК И АЛГОРИТМОВ КЭШИРОВАНИЯ СЕНСОРНЫХ ДАННЫХ В ИНФОРМАЦИОННО-ОРИЕНТИРОВАННЫХ СЕТЯХ ICN

Я. А. Боровская

Поволжский государственный университет телекоммуникаций и информатики

Архитектурная и информационная интеграция Интернета вещей и информационно-ориентированных сетей ICN даёт ряд очевидных преимуществ в части эффективного хранения и оперативного предоставления сенсорных данных пользователю. Анализ трафика Интернета вещей, а также существующих политик кэширования и алгоритмов замещения данных в кэш-памяти показывает необходимость применения новых семантических алгоритмов для управление кешированием сенсорных данных. Возникает

задача разработки обобщенного алгоритма замещения данных в кэш-памяти с учетом семантических тегов, а также в перспективе задача анализа и моделирования статуса актуальности этих данных.

информационно-ориентированная сеть ICN, кэширование контента, ICN Cache, политика кэширования.

В настоящее время концепция Интернета вещей (*Internet of Things*, IoT) является общепризнанным направлением развития сетей, систем и устройств телекоммуникаций, чему свидетельствует большое количество постоянно появляющиеся научные исследования по различным аспектам IoT. Известно, что трафик Интернета вещей увеличивается с каждым днем из-за взрывного роста количества «вещей», подключенных к Интернету. Вследствие этого в отдельное направление исследований IoT выделяют работы, связанные с обработкой и хранением сенсорных данных. Здесь следует отметить два концептуальных подхода к обработке сенсорных данных: облачные вычисления (*Cloud computing*) [1], где обработка данных происходит в «облаке» и граничные/туманные (*Edge*/*Fog*) вычисления – где часть обработки данных производится на промежуточных устройствах (концентраторах) или на конечных сенсорных устройствах, то есть максимально ближе к границе сенсорной сети [2]. В рамках обеспечения повышения эффективности доставки и обработки сенсорных данных, а также для уменьшения задержек переноса данных в сети связи предлагается использовать концепцию внутрисетевого кэширования (In-network Cache) сенсорных данных на узлах информационно-ориентированной сети, ИОС (*Informatic-Centric Network*, ICN), где фрагменты сенсорных данных представляются в виде контента.

Согласно рекомендации МСЭ-Т Y.3075 ICN – это новая концепция сетевой организации, где основными компонентами являются именованные объекты данных. В предыдущих работах [3, 4] рассматривалась возможная архитектурная интеграция сетей 5G/IMT-2020 и ICN сетей. Отмечалось основное преимущество ICN сетей – возможность предоставления гибкого кэширования именованных объектов данных вместе с контентом. Эффективность организации процесса кэширования зависит от выбранной политики и алгоритма замены данных в кэше, которые требуют отдельного рассмотрения.

Алгоритм замещения данных является ключевой составляющей любой системы кэширования – это алгоритм, определяющий какой объект удалять из кэш-памяти в случае переполнения памяти, используя набор определенных правил стратегии замещения. Основной задачей алгоритма замещения является снижение числа возможных промахов (когда в кэш-памяти нет запрашиваемой информации). Ниже в таблице 1 проанализированы основные

алгоритмы замещения данных в кэш памяти, которые могут быть применены в ICN сетях [5, 6].

В зависимости от системы кэширования, объема и параметров данных выбирается тот или иной алгоритм замещения данных в кэше.

ТАБЛИЦА 1. Основные алгоритмы замещения данных в кэш-памяти

Наименование алгоритма замещения и особенности замещения данных в кэше				
LRU (*Least Recently Used Cache*)	Segmented LRU (SLRU) – модификация LRU	LRU-K – модификация LRU	FIFO (*First Input – First Output*)	Least Frequently Used (LFU)
Объект, запрошенный недавно, будет с большей вероятностью запрошен в ближайшее время. Если объект в кэш-памяти, который был запрошен раньше остальных, будет иметь наименьший рейтинг, а вновь добавляемый в кэш-память наивысший, то кандидатом на удаление является первый из них.	Условно делит кэш-память на два сегмента: незащищенный и защищенный. По первому запросу, объект добавляется в незащищенный сегмент. Если объект используется, он перемещается в защищенный сегмент. В сегментах происходит замещение по алгоритму LRU. Из кэш-памяти удаляются объекты из незащищенного сегмента. Добавление в незащищенный сегмент происходит с максимальным значением кэш рейтинга.	Учет не только новизны, но и частоты при определении объекта для вытеснения из кэш-памяти. Для каждого объекта в кэш-памяти вычисляется время не последнего, от момента $T_{current}$ обращения.	Объект добавляется в связанный список, отсортированный по времени поступления в кэш-память. Для объекта в кэш-памяти, можно обновить загрузочное время и перемещать конец списка как самый «свежий». Если элемент не находится в кэш-памяти, которая заполнена, то требуется освободить место новому элементу.	Происходит подсчет числа обращений к каждому объекту. Объект, имеющий наименьшую частоту доступа, является первым кандидатом на вытеснение из кэш-памяти.

Для эффективности реализации внутрисетевого кэширования используют определённые типы политики. С помощью определенной политики кэширования можно производить запись данных в кэш по выбранному алгоритму. Ниже приведены основные политики внутрисетевого кэширования:

– Leave Copy Everywhere (LCE) – данные сохраняются в каждом узле на пути от источника данных к пользователю;

– Leave Copy Down (LCD) – данные сохраняются в соседнем узле от узла-источника на пути от источника данных к пользователю;

– Copy with Probability (Prob) – данные сохраняются в каждом узле на пути от источника данных к пользователю с заданной вероятностью p;

– Probabilistic Cache (ProbCashe) – данные сохраняются в каждом узле на пути от источника данных к пользователю, но с определенной вероятностью *p*, которая рассчитывается на основании расстояния между пользователем и источником данных.

Кроме того, для ICN разработан универсальный алгоритм замены кэш-данных (*Universal Caching*, UC), где решение о замене данных в кэше зависит от параметра, назначенного каждому входящему контенту. Этот параметр основан на расстоянии от источника до текущего узла, доступности маршрутизатора и частоте доступа к контенту.

Результаты показывают, что эта политика работает лучше, чем LRU и FIFO в сетях ICN, с точки зрения обращений к кэшу и среднего количества переходов, необходимых для получения запрашиваемого контента. Кроме того, существует алгоритм замещения с наименьшим значением (*Least Frequently Used*, LVF), который учитывает задержку поиска содержимого в кэше, а также популярность данных. Было показано, что алгоритм LVF превосходит FIFO и LRU с точки зрения времени до попадания в кэш, скорости попадания, задержки в сети [7].

В контексте концепции IoT сенсорные данные, генерируемые разнородными датчиками, являются весьма чувствительными к статусу своей актуальности в определенные моменты времени их получения, хранения и обработки, что приводит к необходимости исследования так называемого «времени жизни» этих данных. Как следствие, копии, хранящиеся в кэш-памяти, могут устареть через определенный достаточно короткий промежуток времени.

Таким образом, данное требование к статусу актуальности, приводит к необходимости выбора семантических параметров и характеристик, при принятии решения по удалению действительно устаревшего содержимого из кэша. Поэтому предлагается в дальнейших исследованиях разработать алгоритм замещения данных в кэш-памяти узлов ICN на основе применения онтологического проектирования и методов имитационного моделирования для прогнозирования статуса актуальности сенсорных данных.

Список используемых источников

1. Reese G. Cloud Application Architectures. Building Applications and Infrastructure in the Cloud // O'Reilly Media. 2009. 208 p.

2. Кашкаров Д. В., Кучерявый А. Е. Анализ приложений и перспектив развития технологий граничных вычислений с множественным доступом в сетях связи // Информационные технологии и телекоммуникации. 2020. Т. 8. N 1. С. 28–33.

3. Боровская Я. А. Разработка решения по обеспечению совместимости сенсорных данных в архитектуре 5G-ICN // Современные средства связи : материалы XXVII межд. научно-техн. конф., Минск, 27–28 окт. 2022 г. Минск : Белорусская государственная академия связи, 2022. С. 26–27.

4. Боровская Я. А., Гребешков А. Ю. Исследование кэширования контента в информационно-ориентированных сетях ICN на базе 5G // Информационные технологии и технические средства управления. V Международная конференция : сб. науч. ст. Астрахань : АГТУ, 2021. С. 22–24.

5. Жуков А. И. Адаптивные алгоритмы кэширования в информационных системах : автореф. дис. ... канд. техн. наук : 05.13.01 / Жуков Александр Игоревич. ДГТУ, 2012. 21 с.

6. Долгих Д. Г. Метод расчета и оптимизации параметров системы кэширования интернет-трафика : автореф. дис. ... канд. техн. наук : 05.13.01 /Долгих Дмитрий Геннадьевич. СГЭУ, 2009. 16 с.

7. Meddeb M., Dhraief A., Belghith A., Monteil T., Drira K., Mathkour H. Least fresh first cache replacement policy for NDN-based IoT networks // Pervasive and Mobile Computing. 2019. N 52. PP. 60–70.

Статья представлена научным руководителем, профессором кафедры ССС ПГУТИ, доктором технических наук, доцентом А. Ю. Гребешковым.

УДК 004.056.5
ГРНТИ 38.31.68

МОНИТОРИНГ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ КАК СРЕДСТВО ОБНАРУЖЕНИЯ АТАК НА ИНФОРМАЦИОННУЮ СИСТЕМУ

Е. С. Бугрова, И. Е. Пестов, Е. О. Романюк, В. А. Шестакова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Облачные инфраструктуры, также, как и любые другие информационные системы, являются объектами возможных атак со стороны злоумышленников. Для обнаружения и предотвращения таких атак необходимо использование средств мониторинга и анализа облачной инфраструктуры. Данная статья рассматривает мониторинг облачной инфраструктуры с использованием системы Grafana и ее роль в обнаружении атак на информационную систему.

система мониторинга, облачная инфраструктура, обнаружение атак, информационная безопасность.

Развитие облачных технологий и увеличение объемов данных, хранимых в облачных системах, увеличило вероятность кибератак со стороны злоумышленников. Openstack [1] – это облачная операционная система, которая управляет большими пулами вычислительных, хранилищных и сете-

вых ресурсов в центре обработки данных, управляемыми и предоставляемыми через API с общими механизмами аутентификации. Она состоит из следующих компонентов: Nova (управление виртуальными машинами), Neutron (управление сетями), Cinder (управление хранилищами), Glance (управление образами виртуальных машин), Keystone (управление аутентификацией и авторизацией) и Horizon (управление веб-интерфейсом).

Компоненты OpenStack предоставляют значительный набор функциональных возможностей для создания и управления облачными вычислительными средами. Однако, как и любая другая система, OpenStack может стать целью кибератак.

Некоторыми из возможных целей атак на OpenStack могут быть: получение несанкционированного доступа к облачным ресурсам, уничтожение или изменение данных в облаке, нарушение целостности и конфиденциальности данных, нарушение доступности сервисов облачной инфраструктуры, выполнение вирусных действий внутри облачной инфраструктуры [2], захват учетных записей пользователей или администраторов облачной инфраструктуры, использование ресурсов облачной инфраструктуры для проведения атак на другие цели, а также получение информации о конфигурации и настройках облачной инфраструктуры для последующего использования в кибератаках.

Для предотвращения таких атак необходимо использовать мониторинг метрик в OpenStack. Одним из эффективных инструментов мониторинга является Grafana [3], который позволяет отслеживать различные метрики и анализировать их для выявления подозрительной активности. В данной статье рассматривается, какие атаки [4] может предотвратить мониторинг метрик с помощью Grafana в OpenStack.

Атаки на учетные записи

Атаки на учетные записи - это виды кибератак, при которых злоумышленник стремится получить несанкционированный доступ к учетной записи пользователя или администратора с целью получения доступа к конфиденциальной информации или проведения деструктивных действий в системе.

Атаки на учетные записи являются одним из наиболее распространенных методов атак на OpenStack.

Существует несколько типов атак на учетные записи в OpenStack:

– Фишинг: атакующие могут отправлять электронные письма, которые кажутся официальными сообщениями от OpenStack или его компонентов, например, Horizon, Keystone или Glance. В этих письмах могут содержаться ссылки на фальшивые веб-страницы, которые запрашивают у пользователя его учетные данные.

– Компрометация внутренней сети: если хакеры получат доступ к внутренней сети OpenStack, они могут использовать уязвимости в системе для получения доступа к учетным записям.

– Утечка учетных данных: учетные данные пользователей могут быть украдены из-за утечки данных, например, из-за уязвимости в системе управления паролями или утечки данных из другой системы.

– Подбор пароля: атакующие могут использовать программы для подбора паролей для взлома учетных записей.

– Атака на API: хакеры могут использовать API для доступа к учетным записям и выполнения вредоносных действий.

Мониторинг Grafana может выявлять подозрительную активность в учетных записях Openstack, такую как попытки входа в систему с неправильными учетными данными, изменения учетных данных или попытки использования учетных данных для несанкционированного доступа к другим компонентам Openstack.

Для обнаружения атак на учетные записи в Openstack, Grafana может использовать следующие метрики [5]: активность учетной записи, попытки неудачной аутентификации, изменения в привилегиях, изменения в конфигурации учетной записи.

Атаки на сеть

Атаки на сеть в OpenStack [6] – это процесс попыток несанкционированного доступа к сетевым ресурсам OpenStack, с целью получения конфиденциальной информации, нарушения работоспособности системы или выполнения вредоносных действий. Атаки могут быть различными и включать в себя такие виды, как DoS-атаки, межсетевые атаки, перехват сетевого трафика, атаки на виртуальные машины и другие.

DDoS-атаки [7], DoS-атаки (отказ в обслуживании) нацелены на затруднение или прекращение доступа к сетевым ресурсам OpenStack. Эти атаки могут быть осуществлены путем создания большого количества запросов к сетевым сервисам или искусственного замедления сетевого трафика [8].

Межсетевые атаки нацелены на доступ к сетям, которые находятся за границами OpenStack. Эти атаки могут быть осуществлены через уязвимости в настройках сети, таких как некорректные правила маршрутизации или настройки брандмауэра.

Перехват сетевого трафика – это атаки, которые осуществляются для перехвата сетевого трафика между клиентом и сервером. Эти атаки могут быть использованы для получения конфиденциальной информации, такой как логины и пароли.

Атаки на виртуальные машины могут быть осуществлены через уязвимости в программном обеспечении виртуальных машин, такие как недостатки в защите файловой системы или привилегий. Атаки могут быть

направлены на получение конфиденциальной информации или установку вредоносных программ.

Для обнаружения атак на сеть в Openstack, Grafana может использовать следующие метрики: мониторинг сетевого трафика, мониторинг пропускной способности, мониторинг использования сетевых портов.

Атаки на хранилища

В Openstack хранилища данных играют важную роль в хранении и управлении данными в облачной инфраструктуре. Они являются центральным элементом для хранения виртуальных дисков, образов и других данных, используемых в виртуальных машинах.

Атаки на хранилища данных могут привести к серьезным последствиям, таким как утечка конфиденциальных данных, нарушение целостности данных и прекращение работы виртуальных машин. Некоторые из наиболее распространенных атак на хранилища данных в Openstack включают следующие:

– Атаки на доступ к хранилищам данных: хакеры могут попытаться получить несанкционированный доступ к хранилищам данных Openstack, используя уязвимости в сетевых протоколах, ошибки в конфигурации или вредоносные программы. Это может привести к краже данных, их модификации или удалению.

– Атаки на виртуальные диски: хакеры могут попытаться получить доступ к виртуальным дискам, используемым в виртуальных машинах Openstack, для кражи данных или изменения их содержимого. Также возможны атаки на саму виртуальную машину, которая использует виртуальный диск, например, с помощью эксплойта уязвимости в гостевой ОС.

– Атаки на каналы связи: хакеры могут попытаться перехватывать сетевой трафик между хранилищами данных и виртуальными машинами Openstack, используя уязвимости в сетевых протоколах или вредоносные программы. Это может привести к утечке конфиденциальных данных или к изменению данных в пути передачи.

– Атаки на компоненты хранилищ данных: хакеры могут попытаться взломать компоненты хранилищ данных, такие как дисковые массивы или контроллеры хранилищ, используя уязвимости в ПО или ошибки в конфигурации. Это может привести к потере данных, их модификации или к отказу в обслуживании хранилищ.

Для обнаружения атак на хранилища в Openstack, Grafana может использовать следующие метрики: пропускная способность дисков, количество операций записи и чтения, использование дискового пространства, использование CPU памяти, скорость передачи данных, частота запросов.

Уязвимости в компонентах Openstack

Уязвимости в компонентах Openstack могут привести к серьезным атакам на систему. Openstack включает множество компонентов, таких как Nova, Neutron, Cinder и другие, которые предоставляют различные функциональные возможности [9]. Некоторые из этих компонентов могут содержать уязвимости, которые могут быть использованы злоумышленниками для атак на систему.

Например, уязвимости в компонентах Nova могут привести к возможности запуска вредоносного кода на хост-системе, либо к выполнению произвольных команд. Некоторые уязвимости могут также позволить злоумышленникам получить доступ к конфиденциальной информации, хранящейся в системе.

Уязвимости в компонентах Neutron могут привести к серьезным атакам на сеть, таким как перехват трафика или внедрение злоумышленных пакетов в сеть. Злоумышленники могут также использовать уязвимости в этом компоненте для получения доступа к сетевым ресурсам, таким как маршрутизаторы, коммутаторы и другие.

Уязвимости в компонентах Cinder могут привести к потере данных, так как этот компонент отвечает за управление блочным хранилищем. Некоторые уязвимости могут также позволить злоумышленникам получить доступ к конфиденциальной информации, хранящейся в хранилище.

Grafana может быть использован для мониторинга уязвимостей в компонентах Openstack. Например, если система запущена с уязвимой версией Keystone, Grafana может показать увеличение неудачных попыток аутентификации и активность необычных учетных записей. Если система работает с уязвимой версией Nova, Grafana может отображать использование CPU и памяти сервера, которое не соответствует ожидаемому использованию. Если система работает с уязвимой версией Neutron, Grafana может отображать необычный трафик сети, который может указывать на атаку на сетевые службы.

В заключении, использование Grafana для мониторинга метрик в Openstack способно помочь предотвратить различные виды атак на облачную инфраструктуру. Мониторинг различных метрик, таких как количество запросов, объем трафика, загрузка процессора, количество соединений и другие, позволяет выявить подозрительную активность и предотвратить атаки.

Grafana предоставляет возможность визуализации метрик в различных форматах и кастомизации уведомлений при изменении данных, что обеспечивает оперативный мониторинг и возможность реагирования на возможные атаки на систему.

Применение визуализации в области информационной безопасности может способствовать уменьшению времени, необходимого для обнаружения и реагирования на кибератаки и аномалии в системе. Благодаря визуальному представлению данных, пользователь может быстрее и точнее определять наличие аномалии и принять необходимые меры для ее нейтрализации. Такой подход может быть особенно полезен для комплексных систем безопасности, где реакция на угрозы должна происходить мгновенно, чтобы минимизировать возможный ущерб.

Таким образом, использование Grafana в Openstack для мониторинга метрик является важным инструментом для обеспечения безопасности приложений в системе и предотвращения возможных атак.

Список используемых источников

1. Openstack. URL: https://www.openstack.org/ (дата обращения 13.02.2023).
2. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы. Том. Часть 1. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича (Санкт-Петербург), 2015. 63 с.
3. Дедухова А. А., Швидкий А. А. Сравнительная оценка систем мониторинга компонентов облачной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 292–296.
4. OpenStack Security Guide. URL: https://docs.openstack.org/security-guide/ (дата обращения 13.02.2023).
5. Grafana Labs. 2017. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/ (дата обращения: 13.02.2023).
6. OpenStack Security Wiki. URL: https://wiki.openstack.org/wiki/Security/Projects (дата обращения 13.02.2023).
7. Гришин Н. А., Косов Н. А., Мазепин П. С. Актуальность методов с DDoS атаками // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 176–179.
8. Васюткин А. В., Власов Д. В., Швидкий А. А. Анализ подходов к повышению доступности сервисов облачной инфраструктуры // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. Т. 1. С. 239–243.
9. Хабр. URL: https://habr.com/ru/company/fgts/blog/590423/ (дата обращения 13.02.2023).

Статья предоставлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.623
ГРНТИ 20.23.19

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ЕЁ МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ

Г. С. Бударный, А. А. Дюсметова, А. А. Казанцев, А. В. Красов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире, где информация является одним из важнейших ресурсов, вопрос обеспечения её безопасности является крайне актуальным. Данный факт объясняется неизменно растущим количеством способов кражи персональных данных, появлением все более и более изощренных средств достижения этой цели. В статье рассмотрен такой приём как социальная инженерия: её методы и способы защиты в каждой ситуации.

социальная инженерия, защита информации, информационная безопасность, фишинг, обфускация, психология.

Информация всегда была актуальным объектом для кражи и дальнейшего её применения в различных целях. Любая система безустанно совершенствуется, становится более защищенной, что нельзя сказать о человеческом факторе. Брешь в системе безопасности нередко возникает со стороны обычных пользователей и из-за их обращения с данными.

Человеческий фактор всегда был одной из проблем в системе защиты данных, но с появлением новых технологий, переносом информации на электронные носители незаконно получать доступ к информации стало еще проще, поскольку данные методы не требуют физического присутствия или непосредственного контакта с объектом, обладающим необходимыми сведениями.

Социальная инженерия – метод несанкционированного доступа без использования технических средств, заключающийся в психологическом манипулировании над объектом, от которого планируется получить информацию для дальнейшего её применения [1].

За последние пару лет количество инцидентов неизменно растет, что можно наблюдать на диаграммах, полученных в ходе исследования в области применения средств социальной инженерии, которое проводилось российской компанией Positive Technologies [2], специализирующейся на разработке решений в сфере информационной безопасности (рис. 1).

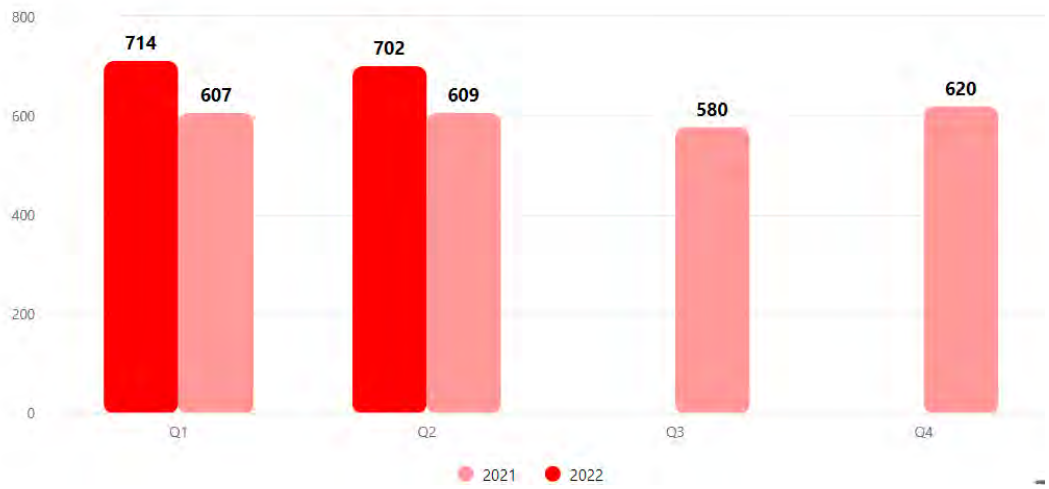


Рис. 1. Количество атак с применением социальной инженерии за 2021 – первое полугодие 2022 года

К основным средствам социальной инженерии относят различные виды фишинга *(phishing*), запугивание всплывающими окнами, подброс USB-накопилетей в общественных местах и т. д. [3, 4].

Различают такие виды фишинга:

- целевой фишинг (отличается от обычного фишинга более тщательной подготовкой к атаке: изучение жертвы, которая в свою очередь необходима лишь для достижения крупной цели);
- голосовой фишинг (использование телефона для сбора личной и финансовой информации).
- SMS-фишинг (использование сообщений с поддельными ссылками на страницы или номером телефона, контролируемым мошенниками)

В качестве средств для фишинга злоумышленники используют различные способы получения информации, с целью войти в доверие к жертве. Среди таких: отправка писем на адрес компании для получения корреспонденции, оформленной в характерном для организации стиле. После чего копируется оформление для фишинговой рассылки от имени компании.

Рассматривая рассылку вредоносных адресов, можно выделить способ, при котором после отправки электронного письма, приходит ответ «Сообщение не доставлено, адрес не существует. Подробнее об ошибке». В качестве ссылки указывается вредоносный адрес.

В атаке с вредоносными адресами применяются бреши, возникающие из-за настроек фаервола. При формально настроенных «черных» и «белых» списках URL возможен переход по вредоносным ссылкам. Атака реализуема в случае, если фаервол смотрит только на часть адреса, следующую после первого http(s), за которым в свою очередь может скрываться вредоносная ссылка. Также подобное может произойти по невнимательности самого человека. (рис. 2).

```
https://avbbank.ru/bitrix/redirect.php?goto=http://plohoyavbbank.ru
http://www.rncb.ru/bitrix/redirect.php?goto=http://zloyrncb.ru
http://www.moscow-bank.ru/bitrix/redirect.php?goto=http://ne-
moscow-bank.ru
http://kbivanovo.ru/bitrix/redirect.php?goto=http://hackkbivanovo.r
u
```

Рис. 2. Маскировка вредоносного адреса

Говоря об адресах, стоит упомянуть символы, задокументированные в стандарте RFC 1738, которые могут применяться в качестве отвлечения внимания. Так, угроза реализуема, если объект привык смотреть на адрес сразу после http(s), считая, что дальнейший URL абсолютно безопасен, ссылки, в которых присутствует символ @, могут быть вовсе не так безвредны, как могло бы показаться. Поскольку символ @ используется в URL в качестве специального разделителя, в случае если необходимо в самой ссылке указать права для доступа к странице. Таким образом, в конструкции вида http://<логин>:<пароль>@<хост> до @ можно указывать практически что угодно, независимо от этого браузер отправит пользователя на хост, указанный после @.

Порой запутывание адреса способствует внушению, что адрес безопасный. Например, в адрес можно добавить кириллицу, закодированную в UTF-8 → HEX, подобный приём запутает пользователя (рис. 3).

```
http://bank.ru@%D0%B7%D0%BB%D0%BE%D0%B9%D1%81%D0%B0%D0%B9%D1%82.%D1
%80%D1%84
```

Рис. 3. Применение кодировки для запутывания вредоносного адреса

Также можно совместить ранее описанные техники (рис. 4) и получить:

```
http://www.moscow-
bank.ru/bitrix/redirect.php?goto=http://www.moscow-
bank.ru@%D0%B7%D0%BB%D0%BE%D0%B9%D1%81%D0%B0%D0%B9%D1%82.%D1%80%D1%
84
```

Рис. 4. Применение нескольких техник для маскировки вредоносных адресов

При наведении мыши на закодированный URL браузеры способны декодировать символы, поэтому для полной маскировки вредоносного адреса (рис. 5) можно прописать адрес сервера, на котором и располагается фишинговый сайт:

```
http://www.moscow-
bank.ru/bitrix/redirect.php?goto=http://www.moscow-
bank.ru@178.248.232.27
```

Рис. 5. Пример использования адреса сервера для маскировки

Или же аналогичный способ маскировки сайта (стоит подметить, вместо домена в URL используем IP сервера, рис. 6).

```
http://www.moscow-bank.ru@178.248.232.27
```

Рис. 6. Упрощенная маскировка вредоносного адреса с помощью IP сервер

Социальные инженеры способны применять различные способы для сокрытия вредоносных адресов. Одним из таких способов считается метод при помощи Морзе [5]. Идея хакеров заключается в подмене символов в ссылках, внедренных в почтовые сообщения, на соответствующие коды азбуки Морзе. В качестве темы письма может использоваться счет для компании получателя, а формат прикрепленного вложения – документ с двойным расширением, например «._xlsx.hTML». Просмотрев вложение в текстовом редакторе, обнаруживается JavaScript-код, сопоставляющий буквы и цифры с кодами азбуки Морзе. После чего происходит расшифровка кода, и на выходе теги JavaScript, которые в свою очередь подставляются в код html-код страницы. Применяемые скрипты содержат в себе ресурсы, необходимые для отображения поддельной электронной таблицы Excel, также сообщение об истечении срока авторизации и необходимости ввести пароль повторно. Для большей убедительности форма авторизации дополняется логотипом компании-получателя, либо же общим логотипом Office365 – что и определяет фишинговую компанию в качестве целевой. Введенный пользователем пароль пересылается на удаленный сайт.

Порой пользователи опрометчиво публикуют информацию, которую можно использовать для получения сведений или же кражи средств [6]. Так, воспользовавшись сведениями о месте отдыха объекта, составляется письмо с просьбой доплаты за услуги, также указывается, что сообщение сгенерировано автоматически, для ответа необходимо воспользоваться формой на официальном сайте в разделе поддержки клиентов. Перейдя по фейковой ссылке, жертва может разгласить возможные данные для авторизации, скачать вредоносное ПО и т. д.

Также существуют способы совершения атак при помощи буллинга [7, 8]. Жертве в комментариях или в личных сообщениях отправляется оскорбление, гневное послание с аккаунта, созданного злоумышленником. Пользователь переходит в профиль обидчика и среди личной информации видит ссылку на другой сайт, социальную сеть, которая не является подлинной. Вследствие перехода по ней могут запроситься учетные данные, для просмотра профиля неизвестного человека, возможно скачивание вредоносного ПО. Учитывая, что пользователи для ведения социальных сетей применяют чаще смартфоны, не имеющие достаточной защиты, можно предположить, что последствия могут иметь гораздо более серьезный характер.

Список используемых источников

1. Краткое введение в социальную инженерию [Электронный ресурс]. URL: https://habr.com/ru/post/83415/ (дата обращения 08.11.2022).
2. Актуальные киберугрозы: II квартал 2022 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q2/ (дата обращения 09.11.2022).
3. Целенаправленная социальная инженерия. Нестандартные техники введения в заблуждение [Электронный ресурс]. URL: https://xakep.ru/2018/10/17/social-engineering-recipes-2/#toc04 (дата обращения 09.11.2022).
4. Методы социальной инженерии [Электронный ресурс]. URL: https://spy-soft.net/social-engineering-methods/ (дата обращения 20.11.2022).
5. Вскрытие вредоносных URL с помощью азбуки Морзе [электронный ресурс]. URL: https://www.securitylab.ru/blog/company/AngaraTech/350259.php (дата обращения 21.11.2022).
6. Социальная инженерия как метод киберпреступлений [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-metod-kiberprestupleniya/viewer (дата обращения 21.11.2022).
7. Социальная инженерия, её техники, методы противодействия [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-ee-tehniki-i-metody-ee-protivodeystviya/viewer (дата обращения 21.11.2022).
8. Возможности социальной инженерии в информационных технологиях [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vozmozhnosti-sotsialnoy-inzhenerii-v-informatsionnyh-tehnologiyah/viewer (дата обращения 21.11.2022).

УДК 004.056
ГРНТИ 49.33.35

СРАВНЕНИЕ СТАТИЧЕСКОГО И ДИНАМИЧЕСКОГО АНАЛИЗА КОДА И ИХ РОЛЬ В МЕТОДОЛОГИИ DEVSECOPS

Г. С. Бударный, А. О. Камалова, А. В. Красов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире безопасность стала главной заботой для компаний. Облачные вычисления, доступ в Интернет, глобализация и использование мобильных телефонов изменили основной сценарий, по которому привыкли работать компании, добавив много рисков безопасности в их системы и информацию. DevSecOps – это новая методология работы, которая улучшает философию DevOps, добавляя компонент безопасности на протяжении всего процесса разработки и помогая создать культуру безопасности на всех уровнях компании.

DevSecOps, разработка, информационная безопасность, безопасность приложений, безопасная разработка.

Введение

DevSecOps (сокращенно от *Development, Security, Operation*) – это практика разработки программного обеспечения, которая предполагает обеспечение безопасности на каждом этапе жизненного цикла разработки программы для создания защищенных приложений.

DevSecOps внедряет безопасность в конвейер непрерывной интеграции и непрерывной доставки (CI/CD) [1]. Это позволяет командам разработчиков решать некоторые из наиболее актуальных проблем безопасности на сегодняшний день со скоростью DevOps.

Как правило, во время разработки программного обеспечения о безопасности и методы ее обеспечения думали только лишь на последних стадиях жизненного цикла разработки. Но количество атак, связанных с кибербезопасностью с каждым годом увеличивается, поэтому практика DevSecOps становится обычной практикой обеспечения безопасности приложений в современной экосистеме разработки.

Сравнение статического и динамического анализа кода

Статический анализ (*Static Application Security Testing,* SAST) – это методология тестирования, которая анализирует исходный код для поиска уязвимостей безопасности [2]. SAST сканирует приложение перед компиляцией кода. Также статический анализа известен как тестирование «белого ящика» [3].

Динамический анализ (*Dynamic Application Security Testing*, DAST) – это тестирование и оценка приложения во время его запуска и выполнения [2].

Уязвимости приложения могут быть выявлены как с помощью статического анализа, так и с помощью динамического. Это два основных подхода, которые дополняют друг друга. Если использовать эти подходы отдельно, то выявить наибольшее количество уязвимостей не получится.

Основное преимущество динамического анализа: динамический анализ выявляет тонкие дефекты или уязвимости, причина которых слишком сложна, чтобы ее можно было обнаружить с помощью статического анализа. Динамический анализ может играть определенную роль в обеспечении безопасности, но его основной целью является поиск и отладка ошибок.

Основное преимущество статического анализа: он проверяет все возможные пути выполнения и значения переменных, а не только те, которые вызываются во время выполнения. Таким образом, статический анализ может выявить ошибки, которые могут проявиться только через недели, месяцы или годы после выпуска. Этот аспект статического анализа особенно ценен для обеспечения безопасности, поскольку атаки на систему безопасности часто воздействуют на приложение непредвиденными и непроверенными способами.

Ключевое различие между статическим и динамическим анализаторами кода заключается в том, насколько углубленным является процесс проверки кода. По умолчанию статический анализ кода просматривает каждую отдельную строку исходного кода для поиска уязвимостей. Для динамического анализа проверяемые строки кода зависят от того, какие строки исходного кода активированы в процессе тестирования. Если со строкой кода не происходит взаимодействия, инструмент динамического анализа проигнорирует ее и продолжит проверку активных кодов на наличие уязвимостей. В результате динамический анализ выполняется намного быстрее, но статический анализ кода дает уверенность в том, что каждая строка исходного кода была тщательно проверена. Он может занять больше времени, но статический анализ кода выполняется в фоновом режиме и имеет решающее значение для создания качественного веб-приложения.

Статические анализаторы кода абсолютно необходимы разработчикам приложений, в то время как динамические анализаторы кода могут использоваться только в сочетании с инструментами статического анализа.

Роль статического анализа

Инструменты статического анализа хорошо интегрируются практически с любой цепочкой инструментов автоматизации программного обеспечения, а также методологией и процессом разработки. В основном это связано с тем, что они могут использоваться локально разработчиками на своем рабочем столе для мгновенной обратной связи и для анализа полной сборки, независимо от того, делается ли это ежечасно или, когда угодно. Кроме того, инструменты SAST полностью автономны, так как не требуют взаимодействия с тестировщиками или разработчиками. Они применимы всякий раз, когда имеет смысл проверять наличие ошибок и уязвимостей безопасности в коде:

Очевидно, что статический анализ играет важную роль в практике DevSecOps. По мере того, как команды разработчиков программного обеспечения начинают интегрировать безопасность в свои DevOps различные инструменты, то эти инструменты становятся частью конвейера автоматизации.

Статические анализаторы автоматически проверяют наличие уязвимостей в исходном коде приложения, байт-коде или двоичных файлах по строкам, гарантируя, что слабые места безопасности, такие как уязвимости, перечисленные в OWASP Top 10 и 2021 CWE Top 25 в исходном коде, обнаруживаются с самого начала, во время разработки. Это позволяет разработчикам выявлять риски и устранять любые уязвимости, прежде чем разработчики запустят код в производство. Таким образом, разработчики имеют возможность перемещаться влево (рис. 1) и распознавать ранние дефекты кода в цикле разработки с помощью лучших практик безопасности.

Рис. 1. «Сдвиг влево»

Роль динамического анализа

Как уже было сказано, динамическое тестирование безопасности приложений выполняется снаружи, то есть это тестирование черного ящика и выявляет уязвимости, когда приложение уже запущено.

Инструменты DAST сканируют веб-страницы, находят конечные точки веб-служб, входы и выходы, поэтому для тестирования требуется рабочая версия веб-приложения. Не изучая исходный код, динамический анализ работает над имитацией тестирования на проникновение, такого как атаки, чтобы выявить эксплуатируемые уязвимости и проблемы бизнес-логики с точки зрения хакера с надежными результатами.

Но поскольку динамический анализ происходит ближе к концу жизненного цикла программного обеспечения (*Software Development Lifecycle*, SDLC), результаты могут быть существенными и часто оказывать давление на DevOps, и чтобы быстро исправить эти уязвимости во время выполнения необходимо обеспечить взаимодействие между командами безопасности и разработки.

Методы и инструменты динамического анализа должны быть частью среды DevSecOps по многим причинам, например:

– инструменты статического анализа не учитывают уязвимости окружающей среды;

– инструменты динамического анализа могут быть намного быстрее, чем инструмент статического анализа;

– инструменты динамического анализа гораздо более эффективны, чем статического, так как количество ложноположительных оповещений очень низкое.

Заключение

Таким образом, при сравнении статического анализа и динамического анализа SAST может показаться лучшим выбором в целом, так как его можно использовать раньше в процессе разработки, когда легче и дешевле устранить обнаруженные проблемы безопасности. Однако полагаться

только на один метод обнаружения крайне проблематично. Комбинированный подход с использованием инструментов как статического, так и динамического анализа позволит найти более широкий спектр уязвимостей и используемых слабых мест.

Также можно добавить другие формы тестирования безопасности, например, интерактивное тестирование безопасности приложений (*Interactive Application Security Testing*, IAST) и самозащита приложений во время выполнения (*Runtime Application Self-Protection*, RASP), может еще больше укрепить безопасность ваших приложений, но это виды анализа выходят за рамки этой статьи.

DevSecOps – это способ подхода к информационной безопасности с подходом «каждый несет ответственность за безопасность» [4]. Эта методология включает в себя внедрение методов безопасности в конвейер DevOps организации. Цель состоит в том, чтобы включить безопасность во все этапы рабочего процесса разработки программного обеспечения. Это противоречит его предшественникам моделей разработки – DevSecOps означает, что вы не сохраняете безопасность на только заключительных этапах SDLC.

Список используемых источников

1. Ганжур М. А., Дьяченко Н. В., Отакулов А. С. Анализ методологий DevOps и DevSecOps // Молодой исследователь Дона. 2021. N 5. С. 8–10.

2. Воротникова Т. Ю. Надежный код: статический анализ программного кода как средство повышения надежности программного обеспечения информационных систем // Информационные технологии в УИС. 2020. N 2. С. 22–27.

3. Демидов П. Д. Статический и динамический анализ исходного кода // Молодой ученый. 2019. N 2. С. 2–4.

4. Миняев А. А., Паршин Е. А. Анализ процессов безопасной разработки DevSecOps // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 683–689.

УДК 621.39
ГРНТИ 49.44

ОЦЕНКА КАЧЕСТВА СВЯЗИ В СОВРЕМЕННЫХ ВЫСОКОСКОРОСТНЫХ ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМАХ

М. С. Былина, С. Ф. Глаголев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современных цифровых высокоскоростных волоконно-оптических системах связи большой протяженности с применением технологии плотного мультиплексирования в волновой области DWDM для формирования сигналов используют многоуровневые форматы амплитудной, фазовой и комбинированной квадратурно-амплитудной модуляции QAM, а для их приема – когерентные методы. Для оценки качества связи в волоконно-оптических системах связи может проводиться измерение коэффициента ошибок или связанного с ним Q-фактора. В работе рассмотрены особенности определения этих параметров в волоконно-оптических системах связи с QAM.

волоконно-оптическая система связи, ВОСС, DWDM, квадратурно-амплитудная модуляция, QAM, когерентный прием, качество связи, коэффициент ошибок, Q-фактор.

Современные цифровые высокоскоростные волоконно-оптические сети связи (ВОСС) большой протяженности с технологией плотного мультиплексирования в волновой области (DWDM) могут иметь сложную топологию [1]. Однако в большинстве случаев в такой сети можно выделить фрагменты (рис. 1), состоящие из двух оконечных пунктов (ОП) и волоконно-оптического линейного тракта (ВОЛТ). ВОЛТ может состоять из пролетов, включающих одномодовое оптическое волокно (ОВ) и линейный оптический усилитель (ОУ).

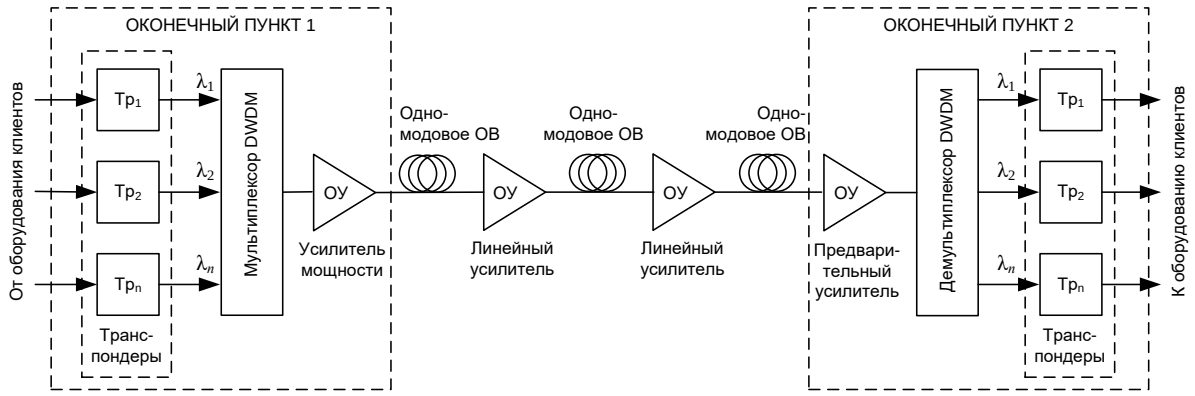


Рис. 1. Фрагмент многопролетной ВОСС

Транспондеры (ТР) осуществляют формирование линейного оптического сигнала (ЛОС) на передающей и его прием, и обработку на приемной стороне. Контроль качества связи осуществляется на приемной стороне в электрическом тракте ТР.

Для ЛОС часто используется многоуровневая квадратурно-амплитудная модуляция (QAM). Количество отдельных сигнальных символов M обычно кратно 2, то есть $M = 2^K$, где K – количество бит, передаваемых за один тактовый интервал. Символ может быть наглядно представлен на фазовой плоскости, образованной синфазной (I) и квадратурной (Q) осями, в виде вектора IQ, длина и азимут которого соответствуют амплитуде и фазе этого символа. Обычно сам вектор не показывают, оставляя только точку на фазовой плоскости. Набор таких точек называют сигнальным созвездием.

На рис. 2 показана схема формирования модулирующих сигналов 16-QAM из битовой псевдослучайной последовательности (ПСП) со скоростью B (бит/с) в программе OptiSystem [2].

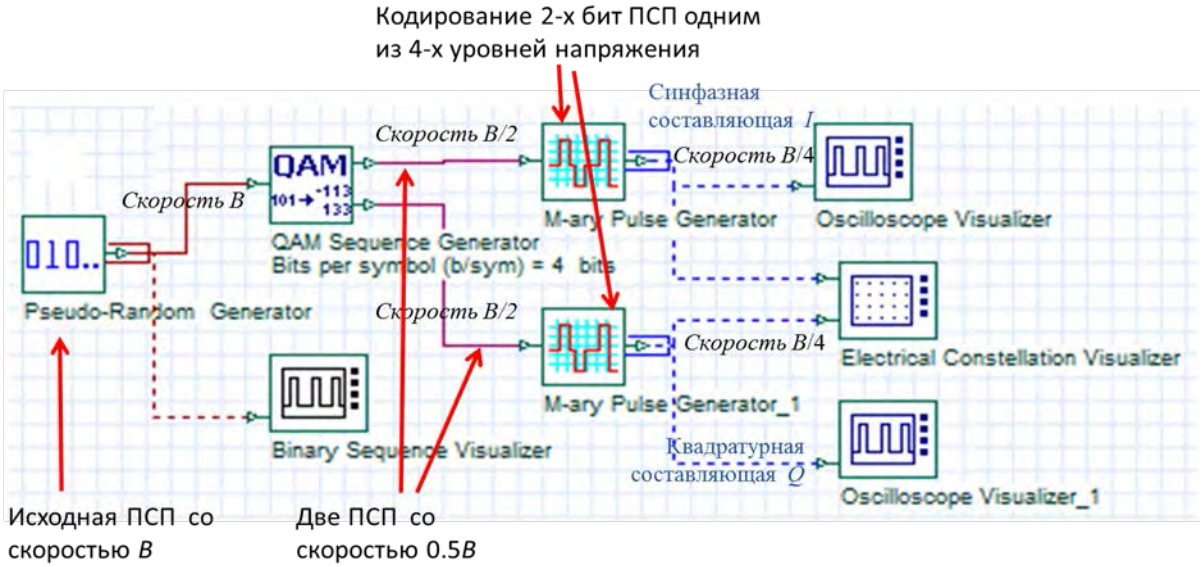


Рис. 2. Схема формирования модулирующих сигналов QAM-16

Исходная передаваемая ПСП со скоростью B от генератора (*Pseudo Random Generator*) разделяется в генераторе QAM последовательности (*QAM Sequence Generator*) на 2 ПСП со скоростью B / 2. В двух генераторах многоуровневых импульсов (*M-ary Pulse Generator*), представляющих собой цифроаналоговые преобразователи, формируются синфазный и квадратурный модулирующие сигналы, которые далее используются для модуляции оптического излучения в передатчике. В результате символьная скорость передачи в оптическом тракте составит B / 4. При информационной скорости B = 100 Гбит/с символьная скорость составляет 25 Гбод.

Как правило, в современных ВОСС битовую скорость передачи B увеличивают в 2 раза за счет использования излучения двух ортогональных поляризаций [1].

На рис. 3 и 4 показаны сигнальное созвездие для модулирующего сигнала QAM-16 [2].

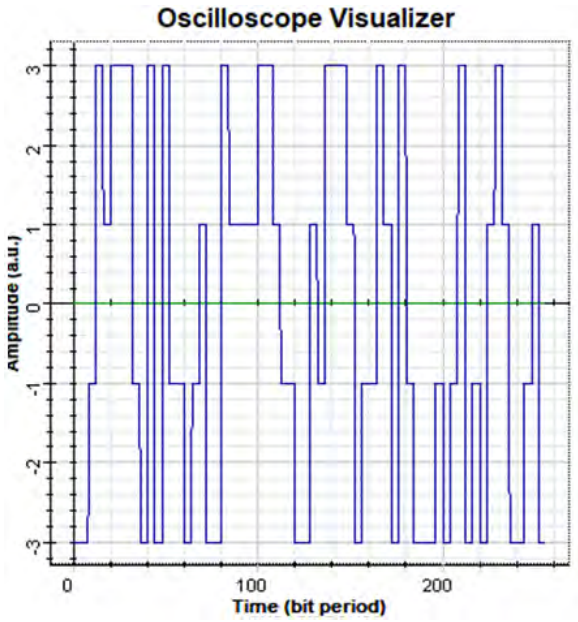


Рис. 3. Синфазная составляющая QAM-16

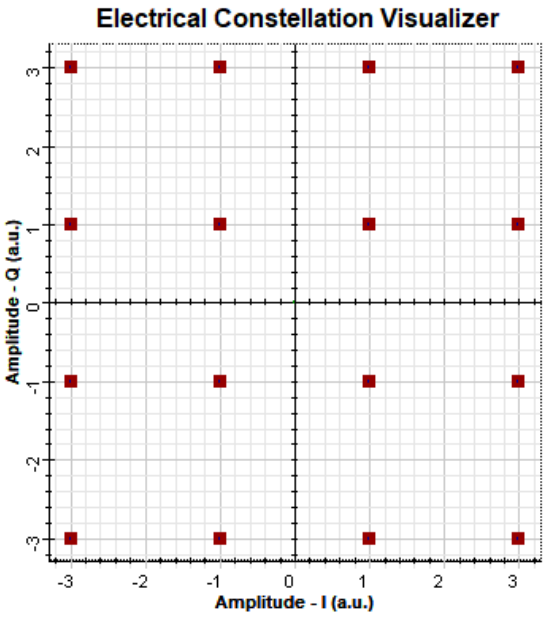


Рис. 4. Сигнальное созвездие QAM-16

После прохождения ВОЛТ оптический сигнал ослабляется, искажается и к нему добавляются шумы ОУ. Он поступает в ФПУ, где преобразуется в электрический сигнал, к которому добавляются искажения и шумы самого ФПУ. На рис. 5 (см. ниже) показаны реальные сигнальные созвездия в ФПУ, полученные при моделировании в программе OptiSystem ВОСС с КП [2] при двух уровнях выходного сигнала передатчика y.

Из рис. 5 видно, что многократно принятый символ представляет собой множество точек на фазовой плоскости, образующих пятно случайной формы и размера, расположенное в определенном для данного символа регионе, который можно считать круговым с диаметром равным одной условной единице (a.u.). Площади занимаемые многократно принятыми символами характеризуют возможный случайный разброс их положения из-за шумов. Центры тяжести распределения символов могут быть смещены относительно центров своих регионов из-за искажений. Для исключения ошибок на приеме распределения отдельных символов не должны пересекаться.

Для оценки качества связи при использовании многоуровневых форматов модуляции обычно используются два метода.

1. Метод оценки символьного Q_s-фактора [2].

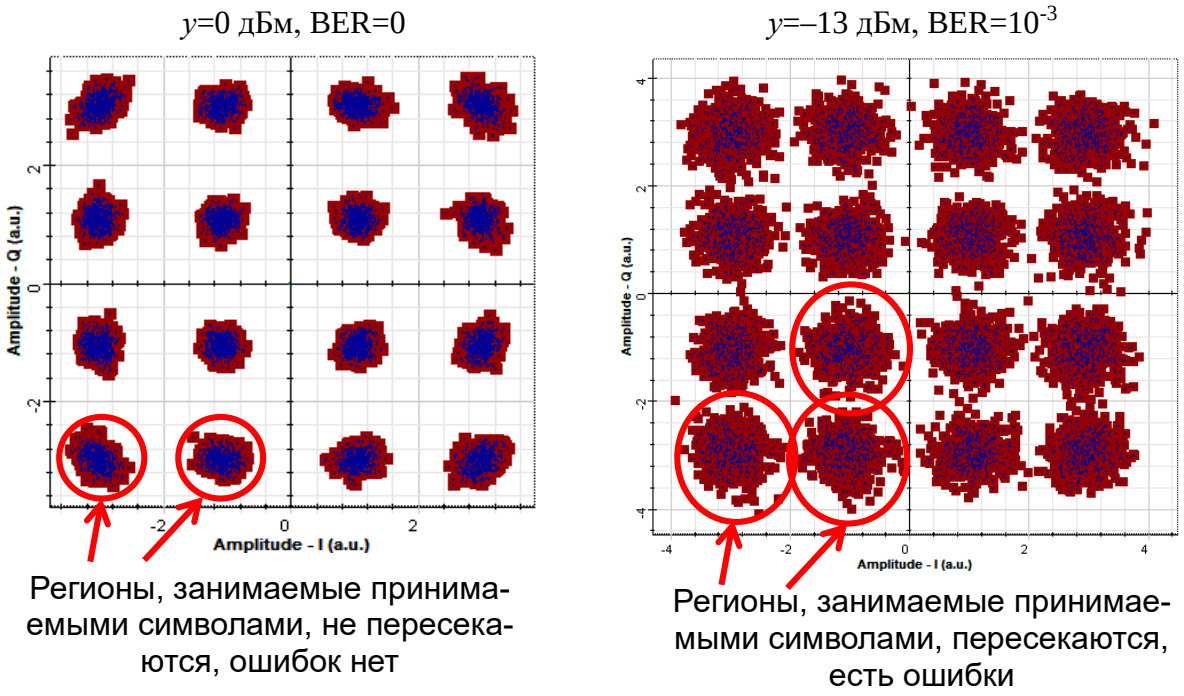


Рис. 5. Сигнальные созвездия на входе решающего устройства цифрового сигнального процессора (DSP)

По аналогии с приемом бинарных сигналов можно ввести $Q_{m,k}$-фактор для оценки вероятности ошибки при переключении символа с номера m на k ($m, k \in 1..M$, $m \neq k$):

$$Q_{m,k} = d_{m,k} \Big/ \left(\sigma_{m,k} + \sigma_{k,m}\right), \qquad (1)$$

где $d_{m,k}$ – расстояние между центрами круговых регионов для символов m и k, $\sigma_{m,k}$ и $\sigma_{k,m}$ – среднеквадратические отклонения (СКО) положения отдельных символов (рис. 6). Второй индекс у СКО указывает на возможную асимметрию распределений символов внутри своих регионов.

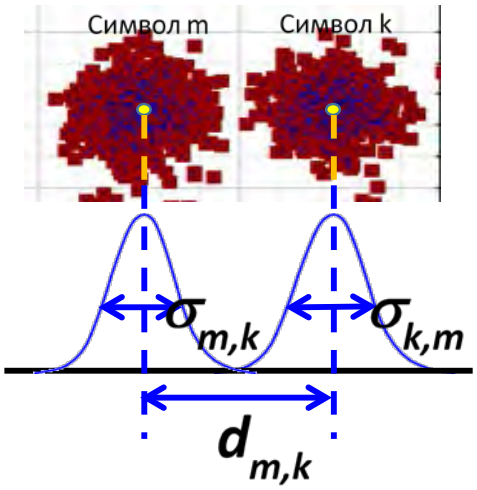


Рис. 6. Определение $Q_{m,k}$ по сигнальному созвездию

Найдя условные вероятности ошибки $p_{e\ m,k}$ при переключениях между символами m и k и перебирая все возможные варианты переключения, можно определить среднюю вероятность символьной ошибки $p_{e\ s}$:

$$p_{em,k} = \frac{1}{2} \cdot \operatorname{erfc}\left(\frac{Q_{m,k}}{\sqrt{2}}\right), \quad p_{es} = \sum_{m=1}^{M} P_m(m) \cdot \left[\sum_{k=1, m \neq k}^{M} p_{em,k}\right], \qquad (2)$$

где $P_m(m)$ – безусловная вероятность появления символа m (обычно можно считать вероятности появления различных символов равными). Символьный Q_s-фактор определяется из соотношения:

$$p_{es} \approx 0{,}5 \cdot \left[1 - \mathrm{erf}\left(Q_s / \sqrt{2}\right)\right]. \qquad (3)$$

2. Метод определения магнитуды вектора ошибок EVM [3]

На рис. 7 показаны IQ_m вектор, соответствующий «правильному» положению символа на фазовой плоскости, и $IQ_{m,l}$ вектор, соответствующий принятому символу при l-м измерении (рис. 6). Разностный вектор $EVM_{m,l}$ можно считать вектором единичной ошибки. Магнитудой вектора ошибок EVM называют величину:

$$EVM = \sqrt{\frac{1}{M \cdot L} \sum_{l=1}^{L} \sum_{m=1}^{M} \left[I_{EVM}^2(m,l) + Q_{EVM}^2(m,l) \right] / d_m^2}\,. \qquad (4)$$

где $I_{EVM}(m,l)$ и $Q_{EVM}(m,l)$ – проекции $EVM_{m,l}$ на оси I и Q, L – число измерений каждого символа. Числитель (4) представляет собой СКО вектора ошибок, а знаменатель некоторое нормирующее значение, например, средний диаметр региона d_m для символов.

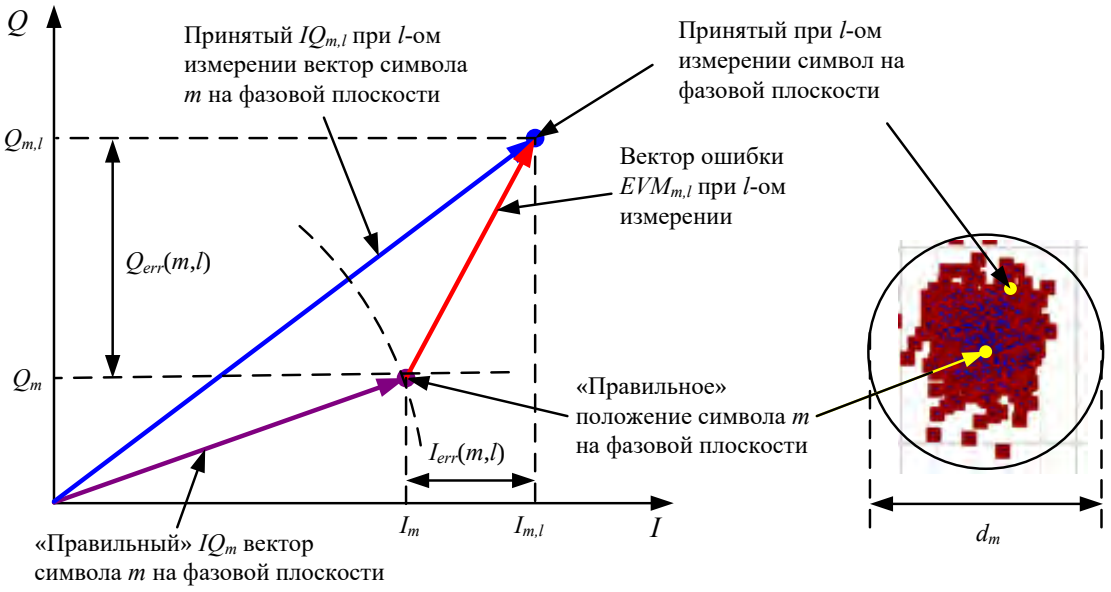


Рис. 7. К определению EVM

Используя EVM можно рассчитать символьную вероятность ошибки:

$$p_{es} = \frac{F\left(1 - M^{-0.5}\right)}{0{,}5 \log_2 M} \mathrm{erfc}\left[\sqrt{\frac{1.5}{(M-1)EVM^2}}\right],\ F = 1 + \frac{\log_2 M}{2\left(\sqrt{M} - 1\right)}. \qquad (5)$$

Выражение (5) получено для QAM в предположении, что EVM обусловлен преимущественно шумами усиленного спонтанного излучения ОУ.

Отметим, что специальные приборы для регистрации сигнальных созвездий позволяют кроме визуальной информации получить численные оценки качества связи для многоуровневых сигналов в соответствии с приведенными выражениями.

Список используемых источников

1. Трещиков В. Н., Листвин В. Н. DWDM-системы. М. : ТЕХНОСФЕРА, 2021. 420 с.

2. OptiSystem User Guide and Reference Manual. Optical Communication System Design Software. Version 19. Optiwave Systems Inc. 2022.

3. Fatadin I. Metrology of Optical Communication Systems Using Error Vector Magnitude // Journal of Applied Mathematics and Physics. 2021. N 9. PP. 2918–2926.

УДК 543.42
ГРНТИ 59.41.29

СОВРЕМЕННЫЕ АНАЛИЗАТОРЫ ОПТИЧЕСКОГО СПЕКТРА И ВОЗМОЖНОСТИ УЛУЧШЕНИЯ ИХ ХАРАКТЕРИСТИК

М. С. Былина, А. В. Фраз

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оптические методы передачи информации широко используются и очень востребованы в телекоммуникациях. Для контроля параметров оптических компонентов и оценки качества связи в волоконно-оптических системах необходимы анализаторы оптического спектра. В этой статье приведены области применения, классификация, параметры и принципы работы спектроанализаторов. Представлен сравнительный анализ современных спектроанализаторов, сформулированы предложения по улучшению их характеристик.

анализатор оптического спектра, АОС, спектроанализатор, спектрометр, параметры АОС, Фурье-спектрометр, интерферометр, спектр, улучшение разрешающей способности.

Анализатором оптического спектра (АОС) называют устройство для измерения зависимости оптической мощности от длины волны [1]. Обобщенная схема АОС представлена на рис. 1. Входной оптический сигнал че-

рез оптическую систему (ОС) попадает на фотоприемник (ФП), где преобразовывается в электрический и после аналого-цифрового преобразования (АЦП) поступает на компьютер, который осуществляет обработку и отображение сигнала, а также управление оптической системой через устройство управления (УП).

Рис. 1. Обобщенная схема анализатора оптического спектра

Основными параметрами АОС являются: диапазон измеряемых длин волн и мощностей излучения, разрешающая способность по длине волны и мощности излучения, погрешность измерения длины волны и мощности излучения, габариты и стоимость.

Оптическая система АОС может быть построена на основе диспергирующего элемента (дифракционной решётки или призмы), а также на основе интерферометра (Майкельсона, Фабри-Перо и др.).

В качестве диспергирующего элемента наиболее эффективно использование дифракционной решётки (ДР), так как она обеспечивает лучшее разрешение по длине волны и меньшие потери сигнала. На рис. 2 (см. ниже) изображена упрощённая схема ОС на основе ДР [3]. Анализируемое излучение через волоконный вход попадет на вход ОС. Линза 1 выполняет функцию коллиматора, преобразуя излучение, выходящее из волокна в параллельный пучок, который попадает на прозрачную ДР с изменяемым углом наклона. Прошедшие через ДР лучи дифрагируют по углам, зависящим от длины волны. Линза 2 с фокусным расстоянием f фокусирует их на неподвижную линейку из N фотодиодов (ФД), распложенную в её фокальной плоскости.

В [3] показано, что общим недостатком подобных ОС является рост габаритов при повышении разрешающей способности. Существенное уменьшение габаритов возможно в АОС с интерферометрами. Такие АОС чаще всего используют Фурье-спектрометрию и ОС на базе интерферометра Майкельсона. На рис. 3 представлена схема, поясняющая принцип работы сканирующего оптического Фурье-спектрометра [4, 5].

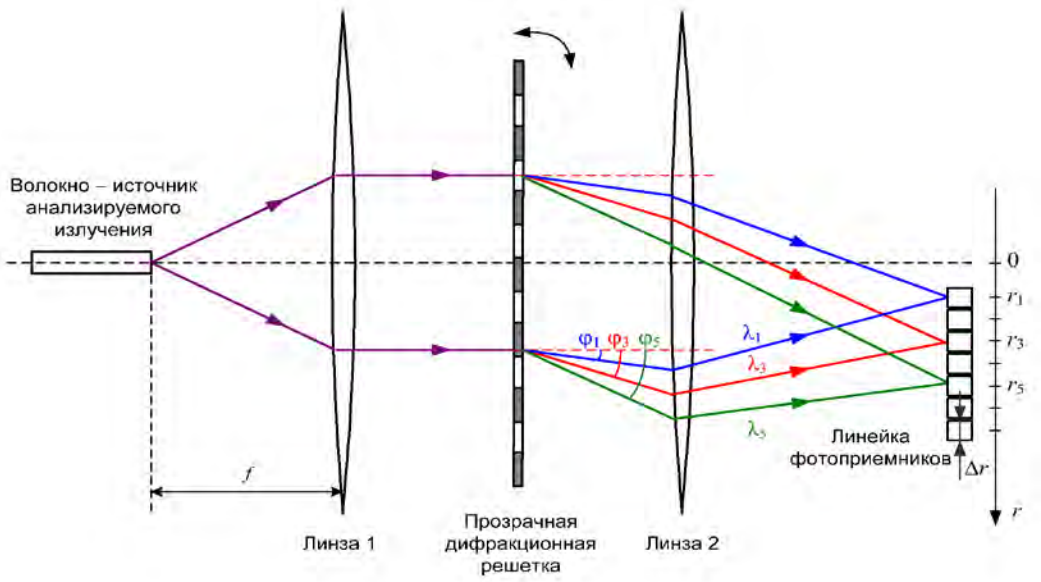


Рис. 2. Упрощенная схема оптической системы АОС на основе ДР

Излучение точечного источника S преобразуется в параллельный пучок входным коллиматором К1, попадает на расположенный под углом к оптической оси прибора светоделитель СД, где разделяется на два пучка: первый (1) отражается в сторону неподвижного зеркала М1, а второй (1') проходит в сторону неподвижного зеркала М2. После отражения от зеркал пучки (2) и (2') возвращаются к СД, который направляет их на фотоприёмник ФП, где когерентные пучки (3) и (3') интерферируют между собой. Оптическая разность хода Δ между (3) и (3') равна удвоенному расстоянию L между двумя отражающими поверхностями: М2 – реального зеркала и М1* – изображения первого зеркала, формируемого СД.

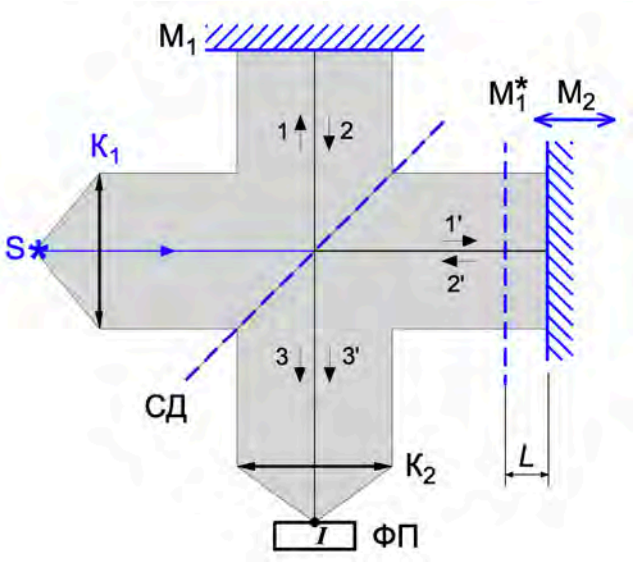


Рис. 3. Оптическая схема Фурье-спектрометра

Если плоскости M_2 и M_1* строго параллельны, то интерференционная картина локализована в бесконечности и для наблюдения ее фокусируют на ФП линзой K_2.

В современных Фурье-спектрометрах используют дискретное изменение оптической разности хода Δ с помощью шаговых микродвигателей на малую величину δΔ. Общее количество отсчетов оптической разности хода Δ_i составит $M = \Delta_m / \delta\Delta$, где Δ_m – максимальная оптическая разность хода.

Для каждого значения Δ_i (i = 0…M–1) ФП регистрирует значение интерферограммы $A_i = A(\Delta_i)$, образованной взаимодействием K монохроматических волн с волновыми числами γ_k на входе ФП справедливо:

$$A_i = 2\Delta\gamma \sum_{k=0}^{K-1} \Phi_{\gamma_0}(\gamma_k) \cdot \cos(2\pi \cdot \gamma_k \cdot \Delta_i), \quad (1)$$

где Φ_{γ_0} – исследуемый спектр. Выходной сигнал ФП подвергается АЦП и обратному дискретному преобразованию Фурье, в результате которого получается дискретный спектр входного излучения. Для j-го отсчета получаемой нормализованной спектральной характеристики Φ_j можно записать

$$\Phi_j = \frac{1}{M} \sum_{i=0}^{M-1} A(\Delta_i) \cdot \cos\left(2\pi \cdot \gamma_j \cdot \Delta_i\right), \quad (2)$$

Теоретическая разрешающая способность Фурье-спектрометра R_F^{th} в общем случае выражается [5]:

$$R_F^{th} = \frac{\nu}{k/\Delta_m}, \quad (3)$$

где ν – волновое число, k – целые или обратные целым числа, Δ_m – максимальная оптическая разность хода. Из (3) видно, что для улучшения разрешающей способности необходимо увеличивать максимальную оптическую разность хода пучков Δ_m, то есть расстояние L между двумя отражающими поверхностями M_2 и M_1* (рис. 4), что приведет к возрастанию габаритов устройства.

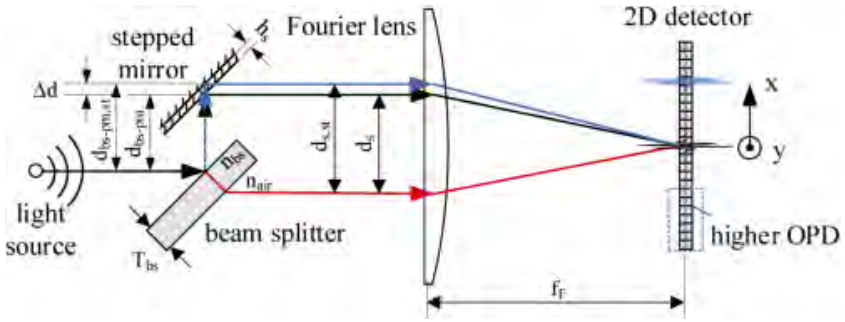


Рис. 4. Схема ОС Фурье-спектрометра со ступенчатым зеркалом

В литературе предлагаются различные способы повышения разрешающей способности без увеличения размеров АОС. Их можно разделить на две группы – технические решения (внесение изменений в конструкцию ОС) и программные решения (внедрение новых методов обработки результатов измерения).

Одно из возможных технических решений предложено в [6]. Авторы описывают ОС с одним ступенчатым зеркалом (рис. 4). В таком спектрометре используется 2D детектор. Регистрируемая интерферограмма расщепляется на две его области, благодаря чему спектральное разрешение увеличивается вдвое.

Другое решение описано в [7]. Авторы предлагают усовершенствованный вариант ОС на основе интерферометра общего пути, построенного на двулучепреломляющих элементах (рис. 6). Эта конструкция получила наименование TWINS (*Translating-Wedge-based Identical pulses eNcoding System*). Ее особенностью является наличие двух клиновидных оптических элемента (рис. 5), один из которых является подвижным.

В конструкции с поперечным размером клиньев 20 мм и размером пучка 5 мм максимально достижимая задержка в среднем ИК диапазоне составляет около 7,5 пс, что соответствует максимальному разрешению 2 см$^{-1}$. Разрешение можно улучшить в два раза, заставив сигнал дважды пройти через клинья TWINS.

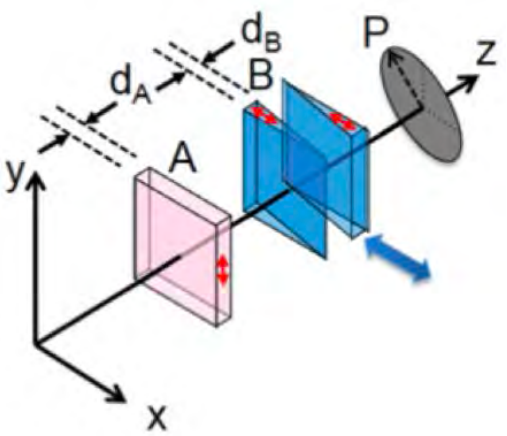


Рис. 5. Интерферометр TWINS

Программные решения могут быть направлены на устранение искажающего влияния аппаратной функции АОС на измеренный спектр. Наиболее известные методики обработки результатов измерений АОС, направленные на разрешение близких линий в спектре, восстановление тонкой структуры отдельных линий, повышение разрешающей способности, описаны в [8]. На рис. 6 в качестве примера проиллюстрирована эффективность обработки спектрограммы методом регуляризации Тихонова.

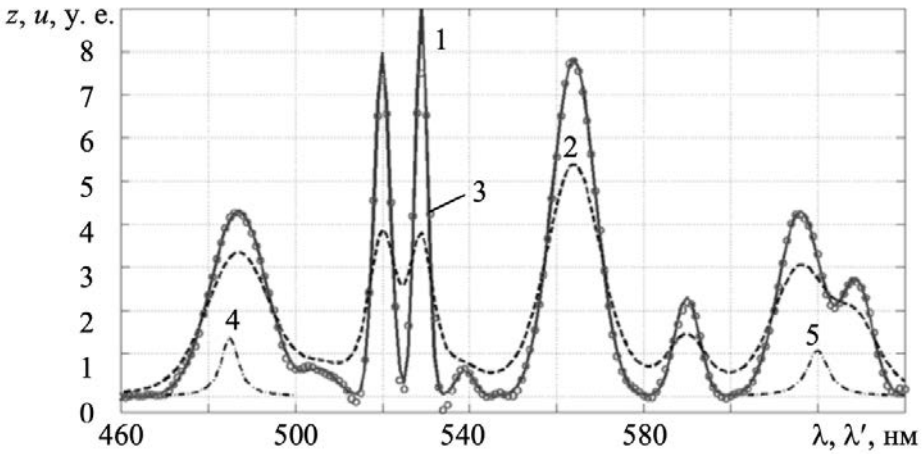


Рис. 6. Пример улучшения измеренного спектра методом Тихонова:
1 – истинный спектр, *2* – измеренный, *3* – восстановленный

Таким образом для улучшения разрешающей способности Фурье-спектрометра можно: увеличивать расстояние между отражающими элементами (увеличить габариты); изменять или улучшать оптические элементы; применить методы обработки зарегистрированных сигналов.

Список используемых источников

1. Мандель А. Е. Метрология в оптических телекоммуникационных системах: учеб. пособие [Электронный ресурс]. Томск : ТУСУР, 2014. 139 с. URL: https://edu.tusur.ru/publications/3733
2. Лебедева В. В. Экспериментальная оптика. 4-е изд. М. : Физический факультет МГУ им. М. В. Ломоносова, 2005. 282 с.
3. Фраз А. В. Оптический анализатор спектра на основе объёмной дифракционной решётки: бакалаврская работа : 12.03.03 / Фраз Алексей Вячеславович. СПб., 2020. 76 с.
4. Былина М. С., Глаголев С. Ф. Методы и приборы для оптических измерений в инфокоммуникациях. Часть 2. Спектральные измерения. Измерения параметров волоконно-оптических линейных трактов: учебное пособие. СПб. : СПбГУТ, 2021. 78 с.
5. Ефимова А. И., Зайцев В. Б., Болдырев Н. Ю., Кашкаров П. К. Инфракрасная Фурье-спектрометрия: учеб. пособие. М. : МГУ, 2008. 133 с.
6. Köhler M. H., Schardt M., Müller M., Kienle P., Wang K., Dong X., Giebeler C., Wiesent B. R., Jakobi M., and Koch A. W. Static Fourier transform mid-infrared spectrometer with increased spectral resolution using a stepped mirror // OSA Continuum. 2020. N 3. PP. 2134–2142.
7. Réhault J., Borrego-Varillas R., Oriana A., Manzoni C., Hauri C. P., Helbing J., and Cerullo G. Fourier transform spectroscopy in the vibrational fingerprint region with a birefringent interferometer // Opt. Express. 2017. N 25. PP. 4403–4413.
8. Сизиков В. С., Лавров А. В. Современные устойчивые математические и программные методы восстановления искаженных спектров // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. N 6. С. 911–931.

УДК 004.043
ГРНТИ 81.93.29

АНАЛИЗ ПОДХОДОВ К АВТОМАТИЧЕСКОЙ ОБРАБОТКЕ РЕЗУЛЬТАТОВ ФАЗЗИНГ-ТЕСТИРОВАНИЯ

Д. Р. Валеев, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Современные подходы к реализации фаззинг-тестирования показывают себя настолько эффективно, что зачастую превосходят возможности ответственных за их обработку аналитиков. Данные факторы приводят к увеличению времени между выявлением дефекта и его исправлением, неоптимальной приоритизации задач обработки и влиянию человеческого фактора. В работе проанализированы доступные подходы к автоматизации обработки результатов фаззинг-тестирования и возможные направления развития этих методик.

фаззинг, автоматическая обработка дефектов, локализация дефекта.

Введение

Фаззинг – это автоматизированная техника тестирования программного обеспечения, заключающаяся в передаче приложению на вход неправильных, неожиданных или случайных данных. Фаззинг особенно эффективен для поиска уязвимостей, связанных с некорректной работой с памятью [1]. Информация от Microsoft и Google свидетельствует, что доля уязвимостей, связанных с некорректной работой с памятью, в их продуктах составляет от 70 % до 90 % [2, 3].

Типичная схема реализации фаззинга включает следующие этапы.

1. *Подготовка*. На этом этапе собираются образцы входных данных для целевого приложения, и подготавливается сборка целевого приложения со встроенным дополнительным кодом, так называемая *инструментированная сборка*, позволяющая получать требуемую информацию о ходе выполнения кода, например, собрать сведения о покрытии или обнаружить ошибки времени исполнения (так называемая санитизация).

2. *Фаззинг*. Результатом этого этапа являются входные данные, приводящие к срабатыванию детектора ошибок, в качестве которого зачастую используется аварийное завершение приложения.

3. *Предобработка ошибок*. Этот этап включает в себя успешное воспроизведение выявленных дефектов и их дедупликацию.

4. *Анализ дефектов*. Результатом этого этапа для каждой уникальной ошибки является отчёт с указанием места ошибки, её классификации, оценки с точки зрения влияния на безопасность приложения, а также дополнительная информация для разработчиков.

Слабость этой схемы – в том, что фаззинг зачастую генерирует большое количество результатов, что приводит к позднему получению результатов и снижению качества анализа.

В индустрии широко распространена автоматизация лишь некоторых этапов обработки результатов, причём распространённые способы зачастую оставляют желать лучшего [4]. Рассмотрим эти этапы и известные варианты их автоматизации.

Воспроизведение

Проблема воспроизведения ошибок связана с тем, что некоторые виды дефектов проявляются с низкой вероятностью или при условиях, которые не всегда получается воспроизвести вне фаззинг-сессии. Примеры таких дефектов – это состояние гонки и повреждение памяти, где воспроизводимость зависит от вероятностного фактора. Авторами было найдено упоминание только одного продукта для решения этой проблемы, находящегося в коммерческой эксплуатации. Это внутренний продукт Microsoft названный TKO [4]. TKO – это детерминированная среда исполнения, позволяю-

щая осуществлять полносистемную эмуляцию. Одним из возможных альтернативных ТКО подходов является решение, пробная реализация которого была осуществлена авторами ранее. Это решение основано на применении специализированной среды исполнения пользовательского уровня, которая фиксирует все источники энтропии в ходе исполнения кода. Примером такой среды может служить проект RR от Mozilla. Согласно замерам авторов RR, в случае использования такой среды, замедление исполнения - не более чем в 2 раза, что существенно ниже, чем у большинства санитайзеров.

Дедупликация

Суть проблемы, лежащей в основе дедупликации заключается в том, что трактовка уникальной ошибки у популярных фаззеров и у аналитиков существенно различается, при этом подходы фаззеров к оценке количества дефектов дают превышение над оценкой аналитиков примерно на 2 порядка [5]. Многие фаззеры для определения уникальности ошибки используют информацию о покрытии, тогда как аналитиков интересуют первопричины возникновения неверного поведения. Анализ тысяч дефектов вручную требует слишком большого количества ресурсов, так что перед началом анализа необходимо осуществить дедупликацию, т. е. разбиение множества всех дефектов на кластеры, соответствующие уникальным дефектам. Такая группировка позволяет избежать анализа всех дефектов, а вместо этого анализировать по одному дефекту из кластера.

Все проанализированные подходы к дедупликации можно отнести к одному из трех классов: основанные на стек-трейсе в момент сбоя, основанные на достигнутом в ходе выполнения приложения покрытии кода, основанные на месте сбоя.

На текущий момент в индустрии широкое применение нашли способы, основанные на анализе стек-трейса. Например, этот подход используется в продуктах ClusterFuzz от Google и OneFuzz от Microsoft. Также, ИСП РАН развивает свой продукт CASR, базирующийся на этом подходе. К достоинствам этого похода можно отнести его низкие накладные расходы, при этом его точность часто подвергается критике, особенно это касается ошибок, связанных с повреждением памяти в случае фаззинга без дополнительной санитизации [4].

Способы основанные на анализе покрытия, получили распространение, так как используются в AFL-подобных фаззерах. Этот подход, в том виде, как он реализован в фаззерах, как правило, является отправной точкой к дедупликации. Дальнейшее его развитие состоит в преобразовании графа покрытия, его упрощении и сравнении на основе полученных результатов. Примером такого подхода является работа [6].

Дедупликация только на основе места сбоя используется редко, так как склонна как к занижению, так и переоценке количества дефектов [4].

Локализация заключается в том, чтобы выявить участок или участки кода с некорректным поведением, которое в конечном итоге приводит к сбою, выявленному в процессе фаззинга. Результатом этого этапа является место или места в коде, которые наиболее вероятно являются причиной сбоя приложения, а также дополнительная информация о том, какие нарушились условия и как, что привело к сбою приложения.

Для решения этой задачи предложены следующие ниже подходы.

1. Основанные на месте сбоя. Это самый простой подход, исходящий из того, что причина сбоя и сам сбой находятся рядом, что зачастую неверно. Другой недостаток этого метода в том, что он не дает информацию о том, нарушение каких условий привело к ошибке.

2. Основанные на разнице в ошибочном и безошибочном поведении приложения. Эти подходы анализируют поведение приложения в случае проявления ошибки и в близких ситуациях, но, когда ошибка не проявляется. Одна из главных практических проблем этого направления – получение большого количества тестовых данных, провоцирующих проявление ошибки и очень похожих, но не провоцирующих его.

3. Основанные на внедрении локализации в процесс непрерывной интеграции, при этом система локализации имеет доступ к истории изменений, вносимых в кодовую базу.

Подводя итог, стоит отметить, что на практике встречается только реализация локализации по месту сбоя.

Классификация и оценка критичности

Задача автоматической оценки влияния обнаруженного дефекта на безопасность, а также его классификация очень полезны для приоритизации исправления. Для автоматизации оценки критичности используются два метода.

1. Основанный на определении того, какого типа дефект произошёл. Чем точнее и конкретнее удается определить тип дефекта, тем более точно можно судить об эксплуатируемости дефекта. Информация о типе дефекта берется либо из имеющегося состояния на момент сбоя приложения, либо из отчетов санитайзеров, если таковые имеются.

2. Основанный на применении техник автоматической генерации эксплоитов, которые будет рассмотрен далее.

Автоматическая эксплуатация

Очевидным, наиболее надежным и общепризнанным вариантом оценки серьезности уязвимости является создание эксплоита. Главный не-

достаток этого подхода в том, что для реализации эксплоита нужны специалисты с развитыми навыками в реверс-инжиниринге и владеющие множеством методик эксплуатации.

Автоматизация генерации эксплоитов, как правило, основана на применении символьного исполнения, использование которого открывает большой простор с точки зрения анализа кода, но в то же время накладывает ограничения на сложность производимого анализа, так как подход является очень ресурсоемким.

Естественными направлениями совершенствования для этих систем является сокращение ограничений на объем исследуемого кода, увеличение количества поддерживаемых типов дефектов и методик смягчения их последствий, реализованных в современных ОС, процессорах и компиляторах.

Сводная таблица

Как можно видеть в таблице 1 (см. ниже), некоторые этапы могут повторно использовать данные других этапов.

Например, имея данные по локализации дефекта, можно повысить точность дедупликации, которая, в идеальном случае, должна производиться на основе данных локализации. Также, зная место нарушения предиката безопасности, можно использовать его для локализации.

Целью исследований авторов является поиск такой комбинации подходов к анализу дефектов, которая бы позволяла существенно сократить общее время обработки результатов фаззинг тестирования при несущественном повышении накладных расходов, не требующих вовлечения квалифицированных аналитиков.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Ding Z. Y., Goues C. L. An Empirical Study of OSS-Fuzz Bugs // arXiv:2103.11518. 2021. P. 4.

2. Miller M. Trends, challenges, and strategic shifts in the software vulnerability mitigation landscape // BlueHat IL, 2019. PP. 11–14.

3. Stoep J. V., Zhang C. Queue the Hardening Enhancements // Google. 2019. URL: https://security.googleblog.com/2019/05/queue-hardening-enhancements.html (дата обращения 02.05.2023).

4. Aquino R. Mitigating vulnerabilities in endpoint network stacks // Microsoft. 2020. URL: https://www.microsoft.com/en-us/security/blog/2020/05/04/mitigating-vulnerabilities-endpoint-network-stacks (дата обращения 02.05.2023).

5. Klees G., Ruef A., Cooper B., Wei S., Hicks M. Evaluating Fuzz Testing // arXiv:1808.09700. 2018. P. 11.

6. Jiang Z., Jiang X., Hazimeh A., Tang C., Zhang C., Payer M. Igor: Crash Deduplication Through Root-Cause Clustering // Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. 2021. PP. 3318–3336.

ТАБЛИЦА 1. Сводная таблица методик, применяемых на разных этапах автоматической обработки результатов фаззинг-тестирования

Этап	Промежуточные и финальные артефакты	Методики
Воспроизведение	Состояния источников энтропии в ходе выполнения целевого приложения; **приложение в состоянии сбоя с возможностью исполнения назад**	Полносистемная эмуляция с записью/ воспроизведением хода исполнения; частичная эмуляция в пользовательском режиме с записью/ воспроизведением источников энтропии
Дедупликация	Состояние и покрытие в момент сбоя приложения; инструментированная сборка (санитизация, покрытие); **сгруппированные по причине сбоя входные данные**	Обратный taint-анализ, позволяющий найти источник данных, приведших к сбою
Локализация	Состояние и покрытие в момент сбоя приложения; трассы с ошибочным и безошибочным выполнением, разнообразные проявляющие дефект образцы выходных данных; **набор вероятных причин дефекта**	Генерация разнообразных входных данных с помощью подхода exploration mode, из фаззера AFL
Классификация и оценка критичности	Инструментированная сборка (санитизация); состояние в момент сбоя приложения; **оценка критичности и класс дефекта**	Обратный taint-анализ; автоматическая эксплуатация
Автоматическая эксплуатация	Место нарушения предиката безопасности; **входные данные, приводящие к эксплуатации дефекта**	Символьное исполнение, taint-анализ

УДК 621.396.677.3
ГРНТИ 47.45.29

ИССЛЕДОВАНИЕ ВОПРОСОВ ВИЗУАЛИЗАЦИИ РЕЛЬЕФА ДЛЯ РЕШЕНИЯ ЗАДАЧ РАДИОТЕХНИКИ

Н. А. Васильев, М. А. Гегельский

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С.М. Буденного

При решении задач радиотехники можно столкнуться с трудностями, которые невозможно решить без использования трехмерной модели местности. Данная проблема является актуальной и по сей день, так как решение задач путем моделирования требует не только правильных математических расчётов, но также требует учитывать рельеф местности, на котором происходит моделирование.

рельеф, радиотехника, исследование.

Одной из задач, где приходится использовать карту является радиолокация. В задачах радиолокации часто используются радиолокационные станции, задачей которых является обнаружение целей, измерение координат и скорости движения объекта, разрешение целей, а также классификация объектов. Для достижения точного определения местоположения цели используются точечные ориентиры, которые выбираются по карте, исходя из их местоположения.

Использование карты позволяет заранее определить место, которое обеспечит наиболее лучшую передачу сигнала. Именно поэтому ее использование может стать необходимым, особенно в городских условиях, а определении места для установки вышек сотовой связи.

Матрицы высот представляет собой растровую модель местности, имеющую трехмерную структуру. Получить ее можно преобразованием исходных данных, которые являются векторами, в растровый вид, в дальнейшем этот вид можно дополнять другими растровыми моделями, используя метод интерполяции. Имея регулярную структуру, матрица высот содержит информацию о элементах, которая представляет из себя высоты рельефа. Каждая такая матрица может содержать в себе информацию о абсолютном рельефе, или относительные высоты, или их сумму [1].

При использовании матрицы с относительными высотами рельеф формируется в виде плоскости, не имеющей высоту, то есть мы получим 2D изображение с изометрическим видом на него.

Для начала работы необходимо открыть нужный нам файл. Далее необходимо узнать с помощью какого драйвера будет происходить чтение файла. Следующим шагом было решено указать размер растра, это необходимо для некоторых операций в будущем.

Для осуществления дальнейших действий необходимо знать над каким слоем будет происходить работа, значит следует вывести сообщение о том в каком слое мы находимся [2].

Далее надлежит узнать систему координат, это необходимо сделать чтобы получить информацию о координатах и привязке изображения к конкретному участку Земли. Данное действие является необходимым, так как исходный файл имеет регулярную структуру и нам нужно знать не только координаты привязки, но и шаг, с которым идут эти координаты.

Следующий важный шаг – это получение высот. Для того чтобы это узнать нужно иметь информацию о слое, из которого мы хотим получить информацию о высотах, что мы уже сделали ранее.

Использованный способ позволяет не только вывести весь массив с высотами, но и посмотреть какую-то отдельную его часть.

Последним шагом является построение трехмерного изображение рельефа местности, который находился в исходном файле.

Стоит отметить, что способ используемый в данной программе создан для неквадратных матриц, что влечет за собой некоторые сложности в реализации, в отличие от квадратных матриц.

В качестве выходных данных имеем информацию, которую мы извлекли из файла после работы кода, а также построенное трехмерное изображение рельефа Земли.

На рис. 1 приведена информация о типе используемого файла.

```
<class 'osgeo.gdal.Dataset'>
------------------------------
```

Рис. 1. Тип используемого файла

На рис. 2 показаны данные о используемом драйвере, для работы с данным типом файла.

```
----------------------------------------------------------------
Driver short name RMF
----------------------------------------------------------------
Driver long name Raster Matrix Format
----------------------------------------------------------------
```

Рис. 2. Используемый драйвер

С помощью драйвера Raster Matrix Format можно извлечь данные о пространственных привязках и метаданных содержащихся в исходном файле.

На рис. 3 указаны размер растра и номер слоя в котором осуществляется работа.

```
Raster size 1781 x 1994
Number of bands 1
```

Рис. 3. Размер растра и номер исследуемого слоя

На рис. 4 указана информация о используемой системе координат, а также информация о привязке, кроме этого показаны координаты левого верхнего угла, от которого начинается построение матрицы высот и показана регулярность структуры файла формата MTW.

```
Projection PROJCS["unnamed",
    GEOGCS["Pulkovo 1942",
        DATUM["Pulkovo_1942",
            SPHEROID["Krassowsky 1940",6378245,298.3,
                AUTHORITY["EPSG","7024"]],
            TOWGS84[23.92,-141.27,-80.9,0,0.35,0.82,-0.12],
            AUTHORITY["EPSG","6284"]],
        PRIMEM["Greenwich",0,
            AUTHORITY["EPSG","8901"]],
        UNIT["degree",0.0174532925199433,
            AUTHORITY["EPSG","9122"]],
        AUTHORITY["EPSG","4284"]],
    PROJECTION["Transverse_Mercator"],
    PARAMETER["latitude_of_origin",-5.729577951308232e-007],
    PARAMETER["central_meridian",45],
    PARAMETER["scale_factor",1],
    PARAMETER["false_easting",8500000],
    PARAMETER["false_northing",0],
    UNIT["Meter",1]]
Geo transform (8492400.0, 119.99999999999999, 0.0, 5995200.0, 0.0, -119.99999999999999)
```

Рис. 4. Информация о системе координат

Из рис. 4 видно регулярность структуры данного файла, на это указывает шаг, с которым изменяются координаты, который равен 119.(9). Из этой информации можно сделать вывод о том, почему данный формат занимает такой малый объем памяти. Это связано с тем что в файле нет необходимости хранить координаты для каждой высоты, вместо этого хранится лишь информация о углах растра и шаг с которым происходит изменение координаты [3]. Именно этот способ позволил заметно уменьшить объем занимаемый файлом.

Чтобы построить трехмерную модель нам необходимо иметь начальные координаты, которые задаются от нуля функции x и y возвращают значения строки для того чтобы построение проходило построчно. Далее мы указываем координаты высоты Z, все высоты нам уже известны из предыдущего шага. Следующим действием является само построение, в котором указывается по каким координатам будет осуществляться построение [4].

На рис. 5 приведено трехмерное изображение рельефа.

Для проверки правильной работы программы сравним полученное трехмерное изображение и сравним с реальным изображением с карт. На рис. 6 представлены два изображения, слева полученное путем моделирования трехмерного изображения местности, справа изображение с топографической карты карты.

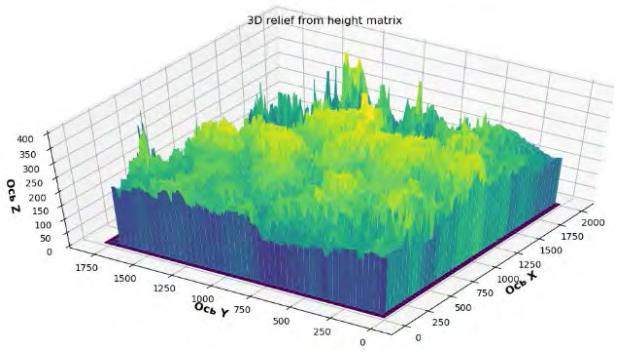


Рис. 5. Трехмерное изображение местности

По рисунку можно заметить некоторые различия, которые связаны с использованием разный цветовых схем на картах, если же сравнивать высоты в конкретных точках, то они совпадают на сто процентов. Шаг исходной карты двадцать минут.

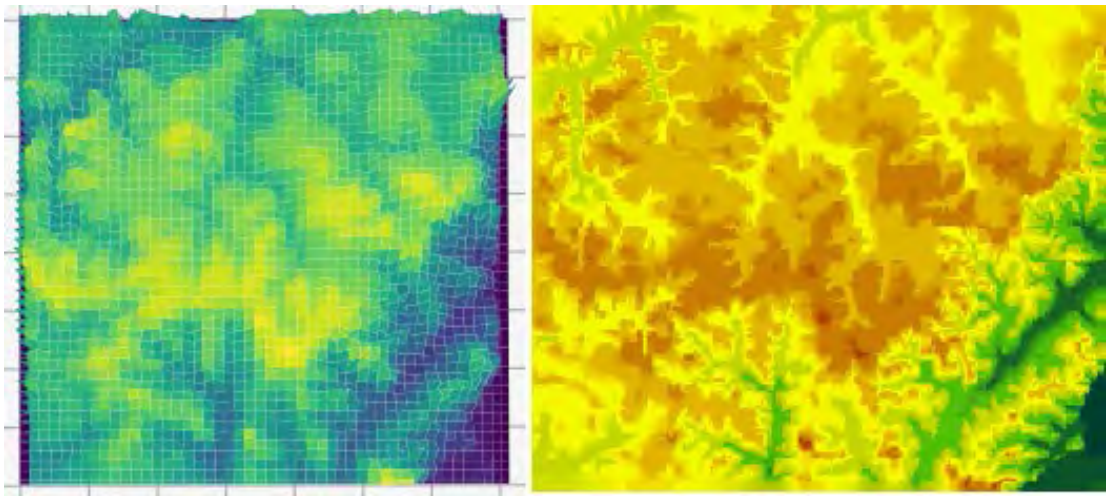


Рис. 6. Рельеф местности Пензенской области

В современном мире моделирование экспериментов используется во многих отраслях науки и промышленности. Одну из ключевых позиций занимает моделирование с использованием трехмерных моделей Земли и отдельных ее участков для различных целей. Популярность данного метода легко объяснить, при моделировании можно использовать не только существующие объекты, но и объекты, находящиеся на стадии проектирования. Это значит, что можно опробовать новые технические решения и внести в них правки, что в свою очередь значительно повышает качество проектов. Именно поэтому моделирование используют и в областях, связанных с радиотехникой.

Список используемых источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр. : пер. с англ. М. : Вильямс, 2003. 1104 с. : ил. ISBN 5-8459-0497-8 (рус.).

2. Тихонов В. И., Хименко В. И. Выбросы траекторий случайных процессов. М. : Наука, 1987. 304 с.

3. Левин Б. Р. Теоретические основы статистической радиотехники. Книга 1. М. : Советское радио, 1974. 552 с.

4. Миронова Ю. Н. Применение систем глобального позиционирования в геоинформационных системах. // Теоретические и прикладные проблемы географии: материалы международной научно-практической конференции (Астана, 9–10 июня 2014 г.). Астана, 2014. Часть II. С. 307–309.

5. ESRI (July 1998). "ESRI Shapefile Technical Description" (PDF). Retrieved 2007-07-04.

Статья представлена научным руководителем, заместителем начальника НИЦ ВАС, кандидатом технических наук О. А. Михалевым.

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ ПРИНЦИПОВ ВЫДЕЛЕНИЯ ВИРТУАЛИЗИРОВАННЫХ РЕСУРСОВ ДЛЯ СЕТЕВЫХ СЕГМЕНТОВ В СЕТЯХ МОБИЛЬНОЙ СВЯЗИ

А. С. Васин, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Возникновение парадигмы сетевой сегментации для сетей 5G предоставляет новые возможности для поставщиков услуг при совместном использовании облачной инфраструктуры. В данной статье проводится анализ существующих моделей динамического масштабирования ресурсов виртуальных сетевых функций для сетевых сегментов. При реализации таких моделей поставщики облачной инфраструктуры могут применять технологии прогнозирования для динамического выделения сетевых ресурсов при соблюдении соглашений об уровне обслуживания сетевых сегментов. Для прогнозирования утилизации ресурсов виртуализированной инфраструктуры используются модели LSTM. Рассмотрена обобщенная модель автоматизированного масштабирования ресурсов на основе архитектуры виртуализации сетевых функций.

NFV, SDN, 5G, сетевая сегментация, глубокое обучение, масштабирование ресурсов, MANO, VNFM, NFVO, Bi-LSTM.

Помимо явных преимуществ в расширении полосы пропускания, уменьшения сквозной задержки и увеличении надежности сети связи, эксплуатация сетей 5G будет зависеть от того как операторы управляют своей

инфраструктурой. В отличие от относительно монолитной (модульной) архитектуры в сетях 3G и 4G, сети 5G построены на основе микросервисной архитектуры. Поэтому сети 5G обеспечивают высокую гибкость: виртуализация сетевых функций способствует внедрению разнообразных услуг и функций по требованию, которые могут быть развернуты с помощью облачной инфраструктуры (IaaS). Данный функционал открывает новые возможности для мобильных операторов: при использовании монолитной архитектуры размещение различных сервисов на одной и той же инфраструктуре невозможно.

Ключевой технологией в сетях 5G является технология сетевой сегментации [1], с помощью которой можно развернуть несколько независимых логических сетей, использующих ресурсы одной общей облачной инфраструктуры. При этом возникают значительные проблемы при выборе требуемых сетевых функций, управлении ресурсами и масштабировании [2]. Необходимо гарантировать предоставление услуг удовлетворяя требования, предъявляемые к уровню обслуживания (SLA), несмотря на изменчивое поведение конечных пользователей в каждом сегменте. Для этого должна быть возможность масштабирования сетевых сегментов в соответствии с потребностями пользователей, т.е. увеличения или уменьшения количества задействованных виртуальных ресурсов для каждой виртуальной сетевой функции (VNF) в зависимости от поведения пользователей.

Модели динамического масштабирования могут быть основаны на предопределенных пороговых значениях и прогнозируемом значении утилизации сетевых ресурсов в будущем с использованием алгоритмов машинного обучения. Модели на основе предопределенных пороговых значений просты в реализации и использовании. В этом случае масштабирование ресурсов занимает некоторое время, так как время развертывания виртуальной машины (VM) колеблется от нескольких секунд до нескольких минут. Это, в свою очередь, может привести к нарушениям в SLA предоставляемых услуг. Модели масштабирования, основанные на прогнозируемом значении утилизации сетевых ресурсов, позволяют своевременно управлять сетевыми ресурсами.

Прогнозирование утилизации ресурсов облачной инфраструктуры является одной из важных областей исследований. Модели на основе различных типов долгой краткосрочной памяти LSTM (Long Short Term Memory) [3, 4] являются примерами данных исследований. Особенностью алгоритма LSTM является способность сохранять информацию в течение длительного периода времени. LSTM состоит из трех уровней: слой фильтра забывания, слой входного фильтра и слой выходного фильтра (рис. 1) [5].

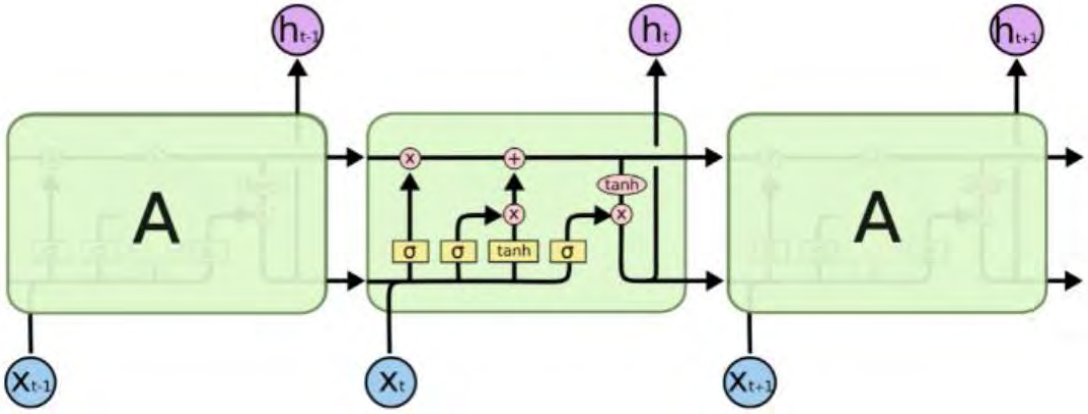


Рис. 1. Модель LSTM алгоритма

Слой фильтра забывания определяет, какая часть предыдущих данных будет забыта и какая часть предыдущих данных будет использоваться на следующем этапе. Значение этого вентиля находится в диапазоне «0-1». «0» определяет забытие предыдущих данных, «1» определяет использование предыдущих данных.

Слой входного фильтра включает слой tanh и отвечает за получение новых данных. Ненужная часть входных данных отфильтровывается сигмовидной функцией, затем с помощью функции tanh определяются новые возможные данные. Умножение результата на выходе сигмовидной функции и результата на выходе функции tanh определяет обновление и получение нового состояния ячейки.

Слой выходного фильтра определяет состояние ячейки с помощью функции tanh. Входные данные фильтруются сигмовидной функцией. Умножение результата фильтрации сигмовидной функцией и результата на выходе функции tanh определяет выходные данные.

Более усовершенствованным алгоритмом прогнозирования является двунаправленная LSTM (Bi-LSTM) (рис. 2) [6]. Алгоритм Bi-LSTM представляет процесс, при котором нейронная сеть получает информацию о последовательности в обоих направлениях: в прямом (из прошлого в будущее) и обратном (из будущего в прошлое). В этом случае происходит обработка входной последовательности в обоих направлениях, по сравнению с обычной LSTM.

В [4] рассматривается эффективный механизм упреждающего прогнозирования утилизации ресурсов с использованием кодера-декодера на основе Bi-LSTM. Модель на основе Bi-LSTM с механизмом внимания, достигает высокой точности при краткосрочном и при долговременном прогнозировании, благодаря чему система отслеживает утилизацию ресурсов VNF и автоматически масштабирует ресурсы каждого сетевого сегмента.

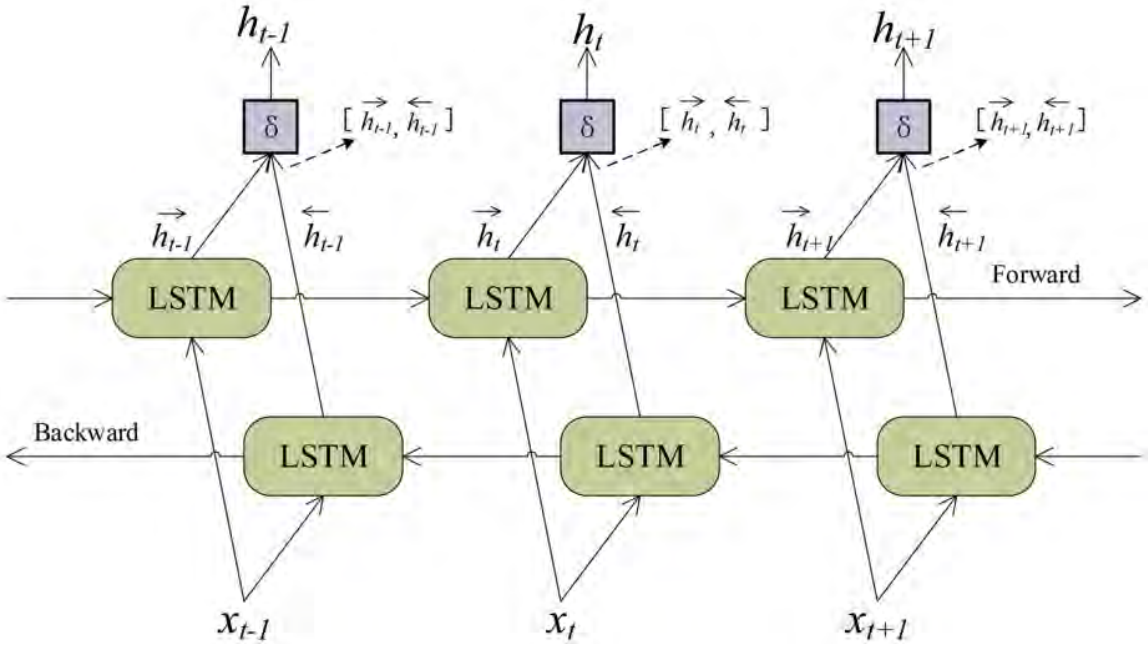


Рис. 2. Модель Bi-LSTM алгоритма

Любая из этих моделей встраивается в архитектуру виртуализации сетевых функций, как показано на рис. 3. NFVO (*Network Function Virtualization Orchestrator*) отвечает за прием статистики утилизации виртуализированных ресурсов VNF, поступающей от VIM (*Virtual Infrastructure Manager*). Далее информация поступает в модуль предварительной обработки статистики утилизации ресурсов VNF, где происходит нормализация данных для более точного прогнозирования. Обработанные данные, представленные в виде временного ряда, поступают в модуль прогнозирования на основе модели Bi-LSTM с механизмом внимания. Временной ряд прогнозируемой утилизации ресурсов VNF поступает на вход механизма принятия решения о масштабировании. Значения принятой последовательности сравниваются с нижним и верхним пороговым значением. На основании этого формируется запрос на добавление или удаление виртуальной машины (VM), который отправляется на VNFM (*Virtual Network Function Manager*). В свою очередь, VNFM посылает запрос к VIM с требованием на выделение или высвобождение ресурсов VM.

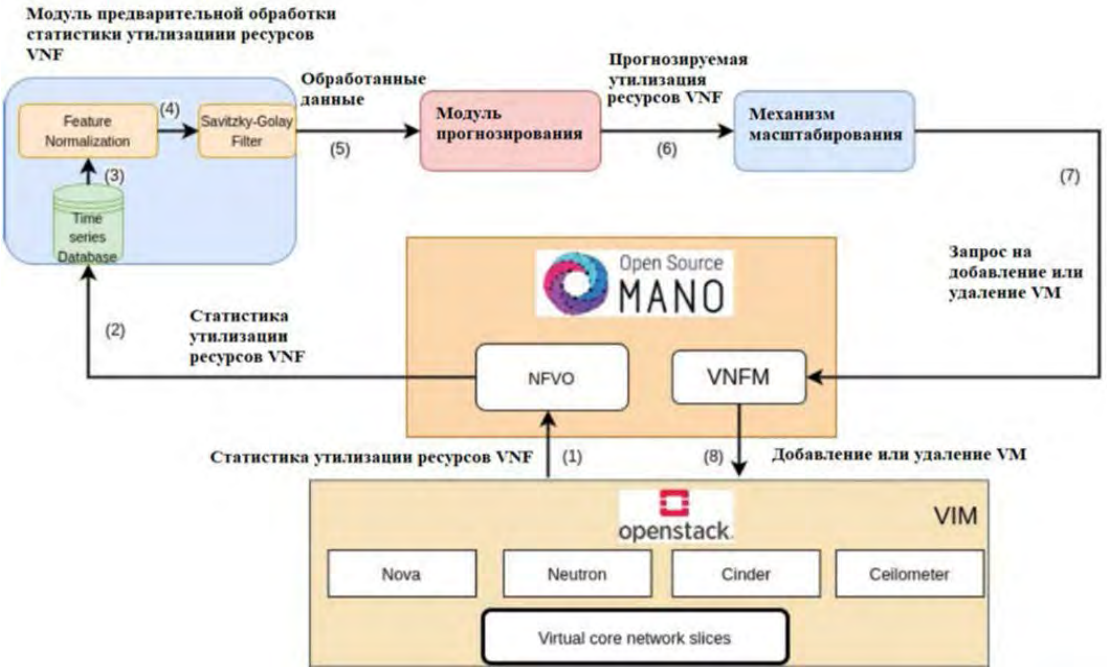


Рис. 3. Модель архитектуры автоматизированного управления виртуализированнми ресурсами

Представленная модель архитектуры автоматизированного управления виртуализированными ресурсами VNF позволяет операторам мобильной связи минимизировать затраты на эксплуатацию облачной инфраструктуры из-за избыточного количества выделенных ресурсов при этом обеспечивая предоставление услуг без нарушений в SLA.

Список используемых источников

1. 3GPP TS 23.501 V17.5.0. System Architecture for the 5G System; Stage 2. 2022. 570 p.

2. Rost P., Mannweiler C., Michalopoulos D. S., Sartori C., Sciancalepore V., Sastry N., Holland O., Tayade S., Han B., Bega D., Aziz D., and Bakker H.. Network slicing to enable scalability and flexibility in 5G mobile networks // IEEE Communications Magazine. May 2017. Vol. 55, N 5. PP. 72–79.

3. Nhu C. N. and Park M. Optimizing resource scaling in network slicing // in Proc. International Conference on Information Networking. Jan. 2022.PP. 413–416,

4. Nhu C. N. and Park M. Dynamic Network Slice Scaling Assisted by Attention-Based Prediction in 5G Core Network // IEEE Access. 2022. Vol. 10. PP. 72955–72972.

5. Akın, Cihan, Kacar, Umit, Kirci, Murvet. Twins Recognition Using Hierarchical Score Level Fusion, URL: http:// https://arxiv.org/ftp/arxiv/papers/1911/1911.05625.pdf/ (дата обращения 23.01.2023).

6. Zheng, Xiao, Chen, Wanzhong. An Attention-based Bi-LSTM Method for Visual Object Classification via EEG // Biomedical Signal Processing and Control, vol. 63, 2021.

УДК 621.396.6
ГРНТИ 49.43.29

ПРИМЕНЕНИЕ МЕТОДА QUASI-QAM МОДУЛЯЦИИ В ЗАДАЧЕ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ ЦИФРОВОГО КАНАЛА СВЯЗИ

Д. А. Веденькин, А. Ф. Гильфанова

Казанский национальный исследовательский университет им. А. Н. Туполева – КАИ

Системы беспроводной связи приобретают все большую популярность благодаря тому, что они обеспечивают высокую скорость передачи данных и малое время задержки в задачах реального времени. Развитие существующих систем цифровой связи, повышение качества связи, а также предложение новых услуг, связаны с необходимостью решения задач электромагнитной совместимости и стабильным функционированием в условиях сложной сигнально-помеховой обстановки.

математическое моделирование, модуляция, квадратурная амплитудная модуляция, сигнальное созвездие, белый шум, цветной шум.

В настоящее время в случае уменьшения уровня сигнал/шум в системах беспроводной связи происходит изменение формата модуляции от более скоростного к более помехоустойчивому и менее скоростному. Кроме того, данный метод улучшения помехоустойчивости может ухудшить качество предоставляемых услуг, а возможно и сделать их предоставление невозможным [1].

Многие авторы проводили исследования для решения данной проблемы. Одни предлагают метод разнесенного приема сигнала, другие реализуют повышение помехоустойчивости путем поворота сигнального созвездия на некоторый угол [2, 3, 4]. Представленный в данном исследовании метод представляет совершенно другой подход к повышению помехоустойчивости.

В [5, 6] предлагается использовать пространство сигналов QAM-64 для передачи QAM-16. Для реализации помехоустойчивой передачи сигнала, предложенного в [7] используется алгоритм, который представлен на рис. 1.

Рассмотрим математическую модель, реализующую данный алгоритм. Для создания исходного информационного сигнала генерируется случайная последовательность из нулей и единиц. Затем формируются передаваемые символы QAM-16, которые подвергаются воздействию аддитивного белого гауссовского шума. В проведенном моделировании отношение сигнал/шум

варьировалось от 0 до 20 дБ. На «приемной» стороне происходит демодуляция и побитовое сравнение «полученной» и исходной последовательностей.

Рис. 1. Блок-схема работы кода

На рис. 2 (см. ниже) показаны местоположения точек на сигнальном созвездии, характеризующие их идеальное, допустимое и ошибочное местоположения.

Для уменьшения количества ошибок, согласно методу quasi-QAM модуляции, точка с наибольшим количеством ошибок должна передаваться с другими координатами. Рассмотрим ситуацию, когда наибольшему воздействию помех подвергается точка с координатами $3 + 1i$. Тогда она может быть перенесена в соседнюю область с координатами $5 + 3i$. Тогда получаем преобразованное сигнальное созвездие (рис. 3). Далее повторяем все операции с сигналом.

Для того чтобы значительно увеличить помехоустойчивость задается условие, при котором сравниваются значения BER сигнала QAM-16 и BER сигнала quasi-QAM-16. Если значение BER сигнала quasi-QAM-16 уменьшилось недостаточно, то информационный сигнал передается еще раз с новой координатой для ошибочной точки (рис. 4).

Для получения наглядных результатов и корректной статистической обработки было проведено исследование 1 000 различных пакетов сигналов по 1 024 бита для каждого уровня шума.

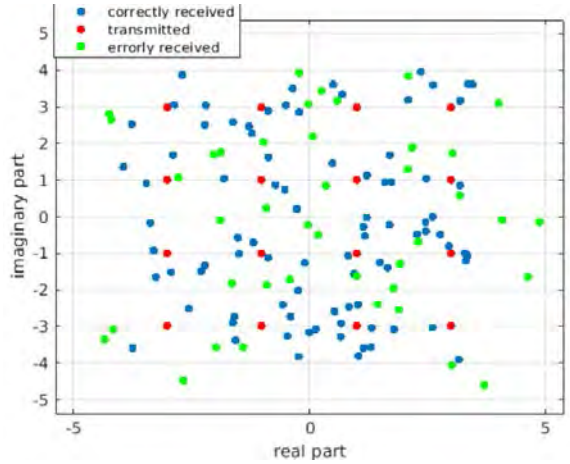


Рис. 2. Сигнальное созвездие принятого сигнала

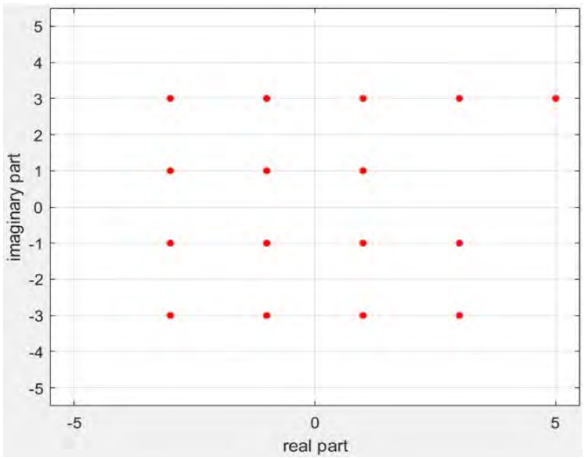


Рис. 3. Измененное сигнальное созвездие

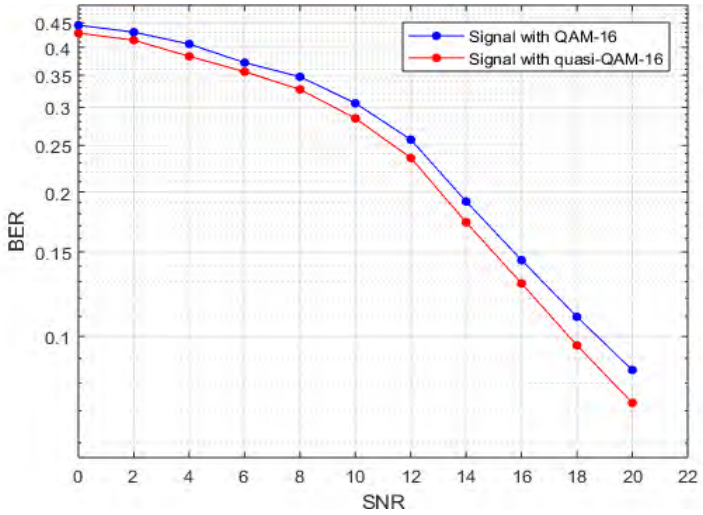


Рис. 4. Зависимость BER от SNR

Таким образом, можно сделать вывод, что представленный в [7] метод, который заключается в выборочном изменении координат точек на сигнальном созвездии, повышает помехоустойчивость сигнала.

Также проводилось исследование канала связи с цветным шумом на основе представленной выше блок-схемы (рис. 1). Информационная последовательность модулируется, после чего к сигналу добавляются различные типы цветного шума.

По результатам проведенного исследования были построены графики (рис. 5), которые показывают зависимость уровня битовых ошибок (BER) от отношения сигнал/шум (SNR) при наличии того или иного типа цветного шума в канале связи.

Из полученных графиков на рисунках 4 и 5 видно, что выигрыш может составлять порядка 10 % при отношении сигнал/шум 10 дБ. Рассмотренный метод позволит увеличить помехоустойчивость сигнала без снижения скорости передачи данных.

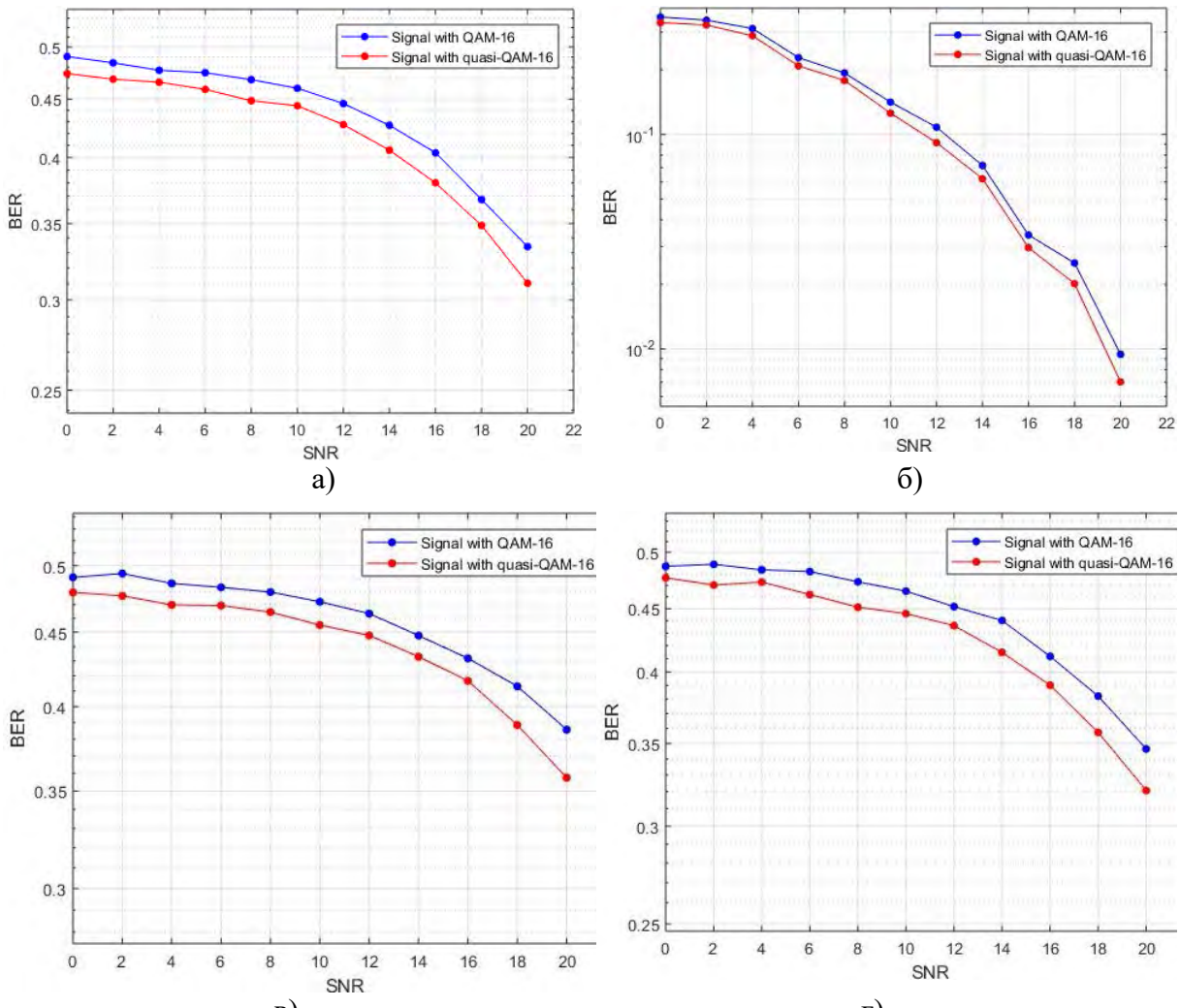


Рис. 5. Зависимость BER от SNR: при воздействии розового шума (а), красного шума (б), синего шума (в), фиолетового шума (г)

Список используемых источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение : пер. с англ. М. : Вильямс, 2003. 1104 с. ISBN 5-8459-0497-8.

2. Шахнович И. DVB-T2 – новый стандарт цифрового телевизионного вещания // Электроника: Наука, Технология, Бизнес. 2009. N 6. С. 30–35.

3. Дворников С. В., Пшеничников А. В., Манаенко С. С. Помехоустойчивая модель сигнала КАМ-16 с трансформированным созвездием // Информационные технологии. 2015. Т. 21. N 9. С. 685–689.

4. Гужва А. Ю. Методика трансформации сигнального созвездия КАМ-16 с изменение его формы // Электросвязь. 2015. N 2. С. 28–31.

5. Гильфанова А. Ф., Веденькин Д. А., Колесникова А. В. Помехоустойчивость цифрового канала связи с quasi-QAM модуляцией под воздействием белого шума // Проблемы техники и технологии телекоммуникаций : материалы XXIV международной научно-технической конференции, Уфа, 23–25 нояб. 2022 г. Уфа : РИК УГАТУ, 2022. С. 21–23.

6. Гильфанова А. Ф., Веденькин Д. А., Колесникова А. В. Помехоустойчивость цифрового канала связи с quasi-QAM модуляцией под воздействием цветных // Проблемы техники и технологии телекоммуникаций : материалы XXIV международной научно-технической конференции, Уфа, 23–25 нояб. 2022 г. Уфа : РИК УГАТУ, 2022. С. 23–24.

7. Гильфанова А. Ф. Повышение помехозащищенности канала связи с квадратурной амплитудной модуляцией // Инженерные кадры – будущее инновационной экономики России. 2019. N 3. С. 22–24.

8. Бердышев В. П., Гарин Е. Н., Фомин А. Н. Радиолокационные системы : учебник / под общ. ред. В. П. Бердышева. Красноярск : Сиб. федер. ун-т, 2011. 400 с.

УДК 654.739
ГРНТИ 49.33.29

ВЫБОР НАИЛУЧШЕГО УЗЛА ДОСТУПА В БЕСПРОВОДНЫХ СЕТЯХ С ВЫСОКОЙ ПЛОТНОСТЬЮ МОБИЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ

Н. А. Верас, В. В. Коньков, Е. А. Махонина, А. В. Поляничева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрена уязвимость браузера Microsoft Edge операционных систем Windows BDU:2022-06064, приведено описание актуальных угроз, основанных на использовании уязвимости. Приводятся описания способов предотвращения нарушений информационной безопасности, а также зафиксированных случаев сетевых атак, проведенных при эксплуатации злоумышленником уязвимости.

информационная безопасность, веб-браузер, Windows, утечки информации.

В настоящее время существует всеобъемлющая потребность пользователей в безопасном использовании веб-ресурсов, а поиск и устранение уязвимостей веб-браузеров являются важными задачами в сфере информационной безопасности. Поэтому исследование уязвимости BDU:2022-06064 является актуальным.

Целью исследования является изучение и описание уязвимости, выявление эффективных решений для борьбы с атаками и утечкой защищаемой информации, возникающими при эксплуатации уязвимости, а также исследование зафиксированных случаев нарушения информационной безопасности с использованием таких атак [1].

Объектом исследования является уязвимость браузера Microsoft Edge с точки зрения возможности проведения спуфинг-атак, при ее выявлении.

Статья нацелена на студентов технических учебных заведений, специалистов, работающих с сетевыми технологиями, а также читателей, которым интересна данная тематика.

Новизна исследования состоит в обобщении изученной литературы, а также данных, публикуемых компаниями по разработке веб-браузеров на тему уязвимостей в сети Интернет, а также изучение отечественных решений по борьбе со спуфинг-атаками [3, 4].

Описание уязвимости

Уязвимость браузера Microsoft Edge операционных систем Windows Уязвимость браузера Microsoft Edge возникает из-за ошибок синхронизации при использовании общего ресурса («ситуация гонки»). Использование данной уязвимости позволяет нарушителям проводить спуфинг-атаки. Уязвимость имеет высокий уровень опасности (базовая оценка CVSS 3.0 составляет 8,1). Уязвимость подтверждена производителем и описывается как, переполнение буфера кучи в графическом процессоре в Google Chrome до 107.0.5304.121, что позволяет удаленному злоумышленнику, скомпрометировавшему процесс рендеринга, потенциально выполнить выход из песочницы через созданную HTML-страницу и имеет идентификатор CVE-2022-4135. По шкале серьезности опасности Chromium уязвимость также оценивается как высокая [5].

Меры защиты

1. Установка обновлений из доверенных источников

3 октября 2022 г. компания Microsoft выпустила последнюю версию Microsoft Edge Stable Channel (*version* 106.0.1370.34), которая включает в себя обновление безопасности проекта Chromium. В Руководстве по обновлению безопасности задокументировано объявление о том, что последняя версия Microsoft Edge (на основе *Chromium*) не является уязвимой при одновременном выполнении с использованием общего ресурса. Однако, компания Google в своих источниках сообщает, что эксплойт для CVE-2022-4135 уже существует. Стоит заметить, что установление любых обновлений программного обеспечения возможно только после оценки всех сопутствующих рисков [2].

2. Использование средств антивирусной защиты с функцией контроля доступа к веб-ресурсам

Антивирусы с функциями контроля использования программ, устройств и веб-ресурсов являются эффективным средством защиты от спуфинг-атак, поэтому целесообразно использование программного обеспечения такого типа для борьбы с угрозами, возникающими на базе

уязвимости BDU:2022-06064. В настоящий момент существуют решения отечественных производителей, позволяющие устанавливать Веб-контроль [2, 3].

3. Применение систем обнаружения и предотвращения вторжений

Такие средства защиты используют метод отслеживания несанкционированных попыток получения доступа к защищаемым ресурсам, называемый мониторингом управления доступом. Задача решений систем обнаружения и предотвращения вторжений состоит в выявлении, а также регистрации уязвимостей в безопасности внутренней инфраструктуры.

Можем выделить и другие эффективные меры защиты, такие как введение регламента по использованию ресурсов сети «Интернет» [3]; отказ от использования запуска браузеров от имени администратора в пользу запуска от имени пользователя минимальными возможными привилегиями в операционной системе и использование альтернативных веб-браузеров, в которых отсутствует рассматриваемая уязвимость.

Далее будет представлена информация об атаках, которая получена с помощью мониторинга открытых источников в сети Интернет и может не соответствовать действительности.

Атаки

1. В Telegram-канале (*https://t.me/itarmyofukraine2022*) с 5 октября 2022 года осуществляется координация DDoS-атаки на сайты российских магазинов торгово-бытового обеспечения военнослужащих «Военторг». Сообщается, что список атакуемых сайтов включает 72 адреса [3, 4].

2. В Telegram-канале (*https://t.me/CyberSquattingChannel*) опубликованы URL-адреса, используемые в атаках с применением социальной инженерии, схожие с адресами интернет-ресурсов крупных российских компаний (такие, как: *new-sber.run.app; sberbank.com.cn; sberget.com; sbertibud.cf; sberukmud.ga; investments-gazprom.online; bonus-vtb24-pozdravlenie.site; sushi-for-you-vtb.ru; sushi-tebe-vtb.ru; sushi-vam-vtb.ru; sushi-vsem-vtb.ru; vtb-bonus.site; gosuslugi-r.ru; gosuslugi.vercel.app; gosuslugl.vercel.app; ozon-hd.hu; wb-ozon-obuchenie.ru; yandex-dellivery.net.ru; yandex-leonteva.ru; yandex-oplata37124.online; yandex-oplata37317.online; yandex-yana.ru; cdek-oplata24127.online; cdek-oplatazakaza.online avito.id13860.ru; avito.id7355.ru; avito.id9217.ru; booking.id1704.ru; cdek.id1789523.ru; cdek.id7355.ru; cdek.id7360.ru; cdek.ord-0125.ru; mvd-oplata.top; mvideo.id1704.ru; ozon.id7354.ru; wildberries.id47218.ru; wildberries.ord1838.ru; yandex-id8512.ru; ozon.id7358.ru; youla-paymo.ru; youla.id11327.ru; youla.id13860.ru; youla.id13875.ru; youla.id5755.ru; youla.id7355.ru; youla.id7358.ru; youla.id9215.ru; youla.id9217.ru; youla.id9218.ru*) [2].

Заключение

В ходе исследования была изучена научная литература, посвященная уязвимостям в веб-браузерах, а также возможным решениям для предотвращения сетевых атак. Полученные результаты были обобщены, а также была выделена уязвимость BDU:2022-06064, приведены ее основные характеристики. Поставленные цели и задачи были достигнуты в полном объеме. Можно сделать вывод о том, что исследование угроз в сети интернет, в том числе атак, проводимых при использовании веб-браузеров остается важной задачей, стоящей перед специалистами информационной безопасности.

Список используемых источников

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 262–266.

2. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление Security Operations Center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 262–266.

3. Пестов И. Е., Гельфанд А. М., Лансере Н. Н., Фадеев И. И.; Программа обеспечения системы компьютерного зрения на основе библиотеки OpenCV; Свидетельство о государственной регистрации программы для ЭВМ № 2020664289 Российская Федерация / Пестов И. Е., Гельфанд А. М., Лансере Н. Н., Фадеев И. И.; заявитель и правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича». № 2020663625; заявл 03.11.2020; опубл 11.11.2020. 1 с.

4. Красов А. В., Гельфанд А. М., Фадеев И. И., Казанцев А. А.; Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры; Свидетельство о государственной регистрации программы для ЭВМ №2020616731 Российская Федерация / Красов А. В., Гельфанд А. М., Фадеев И. И., Казанцев А. А.; заявитель и правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича». № 2020615685; заявл. 29.06.2020; опубл. 10.07.2020. 1 с.

Статья представлена научным руководителем, заведующим кафедрой ЗСС СПбГУТ, доктором технических наук, доцентом А. В. Красовым.

UDK 004+004.93
GRNTI 20.53.19

WEB CONSTRUCTER OF INFOGRAPHICS FOR TRADING PLATFORMS

D. Veselov, T. Ovodova

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents a new application for the improvement of the competitiveness of goods in order to increase the sales coefficient and customer interest. The purpose of this study is to increase the coefficient of sales for goods through the use of the developed web service. The emphasis is placed on trading platforms and opportunities to increase the partners sales by posting beautiful and informative photos of the products offered. It is proposed to create an infographics web service that will allow not only to edit photos uploaded locally, but also to upload all photos of the products from the marketplace by its article number and easily upload them to the marketplace.

web constructor of infographics, an infographics web service, uploading photos of the products, reduction of labor intensity and time costs, synchronization with the trading platform, using API keys of the partners.

The modern market creates a situation where it is necessary to constantly improve the competitiveness of goods in order to increase the sales coefficient and customer interest. There are many ways to do it. In this work, the emphasis is placed on trading platforms and opportunities to increase the sales of partners by posting beautiful and informative photos of the products offered. To solve this problem, it is proposed to create an infographics web service [1] that will allow not only to edit photos uploaded [2, 3] locally, but also to upload all photos of the products from the marketplace by its article number and easily upload them to the marketplace.

The urgency of the task is caused by the reduction of labor intensity and time costs due to synchronization with the trading platform by means of using API keys of the partners.

The purpose of this study is to increase the coefficient of sales for goods through the use of the developed web service.

Application development

1 Description of the system architecture

The CANVAS structure [4, 5] is taken as a basis. It was made specifically to create a two-dimensional image using JavaScript scripts. In other words, most

of the methods and objects have already been created and there is no need to invent anything. Moreover, there are various libraries that further enrich the existing functionality. It allows you to place on the canvas pictures, videos and text, to fill it all with a solid color, to outline the contours or even to add a gradient.

Advantages of using CANVAS:

• Unlike SVG, it is much more convenient to deal with a large number of elements;

• Has hardware acceleration;

• Each pixel can be manipulated;

• Image processing filters can be applied;

• There are many libraries.

The web service consists of the following subsystems [6]:

1. User's personal account.
2. Projects page.
3. The constructor.
4. The module for saving changes.
5. Synchronization module with the trading platform.
6. Template module.

The personal account must provide the display of stored information in the database about the user and provide the opportunity for the user to make changes to this information. The ability to download electronic copies of checks on money transfers carried out by the user through the functionality of the site. All operations should take no more than 2 minutes, if there is a stable Internet connection.

The projects page should display all the projects created by the user from the database, as well as their loading if necessary editing. Request processing time is no more than 1 minute.

The change saving module saves the current version of the project change to the database. Activation occurs when any changes are made to the page with an interval of 2 minutes or when the user clicks on the corresponding button.

The synchronization module with the trading platform should upload photos from the trading platform when the user clicks the upload button. The operation should take an average of 10 to 40 seconds.

The template module provides an operational overlay of data on the user's main photo in accordance with the selected template. The loaded elements must support all the functionality of the constructor module. The operation is processed on the client side, so the time depends on the system capabilities of the user's computer and the Internet.

The constructor module provides interaction with the image by inserting various elements with the possibility of their subsequent configuration. The average response time for any action is 1 second.

If errors occur during the operation of the modules, the user is notified with a corresponding message, and data is sent to the server with a corresponding error.

Diagrams of the functional structures of the service are shown in Fig. 1–2.

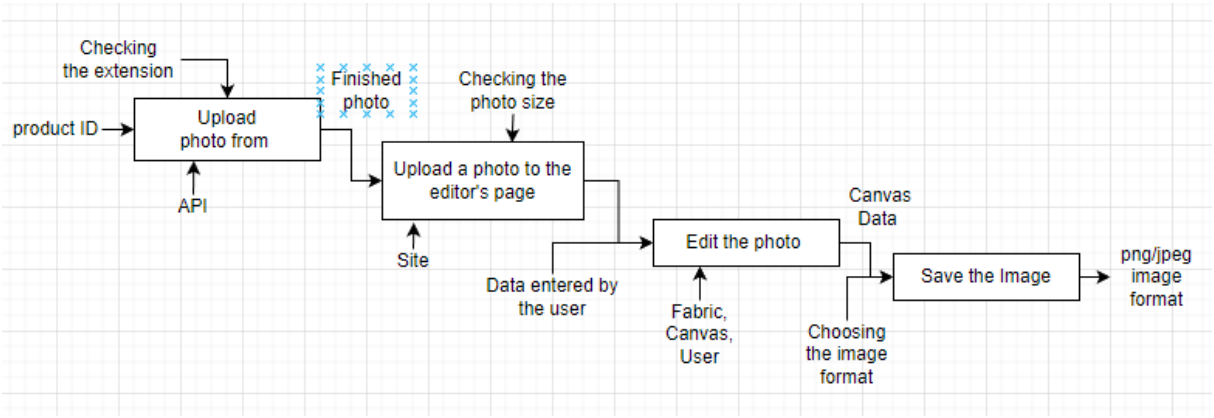


Fig. 1. Extended functional structure diagram

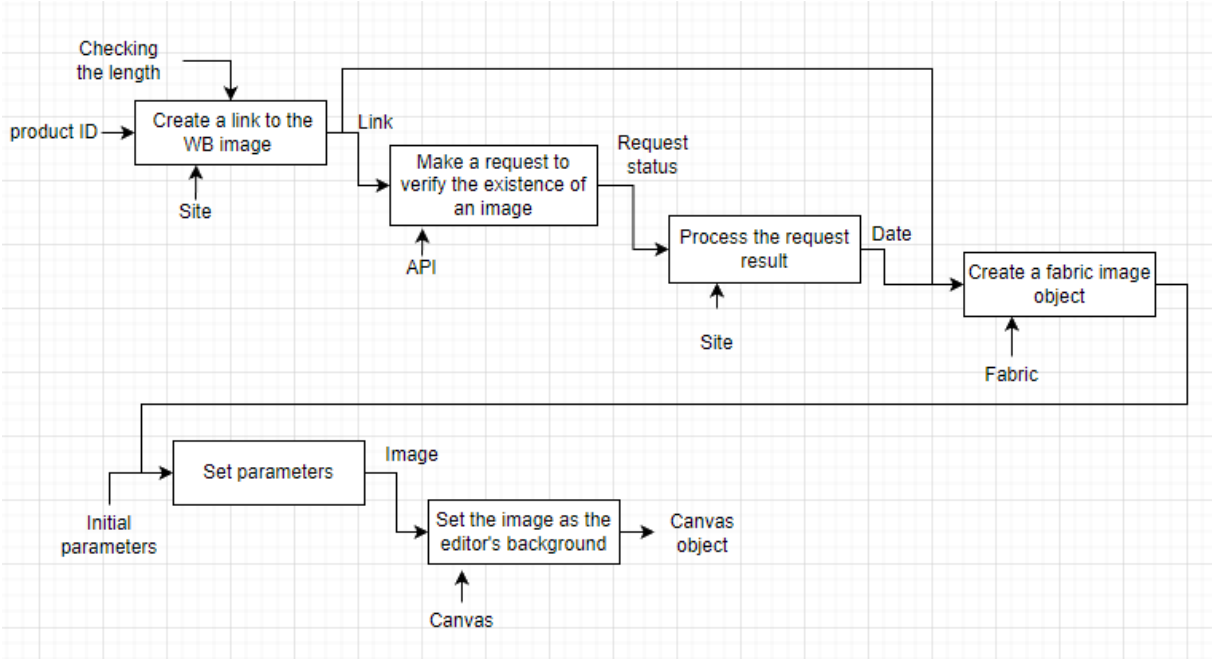


Fig. 2. Decomposition diagram of image loading from a trading platform

2 Ensuring the security of the system

Since the system contains confidential data, it is required to provide access authentication in the system and protect the required information.

To prevent data theft when accessing the database, an Encrypter is used – this is an attribute of changing model fields built into the framework. It provides application-level encryption using the OpenSSL system library and the AES-256-CBC cipher with Message Authentication signature (MAC). We use the main application key as a key that is not stored in the database. It is worth noting that the personal data of users that are used to verify the login, that is, the password, is stored in hashed form thanks to BCRIPT, this prevents the leakage of credentials required to log in. The password is compared using the hash reconciliation

function of the password received and already available in hashed form in the user model.

With the help of a special initial request, we initialize the beginning of the session and the exchange of XSRF tokens, after which the possibility of manipulating this session is provided. XSRF tokens provide protection against cross-site request forgery attacks. When executing a request to the initial endpoint, the session is initialized and the XSRF token is set. If authentication is successful, the session will be marked as "authenticated" with reference to the user ID. All the information of such a session is stored in encrypted cookies, where you can configure the lifetime.

Based on the above information, we can say that the main criterion that the service should implement is to increase the efficiency of working with photos and increase sales revenue. The system must also perform such functions as: synchronization with trading platforms, working with text, working with photos, applying filters to images, working with SVG elements, saving created templates with the possibility of their quick application.

The main motive for creating a service should consist not only in reducing time costs, but also in increasing final sales. The service allows you to achieve a significant increase in quantitative and qualitative indicators in working with images to attract and retain customers, as well as to centralize the storage and processing of various user templates.

References

1. Vladimirov S. S., Nebaev I. A. Internet-texnologii i mul`timedia : laboratorny`j praktikum [E`lektronny`j resurs] / recz. Kognoviczkij O. S.; Federal`noe agentstvo svyazi. Sankt-Peterburg : SPbGUT, 2015. S. 56–58.

2. Filippov F. V. Web-skraping [E`lektronny`j resurs] : uchebnoe posobie / recz. A. V. Shevchenko; Federal`noe agentstvo svyazi, Sankt-Peterburg: SPbGUT, 2020. S. 57–72.

3. Strigina E. V., Sotnikov A. D. WEB-dizajn v e`lektronnom biznese : uchebno-metodicheskoe posobie po vy`polneniyu laboratorny`h i prakticheskih rabot [E`lektronny`j resurs]. Feder. agentstvo svyazi, Federal`noe gosudarstvennoe byudzhetnoe obrazovatel`noe uchrezhdenie vy`sshego obrazovaniya , Sankt-Peterburg: SPbGUT, 2017. S. 34–37.

4. Levchuk Yu. P., Vol`fson M. B., Oxinchenko E. P. Programmny`e sredstva e`lektronny`h predpriyatij uchebnoe posobie [E`lektronny`j resurs] / recz.: S. I. Lutovinov, A. A. Stepanenko; Federal`noe agentstvo svyazi, Sankt-Peterburg: SPbGUT, 2014. S. 89.

5. Korzhinsky S. N. Nastol`naya kniga Web-mastera : e`ffektivnoe primenenie HTML, CSS i JavaScript : monografiya. Moskva, 2000. S. 267–298.

6. Wolfson M. B., Levchuk Yu. P., Oxinchenko E. P. Upravlenie IT-servisami i kontentom : uchebnoe posobie // recz.: A. A. Zaxarov, N. N. Belyaeva; Federal`noe agentstvo svyazi, Sankt-Peterburg: SPbGUT, 2014. S. 62–64.

The article is presented by Associate Professor of the Department of Foreign and Russian Languages of SPbGUT the Candidate of Philological Sciences E. A. Gorshkova.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ SCADA

Н. С. Ветров, Д. Н. Смирнов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья содержит краткий обзор распространенных уязвимостей SCADA-систем, используемых для управления процессами. Описаны основные типы уязвимостей, такие как уязвимости аутентификации, шифрования, ошибок конфигурации, отсутствия обновлений безопасности и программно-аппаратных компонент. Рассмотрены причины возникновения данных уязвимостей, такие как использование слабых паролей, неоптимальные политики безопасности, ошибки программистов и другие.

SCADA, уязвимости, аутентификация, шифрование, конфигурация, обновления безопасности, программно-аппаратные компоненты.

CADA-системы (*Supervisory Control And Data Acquisition*) широко используются в различных отраслях промышленности для мониторинга и управления производственными процессами. Но, как и любая система, SCADA-системы могут стать объектом атак со стороны злоумышленников, что может привести к серьезным последствиям, включая потери человеческих жизней, повреждение оборудования и прерывание производственных процессов [1].

Среди наиболее распространенных уязвимостей SCADA-систем можно выделить:

Уязвимости аутентификации. Плохая практика использования слабых паролей и стандартных инженерных паролей производителями SCADA-устройств создает риски для безопасности системы. Кроме того, пользователи могут использовать простые пароли, которые могут быть легко угаданы злоумышленником. Для предотвращения таких уязвимостей следует использовать сильные пароли и многофакторную аутентификацию.

Уязвимости шифрования. Использование слабых криптографических алгоритмов и управления ключами может привести к возможности для злоумышленников расшифровывать или перехватывать зашифрованные данные. Для защиты от таких уязвимостей следует использовать сильные алгоритмы шифрования и управление ключами.

Уязвимости из-за ошибок конфигурации. Некорректная настройка сетевого оборудования и служб ОС, а также недостаточное разграничение прав доступа и полномочий могут создать уязвимости для злоумышленников. Часто производители SCADA-систем устанавливают неоптимальные

политики безопасности по умолчанию, что также может привести к возможности для атак. Для предотвращения таких уязвимостей следует производить аудит безопасности системы и правильно настраивать политики безопасности [2].

Уязвимости из-за отсутствия обновлений безопасности. Несвоевременная установка обновлений безопасности для различных версий SCADA-систем может привести к возможности для злоумышленников использовать известные уязвимости.

Уязвимости, связанные с управлением доступом и аудитом действий. Некоторые SCADA-системы имеют недостаточно гибкое управление доступом к ресурсам и функциям, что может привести к несанкционированному доступу или повышению привилегий. Кроме того, отсутствие должного аудита действий может привести к невозможности отследить несанкционированный доступ или внесение изменений в систему.

Уязвимости, связанные с удаленным доступом к системе. Использование удаленного доступа к SCADA-системе через интернет может быть небезопасным, особенно при отсутствии необходимых мер безопасности, таких как шифрование трафика, двухфакторная аутентификация и т. д.

Уязвимости, связанные с социальной инженерией. Злоумышленники могут использовать методы социальной инженерии, чтобы получить доступ к системе через обман пользователей или персонала. Например, мошенники могут попытаться получить доступ к паролям или логинам путем обмана пользователей или персонала.

Уязвимости, связанные с эксплуатацией системных уязвимостей. Злоумышленники могут использовать уязвимости в компонентах SCADA-системы, операционной системе, сетевом оборудовании или других компонентах, чтобы получить несанкционированный доступ к системе, повысить свои привилегии или запустить вредоносный код [3].

Уязвимости, связанные с внедрением обновлений и патчей. Несвоевременное внедрение обновлений и патчей может привести к тому, что система останется уязвимой для атак, которые могут быть предотвращены патчами или обновлениями [4, 5].

Уязвимости, связанные с эксплуатацией брешей в SCADA-протоколах. В протоколах SCADA могут существовать уязвимости, связанные с обработкой данных, которые могут быть использованы злоумышленниками для внедрения вредоносного кода, получения доступа к системе, снижения производительности системы и т. д.

Уязвимости, связанные с недостаточной защитой от внешних атак. К таким атакам могут относиться атаки типа Man-in-the-Middle (MITM), атаки перебора паролей, атаки на бреши в системе, направленные на получение прав администратора, и другие.

Уязвимости, связанные с использованием устаревших версий SCADA-программного обеспечения и операционных систем. Устаревшие версии программного обеспечения и операционных систем могут содержать уязвимости, которые были устранены в более новых версиях, поэтому необходимо регулярно обновлять систему SCADA и все ее компоненты [6].

Уязвимости, связанные с использованием подключенных устройств и систем, таких как маршрутизаторы, коммутаторы, мобильные устройства и т. д. Эти устройства могут быть использованы злоумышленниками для получения доступа к системе SCADA или для проведения атаки на систему [7].

Обнаружение и устранение уязвимостей SCADA-системы является важным шагом в обеспечении безопасности системы. Регулярный анализ уязвимостей, аудит системы и реагирование на обнаруженные уязвимости помогут улучшить безопасность системы и защитить ее от возможных атак. Для анализа угроз безопасности SCADA необходимо провести комплексную оценку уязвимостей и рисков, которые могут повлиять на систему SCADA. Для этого можно использовать следующие методы анализа угроз:

Анализ уязвимостей позволяет выявить уязвимости в системе SCADA, которые могут быть использованы злоумышленниками для взлома системы. Анализ уязвимостей может быть проведен путем сканирования портов, тестирования на проникновение и анализа уязвимостей программного обеспечения.

Анализ рисков помогает определить потенциальные угрозы безопасности SCADA и оценить вероятность их возникновения, а также оценить возможные последствия. Анализ рисков может быть проведен путем определения угроз, уязвимостей и оценки важности системных ресурсов.

Анализ доступа позволяет оценить доступ к системе SCADA и определить, кто имеет доступ к критическим ресурсам и данным. Анализ доступа может быть проведен путем проверки прав доступа и аудита системы.

Анализ конфигурации позволяет оценить настройки системы SCADA и определить, насколько они соответствуют рекомендациям по безопасности. Анализ конфигурации может быть проведен путем проверки настроек безопасности, наличия антивирусного программного обеспечения, использования паролей и т. д. [8].

Анализ логов позволяет отслеживать действия пользователей и выявлять несанкционированный доступ или подозрительные действия. Анализ логов может быть проведен путем аудита журналов событий и мониторинга активности пользователей [9, 10].

Социальная инженерия может быть использована злоумышленниками для получения доступа к системе SCADA путем обмана пользователей. Анализ социальной инженерии позволяет определить уязвимости в поведении пользователей и улучшить обучение персонала в области безопасности [11].

В целом, уязвимости SCADA-систем являются серьезной угрозой для критически важных инфраструктур, таких как энергетика, транспорт и производство. Поэтому необходимо принимать все необходимые меры для защиты SCADA-систем от атак, включая использование современных методов шифрования, усиление аутентификации, обновление программного обеспечения и патчей, регулярный аудит системы безопасности, а также обучение персонала.

Список используемых источников

1. Stuart A. Boyer. Scada: Supervisory Control and Data Acquisition. International Society of Automation, USA 2009. 257 p.

2. Ахметов Ф. Р. Причинный анализ критических уязвимостей системы контроля и сбора данных SCADA. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/prichinnyy-analiz-kriticheskih-uyazvimostey-sistemy-kontrolya-i-sbora-dannyh-scada (дата обращения 19.03.2023).

3. Шевяков И. А. Анализ актуальных уязвимостей Scada-систем // Безопасность информационного пространства – 2017. XVI Всероссийская научно-практическая конференция студентов, аспирантов и молодых ученых. Екатеринбург : Южно-Уральский государственный университет, 2018. С. 70–73.

4. Шахновский Г. Безопасность Систем SCADA и АСУТП. [Электронный ресурс] URL: http://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/bezopasnost_sistem_scada_i_asutp (дата обращения 19.03.2023).

5. Кангин В. В. Разработка SCADA-систем. М. : Инфра-Инженерия, 2019. 564 с.

6. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление Security Operations Center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 590–595.

7. Гельфанд А. М., Казанцев А. А., Кузнецов С. А., Смирнов Д. Н. Области применения аналитики больших данных в критических информационных инфраструктурах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022 Т. 4. С. 438–440.

8. Цветков А. Ю. Анализ существующих методов атак типа переполнения буфера на операционные системы семейства Microsoft // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019 Т. 1. С. 751–756.

9. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure // International Russian Automation Conference (RusAutoCon): Institute of Electrical and Electronics Engineers Inc., 2019. PP. 1–5.

10. Бударный Г. С., Казанцев А. А., Красов А. В., Поляничева А. В. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 4. С. 406–411.

11. Макарова А. К., Поляничева А. В., Саматова К. А. Анализ уязвимостей оборудования передачи голосового трафика // Актуальные проблемы инфотелекоммуникаций

науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 665–669.

Статья представлена научным руководителем, заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.413.4
ГРНТИ 28.17.31

МЕТОДОЛОГИЯ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОЦЕНИВАНИЯ ПОКАЗАТЕЛЕЙ РИСКА УПРАВЛЯЮЩИХ РЕШЕНИЙ ПО СОЗДАНИЮ СОВРЕМЕННЫХ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ

Р. М. Вивчарь, С. О. Румянцев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлена методология разработки программного обеспечения для оценивания рисков управляющих решений по созданию систем передачи данных. Определенна методология для оценивания показателей риска. Предложена структура программного обеспечения и обоснована её техническая часть.

риск, имитационное моделирование, управленческое решение, качество, ситуация.

Введение

В сфере телекоммуникаций принятие качественных решений имеет огромное значение, так как это позволяет сохранять конкурентоспособность и эффективность бизнеса, обеспечивать требуемый уровень обслуживания клиентов и удовлетворять их потребности.

Принятие решений по созданию современных сетей передачи данных связано с выбором их архитектуры, основных параметров, например, таких как количество каналов связи, продолжительность обслуживания, режимы их работы и т. д. При этом создание сетей передачи данных сопровождается наличием неопределенности знаний о процессе функционирования данных систем, что, в свою очередь, может привести к тому, что каждое решение, принимаемое в этих условиях может не достигнуть своей цели, а значит будет связано с появлением риска, под которым буде понимать свойство качества решения, характеризующего возможность и последствия недостижения его целей [1].

В таких условиях традиционный подход к управлению процессом создания сетей передачи данных, основанный на реакции на события и минимизации потерь, становится недостаточным. Поэтому целесообразным выглядит переход при управлении созданием сетей передачи данных к риск-ориентированному подходу, который предполагает оценивать каждое управляющее решение с позиций риска недостижения его целей путем анализа и оценки вероятности и последствий возможных нежелательных событий, а также на выборе наиболее эффективных мер по их предотвращению или смягчению последствий.

Переход к риск-ориентированному подходу позволит разработчикам сетей передачи данных более эффективно принимать решения, снизить потери и повысить устойчивость к неблагоприятным событиям и тем самым повысить качество своей продукции и, следовательно, сохранять конкурентоспособность, удовлетворять потребности клиентов и обеспечивать рост и развитие бизнеса.

Подход к оцениванию показателей риска решений по созданию сетей передачи данных

Приведенные обстоятельства обусловливают необходимость наличия научно-методического аппарата, позволяющего оценить показатели риска решений по созданию систем передачи данных. В качестве такого аппарата рекомендуется использовать подход, предложенный в [2] и основанный на имитационном моделировании процесса функционирования создаваемых систем передачи данных с учетом возможности появления различных нежелательных факторов, сопровождающих этот процесс.

Использование имитационного моделирования позволит решить, как задачу оценивания показателей риска решений по управлению созданием сетей передачи данных, так и задачу последовательного управления целевыми результатами за счет последовательной коррекции решений, не позволяющих достигнуть требуемых целей.

Это становится возможным за счет того, что при имитационном моделировании функционирования сети передачи данных, которое по факту является исполнением управляющих решений по ее созданию, фиксируются не только финальные результаты, но и ряд промежуточных, которые позволяют определить причины недостижения целей решения.

Однако, использование такого подхода для оценивания показателей риска решений связано с большими вычислительными сложностями и наличием высокого уровня квалификации у лица, занимающегося этим процессом, что может вызвать определенные трудности у разработчиков сетей передачи данных.

Выходом из этой ситуации является разработка специализированного программного обеспечения, в основе которого будет положен представленный выше подход к оцениванию показателей риска.

Программное обеспечение позволит компаниям или частных лицам оптимизировать процесс принятия решений в области создания систем передачи данных, путём сокращения временных и экономических затрат. Использование специализированного программного обеспечения предполагает, что оператору не придется проделывать все вычислительные операции, связанные с оцениванием показателей риска самостоятельно, а предоставить расчеты машине.

В свою очередь, программное обеспечение будет выдавать лицу, принимающему решение, всю необходимую информацию для выбора рационального решения, такую как статистика, графики и расчетные единицы, а также расчетные данные.

Методология разработки программного обеспечения для оценивания показателей риска решений

Программное обеспечение, позволяющее оценить показатели риска управляющих решений по созданию сетей передачи данных, должно включать в себя:

- Алгоритмы возможных сценариев недостижения целей управляющих решений;
- Вероятностные модели событий, которые могут возникать в процессе реализации этих сценариев и влиять на ход их развития;
- Алгоритмы выполнения принятых решений по управлению целевыми результатами (совокупным риском).

Программное обеспечение для оценивания показателей риска управляющих решений может включать в себя следующие функции:

1. Анализ и оценка показателей риска. Программа позволяет проводить анализ показателей риска на основе сценариев недостижения целей управляющих решений. Она также предоставляет инструменты для оценки вероятности возникновения каждого сценария.

2. Моделирование ситуаций. Программа может создавать модели ситуаций, которые могут возникнуть при принятии управленческих решений. Она также может проводить симуляции, чтобы определить, как изменения в условиях могут повлиять на риски.

3. Мониторинг и оценивания показателей риска. Программа предоставляет инструменты для мониторинга и оценки показателей риска, которые были выявлены в результате анализа. Она также может предоставлять рекомендации по управлению рисками и снижению их влияния на современные сети связи.

4. Отчетность и аналитика. Программа предоставляет отчеты и аналитику по результатам анализа и оценки рисков, что позволяет принимать обоснованные управленческие решения на основе данных.

Программное обеспечение для оценивания показателей риска управляющих решений может быть полезным для компаний любого размера и отрасли, которые хотят повысить эффективность своих бизнес-процессов. На рис. 1 можно увидеть диаграмму развертывания модулей специализированного программного обеспечения.

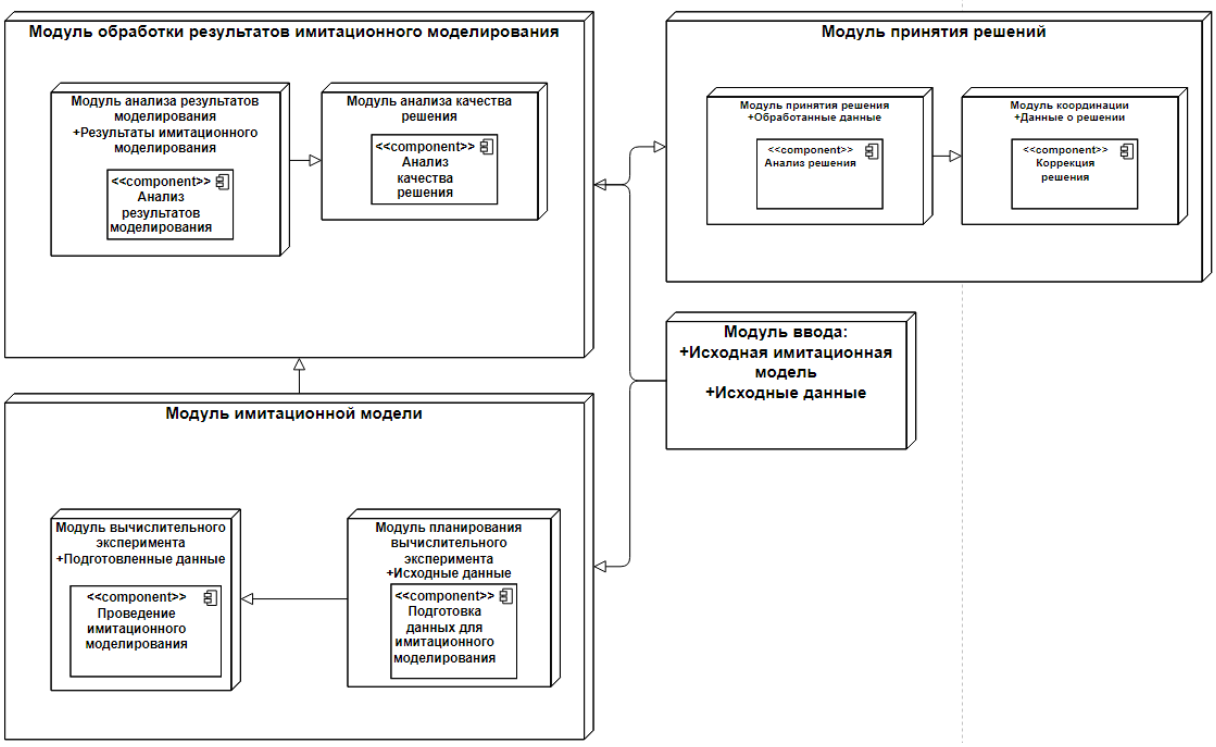


Рис. 1. UML-Диаграмма развертывания программного обеспечения оценивания показателей риска управляющих решений

Выбор средств по созданию программного обеспечения для оценивания показателей риска управляющих решений

В качестве основы для разрабатываемого программного обеспечения, предлагается использовать язык программирования Java. Данный язык был выбран для создания программного обеспечения для оценивания показателей риска управляющих решений по следующим причинам:

1. Платформонезависимость. Java позволяет создавать программное обеспечение, которое может работать на различных операционных системах, таких как Windows, Mac и Linux.

2. Безопасность. Java имеет встроенные механизмы безопасности, такие как проверка типов и контроль доступа, что делает его более надежным для создания программного обеспечения, связанного с оценкой рисков.

3. Большое сообщество разработчиков. Java имеет широкое сообщество разработчиков и множество библиотек и инструментов, которые могут быть использованы для ускорения разработки.

4. Высокая производительность. Java использует виртуальную машину для выполнения кода, что позволяет достичь высокой производительности и оптимизации работы программы.

5. Легкость поддержки и обновления. Java имеет стабильную версию и постоянно обновляется, что делает его легким в поддержке и обновлении программного обеспечения.

В целом, выбор языка программирования Java для создания программного обеспечения оценивания показателей риска управляющих решений является логичным и обоснованным выбором, который позволит создать надежное и эффективное программное обеспечение.

Заключение

Использование предлагаемой методологии разработки программного обеспечения оценивания показателей риска управляющих решений по созданию сетей передачи данных имеет большую актуальность для принятия решений в телекоммуникационной отрасли. Это позволит предприятиям-разработчикам сетей передачи данных принимать эффективные решения по их созданию, которые смогут помочь им сохранять конкурентоспособность, удовлетворять потребности клиентов и обеспечивать рост и развитие бизнеса.

Список используемых источников

1. Звягин В. И., Птушкин А. И., Трудов А. В. Риск как одно из свойств качества решений, принимаемых в условиях неопределенности // Надежность. 2018. N 18 (4). С. 45–50.

2. Вивчарь Р. М., Птушкин А. И., Соколов Б. В. Риск-ориентированное управление созданием организационно-технических систем на основе использования имитационных моделей их функционирования // Вестник ВГУ. Серия: Системный анализ и информационные технологии. 2021. N 2. С. 17–31.

УДК 004.725.5
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ ВЕКТОРА ОШИБКИ СИГНАЛЬНОГО СОЗВЕЗДИЯ QAM ОТ ИЗМЕРЕННОГО ОТНОШЕНИЯ СИГНАЛ/ШУМ В СЕТИ IEEE 802.11

А. С. Викулов, С. А. Скоробогатова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе рассмотрены параметры, характеризующие качество принимаемого сигнала: величина вектора ошибки сигнального созвездия и отношение сигнал/шум. Показана необходимость проведения эксперимента с анализом спектра с целью определения зависимости параметра вектора ошибки от отношения сигнал/шум. По результатам эксперимента исследован вид корреляции между отношением сигнал/шум и вектором ошибки.

EVM, RCE, SNR, анализ спектра, сигнальное созвездие, QAM, Wi-Fi.

Введение

При проектировании беспроводных сетей передачи данных [1] (БСПД) одним из важнейших параметров является относительная ошибка сигнального созвездия (*Relative Constellation Error*, RCE) или, иначе говоря, вектор ошибки (*Error Vector Magnitude*, EVM). В стандарте IEEE 802.11 определено, что для работы соответствующей схемы модуляции и кодирования (*Modulation and Coding Sequence*, MCS) параметр RCE, ее определяющий, не должен быть хуже пороговых значений. В таблице 1 (см. ниже) приведены значения RCE соответствующие режимам HT20/VHT20 [2].

Для того, чтобы принимающее устройство было способно корректно демодулировать QAM-сигнал, распознать точки на диаграмме созвездий и соотнести их с идеальным положением на диаграмме необходимо чтобы отношение сигнал/шум (SNR) соответствовало допустимому значению [3]. Чем выше значение SNR, тем более сложные схемы модуляции могут быть использованы при передаче данных.

Таким образом, EVM и SNR используются при выборе скоростного режима в БСПД с точки зрения правильности приема. Отметим, что с точки зрения проектирования БСПД, ключевым критерием является отношение сигнал/шум, поскольку именно эта величина является мерой относительной мощности сигнала по сравнению с шумом.

ТАБЛИЦА 1. Допустимая относительная ошибка созвездия в зависимости от размера созвездия и скорости кодирования

Модуляция	Скорость кодирования	RCE (дБ)
BPSK	1/2	–5
QPSK	1/2	–10
QPSK	3/4	–13
16-QAM	1/2	–16
16-QAM	3/4	–19
64-QAM	2/3	–22
64-QAM	3/4	–25
64-QAM	5/6	–27
256-QAM	3/4	–30
256-QAM	5/6	–32

Постановка задачи и схема эксперимента

EVM показывает как измеренная при приеме точка на I/Q-диаграмме отличается от идеального (референсного) положения, то есть EVM – это расстояние между идеальным положением точки сигнального созвездия и фактически полученным (рис. 1). Ниже представлена формула [4] для измерения EVM одной точки в децибелах:

$$EVM_T = 10\log_{10}\left(\frac{\left|S_n - S_{0,n}\right|^2}{\left|S_{0,n}\right|^2}\right), \text{ дБ}$$

где S_n – вектор точки, полученной при передаче сигнала, $S_{0,n}$ – вектор идеальной точки.

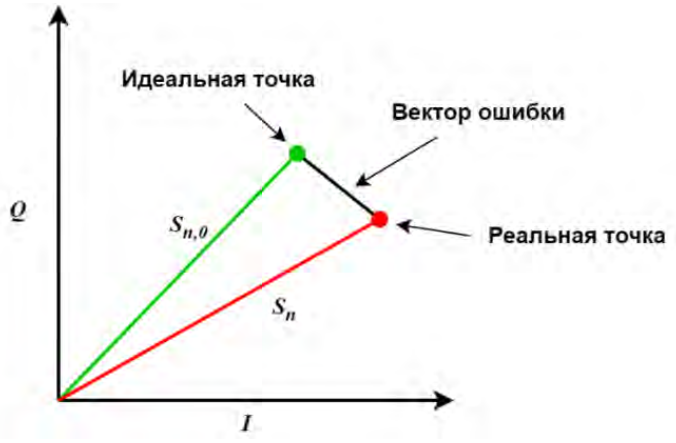


Рис. 1. Иллюстрация EVM на I/Q-диаграмме

Смещение точки от идеального положения может быть вызвано разнообразными нарушениями, включая: шум, гармонические искажения, фазовый шум, фазовую ошибку, сжатие и др.

Преобразование значения из $EVM_{\%}$ в EVM_{dB} происходит согласно:

$$EVM_{dB} = 20\log_{10}\left(\frac{EVM_{\%}}{100}\right), \text{ дБ} \quad (1)$$

Среднее отношение сигнал/шум (дБ) для символа определяется как:

$$\langle SNR_{dB}\rangle = \langle P_{изм}\rangle - \langle P_n\rangle, \text{ дБ} \quad (2)$$

где $<P_{изм}>$ – измеренное среднее значение уровня мощности сигнала в точке, соответствующей исследуемому символу на временной диаграмме, дБм;

$<P_n>$ – рассчитанное среднее значение уровня шума, дБм.

Из выше представленного мы видим физическую разницу между EVM, (как характеристику QAM-модулированного сигнала) и SNR (как спектральный параметр), однако их часто считают одной и той же величиной. Подобный вывод делают в том числе и признанные в отрасли эксперты-практики [5, 6], что строго формально не является корректным, но может быть допустимо на практике.

Как правило, устройства с радиомодулем IEEE 802.11 рассчитывают SNR основываясь на информации из потока данных в канале передачи и в ряде случаях опираясь на данные о потерянных кадрах, о вероятности битовой ошибки и о фактической битовой ошибке, поэтому для анализа SNR, необходим анализатор спектра.

Сформулируем задачу следующим образом: проверить в процессе натурных измерений вид корреляции между SNR и EVM.

Экспериментальный стенд содержит:

– анализатор спектра реального времени Tektronix RSA306B;
– антенна Extreme ML-2452-HPAG4A6-01;
– ПК, используемый в роли клиентского устройства;
– точка доступа Extreme AP8432;
– ПК со специализированным программным обеспечением SignalVu.

Измерения проводились в радиосреде с сигналом IEEE 802.11ac, с модуляцией 16-QAM в канале № 36. В процессе эксперимента измеренными параметрами являлись:

– вектор ошибки $EVM_{\%}$ для каждой поднесущей в рамках символа (по диаграмме сигнального созвездия). Получено 52 значения по числу поднесущих, включая пилотные;

– уровень мощности принимаемого сигнала $<P_{изм}>$, усредненный для принятого символа целиком, дБм (по временной диаграмме для канала);

– уровень мощности фонового шума P_n, дБм (по временной диаграмме для канала в отсутствие передачи). Получено 20 значений для последующего усреднения.

Всего выполнено 15 измерений. EVM измерен в процентах и, по формуле (1), переведен дБ. Отметим, что при измерениях имеет место большая дисперсия значений между 52-мя поднесущими. Для оценки EVM в каждом измерении, полученные значения были усреднены по всем поднесущим. Ввиду особенности работы анализатора спектра реального времени, значение SNR определяется из временной диаграммы сигнала для каждой точки измерений, определяемой парой координат: частотой поднесущей в спектре и временной координатой в рамках передаваемой символьной последовательности (рис. 2).

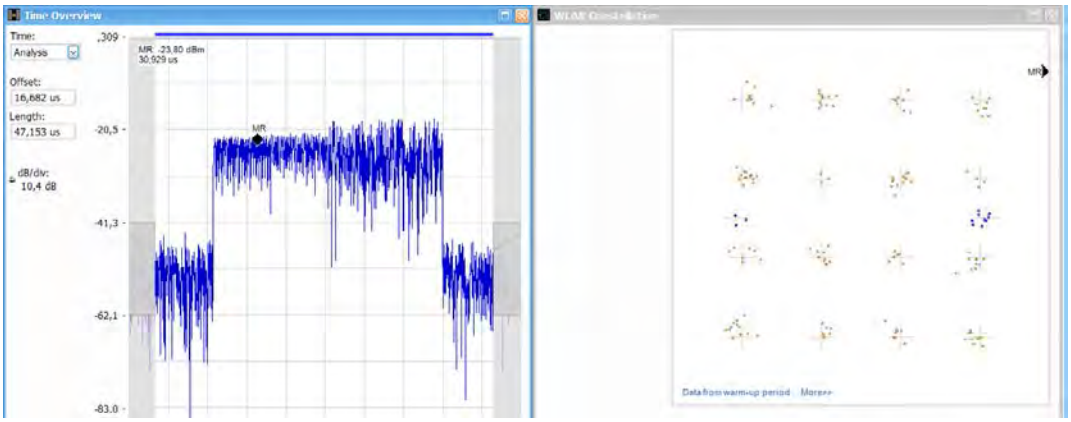


Рис. 2. Скриншот ПО SignalVu-PC

В процессе обработки результатов для каждого из измерений были рассчитаны:

– среднее значение вектора ошибки $<EVM_{dB}>$, дБ;
– отношение сигнал/шум *SNR* согласно (2), дБ.

Анализ результатов измерений

В результате эксперимента рассчитаны значения SNR и EVM для 15 отдельных измерений. Полученная зависимость EVM от SNR представлена на рис. 3.

На графике наблюдается обратная линейная зависимость: увеличение SNR приводит к уменьшению EVM.

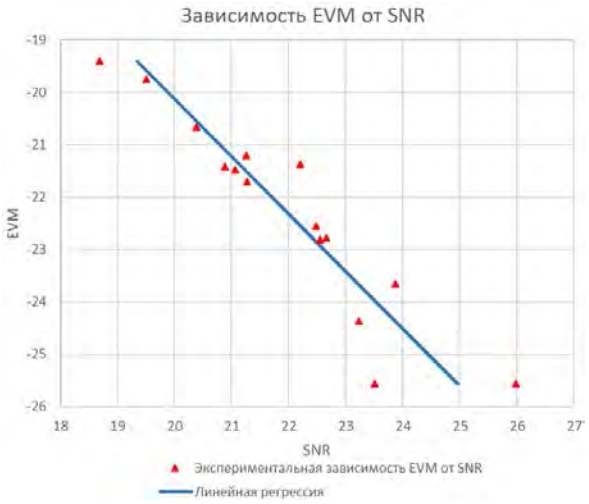


Рис. 3. График зависимости EVM (SNR)

Для количественной оценки корреляции между EVM и SNR, воспользуемся выборочным коэффициентом корреляции Пирсона:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}}, \quad (3)$$

где n – размер выборки, x_i и y_i – отдельные точки выборки, $\bar{x}$ и $\bar{y}$ – средние значения выборок. В результате расчета по формуле (3), получено r_{xy} равное –0,935, что подтверждает линейную зависимость двух величин, а также свидетельствует об очень высокой отрицательной корреляции – более высоким значениям одного признака соответствуют более низкие значения другого. Полученная линейная регрессия также приведена на рис. 3.

Выводы

В результате работы можно отметить, что:

1. Проведен краткий анализ значения SNR и EVM для процесса проектирования БСПД.
2. Экспериментально подтверждена обратная линейная зависимость между отношением сигнал/шум и вектором ошибки сигнального созвездия.
3. Измерениями показано, что значение коэффициента корреляции Пирсона близко к –1.

Список используемых источников

1. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. Л. Широкополосные беспроводные сети передачи информации. М. : Техносфера, 2005. 592 с.

2. IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016). IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. DOI: 10.1109/IEEESTD.2021.9363693.

3. Викулов А. С., Парамонов А. И. Модель канала OFDM в задаче оценки эффективности сети IEEE 802.11 // Инфокоммуникационные технологии. 2018. Т. 16. N 3. С. 290–297.

4. D. Weller, R. D. Mensenkamp, A. v. d. Vegt, J.-W. v. Bloem and C. d. Laat // Wi-Fi 6 performance measurements of 1024-QAM and DL OFDMA: ICC 2020 – 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020. PP. 1–7. DOI: 10.1109/ICC40277.2020.9149106.

5. Parsons, K. Ekahau Site Survey Heatmap Visualizations. Part 6: Data Rate [Электронный ресурс] // Ekahau. URL: https://www.ekahau.com/blog/2015/06/22/ekahau-site-survey-heatmap-visualizations-part-6-data-rate/ (дата обращения 28.03.2023).

6. Von Nagy, A. Visualizing How Wi-Fi SNR Helps Determine the Achievable MCS Data Rate [Электронный ресурс] // Revolutionwifi. URL: http://www.revolutionwifi.net/revolutionwifi/2014/08/visualizing-how-wi-fi-snr-helps.html (дата обращения 28.03.2023).

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ВЛИЯНИЯ АТАК НА БЕСПРОВОДНУЮ СЕТЬ НА БАЗЕ ОБОРУДОВАНИЯ CISCO

С. А. Винников, М. М. Ковцур, В. И. Трезоров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В сегодняшних реалиях беспроводные сети занимают значительное место в жизни каждого. Это связано с быстрым ростом потребностей пользователей, что в свою очередь является причиной постоянного развития вычислительных машин и телекоммуникационных устройств. С быстрым развитием Wi-Fi-оборудования, приходит все большее количество ошибок и уязвимостей, которые могут крайне негативно сказаться как на работе обычных пользователей, так и на целой бизнес-инфраструктуре ввиду появления новых угроз безопасности беспроводного оборудования. В работе представлен отчёт об исследовании влияния различных атак на инфраструктуру на базе беспроводных устройств Cisco, что даст общее понимание работы и уязвимостей беспроводного оборудования, работающего по стандартам IEEE 802.11.

беспроводные локальные сети, сетевая безопасность, WLC, информационные атаки, Wi-Fi, отказ в обслуживании.

Популярность беспроводных локальных сетей возрастает с каждым днём, что дает больше возможностей злоумышленникам. Одной из популярнейших атак является атака отказа в обслуживании (*Denial of Service,* DoS), которая может принести значительные неудобства и может стать причиной убытков бизнеса.

В данной работе будет рассмотрено несколько простейших DoS-атак [1] на примере беспроводной инфраструктуры Cisco. Представленные атаки являются базовыми и простыми в исполнении, что обосновывает их актуальность.

По информации из новостного издания [2] на момент 2022 года оборудование Cisco занимает пятую часть всего сетевого оборудования, используемого в России, так что проблема безопасности оборудования этого вендора остаётся актуальной и на 2023 год.

В статье рассмотрены следующие атаки, которые могут быть использованы в качестве первого шага более сложных и комплексных атак:

Атака рассылки маячковых кадров [3] (*Beacon Flood*). Представляет из себя предумышленное запутывание беспроводного клиента.

Атака наводнения аутентификационными пакетами (*Auth Flood*). Является злонамеренным использованием особенности алгоритма подключения беспроводного клиента к беспроводной точке доступа (ТД).

Атака зондирования сетей (*Probe Flood*). Представляет из себя нелегитимное использование простейшего зондирования Wi-Fi-сетей, направленное конкретно на целевую сеть.

EAPoL Start Flood. Представляет из себя частые злонамеренные запросы на подключение нелегитимного беспроводного клиента к целевой сети, использующей аутентификацию по стандарту IEEE 802.1X.

Атака наводнения деаутентификационными пакетами (*Deauth Flood*). Это предумышленное разъединение беспроводного клиента и точки доступа с целью дальнейших неправомерных действий.

Для тестирования безопасности собран лабораторный стенд, который состоит из легковесной точки доступа (ТД) Cisco Aironet 1600, виртуального беспроводного контроллера *Cisco* vWLC и беспроводного Wi-Fi-адаптера с поддержкой режима мониторинга.

Схема лабораторного стенда показана на рис. 1.

Рис. 1. Схема лабораторного стенда

Для изучения безопасности беспроводного сетевого устройства необходимо получить характеристики целевой сети: SSID, BSSID, тип шифрования и используемый канал).

Это можно сделать с помощью утилиты Bettercap [4] (рис. 2).

RSSI	BSSID	SSID	Encryption	WPS	Ch	Clients
-59 dBm	e8:ed:f3:fc:f2:3f	TEST_NET	WPA2 (CCMP, PSK)		44	1

Рис. 2. Вывод команды wifi.show утилиты Bettercap

До проведения атаки Beacon Flood на рис. 3 показаны показатели состояния беспроводной сети до и во время атаки: скорость скачивания, скорость загрузки, пинг и джиттер.

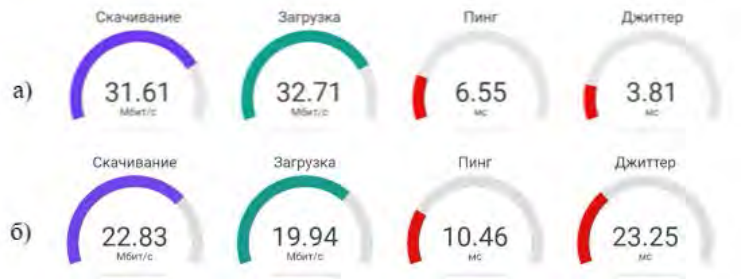


Рис. 3. Показатели беспроводной сети: а) до атаки Beacon Flood, б) во время до атаки Beacon Flood

Атака осуществляется с помощью следующей утилиты mdk4 [5] со скоростью 500 пакетов в секунду.

Как можно заметить, показатели ухудшились. Это связано с большим количеством отправляемых нелегитимных маячковых пакетов.

Атака Auth Flood осуществлялась с помощью утилиты mdk4.

На рис. 4 показаны характеристики сети.

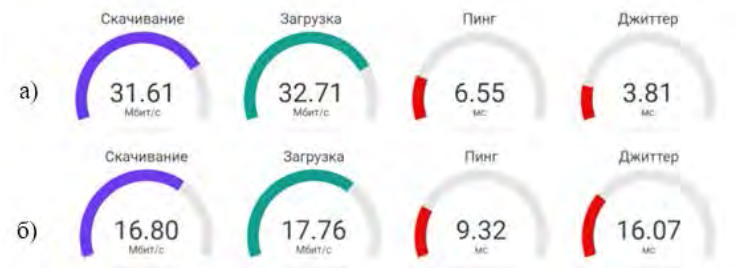


Рис. 4. Показатели беспроводной сети: а) до атаки Auth Flood, б) во время до атаки Auth Flood

Показатели сети также ухудшились. На графике 1 показана зависимость занятости эфира Q от количества атакующих пакетов в секунду N.

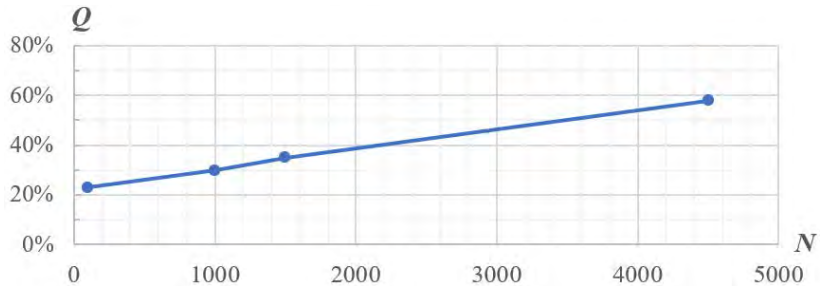


График 1. Зависимость занятости эфира от количества нелегитимных пакетов

Можно сделать вывод, что при ограниченных ресурсах контроллера, возможно добиться ситуации, когда контроллер не способен обработать все поступающие запросы и при этом жертвует качеством беспроводной сети.

Атака Probe Flood осуществлялась с помощью утилиты mdk4.

На рис. 5 показаны характеристики сети.

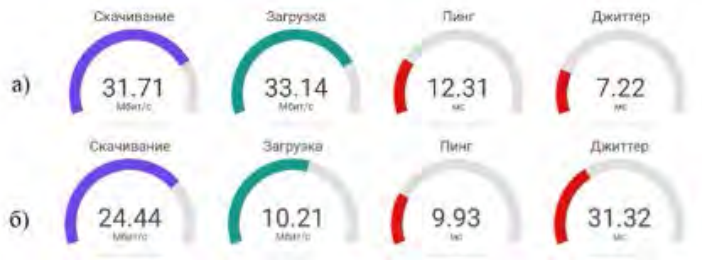


Рис. 5. Показатели беспроводной сети: а) до атаки Probe Flood,
б) во время до атаки Probe Flood

На рис. 6 видно, что атака зафиксирована встроенной системой обнаружения вторжений (WIDS) на контроллере.

Trap

Rogue client: 50:8a:06:e3:03:28 is detected by 1 APs Rogue Client Bssid: 5c:a6:e6:68:34:88, State: Alert, Last detecting AP :e8:ed:f3:fc:f2:30 Rogue Client gateway mac 5c:a6:e6:68:34:88.

Рис. 6. Логи во время атаки Probe Flood

Во время исполнения атаки нагрузка на центральный процессор контроллера повысилась с 1 до 7 %.

Зависимость занятости эфира Q от количества пакетов атаки N показана на графике 2.

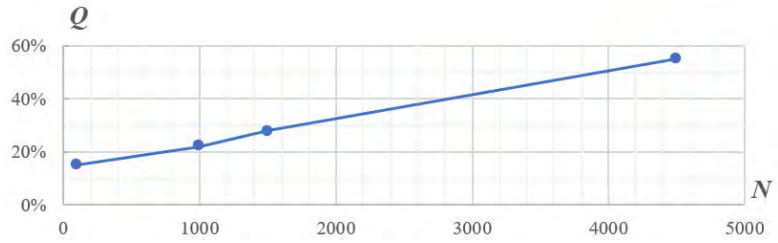


График 2. Зависимость занятости эфира от количества атакующих пакетов

Для проверки воздействия атаки EAPoL Start Flood на беспроводную сеть был активирован режим аутентификации EAP.

Для осуществления этой атаки используется утилита mdk4.

Во время исполнения атаки можно заметить, что клиенты деассоциируются, хотя PMF (*Protected Management Frame*) включен, что в итоге позволяет перехватить handshake. Это видно на рис. 7 при сканировании в Bettercap.

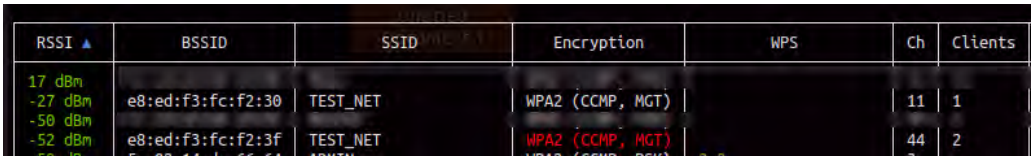


Рис. 7. Клиент был отключен от сети,
что позволило перехватить handshake второй сети

WIDS зафиксировала атаку, как видно на рис. 8.

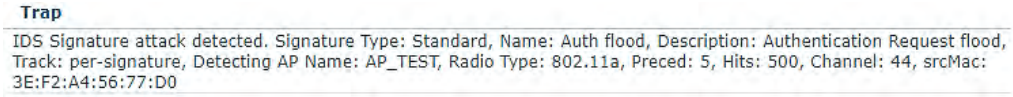


Рис. 8. Логи во время атаки EAPoL Start Flood

Можно сделать вывод, что эта атака позволит не только прерывать связь клиентов с ТД, но и даст начало для взлома пароля 802.11X.

Атака Deauth Flood [6, 7] также может быть осуществлена с помощью Bettercap.

При этом программа обнаруживает BSSID ТД и пытается деаутентифицировать клиента (рис. 9).

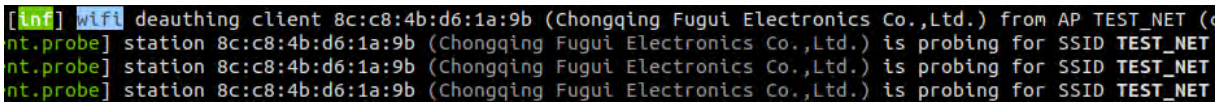


Рис. 9. Деаутентификация клиента – Bettercap

А WIDS регистрирует событие (рис. 10). При этом клиент не был отключен от сети, так как включен PMF [8].

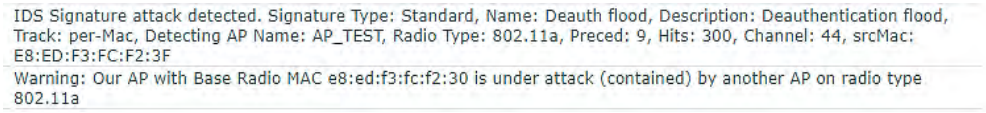


Рис. 10. Логи во время атаки Deauth Flood

Таким образом, можно сделать вывод, что даже при использовании простейших атак и инструментов, можно нарушить работу беспроводной сети и причинить неудобства, что может принести значительные убытки бизнесу.

Список используемых источников

1. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning // Studies in Computational Intelligence. 2020. V. 868. PP. 350–355.

2. Эксперты рассказали о последствиях приостановки деятельности Microsoft и Cisco в России // i38.ru URL: https://i38.ru/technologii-pervie/eksperti-rasskazali-o-posledstviyach-priostanovki-deyatelnosti-microsoft-i-cisco-v-rossii (дата обращения 19.03.2023).

3. Ушаков И. А., Котенко И. В., Овраменко А. Ю., Преображенский А. И., Пелёвин Д. В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 4. С. 66–71.

4. bettercap // Инструменты Kali Linux. URL: https://kali.tools/?p=3870 (дата обращения 04.02.2023).

5. mdk4 // Инструменты Kali Linux. URL: https://kali.tools/?p=4246 (дата обращения 04.02.2023).

6. Киструга А. Ю., Ковцур М. М., Петров М. П., Шабанов В. П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция. : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. С. 561–564.

7. Красов А. В., Савинов Н. В., Ушаков И. А. Использование инфраструктуры, ориентированной на приложения компании CISCO SYSTEM INC. в современных сетях ЦОД // Актуальные проблемы инфотелекоммуникаций в науке и образование. VI Международная научно-техническая и научно-методическая конференция. : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. С. 453–457.

8. Гельфанд А. М., Казанцев А. А., Красов А. В., Уляшева В. Р. Интернет вещей (IoT): угрозы безопасности и конфиденциальности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная науно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 215–220.

УДК 004.056.53
ГРНТИ 81.93.29

МОДЕЛЬ ИНФОРМАЦИОННЫХ АТАК В МЕДИА-ПРОСТРАНСТВЕ

Л. А. Виткова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В современном медиатизированном мире, важнейшие смыслы формируются в массовом сознании по каналам СМИ и социальных сетей. При этом проблема обнаружения информационных атак в социальных сетях приобретает особую актуальность. Стоит вопрос о пересмотре терминологии, о классификации, идентификации признаков информационных атак, о разработке моделей, методик и алгоритмов их обнаружения. В работе предложены термины и определения, которые составляют общий для социо-гуманитарных и технических наук понятийный аппарат. А также представлена модель информационных атак, позволяющую перейти к выбору признаков для обнаружения и сформировать требования к алгоритмам анализа и оценки информационных атак.

информационные атаки, информационное пространство, вектор информационной атаки, медиа ресурс, анализ социальных сетей.

Введение

В современном медиатизированном мире, важнейшие смыслы формируются в массовом сознании по каналам СМИ и социальных сетей [1, 2].

Любое событие превращается в важнейший источник, из которого государства, общество и обыкновенные люди черпают, казалось бы, объективную информацию о мире. В [3] автор подчеркивает, что факт сам по себе нейтрален и именно интерпретация факта формирует событие. При этом интерпретация события всегда связана с фреймом. И в связи с тем, что исследование коммуникаций относится скорее к гуманитарным аспектам, а обнаружение атак к техническим, необходимо создать некоторый общий понятийный аппарат.

Вот, например, рассмотрим термин информационная атака (ИА). В журнале «Политическая лингвистика» автор Коцюбинская Л.В. сформулировала определение ИА следующим образом: *«Информационная атака – это спланированное, целенаправленное, массированное информационное воздействие на адресата, результатом которого будет формирование запрограммированного общественного мнения, а, следовательно, и поведения»* [4]. В информационной безопасности под ИА понимается действие, направленное на нарушение конфиденциальности, целостности и доступности информации, то есть трактуется как «атака на информацию» [5]. В результате возникает как научное, так и практическое противоречие, достижения и успехи социо-гуманитарных наук в описании и классификации информационных атак фактически не применимы для технических специалистов.

Для разрешения противоречия, возможно ввести термин «пространство информационных атак (ПИА)» – совокупность информационных систем и их интерфейсов взаимодействия с субъектом, в которых реализуются информационные атаки. Далее можно также ввести термин «поверхность информационной атаки». А поверхность в пространстве, как правило, можно рассматривать как геометрическое место точек, удовлетворяющих какому-либо условию. Линию же в пространстве можно рассматривать как линию пересечения двух поверхностей, и одновременно как траекторию движения точки. Следовательно, мы можем отойти от спорного восприятия термина «информационная атака» и ввести понятие «вектор информационной атаки». Тогда по сути «ИА» будет определяться как скаляром, так и направлением и по сути будет уже векторной величиной.

Предложенные термины и определения составляют общий для социо-гуманитарных и технических наук понятийный аппарат и дают возможность создать модель информационных атак, позволяющую сформировать требования к алгоритмам анализа и оценки информационных атак.

Модель информационных атак

Рассмотрим модель информационных атак в медиа-пространстве (рис. 1). Объекты модели:

1. Факт – элементарное, нейтральное событие.

2. Событие (*event*) – отражение факта в процессе коммуникации.

3. Фрейм – формируемое восприятие у индивида или масс, в процессе коммуникации.

4. Медиа-ресурс – социальная сеть, веб-страница, видео-хостинг и другие формы медиа, через которых распространяется информация.

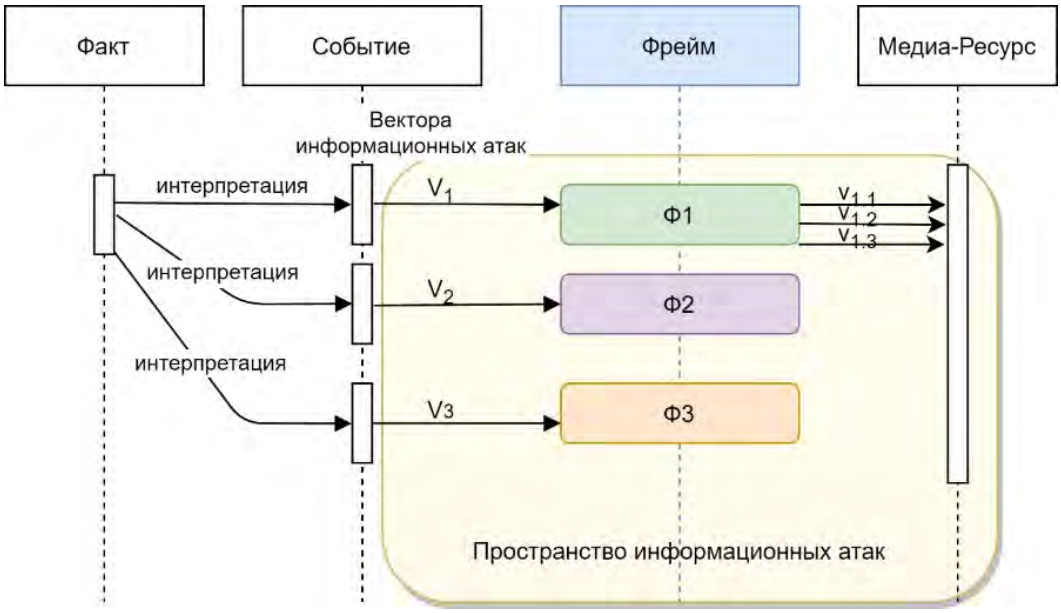


Рис. 1. Модель информационных атак

Тогда вектор информационной атаки начинается от события и проходит через фрейм. Таким образом, пересекается понимание ИА, как «*целенаправленного воздействия на адресата»,* а поверхность ИА может быть выражена через площадь (определитель матрицы).

В процессе распространения информации инициатором (актором) может быть выбран не только фрейм, но и медиа-ресурс или их набор. Таким образом вектор информационной атаки находит свое отражение в медиа файлах, в текстах и может быть исследован и оценен.

Заключение

Предложенные понятийный аппарат и модель информационных атак позволяют перейти к выбору признаков. Так, например, для разных медиаресурсов характерны свои признаки (лайки, просмотры, количество сообщений). А все сообщения, связанные с общим фактом, могут быть разделены по фреймам. Благодаря векторному восприятию информационной атаки, вектора могут быть оценены, как и площади пространств, связанных с тем или иным набором.

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094-П) в СПб ФИЦ РАН.

Список используемых источников

1. Couldry N., Hepp A. The Mediated Construction of Reality, Cambridge: Polity Press. 2018. PP. 38–52.

2. Namyatova K., Vitkova L., Chechulin A. An approach to automated assessment of the image of a territorial entity in the media discourse of a foreign states // Proceedings of 14th International Symposium on Intelligent Distributed Computing – IDC'2021. Sep 16–18, 2022, Online Conference, Italy // Studies in Computational Intelligence. 2022. V. 1026. PP. 215–224. DOI: 10.1007/978-3-030-96627-0_20.

3. Гавра Д. Основы теории коммуникации : учебное пособие. СПб. : Питер, 2011. 288 с. ISBN 978-5-459-00385-7.

4. Коцюбинская Л. В. Информационная атака: понятие и онтологические свойства // Политическая лингвистика. 2017. N 6 (66). С. 106–111.

5. Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. М. : Горячая линия – Телеком, 2012. 542 с.: ил. ISBN: 978-5-9912-0253-4.

УДК 004.056.53
ГРНТИ 81.93.29

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Л. А. Виткова, А. Л. Зрелова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена проблеме защиты персональных данных в Российской Федерации. Особое внимание уделяется киберпреступлениям, направленным на кражу и распространение баз персональных данных пользователей, произошедшим за последний год. Отмечается, что на данный момент происходит ужесточение требований к операторам персональных данных, направленное на усиление защиты субъектов персональных данных и обеспечение неприкосновенности частной жизни. В работе проведен анализ изменений внесенных в законодательство РФ о персональных данных после участившихся атак на крупные компании и утечку личной информации пользователей.

кибератаки, персональные данные, анализ законодательства, утечки персональных данных.

В современном мире очень актуальна проблема обеспечения защиты персональных данных. В 2022 году количество кибератак на Российскую Федерацию выросло вдвое по сравнению с 2021 годом. Вторыми по частоте

распространения стали атаки, направленные на кражу персональных данных. При этом изменилась мотивация киберпреступников. Раньше украденные базы персональных данных продавали на теневых и «полутеневых» ресурсах, таких как форумы в ДаркВебе. Сейчас же их выкладывают в публичный доступ для нанесения репутационного и экономического ущерба бизнесу и клиентам.

Из отчетов экспертно-аналитических центров следует, что количество утекших записей персональных данных в Российской Федерации аномально возросло по сравнению с предыдущими годами. Так, к середине 2022 года количество утекших записей достигло рекордных 187,6 млн записей, что превышает численность населения страны (рис. 1). Выделяют несколько причин аномального роста утечек:

- всплеск хакерской активности из-за геополитической ситуации в мире;
- ослабление контроля за информационными активами в период пандемии COVID-19;
- уход иностранных вендоров, приведший к потере функциональности ряда сервисов и отсутствию обновлений, устраняющих уязвимости.

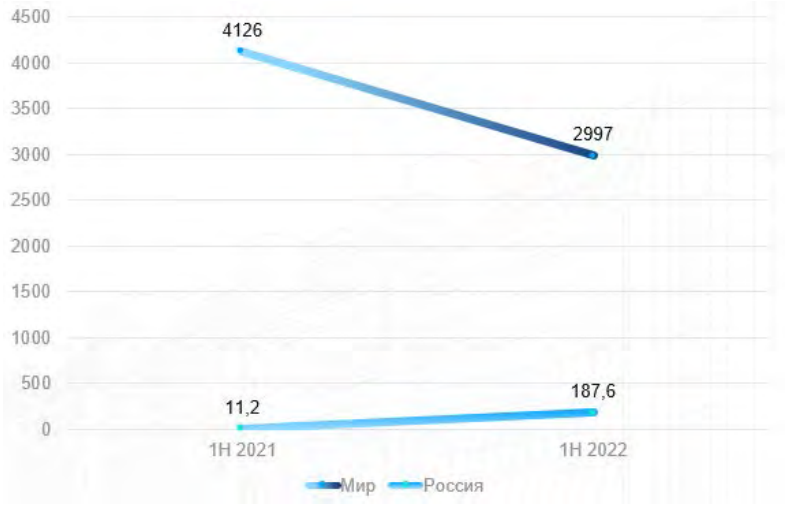


Рис. 1. Сравнение количества утекших записей за 1 полугодие 2021 и 2022 года

За 2022 год произошли крупные утечки из российских компаний и госорганов, в их числе: РЖД, авиакомпания «Победа», телекоммуникационные компании «Ростелеком» и «ВымпелКом», информационный портал Ykt.ru, сервисы «Мир Тесен», Fotostrana.ru и Text.ru, развлекательный ресурс Pikabu, сервисы доставки «Яндекс.Еда», Delivery Club и 2 Berega, школа управления «Сколково», образовательный портал GeekBrains, «Почта России» и «Гемотест». Всего за первое полугодие 2022 года в России произошло 305 утечек, что на 50 % больше, чем в первом полугодии 2021 года (рис. 2) [1].

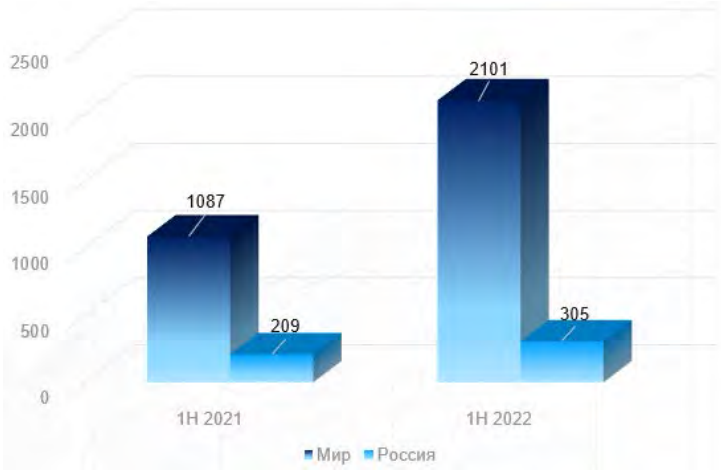


Рис. 2. Сравнение количества утечек за 1 полугодие 2021 и 2022 года

Компания InfoWatch в своём отчете об исследовании утечек информации в первой половине 2022 года приводит распределение утечек в ДаркВебе по отраслям организаций в России (рис. 3). Так, больше всего данных было украдено из сферы торговли и высоких технологий, но большинство данных продаются без привязки к сфере деятельности компании, но с уточнением «персональные данные россиян».

Также атакам подвергаются крупные Интернет-провайдеры, правительственные сайты, и сайты госструктур, что приводит к увеличению внимания государства к вопросам обеспечения безопасности персональных данных.

Рис. 3. Распределение украденных данных по отраслям организаций в России

В связи со сложившейся ситуацией были внесены кардинальные изменения в законодательные акты, регулирующие работу с персональными данными.

Так, с 1 сентября 2022 были внесены изменения в 152 Федеральный закон «О персональных данных», направленные на ужесточение требований к работе с персональными данными. Изменения затрагивают не только операторов и сторонних обработчиков персональных данных, но и регуляторов, и органы государственной власти. Изменения коснулись всего порядка работы с персональными данными: от особенностей согласия и уведомления Роскомнадзора до правил трансграничной передачи и прекращения обработки.

Данные правки должны усилить защиту персональных данных субъектов и обеспечить неприкосновенность их частной жизни.

С 2022 года все нормативно правовые акты Российской Федерации, касающиеся трансграничной передачи персональных данных, обработки специальных категорий данных (например, состояние здоровья человека), биометрических данных; персональных данных несовершеннолетних лиц; а также вопросы предоставления и распространения персональных данных, полученных в результате обезличивания, должны согласовываться с Роскомнадзором [2].

Ужесточаются требования к трансграничной передаче. С 1 марта 2023 года вступают в силу изменения ст. 12 ФЗ № 152 «О персональных данных», согласно которым Роскомнадзор вправе ограничить или запретить передачу персональных данных в страну, не обеспечивающую адекватную защиту.

В приказе Роскомнадзора от 05.08.2022 № 128 был утвержден список стран, обеспечивающих адекватную защиту прав субъектов персональных данных. В него вошли 89 государств, среди которых есть и участники конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, и страны, не являющиеся участниками конвенции, но чьи нормы права и принимаемые меры соответствуют ее положениям [3].

Вводится также обязанность по уведомлению Роскомнадзора об уже произошедших инцидентах. Так, с момента обнаружения неправомерной или случайной передачи персональных данных оператор должен уведомить об этом Роскомнадзор в течение 24 часов с момента обнаружения, а в течение 72 часов должен предоставить результаты внутреннего расследования.

Сформулируем выводы. Персональные данные остаются самым «желанным» ресурсом для киберпреступников.

Согласно статистическим данным экспертно-аналитических центров каждый год увеличивается процент пользователей, сталкивающихся с утечкой своих персональных данных. В 2023 году также прогнозируется увеличение количества утечек и скомпрометированных баз персональных данных. С увеличением утечек возможно появления нового тренда среди киберпреступников, а именно объединения различных баз данных для формирования папки с личными данными человека. Эти сведения позволят реализовывать более сложные схемы для социальной инженерии и атак на организации.

Многочисленные атаки, произошедшие в 2022 году, показали, что необходимо увеличивать меры и улучшать средства защиты персональных данных. Произошедшие на законодательном уровне ужесточения требований к операторам персональных данных позволит улучшить ситуацию в стране, но этого недостаточно. Для обеспечения безопасности частной информации необходим не только строгий контроль государства за операторами, ведущими работу с персональными данными, но и формирование культуры бережного обращение с персональными данными.

Список используемых источников

1. Аналитический отчет // Отчёт об утечках данных за 1 полугодие 2022 года. URL: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda (дата обращения 22.02.2023).

2. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности».

3. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций приказ от 5 августа 2022 г. № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных».

УДК 004.932.2
ГРНТИ 28.23.15

ДЕТЕКТИРОВАНИЕ ОБЪЕКТОВ НА ИЗОБРАЖЕНИЯХ

Л. А. Виткова[1,2], А. М. Лешукова[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Детекторы являются основой многих алгоритмов компьютерного зрения, главной задачей которого является научить машину распознавать объекты. В данной статье рассматривается применение сверхточных нейронных сетей для детектирования объектов на изображениях. В статье описаны несколько наборов данных и приведены метрики оценки качества детекции. Также представлены несколько основных типов архитектур нейронных сетей для Object Detection.

детектор, компьютерное зрение, метрика, изображение, нейронные сети.

В современном мире возможностью видеть наделены не только живые существа, но и машины. Это стало возможно благодаря развитию компьютерного зрения. Компьютерное зрение представляет собой область искусственного интеллекта, которая помогают компьютерным системам понять мир посредством распознания зрительных образов и обнаружения объектов [1, 2]. Эта технология используется во многих сферах, она значительно упрощает нашу жизнь и делает ее более безопасной. По оценкам разных экспертов востребованность в компьютерном зрении в ближайшие годы будет только расти, что и позволяет данной сфере развиваться как в сторону качества, так и производительности. Эта технология имеет большое количество разделов, каждый из которых выполняет разные функции. В статье будет

рассмотрен один из наиболее востребованных разделов компьютерного зрения – Object Detection (обнаружение объектов). Object Detection – это технология, которая определяет объект на изображении или видео.

На данный момент существует большое количество детекторов изображений. Каждый имеет свои преимущества и недостатки. Например, детекторы вида Region-based, к ним относятся такие детекторы, как: R-CNN, Fast R-CNN, Faster R-CNN и другие [3]. Принцип их работы заключается в том, что вначале из изображения извлекается большое количество регионов, все они имею разные пропорции (высота, ширина) и взяты из разных участков изображения. Далее эти регионы приводятся к одному размеру, а поверх используют сверточную сеть, на предсказаниях которой, обучается классификатор. Отдельно производится классификация бокса, и отдельно записываются координаты каждого бокса. Главным минусом такой модели является медленная скорость работы. Поэтому вслед за R-CNN появляются Fast R-CNN и Faster R-CNN главной задачей, которых является оптимизировать работу и тем самым увеличить ее скорость.

Спустя время был придуман абсолютно другой подход, кратко его концепцию можно описать как «Все в одной архитектуре» или «You Only Look Once» сокращенно YOLO [4]. Главным отличием от Region-based является то, что предсказания расположения боксов и их классов производится одновременно в одной нейронной сети, а не поэтапно, что значительно повлияло на время работы, ускорив процесс во много раз.

В рамках данной статьи рассматривались метрики для двух моделей Object Detection, а именно YOLOv3 и Faster R-CNN. Тестирование проводилось в Colaboratory с использованием TensorFlow Object Detection API – это удобный инструмент для запуска и обучения нейросетевых архитектур детектирования.

Самое важное в работе Object Detection – это этап обучения. Машинное обучение производится с использованием набора данных (*data set)*. Data set – это набор данных, который используется при обучении разных нейронных сетей. Причем качество обучения напрямую зависит от объема используемой информации: чем ее больше, тем точнее будет работать искусственный интеллект. Для каждой цели используется конкретный набор данных, он выбирается из уже существующих или составляется самостоятельно, если задача имеет узконаправленный характер. Для Object Detection в глобальной сети существует много различных наборов данных, самые известные из них: PASCAL VOC 2012, MS COCO 2017, IMAGENET, GOOGLE OPEN IMAGES V4 и другие. Обучение детекторов в рамках тестирования проводилось с использованием data set MS COCO 2017 [5].

Оценка качества и скорости работы моделей проводится с помощью метрик, таких как IoU и AP. IoU или Intersection over Union (*Jaccard index*) –

метрика степени пересечения между двумя ограничивающими рамками [6]. Вычисляется по формуле:

$$\boldsymbol{IoU} = \frac{\boldsymbol{S}\ \text{Пересечения}}{\mathbf{S}\ \text{Объединения}}.$$

AP – это популярная метрика измерения точности детекторов объектов. AP вычисляет среднюю точность для recall в диапазоне от 0 до 1 [6]. Существует четыре возможных предсказания детектора, такие как:

- True positive (TP) – истинный положительный, это предсказание, при котором детектор правильно опередил объект на изображении;
- True negative (TN) – истинный отрицательный, предсказание, при котором детектор не определил объект, и его там на самом деле не было;
- False positive (FP) – ложный положительный, предсказание, при котором детектор определил объект на изображении, но его там нет;
- False negative (FN) – ложный отрицательный, это предсказание, при котором детектор не нашел объект, но он там был.

Исходя из этих результатов происходит расчет критерия Precision (доля верных на все предсказания) по формуле:

$$Precision = \frac{TP}{TP + FP}.$$

Recall – доля верных предсказаний делим на сумму верных и тех, которые детектор не увидел:

$$Recall = \frac{TP}{TP + FN}.$$

Одним из основных критериев сравнения моделей является средняя точность для определения качества модели обнаружения объектов. Средняя точность включает в себя различные метрические показатели. Наиболее используемым вариантом является значение AP при IoU не меньше 0,5 и среднее значение AP при пороговых значениях IoU в диапазоне от 0,5 до 0,95 с шагом 0,5, которые обозначаются AP@.5 и AP@.5:.95 [7].

Анализ скорости работы модели производится с помощью показателя количество кадров в секунду. По общепринятым нормам считается, что показатель FPS выше 30 достаточен для выполнения обнаружения в потоковом режиме. По итогам работы моделей была составлена таблица 1.

ТАБЛИЦА 1. Результаты работы моделей

Модель	Точность, %	Полнота, %	AP@.5, %	AP@.5:.95, %	FPS, к/с
YOLOv3	97,4	92,6	95	50,4	51,9
Faster R-CNN	93,2	92,8	93,3	52	7,56

По результатам работы, которые были представлены в таблице 1, можно сделать несколько выводов, а именно значение показателей AP@.5 и FPS у YOLOv3 выше, чем у Faster R-CNN. Но показатель AP@.5:.95 у YOLOv3 ниже, чем у Faster R-CNN. Данные показатели говорят, нам о том, что YOLOv3 быстрее справится с обнаружением и имеет большую точность при небольшом пороговом значение IoU.

Что касается Faster R-CNN, то он не удовлетворяет требованиям обнаружения в потоковом режиме. Однако данную модель можно использовать в тех случаях, когда необходима более точная степень обнаружения, или, когда используются изображения в разных средах без повторного обучения.

YOLOv3 проигрывает в точности Faster R-CNN, особенно, когда используются изображения из нескольких разных сред. Но скорость работы модели позволяет использовать ее в потоковом режиме, например, YOLOv3 отлично подойдёт для анализа изображения с камер видеонаблюдения в настоящем времени.

Работа выполнена при финансовой поддержке Гранта РНФ (проект РНФ № 18-71-10094-П) в СПб ФИЦ РАН.

Список используемых источников

1. Виткова Л. А. Место и роль мониторинга и противодействия нежелательной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. Т. 1. С. 209–212.

2. Коул А., Ганджу С., Казам М. Искусственный интеллект и компьютерное зрение. Реальные проекты на Python, Keras и TensorFlow. СПб. : Издательский дом Питер, 2023.

3. Андриянов Н. А., Дементьев В. Е., Ташлинский А. Г. Обнаружение объектов на изображении: от критериев Байеса и Неймана–Пирсона к детекторам на базе нейронных сетей EfficientDet // Компьютерная оптика. 2022. Т. 46. N. 1. С. 139–159.

4. Gunawan C. R., Nurdin N., Fajriana F. Design of A Real-Time Object Detection Prototype System with YOLOv3 (You Only Look Once) // International Journal of Engineering, Science and Information Technology. 2022. Vol. 2. No 3. C. 96–99.

5. Davis J. et al. Spatial Relationship-Driven Computer Vision Image Data Set Annotation // 2022 International Joint Conference on Neural Networks (IJCNN). IEEE, 2022. PP. 1–8.

6. Михайлин С., специалист машинного обучения «Инфосистемы Джет». Object Detection. Распознавай и властвуй. Часть 1, 2, 2020 [Электронный ресурс]. URL: https://habr.com/ru/company/jetinfosystems/blog/498294/ (дата обращения 13.02.2023).

7. YOLOv4 – самая точная real-time нейронная сеть на датасете Microsoft COCO, 2020 [Электронный ресурс]. URL: https://habr.com/ru/post/503200/ (дата обращения 13.02.2023).

УДК 004.353, 621.397
ГРНТИ 20.53.21

УСТРОЙСТВО УПРАВЛЕНИЯ И СИНХРОННОГО ВЫВОДА АУДИОДАННЫХ ДЛЯ ГОЛОГРАФИЧЕСКОГО ВЕНТИЛЯТОРА DSEE-65H

С. С. Владимиров, В. Д. Волков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Работа представляет структуру и принцип построения устройства управления и синхронного вывода аудиоданных для голографического вентилятора Dsee-65H. Разработана структурная схема устройства управления и предложены варианты ее реализации на основе различных аппаратных платформ. С учетом особенностей работы голографического вентилятора разработан и протестирован принцип синхронного вывода аудиоданных. Представлены направления дальнейшего развития устройства управления.

голографический вентилятор, синхронизация вывода данных, одноплатный микрокомпьютер, Raspberry Pi.

Концепция голографии, то есть принципа воспроизведения объемных (трехмерных) изображений в пространстве, повилась в 1947 году [1, 2]. В последние годы интерес к голографии возрастает, что связано с развитием услуг телеприсутствия, включающих в себя воспроизведение и передачу по сетям связи голографических копий человека – аватаров – и изображений дополненной реальности [3].

На практике вместо реальных трехмерных голограмм речь часто ведут о так называемых псевдоголографических изображениях, которые лишь создают иллюзию объемности, выводя изображение, которое как бы парит в воздухе. К методам воспроизведения таких «голограмм» относят, например, отображение на скрытых экранах, проецирование изображений на прозрачных пленках, отображение при помощи голографических вентиляторов и некоторые другие [1, 2].

На кафедре сетей связи и передачи данных СПбГУТ для изучения принципов передачи и воспроизведения псевдоголограмм используется голографический вентилятор Dsee-65H компании DSeeLab Hologram [4].

Данное устройство по умолчанию позволяет воспроизводить только видеоизображения в виде отдельных файлов и не способно ни работать с видеопотоком, ни воспроизводить звуковую дорожку видеофайлов. Новые версии официального управляющего программного обеспечения, расширяющие его возможности, доступны только для операционных систем (ОС)

семейства MS Windows и не предназначены для работы в отечественных ОС, основанных на ядре Linux. Для расширения возможностей работы с голографическим вентилятором Dsee-65H в отечественных ОС была поставлена задача разработки программно-аппаратного комплекса, который позволит управлять голографическим вентилятором и обеспечит вывод аудиоданных.

Dsee-65H использует два управляющих командных интерфейса:

1. Командный управляющий протокол по беспроводному каналу 802.11b/g/n. В вентилятор встроена точка доступа 802.11, к которой подключается клиентское управляющее устройство. Взаимодействие с вентилятором производится через TCP-соединение.

2. Командный протокол по проводному каналу UART/TTL/RS-485, используемому в том числе для каскадирования вентиляторов. Вентилятор имеет входной интерфейс и выходной интерфейс, в который дублируются команды, полученные на вход вентилятора (в том числе и по радиоканалу).

Разрабатываемое управляющее утройство должно иметь возможность использовать оба управляющих интерфейса.

Учитывая указанные особенности, управляющее устройство может быть реализовано в двух вариантах.

Первый вариант основан на использовании обычной персональной ЭВМ, к которой по стандартным интерфейсам подключены беспроводная сетевая карта 802.11b/g/n и модуль UART/TTL/RS-485. Проведенное авторами тестирование распространенных бюджетных UART-модулей USB–TTL и USB–RS-485 на основе микросхем CH340 и PL2303 показало, что модули USB–RS-485 на основе микросхемы CH340 обеспечивают более стабильную работу при взаимодействии с вентилятором Dsee-65H.

Второй вариант основан на использовании одноплатных микрокомпьютеров, имеющих встроенные интерфейсы UART и 802.11b/g/n. Для построения данного варианта реализации управляющего устройства авторами выбран одноплатный микрокомпьютер Raspberry Pi 4, который поддерживается различными дистрибутивами ОС, основанными на ядре Linux, в том числе отечественными.

Структурные схемы обоих вариантов реализации управляющего устройства представлены на рис. 1 (см. ниже). Слева представлена схема управляющего устройства на основе персональной ЭВМ, справа – на основе Raspberri Pi 4.

Синхронизация запуска видеофайла на голографическом вентиляторе и соответствующего ему аудиофайла на управляющем устройстве производится по подтверждению приема команды запуска видеофайла, получаемому от вентилятора через выходной интерфейс UART либо через TCP-соединение в канале 802.11. Временная диаграмма взаимодействия при синхронизации вывода аудиоданных представлена на рис. 2.

Для управления голографическим вентилятором по проводному каналу UART разработано специализированное программное обеспечение «DSee Holo Fan UART Operator Panel» [5]. Программа управления написана на языке программирования Python версии 3.10, что позволяет использовать ее без изменений на управляющих устройствах, основанных как на обычных персональных ЭВМ, так и на одноплатных микрокомпьютерах. Взаимодействие управляющего программного обеспечения в рамках аппаратно-программного комплекса устройства управления протестировано при использовании отечественной операционной системы Alt Linux P10.

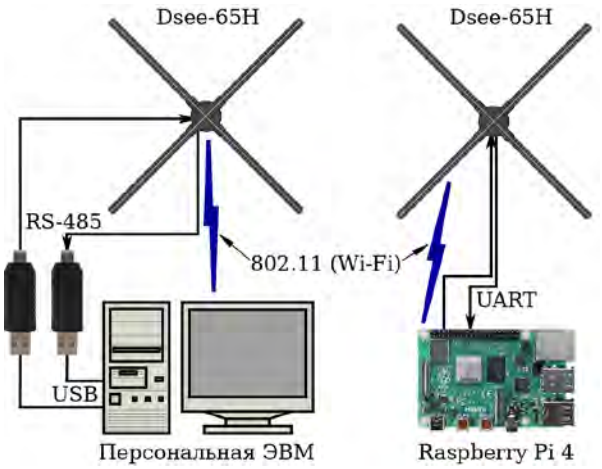


Рис. 1. Структурная схема устройства управления и синхронного вывода аудиоданных для голографического вентилятора Dsee-65H

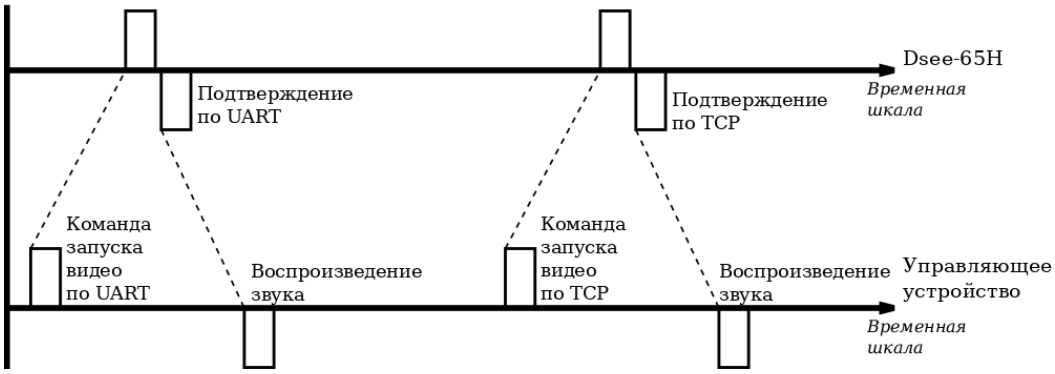


Рис. 2. Временная диаграмма взаимодействия устройства управления и голографического вентилятора Dsee-65H при синхронизации вывода аудиоданных

На рис. 3 (см. ниже) представлен внешний вид устройства управления голографическим вентилятором Dsee-65H на основе одноплатного микрокомпьютера Raspberry Pi 4, а на рис. 4 (см. ниже) показан общий вид аппаратно-программного комплекса с работающим голографическим вентилятором.

В дальнейшем планируется разработка универсального управляющего программного интерфейса, в том числе с доступом через локальную сеть.

Исследование выполнено в рамках мегагранта Минобрнауки России по соглашению № 075-15-2022-1137.

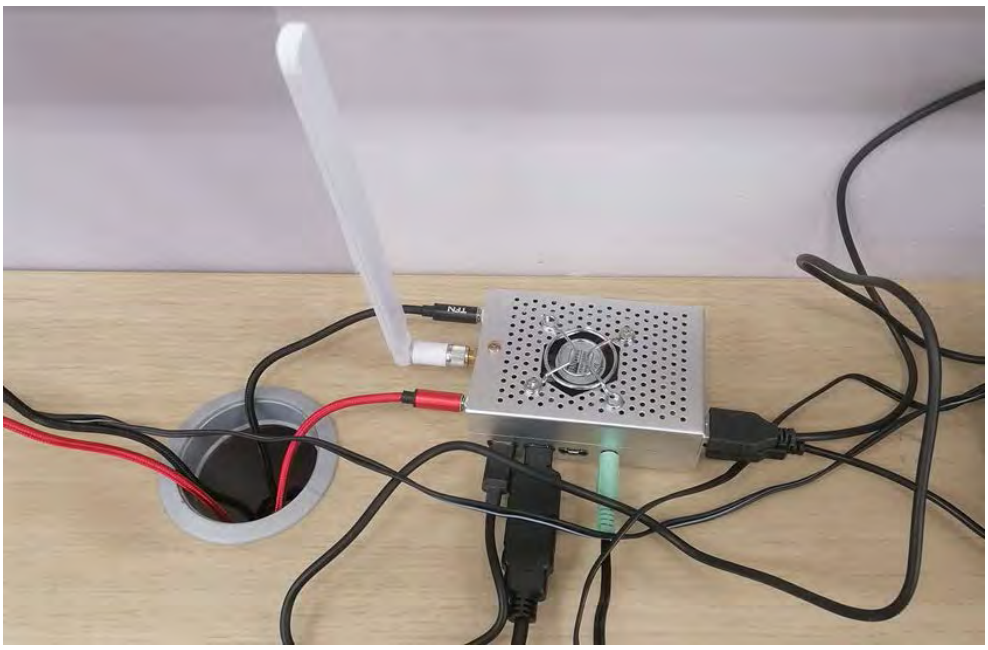


Рис. 3. Устройство управления голографическим вентилятором Dsee-65H на основе одноплатного микрокомпьютера Raspberry Pi 4

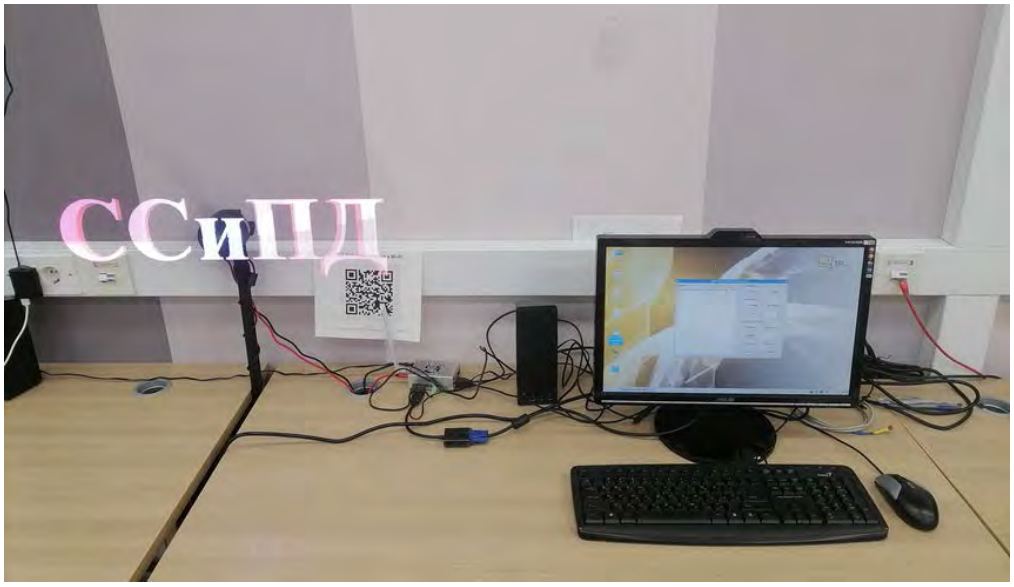


Рис. 4. Общий вид аппаратно-программного комплекса с работающим голографическим вентилятором

Список используемых источников

1. Баталов Д. Я., Баталова Д. В. Голографический вентилятор. Визуализация трехмерных изображений в воздухе // Актуальные проблемы радио- и кинотехнологий : Материалы III Международной научно-технической конференции, посвященной 100-летию со дня основания Санкт-Петербургского государственного института кино и телевидения, Санкт-Петербург, 23–26 октября 2018 года. Санкт-Петербург : Санкт-Петербургский государственный институт кино и телевидения, 2019. С. 88–94.

2. Овечкис Ю. Н. Голография без голографии. Мифы и реальность // Мир техники кино. 2017. Т. 11, N 3. С. 3–5.

3. Кучерявый А. Е., Киричек Р. В., Маколкина М. А., Парамонов А. И., Дунайцев Р. А., Пирмагомедов Р. Я., Бородин А. С., Владыко А. Г., Мутханна А. С. А., Выборнова А. И., Владимиров С. С., Гришин И. В. Новые перспективы научных исследований в области сетей связи на 2021–2024 годы // Информационные технологии и телекоммуникации. 2020. Т. 8, N 3. С. 1–19.

4. Кучерявый А. Е., Маколкина М. А., Парамонов А. И., Выборнова А. И., Мутханна А. С., Матюхин А. Ю., Дунайцев Р. А., Владимиров С. С., Ворожейкина О. И., Захаров М. В., Фам В. Д., Марочкина А. В., Горбачева Л. С., Паньков Б. О., Анваржонов Б. Н. Модельная сеть для исследований и обучения в области услуг телеприсутствия // Электросвязь. 2022. N 1. С. 14–20.

5. Владимиров С. С. Свидетельство о государственной регистрации программы для ЭВМ № 2022664046 Российская Федерация. Программа для ЭВМ "DSee Holo Fan UART Operator Panel" : № 2022663438 / С. С. Владимиров ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» : заявл. 15.07.2022 : опубл. 22.07.2022.

УДК 519.725, 621.391
ГРНТИ 49.33.29

ПРИМЕНЕНИЕ КОДА ГОЛДА ДЛЯ СЕТЕВОГО КОДИРОВАНИЯ В ДВУСТОРОННЕМ РЕЛЕЙНОМ КАНАЛЕ

С. С. Владимиров, И. Р. Скакунов, В. В. Трофимов, Е. Д. Фищев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

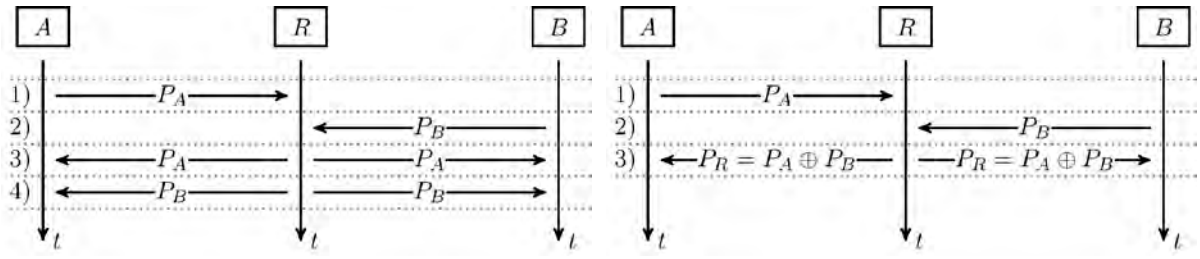
Работа представляет вариант применения помехоустойчивого кода Голда, образованного двумя кодами максимальной длины для сетевого кодирования в двустороннем релейном канале. Показан принцип восстановления пораженных ошибками данных с учетом особенностей построения кодового слова Голда и принципов сетевого кодирования. Выполнено математическое моделирование и представлены вероятностные характеристики различных вариантов декодирования кодового слова.

код максимальной длины, код Голда, сетевое кодирование, двустороний релейный канал.

В 1999 году группой китайских исследователей был предложен механизм сетевого кодирования, представляющий собой обратимое линейное преобразование данных на промежуточных узлах сети с помощью соответствующих математических операций [1, 2, 3, 4, 5]. Простейшей такой обратимой операцией, традиционно применяемой в системах с сетевым кодированием, является поразрядное сложение по модулю 2 [2, 3, 4, 5].

Применение сетевого кодирования позволяет уменьшить количество передаваемых по сети пакетов при сохранении объема передаваемой полезной информации. Одним из важных вариантов применения сетевого кодирования является организация двустороннего релейного канала (ДРК), применяемого, в частности для создания радиорелейных линий с ретрансляцией пакетов, использующих технологии передачи с общей разделяемой средой [6, 7].

На рис. 1 представлена схема ДРК для случая работы без сетевого кодирования (рис. 1а) и с сетевым кодированием (рис. 1б). Показано, что применение сетевого кодирования позволяет выиграть один временной интервал передачи за счет отправки ретранслятором R не самих исходных пакетов, а их линейной комбинации, из которой оконечные узлы A и B декодируют направленную им информацию [4, 6, 7].



а) б)

Рис. 1. Двусторонний релейный канал без сетевого кодирования (а) и с сетевым кодированием (б)

Из схемы ДРК на рис. 1б видно, что в случае поражения помехой одного из пакетов P_A, P_B или P_R во время передачи, данные не смогут быть восстановлены на оконечных узлах – получателях информации. Также следует отметить, что в случае поражения помехой исходных пакетов P_A и P_B, результат сетевого кодирования P_R будет содержать ошибки обоих исходных пакетов. Таким образом, сетевое кодирование может приводить к размножению ошибок [8, 9, 10].

Поэтому, при использовании систем с сетевым кодированием важную роль играет применение помехоустойчивых кодов для обнаружения и исправления ошибок [8, 9, 10].

В статье рассмотрим применение в сетевом кодировании в ДРК помехоустойчивого кода Голда на основе кодов максимальной длины (КМД).

Кодовое слово (n, k_G) кода Голда v_G образуется в результате сложения кодовых слов двух КМД (n, k) над разными полями Галуа GF(2^k). Количество информационных элементов в кодовом слове такого кода Голда $k_G = 2k$, т. е. кодовое слово Голда переносит в кодовом слове информацию, соответствующую информации, переносимой обеими исходными кодовыми словами КМД [11, 12, 13, 14].

Таким образом, при использовании кода Голда и КМД в ДРК с сетевым кодированием возникает два режима работы:

1. Обычное сетевое кодирование, когда каждый узел запоминает отправленные кодовые слова КМД во внутреннем буфере памяти и использует их для восстановления направленных ему второй стороной кодовых слов КМД при сетевом декодировании.

2. Работа без буфера памяти, при которой принимающий узел не выполняет сетевое декодирование и напрямую декодирует принятые кодовые слова кода Голда.

На рис. 2 представлена схема моделирования ДРК с помехоустойчивым кодированием. На обоих участках *A–R* и *B–R* канала (рис. 1) используется модель двоичного симметричного канала (ДСК) с одной и той же вероятностью битовой ошибки p_0.

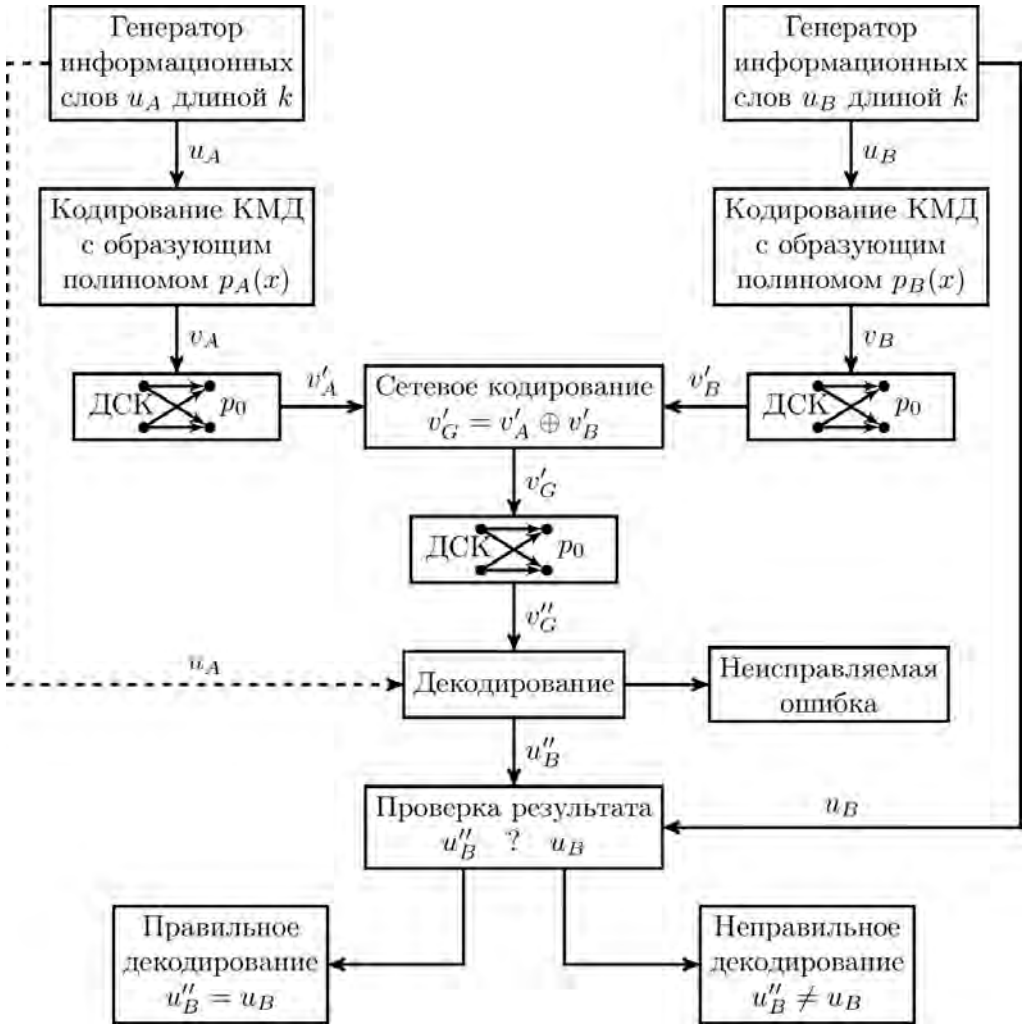


Рис. 2. Схема моделирования ДРК с сетевым и помехоустойчивым кодированием

На рис. 3 представлены вероятностные характеристики декодирования пакетов принимающим оконечным узлом для двух указанных выше режи-

мов работы. На графиках представлены вероятность правильного декодирования $P_{ПД}$, т. е. вероятность получения узлом A правильного информационного слова u_B; вероятность неправильного декодирования $P_{НД}$, т. е. вероятность необнаруженной ошибки; вероятность отказа от декодирования $P_{ОД}$, т. е. вероятность обнаружения неисправляемой ошибки. В качестве алгоритма декодирования помехоустойчивых кодов использовалось мажоритарное декодирование по k-элементным участкам.

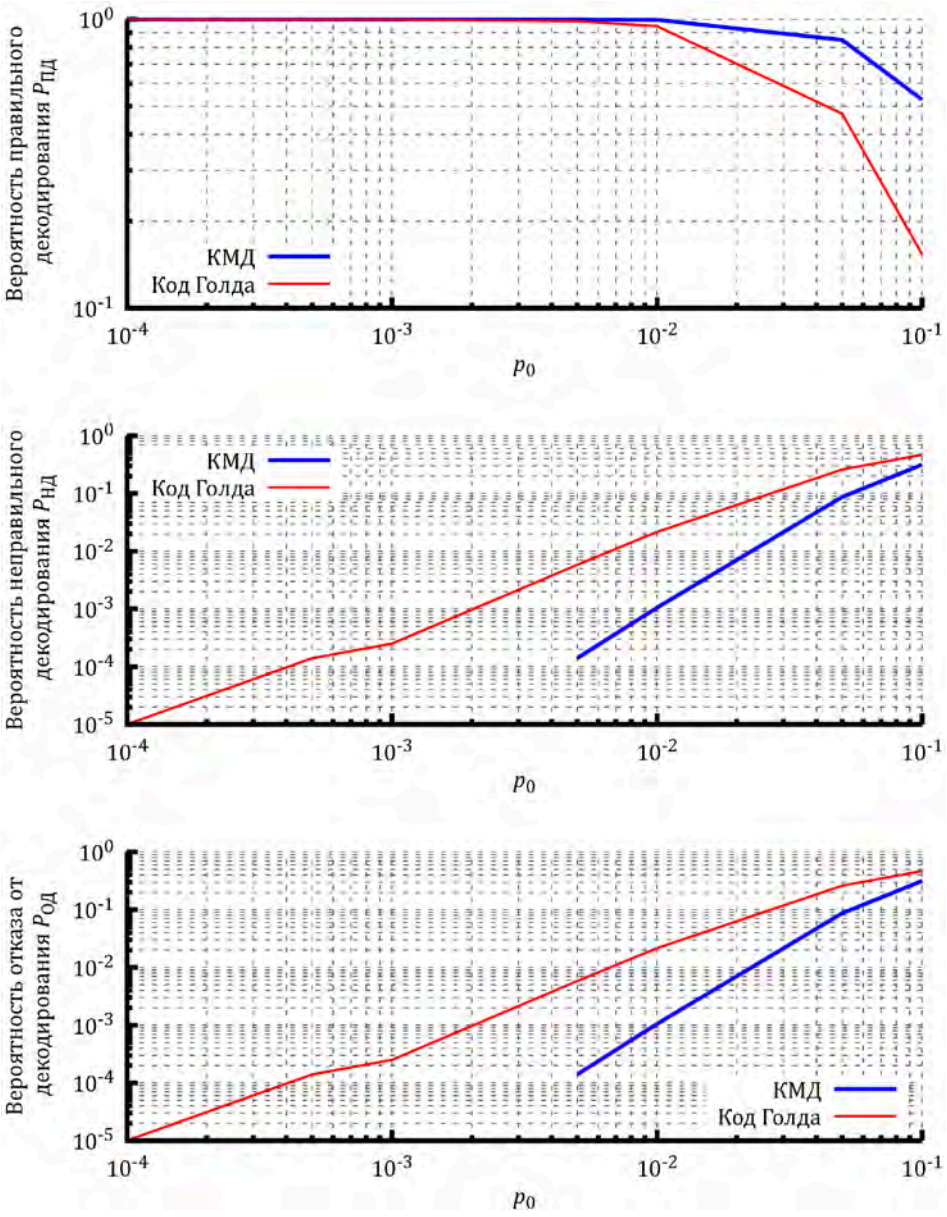


Рис. 3. Вероятностные характеристики декодирования пакетов принимающим оконечным узлом

Полученные результаты показывают, что сетевое кодирование с запоминанием исходных кодовых слов, использования их для сетевого декодирования и декодирование восстановленных кодовых слов собеседника

кодом максимальной длины обеспечивает лучшие вероятностные характеристики, хотя и требует использования буфера памяти. С другой стороны, вероятностные характеристики декодирования кодом Голда несколько хуже, но при этом не требуют хранить весть исходный пакет.

Таким образом, при выборе режима работы следует проводить моделирование и производить выбор с учетом качества канала связи требований к вероятности необнаруженной ошибки. При этом, если аппаратные возможности системы позволяют обеспечить реализацию сразу двух режимов работы, можно проводить динамическую проверку качества канала связи и в зависимости от результата переключаться между режимами работы.

Исследование выполнено в рамках исполнения ПНИ по государственному заданию СПбГУТ на 2023 год.

Список используемых источников

1. Yeung R., Zhang Z. Distributed source coding for satellite communications // IEEE Transactions on Information Theory. 1999. Vol. 45. Iss. 4. PP. 1111–1120.

2. Ahlswede R., Cai N., Li S. R., Yeung R. W. Network information flow // IEEE Transactions on Information Theory. 2000. Vol. 46. Iss. 4. PP. 1204–1216.

3. Li S.-Y. R., Yeung R. W., Cai N. Linear network coding // IEEE Transactions on Information Theory. 2003. Vol. 49. Iss. 2. PP. 371–381.

4. Fragouli C., Soljanin E. Network Coding Fundamentals // Foundations and Trends in Networking. 2007. Vol. 2. No. 1. PP. 1–133.

5. Габидулин Э. М., Пилипчук Н. И., Колыбельников А. И., Уривский А. В., Владимиров С. М., Григорьев А. А. Сетевое кодирование // Труды МФТИ. 2009. Том 1. № 2. С. 3–28.

6. Halloush R., Liu H., Dong L., Wu M., Radha H. Hop-by-hop Content Distribution with Network Coding in Multihop Wireless Networks // Digital Communications and Networks. 2017. Vol. 3. Iss. 1. PP. 47–54.

7. Amanowicz M., Krygier J. On Applicability of Network Coding Technique for 6LoWPAN-based Sensor Networks // Sensors. 2018. Vol. 18 (6). PP. 1–20.

8. Cai N., Yeung R. W. Network coding and error correction // Proceedings of the IEEE Information Theory Workshop. Bangalore, India: IEEE, 2002. PP. 119–122.

9. Владимиров С. С. 8-разрядные коды с прямой коррекцией ошибок в линейном сетевом кодировании // Электросвязь. 2020. N 7. С. 51–58.

10. Владимиров С. С., Гутовский А. С., Фомин А. И. Линейное сетевое кодирование с прямой коррекцией ошибок в системе беспроводного ретранслятора пакетов // Информационные технологии и телекоммуникации. 2022. Том 10. N 1. С. 21–33.

11. Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях. СПб. : Линк, 2009. 423 с.

12. Кларк Д. К., Кейн Д. Б. Кодирование и исправление ошибок в системах цифровой связи. Статистическая теория связи. М. : Радио и Связь, 1987. 392 с.

13. Gold R. Optimal binary sequences for spread spectrum multiplexing (Corresp.) // IEEE Transactions on Information Theory. IEEE, 1967. Vol. 13. No. 4. PP. 619–621.

14. Владимиров С. С. Коды Голда и коды максимальной длины в сетевом кодировании // Электросвязь. 2020. N 1. С. 61–66.

УДК 004.056
ГРНТИ 81.93.29

СОЗДАНИЕ СИСТЕМЫ ОХРАННОЙ СИГНАЛИЗАЦИИ НА БАЗЕ IOT-УСТРОЙСТВ В СРЕДЕ УМНОГО ДОМА ЯНДЕКС

В. Н. Волкогонов, А. А. Казанцев, А. С. Кривец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день высокий темп развития киберфизических систем позволяет каждому интегрировать в свою жизнь новейшие инженерные методы защиты, что приводит к появлению на рынке большого количества систем и устройств «умного дома». Но системы, созданные для домашней установки, обыкновенно имеют ограниченный производителем функционал и невозможность исправить или доработать устройства для необходимых условий и требований. В связи с этим появилась идея создания собственной системы охранной сигнализации, которая будет интегрирована с системой «умного дома» от Яндекса. Работа освещает процесс самостоятельной реализации системы охраны, ее возможности и пути её усовершенствования, а также рентабельность подобного проекта.

VK API, киберфизические системы, охранная сигнализация, NodeMCU, OrangePi, умный дом.

На сегодняшний день высокий темп развития киберфизических систем позволяет каждому интегрировать в свою жизнь новейшие инженерные методы защиты, что приводит к появлению на рынке большого количества систем и устройств «умного дома». Но системы, созданные именно для домашней установки, обыкновенно имеют ограниченный функционал и невозможность исправить или доработать эти устройства для необходимых условий и требований.

Проживание в студенческом общежитии обыкновенно сопровождается простотой замков и дверей, отсутствием внутренней охраны, а также сезонным опустением. Эти факторы могут показаться привлекательными для недобросовестных людей и подтолкнуть их к совершению кражи. В связи с этим появилась идея реализации собственной системы охранной сигнализации.

Перед началом работы были определены задачи, которые должна выполнять система охраны:

- Возможность активации смарт-картой или через смартфон – такой способ удобен, так как одна и та же карта используется и для входа в общежитие и для входа в комнату, а контроль через смартфон даёт возможность установить сигнализацию дистанционно;
- Интеграция с Умным домом Яндекс раскрывает большой спектр возможностей в создании различных сценариев работы устройств (включение музыки и света при входе, либо выключение электричества во всей комнате при выходе), возможность подключения дополнительных устройств без привязки к определенному вендору;
- Индикация состояния – звуковая и световая индикация обязательна, для тестирования и отпугивания нежелательных лиц;
- Логирование работы системы – для контроля и понимания произошедших событий;
- Наличие резервного питания – принципиально важный момент, так как выключить электричество можно извне комнаты;
- Связь с VK API – связь с API позволяет при срабатывании сигнализации автоматически отправлять сообщение в беседу общежития с просьбой проверить комнату, что будет самым быстрым способом реагирования на проникновение в комнату общежития;
- Поддержка различных режимов и расписания их работы – возможность переключения вариантов реагирования на проникновение, в зависимости от времени суток.

Основной алгоритм работы охранной сигнализации на вход и на выход (рис. 1) был разработан в соответствии с задачами, но в зависимости от необходимого режима работы меняется.

а) б)

Рис. 1. Алгоритм работы охранной сигнализации: (а) на вход, (б) на выход

Состав охранной системы, представленной на рис. 2:

• микроконтроллер NodeMCU – обрабатывает все поступающие сигналы и отправляет их mqtt брокеру (серверная система, которая координирует сообщения между клиентами);

• RFID считыватель для обнаружения поднесённых смарт-карт и считывания их ID;

• датчик Холла передает сигнал микроконтроллеру при открывании и закрывании двери;

• зуммер воспроизводит последовательные звуковые сигналы при установке сигнализации в охранный режим для понимания оставшегося времени на выход;

• светодиод для уведомления о считывании авторизованной смарт-карты, а также индикации оставшегося времени на снятие сигнализации с охранного режима при входе в помещение.

Код для микроконтроллера был написан на языке C++ при помощи приложения FLProg [1, 2].

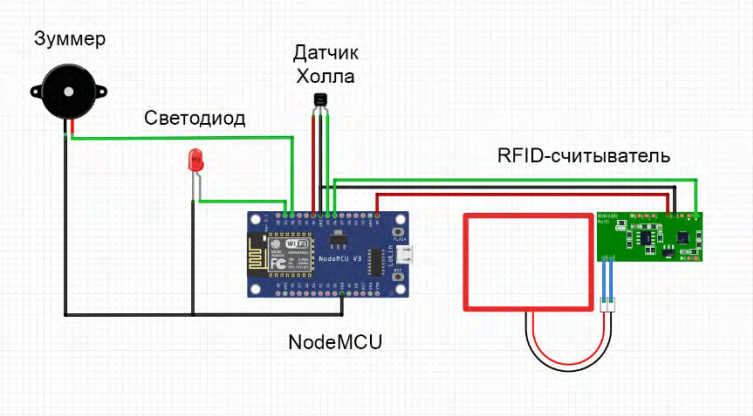


Рис. 2. Схема подключения устройств к NodeMCU

Микроконтроллер NodeMCU был выбран по нескольким причинам:

• возможность подключения к сети по WI-FI благодаря esp8266;

• низкая стоимость (около 130 рублей);

• возможность подключения в схему дополнительных контроллеров;

• простая архитектура и возможность быстрого редактирования программного кода при помощи программы FLProg [1];

• наличие большого количества библиотек и реализованных проектов.

Для реализации работы с VK API был написан бот на python [3], который запущен на микрокомпьютере OrangePi [4]. Микрокомпьютер расположен непосредственно в комнате и имеет подключение к 4g модему для бесперебойной связи.

Основной причиной выбора микрокомпьютера OrangePi является его производительность, так как NodeMCU не рассчитана на выполнение таких задач, также он позволяет выполнять роль шлюза для микроконтроллеров

при построении иных топологий сети, имеет интерфейсы для подключения USB (используется для подключения 4g модема), Ethernet, HDMI, Jack 3,5, а также в целом имеет мощности для развития проекта. Между собой NodeMCU, OrangePi и приложение Умный Дом общаются по протоколу mqtt. Все устройства подключены к mqtt брокеру и прослушивают его, либо отправляют туда сообщения (рис. 3). Для обеспечения бесперебойного питания NodeMCU и OrangePi подключены к портативному аккумулятору, что позволит им работать в течении нескольких часов в случае отключения электричества.

Рис. 3. Схема сети

К такой системе существует возможность подключения умного дверного замка, что позволит входить в комнату не только с помощью ключа, а только по смарт-карте [5]. Но этот вариант труднореализуем в условиях студенческого общежития и уже кратно дороже чем вся система, поэтому в настоящей версии охранной сигнализации он не используется [6].

Итогом проделанной работы стал полностью рабочий прототип охранной сигнализации (рис. 4), который способен выполнять все поставленные задачи. После сравнения его с уже существующими охранными системами на базе IoT-устройств выяснилось, что производство собственной системы выходит дешевле по всем аспектам, если в расчет не брать затраченное на разработку время. Однако, не было найдено серийной системы, способной работать с API Telegram или VK, что является довольно перспективным направлением [7], и этим собственная разработка действительно удобна и предоставляет больше возможностей.

Рис. 4. Прототип охранной сигнализации

Список используемых источников

1. Кривец А. С., Киричек Р. В. Программирование киберфизических систем с использованием визуального программирования в приложении FLProg // Актуальные про-

блемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 531–534.

2. Что такое FLProg. URL: https://flprog.ru/chto-takoe-flprog/ (дата обращения 15.01.2023).

3. VK для разработчиков. URL: https://dev.vk.com/reference (дата обращения 27.01.2023).

4. Dhairya Parikh. Raspberry Pi and MQTT Essentials: Packt Publishing, 2022. 272 с.

5. Штеренберг С. И. Разработка модели программно-аппаратного комплекса охраны объектов ssp_ai_3. 0 // Молодежь. Техника. Космос. 2018. С. 145–149.

6. Сахаров Д. В., Сахаров Д. В., Гельфанд А. М., Казанцев А. А., Пестов И. Е. Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. N 4. С. 14–20.

7. Гельфанд А. М., Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Оценка рисков и угроз безопасности в среде «умный дом» // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2020. Т. 1. С. 316–321.

УДК 004.056.5
ГРНТИ 81.93.29

ОБРАБОТКА ТЕХНИЧЕСКИМИ СРЕДСТВАМИ СЛУЖЕБНЫХ ДОКУМЕНТОВ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ

В. А. Волостных[1], П. В. Воробьев[1], П. А. Кононов[2]

[1]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного

[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы обработки служебных документов ограниченного распространения и служебных документов, содержащих служебную тайну в области обороны, не отнесенную к государственной тайне. Изложены требования к информационным системам, предназначенным для обработки служебных документов организаций и предприятий. Рассмотрены вопросы перехода к защищенному электронному документообороту. Предложены пути обеспечения безопасности документированной информации. Статья может быть полезна руководящему составу предприятий и специалистам подразделений обеспечения информационной безопасности, а также студентам и аспирантам образовательных организаций.

безопасность информации, защита информационных систем, информация ограниченного распространения, служебная тайна в области обороны, подготовка специалистов, служебные документы, электронный документооборот.

Анализ изменений нормативной правовой базы Российской Федерации показал, что имеется тенденция к усилению мероприятий по защите информации от несанкционированного доступа и бесконтрольного распространения.

Так, включением 11 июня 2021 года в Федеральный закон 1996 N 61-ФЗ «Об обороне» статьи 3.1. «Служебная тайна в области обороны» введено понятие «Служебная тайна в области обороны» и установлены требования по обеспечению защиты категории сведений отнесенной к Служебной тайне [1].

В развитие законодательства, постановлением Правительства Российской Федерации от 26.11. 2021 № 2052 утверждены «Правила обращения со сведениями, составляющими служебную тайну в области обороны» [2].

Анализ Правил показал, что утвержденный порядок работы с документами, содержащими информацию отнесенной к служебной тайне близок по сущности и деталям к порядку, утвержденному постановлением Правительства Российской Федерации 1994 года №1233 «Положению о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» [3]. Но на документе, содержащем информацию отнесенной к служебной тайне в области обороны под пометкой *«Для служебного пользования»* необходимо будет указывать пункт перечня, на основании которого, эта информация отнесена к информации ограниченного доступа.

Во исполнение ст. 3.1 Федерального закона «Об обороне», Министерством обороны Российской Федерации издан приказ «Об утверждении Перечня сведений Вооруженных Сил Российской Федерации, подлежащих отнесению к служебной тайне в области обороны». Данные изменения в законодательстве потребуют внесения соответствующих изменений в нормативных документах (по делопроизводству) предприятий и организаций оборонно-промышленного комплекса, научно-исследовательских организаций, выполняющих работы по заказу МО РФ, образовательных организаций, имеющих в своем составе военные учебные центры и др.

Анализ практики обращения со служебными документами ограниченного распространения и с документами, содержащими служебную тайну в области обороны (далее документы ДСП) выявил следующие проблемы.

1. Поскольку перечисленные категории документов ДСП имеют сходную пометку «*Для служебного пользования»*, то возникают трудности с их классификацией, и как следствие, затруднение порядка обращения с ними.

2. Учет получения, создания, отправки и использования документов ДСП ведется, в основном, в журналах учета неавтоматизированным спосо-

бом. На некоторых предприятиях при обработке документов ДСП в информационную систему вводят только регистрационные данные о документе, текст самого документа остается только на бумажном носителе, что затрудняет работу с этими документами.

3. При создании документов ДСП зачастую используются информационные системы, не отвечающие требованиям безопасности информации данной категории [4].

4. При передаче документов ДСП (проектов) внутри организации учет событий осуществляется журнальным способом, а информация передается путем передачи файлов, однако скопированные файлы не содержат сведений о первоисточнике, что является нарушением установленных правил.

5. Передача документов ДСП другим предприятиям или органам государственной власти осуществляется путем пересылки документов, исполненных на бумажных носителях или на машинных носителях. Время доставки документов таким порядком в ряде случаев не соответствует потребностям системы управления. Поскольку в нормативных документах определено, что возможна передача документов в электронном виде, но только по защищенным каналам связи, то возникает необходимость создания защищенных каналов связи между корреспондентами или передачи документов в зашифрованном виде.

6. Поскольку, документы должны иметь юридическую силу, то они должны быть подписаны соответствующими должностными лицами, следовательно, при создании, отправке и получении документов в электронном виде должны использоваться средства электронной подписи, что влечет за собой необходимость установки соответствующего программного обеспечения и использования ключевых носителей с ключевой информацией [5].

Перечисленные особенности обработки документов ДСП влекут за собой необходимость создания защищенных систем электронного документооборота (ЗСЭДО), средства защиты которых должны быть сертифицированы соответствующим порядком.

Анализ рынка средств обработки документированной информации показал, что основная масса СЭДО не предназначены для обработки документов ДСП и не обеспечивают выполнения требований законодательства, а именно они или не обеспечивают защиту информации от несанкционированного доступа, или не обеспечивают учет движения документов, и кроме того документы ДСП должны иметь реквизиты, установленные правовыми документами, в том числе номер экземпляра, в том числе копийного (тиражного). Все это затрудняет переход от классических документов ДСП к электронным и требует, как новых технических и технологических решений, так и совершенствования нормативной базы в области делопроизводства и архивного дела.

Кроме того, массовое внедрение ЗСЭДО потребует дополнительной подготовки работников подразделений предприятий, которые выполняют функции документационного обеспечения управления.

На основе анализа задач по обеспечению безопасности служебных документов ограниченного распространения в организациях и на предприятиях сделаны выводы и разработаны следующие предложения.

Выводы и предложения.

1. Поскольку постановление Правительства РФ от 1994 г. № 1233 разрабатывалось в расчете на существующие в тот период технологии работы с документами и вопросы применения средств вычислительной техники в нем практически не отражены, то можно считать, что назрела необходимость его переработки.

2. Анализ действующих постановлений Правительства РФ о служебной информации ограниченного распространения [2] и о служебной тайне в области обороны [3] показал что они во многом дублируют друг друга, но при этом в первом говорится об информации ограниченного распространения, а во втором об информации ограниченного доступа, что может вызывать разные юридические последствия, а следовательно назрела необходимость в разработке единого документа, поскольку на всех служебных документах должна проставляться одинаковая пометка (или, возможно, гриф) – *Для служебного пользования*.

3. При переходе к автоматизированной обработке служебных документов ограниченного распространения и/или доступа в организациях и на предприятиях необходимо создавать СЭДО в защищенном исполнении. Поскольку эти системы предназначаются для обработки служебной информации ограниченного доступах ЗСЭДО должны быть аттестованы по соответствующему классу [4] в соответствии с [6].

4. Наличие на предприятии организационно-распорядительной, технической и технологической документации ДСП со значительными сроками хранения (10 лет и более) повлечет за собой необходимость совершенствования системы архивного хранения предприятий и организаций.

5. При необходимости обмена служебными документами в электронном виде с подразделениями организации и организациями, находящимися за пределами контролируемой зоны основного административного здания (офиса), необходимо обеспечить защиту ЭДО средствами криптографической защиты информации в соответствии с [7].

6. При незначительном объеме служебных документов ограниченного распространения и/или доступа их учет можно вести журнальным способом, а их создание осуществлять на автономных СВТ без подключения к общим информационным сетям предприятия и без подключения к сети «Интернет».

7. Исходя из тенденций увеличения объема служебных документов и возросшей необходимости обеспечения их защиты целесообразно в учебные программы подготовки специалистов информационной безопасности ввести тему «Обеспечение защиты служебной информации ограниченного распространения и доступа в организациях, учреждениях и на предприятиях» [8].

8. Внедрение ЗСЭДО потребует подготовки работников канцелярий, общих отделов к эксплуатации этих систем, а также переработки инструкций по делопроизводству.

Список используемых источников

1. Федеральный закон от 31.05.1996 N 61-ФЗ (ред. от 02.07.2021) «Об обороне».

2. Постановление Правительства РФ от 26.11.2021 N 2052 «Об утверждении Правил обращения со сведениями, составляющими служебную тайну в области обороны».

3. Постановление Правительства РФ от 03.11.1994 N 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».

4. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи».

6. Приказ ФСТЭК России от 29.04.2021 N 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну».

7. Приказ ФСБ России от 24.10.2022 N 524 Об утверждении требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств.

8. Викулова А. Ю., Волостных В. А., Кононов П. А. Подготовка специалистов для подразделений технической защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). X Юбилейная международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 194–199.

УДК 005.92
ГРНТИ 20.53.23

ТЕНДЕНЦИИ РАЗВИТИЯ СИСТЕМЫ МЕЖВЕДОМСТВЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ВЫСШЕЙ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

В. А. Волостных[1], П. А. Кононов[2]

[1]Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного

[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются задачи и цели межведомственного электронного документооборота, рассмотрены особенности системы МЭДО применительно к высшим образовательным организациям, описано текущее состояние разработки и внедрения системы. Предложены варианты архитектуры решений реализации МЭДО. Авторы рассматривают особенности и преимущества перехода к межведомственному электронному документообороту. Также описаны основные перспективы развития в данном направлении.

межведомственный электронный документооборот, система электронного документооборота, средства защиты информации, высшая образовательная организация, электронная подпись.

Несмотря на то, что обмен юридически значимыми документами в бумажном виде по-прежнему занимает важное место в документообороте организаций, на сегодняшний день все большее число компаний отдает предпочтение электронному взаимодействию. Применение современных технологий при подписании и обмене документами помогает решать различные задачи – от ускорения и упрощения процесса до повышения уровня доверия к содержанию подписываемых и передаваемых документов.

В начале 2020 года Президент Российской Федерации заявил о необходимости осуществления цифровой трансформации страны в ближайшие десять лет. Неотъемлемой частью данного процесса является переход на электронный документооборот (ЭДО), что напрямую влияет на выполнение задач.

Развитие межведомственного электронного документооборота (МЭДО) определяется тем, что в условиях стремительного развития информационных потоков, функционирование и взаимодействие организаций с федеральными органами власти невозможно без четкого налаживания про-

цедур документационного обеспечения. Участниками МЭДО могут являться федеральные органы исполнительной власти, аппарат Правительства РФ, органы исполнительной власти субъектов РФ, иные государственные органы, государственные организации, включая высшие образовательные организации (ВОО) [5]. В настоящей статье рассмотрим задачи и цели МЭДО применительно к ВОО.

Под межведомственным электронным документооборотом понимается взаимодействие информационных систем электронного документооборота федеральных органов государственной власти, органов государственной власти субъектов РФ и иных государственных органов, а также организаций [1].

Основными целями создания МЭДО в высшей образовательной организации являются:

1. Повышение эффективности управления в ВОО за счет сокращения времени обработки и прохождения документов.

2. Ускорение процессов принятия решений руководством ВОО.

3. Минимизация затрат на обработку и отправку документов при взаимодействии ВОО с органами исполнительной власти [3].

При внедрении в ВОО межведомственного электронного документооборота допускается обмен информацией, содержащей общедоступную информацию и информацию, доступ к которой ограничивается в соответствии с законодательством РФ. Обмен между участниками МЭДО информацией, доступ к которой ограничивается в соответствии с законодательством РФ, осуществляется при выполнении ими требований по защите такой информации, установленных в отношении информационных систем электронного документооборота.

Обеспечение безопасности МЭДО является важным аспектом работы высшей образовательной организации, поскольку это позволяет защитить конфиденциальные данные и предотвратить возможные угрозы для его деятельности.

Для обеспечения безопасности межведомственного электронного документооборота в ВОО могут использоваться различные меры, такие как:

1. Использование электронной подписи, что гарантирует подлинность и целостность документов, а также их юридическую значимость.

2. Шифрование данных – позволяет защитить данные от несанкционированного доступа и их использования.

3. Использование защищенных каналов связи – позволяет обеспечить безопасную передачу данных между учреждениями.

4. Регулярное обновление программного обеспечения – позволяет предотвратить возможные уязвимости системы и обеспечить ее стабильную работу.

5. Обучение работников – позволяет повысить осведомленность работников в области безопасности информации и снизить риск возникновения ошибок.

Реализация МЭДО в высших образовательных организациях может осуществляться с помощью специализированных программных решений, которые обеспечивают безопасную передачу и обработку электронных документов. В таких системах используются современные методы шифрования и аутентификации, которые гарантируют конфиденциальность и надежность передачи данных.

Для реализации МЭДО необходимо также установить соответствующие правила и процедуры, которые определяют порядок обмена документами, требования к электронной подписи и другие важные аспекты. Важно, чтобы все участники процесса были ознакомлены с этими правилами и следовали им при работе с электронными документами.

В МЭДО реализован и полностью поддерживается механизм передачи официальной документации [2]. Для обеспечения электронного взаимодействия с федеральными органами власти в рамках МЭДО высшей образовательной организации необходимо:

1. Получить адрес и идентификатор, чтобы стать участником системы – путем обращения в ФСО РФ.

2. Организовать и обеспечить техническую инфраструктуру ВОО и собственную СЭД, которая будет подключена к МЭДО;

3. Обеспечить должный уровень сопряжения систем – иметь современный и качественный «адаптер» в виде технического решения.

Основной принцип МЭДО – интеграция имеющихся СЭД участников МЭДО и транспортной системы, обеспечивающей в автоматизированном режиме защищенный обмен электронными сообщениями между участниками МЭДО.

В основе реализации МЭДО могут лежать следующие технические решения:

1. Все участники МЭДО используют единый формат обмена электронными сообщениями;

2. Каждый участник МЭДО использует программно-аппаратный комплекс (шлюз), обеспечивающий обмен электронными сообщениями между своей СЭД и МЭДО (хранение, просмотр, поиск, выгрузку и загрузку).

3. Каждый участник МЭДО использует программный комплекс сопряжения (адаптер) своей СЭД с МЭДО [4].

Предлагаемая схема организации системы межведомственного электронного документооборота применительно к высшей образовательной организации представлена на рис. 1.

Межведомственный электронный документооборот в высшей образовательной организации может строиться по следующей схеме:

1. Инициатор (работник ВОО) создает электронный документ и подписывает его электронной подписью.

2. Документ отправляется через защищенный канал связи на сервер получателя (например, федерального органа исполнительной власти).

3. Сервер получателя проверяет подлинность электронной подписи и расшифровывает документ.

4. Получатель принимает решение и создает ответный документ, который также подписывается электронной подписью.

5. Ответный документ отправляется обратно через защищенный канал связи на сервер инициатора.

6. Сервер инициатора проверяет подлинность электронной подписи и расшифровывает ответный документ.

7. Инициатор получает ответ и принимает соответствующие меры.

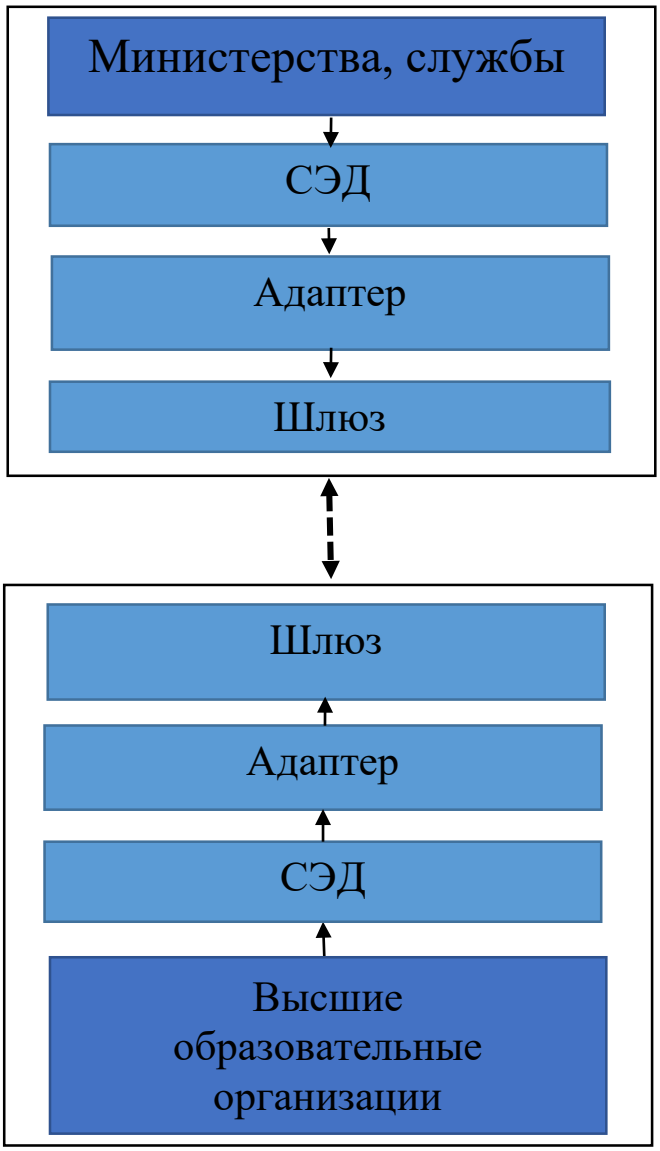


Рис. 1. Схема организации системы межведомственного электронного документооборота применительно к высшей образовательной организации

В процессе межведомственного электронного документооборота могут быть задействованы несколько учреждений, каждое из которых выполняет свою роль в обеспечение безопасности и целостности данных.

Внедрение межведомственного электронного документооборота в систему высшей образовательной организации позволяет сделать следующие выводы.

1. Внедрение механизмов межведомственного электронного документооборота позволяет значительно упростить процесс организации переписки с федеральными органами исполнительной власти.

2. МЭДО является необходимым инструментом для современного ВОО, который позволяет ему быть более эффективным и конкурентноспособным.

3. В целях внедрения и поддержания работоспособности МЭДО необходимо выделение финансовых, технических ресурсов.

4. Немаловажным моментом при внедрении МЭДО является обучение работников, которое позволяет повысить осведомленность работников в области безопасности информации и снизить риск возникновения ошибок.

Список используемых источников

1. Постановление Правительства РФ от 22.09.2009 № 754 «Об утверждении Положения о системе межведомственного электронного документооборота».

2. Постановление Правительства РФ от 17.02.2022 № 198 «Об утверждении Положения об информационной системе обеспечения внутри ведомственного и межведомственного документооборота и контроля исполнения поручений, в том числе с использованием облачных сервисов».

3. Шибаев Д. В. Правовое регулирование электронного документооборота : учебное пособие. 2-е изд., перераб. и доп. Вологда : Фонд развития филиала МГЮА имени О.Е. Кутафина в г. Вологде, 2019. 81 с.

4. Владимиров В. Л., Герцев К. Н., Докучаев В. А., Маклачкова В. В., Ступакова Ю.В. Организационно-технические средства защиты электронного документооборота. Ч. 2. Особенности организации взаимодействия и регулирования информационных систем государственных организаций : учебное пособие / Под ред. д.т.н., профессора В. А. Докучаева; МТУСИ. М., 2019. 38 с.

5. «Методические рекомендации по реализации Требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде» версия 1.1, одобренные подкомиссией по использованию информационных технологий при предоставлении государственных и муниципальных услуг Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 27.12.2016 № 558пр).

5. Викулова А. Ю., Волостных В. А., Кононов П. А. Анализ систем электронного документооборота // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. С. 84–88.

УДК 003.26.09
ГРНТИ 28.29.19

ОПИСАНИЕ СТРУКТУРЫ ЗАЩИЩЕННОГО КАНАЛА СВЯЗИ С АУТЕНТИФИКАЦИЕЙ

А. А. Воронцов, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В сетях передачи данных большое значение имеет защита передаваемых сообщений. Нарушители могут использовать различные методы подмены истинных сообщений или навязывать ложные сообщения. Для защиты от таких действий используются механизмы аутентификации сообщений. В статье предлагается структура защищенного канала связи с помехоустойчивым кодированием и аутентификацией для защиты от навязывания и подмены сообщений.

информационная безопасность, защищенная связь, сети передачи данных, аутентификация, криптография.

Введение

В современных сетях связи информация передается по открытым и закрытым каналам. Передача информации по закрытым каналам связи позволяет обеспечить конфиденциальность, целостность и доступность отправляемой информации. Однако, организация таких каналов доставки достаточно дорога и не обеспечивает вычислительную стойкость для основной массы пользователей. Передача данных по открытому каналу требует мероприятий по обеспечению защиты информации. Для этих целей могут использоваться разные методы защиты информации. Одним из таких методов является организация защищенного канала связи, который позволит обеспечить защиту от действий злоумышленника.

Коды аутентификации

Аутентификация информации крайне важна в защищенном канале связи. Аутентификация позволяет проверить подлинность как участников обмена информацией, так и подлинность самих передаваемых между этими участники сообщений. В модели аутентификации есть три участника [1]:

- Передающий корреспондент (отправитель). Он наблюдает источник информации и желает передать в сообщении наблюдаемое состояние источника.

• Принимающий корреспондент (получатель). Он желает узнать состояние источника, наблюдаемое передатчиком, и быть уверенным в подлинности предъявляемых ему сообщений.

• Нарушитель. Он имеет доступ к сообщениям и возможность осуществления активных атак. Нарушитель имеет возможность выполнять следующие действия: изменение сообщения, т.е. атаку подмены и введение нового сообщения, т. е. атаку имитации. Нарушитель рассчитывает на то, что поддельное сообщение будет принято, как аутентичное и принимающий корреспондент будет дезинформирован об истинном сообщении. Его целью является дезинформирование получателя о передаваемом состоянии источника.

Пусть S, K, C – конечные множества, $|S| > 2$, $|K| > 3$, $|C| > 3$, называемые, соответственно, множествами состояний источника, правил кодирования и сообщений. Каждое правило кодирования $k \in K$ – инъективное отображение $k:S \rightarrow C$.

Тогда множество АС = (S, K, C) называется кодом аутентификации или А-кодом [2].

Для защиты сообщений от активных атак, к которым относятся атаки имитации и подмены, отправитель и получатель выбирают общее (секретное) правило кодирования k. Отправитель вычисляет $c = k(s)$ и направляет сообщение c получателю [3]. Будем полагать, что элементы множеств S, K, C упорядочены.

Стойкость А-кода к атаке имитации оценивают вероятностью p_0 успеха имитации. Стойкость к атаке подмены оценивается вероятностью p_1 успеха подмены [4].

Идеальное шифрование

Идеальная система шифрования может обеспечить невозможность прочтения атакующим передаваемого сообщения при наличии у него любого вычислительного ресурса.

Введем понятие имитостойкости. Имитостойкость – способность шифра противостоять попыткам нарушителя по имитации или подмене сообщения [6].

Идеальный имитостойкий шифр – это шифр, для которого вероятности успеха имитации p_0 и успеха подмены p_1 принимают минимально возможное значение [5].

Главная проблема практического использования идеального шифрования состоит в том, что длина ключа шифрования при таком шифровании возрастает пропорционально длине сообщения. Это обстоятельство существенно ограничивает сферы применения безусловно стойкого шифрования.

В предлагаемой схеме используется вычислительно-стойкое шифрование, при котором дешифрование криптограммы требует необозримо большого времени и вычислительного ресурса. С точки зрения аутентификации сообщений это означает, что для обеспечения вычислительной стойкости системы аутентификации необходимо обеспечить минимально возможные вероятности имитации и подмены сообщения.

Описание схемы защищенного канала

Основной задачей защищенного канала связи является доставка передаваемых сообщений от источника сообщений к получателю с обеспечением целостности передаваемых данных. Задача обеспечения конфиденциальность в предложенной схеме не рассматривается.

В описываемой структуре используется комбинация, состоящая из помехоустойчивого кодирования и механизма аутентификации, основой построения которого служит система идеального шифрования. Получателю информации отправляются преобразованные данные и ключи аутентификации.

Схема защищенного канала (рис. 1) состоит из следующих элементов:

- источник и приемник сообщений;
- кодер и декодер помехоустойчивого кодирования;
- кодер и декодер системы аутентификации передаваемых сообщений;
- канал передачи информации.

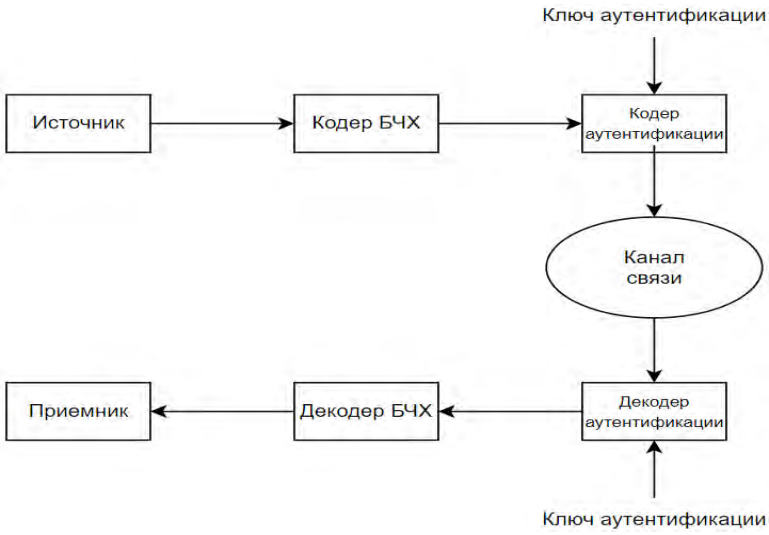


Рис. 1. Схема защищенного канала связи

Передача сообщений осуществляется следующим образом. Источник генерирует необходимые сообщения для передачи приемнику.

Далее передаваемые сообщения, представляемые в виде двоичных битовых последовательностей, подвергаются помехоустойчивому кодированию. Этот шаг необходим для обеспечения стойкости передаваемых данных

к ошибкам в канале передачи. Помехоустойчивое кодирование вносит избыточность в передаваемые сообщения. Можно предложить любой корректирующий код, в частности в предложенной схеме используется следующий корректирующий код Боуза-Чоудхури-Хоквингема (БЧХ). В поле, порождаемом примитивным многочленом $p(x) = x^4 + x + 1$, многочлен $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ порождает двоичный (15, 5, 7) код БЧХ с длиной кодового слова, равной 15 символам, обнаруживающий три ошибки [7]. Коды БЧХ имеют достаточно простую аппаратную и программную реализацию, однако они подходят лишь для защиты от помех среды передачи и не обеспечивают защиту от нарушителей.

Алгоритм аутентификации предполагает введение некоторого количества избыточных символов, гарантирующих целостность сообщения. Для аутентификации предлагается использовать алгоритм, изложенный в [5]. Аутентификация каждого бита входной информации производится с помощью таблицы функций шифрования, пример которой показан в таблице 1 (см. ниже).

Преобразование осуществляется следующим образом. На вход шифратора поступают данные в виде битовой последовательности. Кроме того, на шифратор поступают ключи шифрования в виде псевдослучайных двоичных последовательностей или гаммы. Преобразование осуществляется согласно матрице кодера путем побитного сопоставления входного значения и ключа. Отличительной особенностью данной схемы является то, что для представления одного бита исходной информации требуется два бита зашифрованного текста [5]. При таком преобразовании вероятность навязывания будет зависеть от количества избыточных символов.

ТАБЛИЦА 1. Таблица функций шифрования

S / *K*	$s_0(0)$	$s_1(1)$
k_1	01	10
k_2	01	11
k_3	10	01
k_4	10	11
k_5	11	01
k_6	11	10

После аутентификации пакеты данных поступают в канал связи для передачи получателю. В канале связи на передаваемые данные оказывает воздействие среда передачи, вследствие чего возникают различного рода помехи. Распределение ключей шифра имитозащиты в данной статье не рассматривается.

Принятые из канала связи данные, поступают на шифратор. Он реализует функцию дешифрования согласно той же таблицы, которая использовалась в прямом преобразовании. В шифраторе удаляются избыточные символы из принятых сообщений и на выходе выдается кодовое слово БЧХ.

Расшифрованные слова кода БЧХ поступают на декодер помехоустойчивого кода. Существует несколько способов дешифрования кодов БЧХ. В данной схеме декодер работает только в режиме обнаружения ошибок. Это означает, что при получении принимающим корреспондентом кодового слова с ошибкой, слово отбрасывается. Принимающий корреспондент в таком случае отправляет запрос повторной отправки отброшенного сообщения, подобный тому, как это реализовано в протоколе TCP.

После отбрасывания избыточной части при декодировании, сообщения поступают на приемник и преобразуются в вид, доступный для их прочтения принимающим корреспондентом.

Заключение

В статье предлагается схема защищённого канала передачи данных. Описываемая схема позволяет обеспечить целостность передачи информации по каналу связи. Достоинством данной схемы является применение кода аутентификации, основанного на вычислительно-стойком шифровании, стойкость которого доказана в [5]. Однако, следует отметить, что применение такого кодирования вносит существенную избыточность в передаваемые данные, что не позволяет применять предложенную схему в каналах связи недостаточно высокого качества.

Список используемых источников

1. Зубов А. Ю. Коды аутентификации : монография. М. : Издательство Гелиос АРВ, 2017. 256 с. ISBN 978-5-85438-262-5.

2. Зубов А. Ю. Коды аутентификации с секретностью (обзор) // Математические вопросы криптографии. 2017. Т. 8, N 3. С. 5–40. DOI: https://doi.org/10.4213/mvk230.

3. Зубов А. Ю. Код аутентификации с секретностью на основе проективной геометрии // Математические методы криптографии. 2013. N 2 (20). С. 39–49.

4. Зубов А. Ю. Криптосистема шифрования с аутентификацией на основе кода аутентификации с секретностью // Математические методы криптографии. 2019. N 43. С. 60–69.

5. Зубов А. Ю. Совершенные шифры : монография. М. : Издательство Гелиос АРВ, 2003. 160 с. ISBN 5-85438-076-5.

6. Коржик В. И., Просихин В. П., Яковлев В. А. Основы криптографии : учебное пособие / рец.: Р. Р. Биккенин, Б. В. Изотов. СПб. : СПбГУТ, 2014. 277 с. ISBN 978-5-89160-097-3 : Б. ц.

7. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применения : учебное пособие. М. : Техносфера, 2005. 320 с. ISBN 5-94836-035-0.

УДК 004.054
ГРНТИ 49.33.35

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ТЕСТИРОВАНИЯ БЕСПРОВОДНЫХ СЕТЕЙ СЕМЕЙСТВА IEEE 802.11

Г. Е. Ворошнин, В. Е. Дрепа, М. М. Ковцур

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Беспроводные сети Wi-Fi стали неотъемлемой частью повседневной жизни почти каждого человека. Они используются как в самых малых домашних сетях, так и в крупных корпоративных сетях. При этом очень незначительная часть пользователей беспроводных сетей задумываются о том, насколько защищены данные, которые они передают. Количество инцидентов информационной безопасности с каждым годом увеличивается. Одним из самых распространённых объектов атак является сетевое оборудование, которое, в частности, обеспечивает подключение клиентов к сети семейства IEEE 802.11. Наряду с процессом постоянного совершенствования протоколов и стандартов безопасности сетей, модернизируются и механизмы обхода или взлома этих стандартов. Даже самое современное сетевое оборудование подвержено простейшим видам атак, заметно снижающих качество обслуживания. В связи с этим, разработка программного обеспечения для тестирования сетей семейства IEEE 802.11, актуальна как для проверки устойчивости сети, так и для создания методов борьбы с реальными случаями атак.

информационная безопасность, безопасность беспроводных сетей, тестирование сетей Wi-Fi.

Трудно поспорить с тем, что беспроводные сети семейства IEEE 802.11 имеют огромную популярность как средство для удобного и быстрого получения доступа к мировой сети Интернет. В то же время ежегодно количество атак на сети возрастает [1, 2, 3], в том числе и на Wi-Fi [4]. При этом мало кто задумывается, насколько безопасно передавать данные с использованием рассматриваемой технологии.

Одним из основных методов защиты корпоративных сетей Wi-Fi являются WIDS (*wireless intrusion detection system*) и WIPS (*wireless intrusion prevention system*) – системы обнаружения и предотвращения вторжений соответственно. Для проверки эффективности и качества работы таких систем, а также в соответствии с 17 и 21 приказами ФСТЭК [5, 6], данные системы должны проходить контроль эффективности [7].

С целью обеспечения данной потребности были изучены существующие инструменты [8], их классификация [9] и создан программный инструмент автоматизированного тестирования беспроводных сетей семейства

IEEE 802.11. Автоматизированное тестирование осуществляется путём выбора вида, типа атаки и передачи необходимых для её выполнения аргументов. Аргументы могут быть переданы как интерактивно, так и вместе с командой из терминала операционной системы.

Процесс создания программного инструмента производился по SDLC (*systems development life cycle*) – жизненный цикл программного обеспечения. Условная схема данного процесса представлена на рис. 1. Основные этапы процесса: анализ потребностей, планирование, разработка архитектуры и дизайна, написание программного года, тестирование, внедрение. При создании инструмента были пройдены все этапы, за исключением внедрения. Этап внедрения будет осуществлён после прохождения процедуры патентования и выявления интереса со стороны потребителя.

Рис. 1. Жизненный цикл программного обеспечения

Необходимость создания настоящего программного инструмента обоснована в начале статьи. На этапе планирования определено, что код будет написан на языке Python 3.

Язык программирования выбран на основе наличия готовых сетевых библиотек, таких как Scapy. Основные преимущества библиотеки:

- может легко обрабатывать большинство классических задач, таких как сканирование, трассировка, зондирование, модульные тесты, атаки или обнаружение сети;
- активно поддерживаемый проект;
- создана в результате тестирования сетей на проникновение.

При построении решения, использовалась операционная система Ubuntu, так как она более оптимизирована и в ней программному инструменту будет проще использовать системные ресурсы. Для описания алгоритма функционирования программного обеспечения составлена схема этапов его работы, представленная на рис. 2.

В программном продукте реализованы следующие функции:

- изменение режима работы беспроводного интерфейса;
- изменение канала беспроводного интерфейса;
- сбор и отображение информации о беспроводных сетях;
- атака beacon flood в двух вариантах: фаззинг-кадров, флуд кадрами с именами сетей из файла;
- атака probe request flood в двух вариантах: широковещательный флуд, одноадресный флуд;

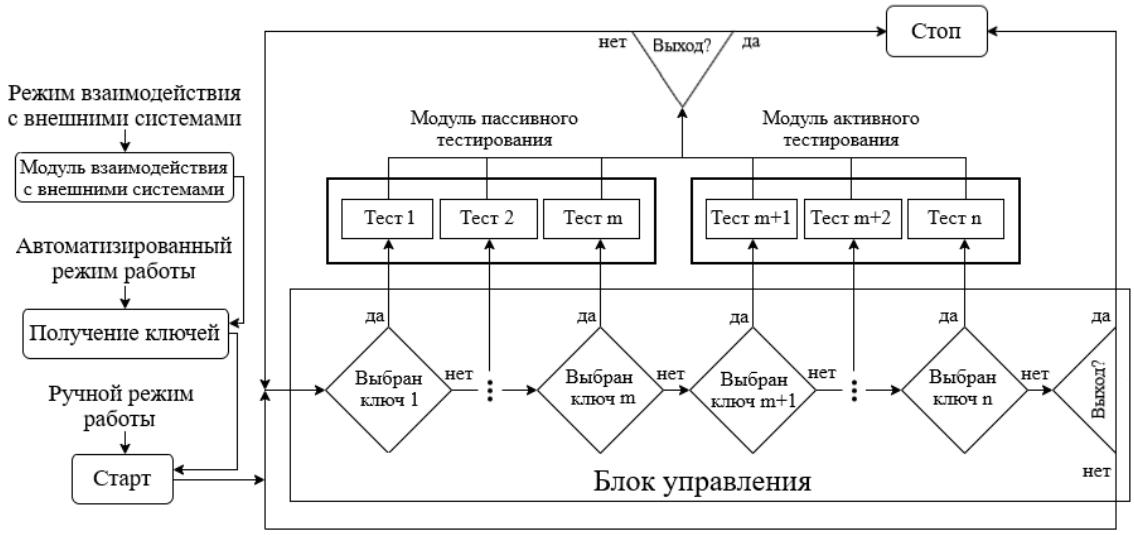


Рис. 1. Схема этапов работы инструмента тестирования

- атака authentication flood;
- атака deauthentication flood в 3 вариантах: флуд кадрами от имени клиента к точке доступа, флуд кадрами от имени точки доступа к клиенту, флуд кадрами от имени точки доступа в широковещательном режиме;
- атака SYN flood;
- атака ARP spoofing;
- атака Fake AP;
- атака DNS spoofing;
- перехват 4-х стороннего рукопожатия и подбор пароля WPA-2 по словарю.

Данные функции могут быть запущены как в интерактивном режиме, так и при помощи команды с аргументами из командной строки. Основными аргументами, как показано на рис. 3 (см. ниже), являются: беспроводной интерфейс, режим работы интерфейса, канал работы интерфейса, тип атаки (при выполнении атаки, реализованной в нескольких вариантах), количество кадров, отправляемых в секунду, общее количество отправляемых кадров, файл для чтения (для атак, получающих данные из файлов), MAC-адрес, BSSID (канальный адрес точки доступа), порт, IP-адрес, имя точки доступа.

В дальнейшем планируется реализовать следующие нововведения:

- создание веб-интерфейса [10];
- тестирование разработки в «боевых условиях» – оценка эффективности выбранных методов тестирования;
- оценка ресурсоёмкости инструмента;
- проверка работоспособности инструмента на других платформах;
- интеграция с системой wIPS и тестирование работы wIPS решения;

- тестирования совместной работы с wIPS решением в реальных условиях;
- сбор и анализ появившихся потребностей и выход на новый цикл разработки.

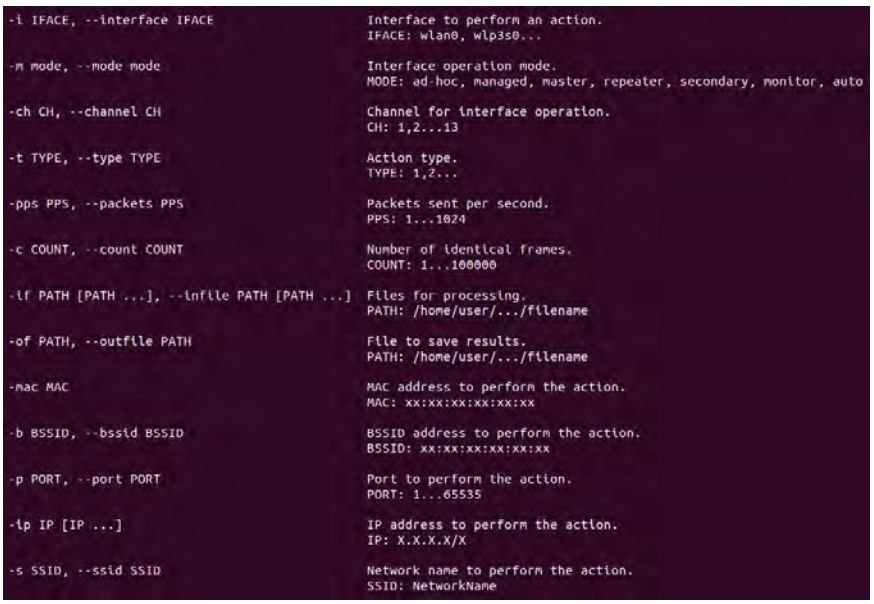


Рис. 3. Аргументы запуска инструмента тестирования

В завершение можно сказать, что инструменты тестирования постоянно совершенствуются наравне с развитием технологий [11]. Важно заметить, что чаще всего они создаются не для аудита безопасности, а для атак со стороны злоумышленников, поэтому инструменты часто носят узконаправленный характер. В настоящей работе реализовано комплексное решение, позволяющее тестировать беспроводные сети семейства IEEE 802.11 как в интерактивном режиме, так и в режиме командной строки. Таким образом можно сделать вывод, что цель работы была достигнута.

Список используемых источников

1. Актуальные киберугрозы: IV квартал 2022 года: сводная статистика. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/#id3 (дата обращения 11.03.2023).

2. Актуальные киберугрозы: IV квартал 2021 года: сводная статистика. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/#id2 (дата обращения 11.03.2023).

3. Актуальные киберугрозы: IV квартал 2020 года: сводная статистика. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q4/#id2 (дата обращения 11.03.2023).

4. Волкогонов В. Н., Казанцев А. А., Катасонов А. И., Орлов Г. А. Анализ безопасности Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб. : 2019. Т. 1. С. 270–275.

5. ФСТЭК Приказ от 18 февраля 2013 г. N 21: об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691 (дата обращения 11.03.2023).

6. ФСТЭК Приказ от 11 февраля 2013 г. N 17: об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения 11.03.2023).

7. Карельский П. В., Зуев И. П., Ковцур М. М., Миняев А. А. Разработка методики тестирования IPS модуля // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. N 1. С. 25–31.

8. Карельский П. В., Ковцур М. М., Штеренберг С. И., Малинин Н. И. Анализ современных средств автоматизированной проверки функций безопасности коммутационного оборудования // Информационная безопасность регионов России. XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург : Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2021. С. 385–386.

9. Ворошнин, Г. Е., Ковцур М. М., Юркин Д. В. Анализ и классификация программных инструментов для тестирования на проникновение беспроводных сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т., СПб. : СПбГУТ, 2022. Т. 1. С. 310–314.

10. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании: VIII Международной научно-технической и научно-методической конференция: сб. науч. ст. в 4 т., СПб. : СПбГУТ, 2019. Т. 1. С. 734–739.

11. Василишин Н. С., Ушаков И. А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении: материалы 9-й конференции по проблемам управления. 2016. N 6. С. 670–675.

УДК 004.750
ГРНТИ 49.33.29

ВНЕДРЕНИЕ В ТУМАННЫЕ ВЫЧИСЛЕНИЯ СИСТЕМЫ КОНТЕЙНЕРОВ DOCKER

А. И. Выборнова, В. М. Елагин, Д. С. Королев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные устройства предполагают все большее уменьшение их физических размеров, также меняются и технологии, реализуемые на их основе. Проблема перехода

современных сетей, основанных на виртуальных машинах к инфраструктуре, основанной на технологии Docker заключается в нерациональном использовании ресурсов микрокомпьютеров. Docker требует высокую производительность, дополнительные надстройки на системе приводит к увеличению нагрузки и расходов ресурсов. В данной статье рассматриваются разные методы оптимизации, ускоряющие развертывание контейнеров.

Docker, контейнеры, Kubernetes, слои, образ, оркестратор, туманные вычисления.

В настоящее время туманные вычисления значительно расширяют возможности облачных платформ на базе центров обработки данных [1]. Архитектура облачных вычислений построена на централизованной системе, где все операции проходят через крупные ЦОДы, которые связаны сверхскоростными сетями, в то время как туманные вычисления являются децентрализованной системой. Типовая архитектура представлена на рис. 1.

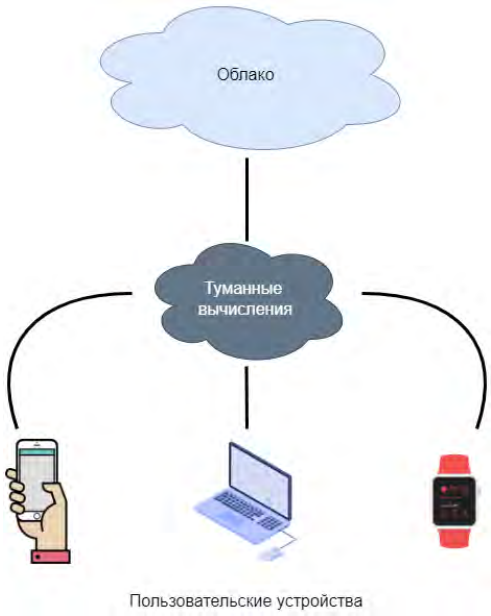


Рис. 1. Архитектура туманных вычислений

В качестве узлов, применяемых в туманных вычислениях, зачастую используются микрокомпьютеры, расположенные наиболее близко к конечным устройствам. Небольшие размеры микрокомпьютеров приводят к очевидным аппаратным ограничениям, в связи с этим остро возникает вопрос оптимизации их работы и эффективного распределения программных ресурсов. В данной статье обозреваются и приводятся возможные методы оптимизации системы контейнеров Docker при работе с маломощными устройствами.

Последовательная загрузка слоя образа

Загрузка нескольких образов одновременно направлена на максимизацию пропускной способности сети. Такой метод негативно влияет на скорость распаковки, так как Docker имеет свою политику копирования при записи драйверов, что обязывает процессы загрузки и извлечения каждого слоя образа выполняться последовательно, что приводит к задержкам [2]. Далее сравнивается два метода загрузки образов – последовательный и параллельный.

На рис. 2 демонстрируется эффективность загрузки слоев последовательно, а не параллельно.

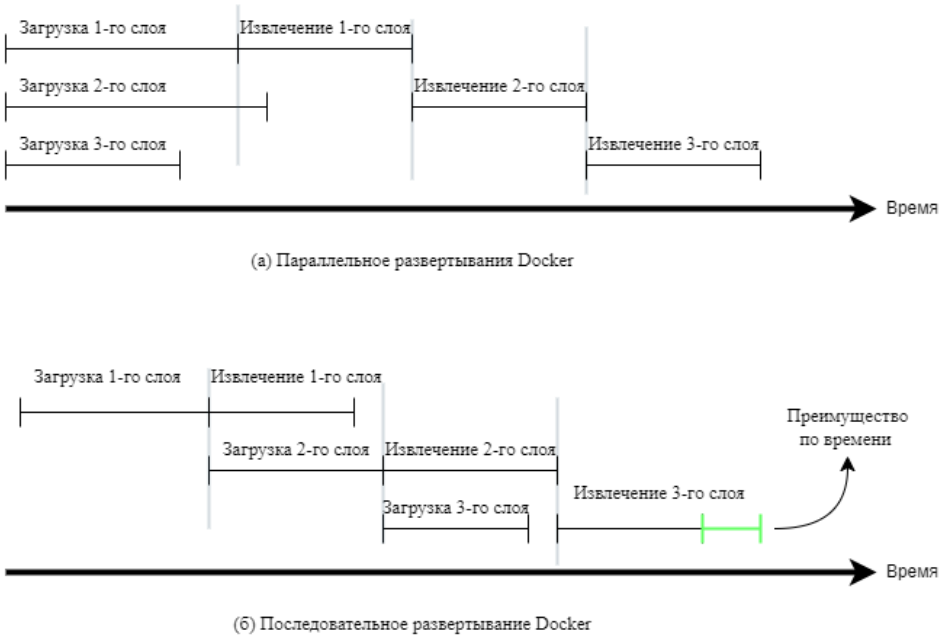


Рис. 2. Методы развертывания Docker

На рис. 2а представлен метод параллельной загрузки слоев при котором загрузка и извлечение n-го слоя может начаться только после загрузки и извлечения n – 1 слоя. На рис. 2б представлен метод последовательной загрузки и извлечения, при котором n + 1 слой начинает свою загрузку только после завершения загрузки n-го слоя. Параллельно загрузке n + 1 слоя происходит распаковка и извлечения на диск n-го слоя, что позволяет быстрее начать извлечение n-го слоя. Данный метод позволяет использовать ресурсы микрокомпьютеров, которые имеют невысокую производительность, более эффективно.

Для того чтобы применить метод параллельной загрузки необходимо в конфигурационном файле /etc/docker/daemon.json изменить значение параметра “max-concurrent-downloads”. Данный параметр определяет максимальное количество одновременных загрузок, установка значения «1» позволяет реализовать последовательную загрузку слоев.

Метод управления ресурсами контейнеров Docker

В технологии Docker используются контейнеризация – это способ упаковки приложения и всех его зависимостей в один образ, который запускается в изолированной среде, не влияющей на основную операционную систему. При большом количестве контейнеров появляются

сложности в их управлении, поэтому возникает необходимость использование специальных платформ, например, Kubernetes, которая часто используется в связке с Docker.

Kubernetes предназначен для оркестрации контейнеров, что облегчает их настройку и автоматизацию. С точки зрения операционной системы, ак-

тивные контейнеры ничем не отличаются от обычных процессов, где распределение ресурсов контролируется системой. Виртуальные машины используют фиксированное количество системных ресурсов, в то время как при инициализации к вновь созданным контейнерам по умолчанию не применяются ограничения ресурсов. На рис. 3 предлагается команда, которая позволяет ограничить потребление ресурсов процессора для созданных контейнеров [3].

```
docker run -it --cpus=\.7" spark /bin/bash
```

Рис. 3. Команда ограничения процессорных ресурсов

Данная команда позволяет сделать так, чтобы новый контейнер загружал процессор не более чем на 70 %. Также существуют команды, которые способны установить ограничения использования оперативной памяти. Бывают жесткие и мягкие ограничения ресурсов оперативной памяти для контейнеров. Жесткое ограничение предполагает установку абсолютного лимита памяти, превысив который, завершается процесс выполнения контейнера из-за отсутствия памяти в ядре. На рис. 4 представлен данный лимит, который задается флагом –m или –memory команды docker run.

```
docker run --memory=512m my-app:latest
```

Рис. 4. Команда жесткого ограничения памяти

Устанавливается ограничение памяти в 512 мегабайт. Реализация мягкого ограничения памяти позволяет использовать больше памяти при наличии свободного места. Однако, если дополнительно разрешенная память устройства закончится, процесс выполнения контейнера также завершится. На рис. 5 представлена команда установки мягких ограничений, которые устанавливаются флагом –memory-reservation.

```
docker run --memory=512m --memory-reservation=256m my-app:latest
```

Рис. 5. Команда мягкого ограничения памяти

Команда разрешает использовать 256 МБ памяти при доступных 512 МБ. Представленные команды по ограничению ресурсов процессора и памяти позволяют более эффективно распределять ресурсы микрокомпьютеров, в которых данные показатели сильно ограничены.

Метод объединения команд RUN

Данный метод эффективен тогда, когда ведется работа с временными файлами (их загрузка, установка, а затем последующее удаление). Для оптимизации такого процесса необходимо создание всего одной команды

RUN, которая объединит все шаги вместе, вместо нескольких команд RUN, которые будут занимать больше памяти [4]. На рис. 6 приводится пример неэффективного использования команды, в котором происходит временная загрузка исходного кода для его компиляции, а затем его удаление.

```
FROM dedian:latest
WORKDIR /app
RUN git clone https://some.platypus.git
RUN cd platypus
RUN make
RUN mv ./binary /usr/bin/
RUN cd .. && rm -rf platypus
```

Рис. 6. Неэффективное использование команды RUN

Неэффективность данного метода заключается в том, что каждая команда RUN создает новый слой, занимающий дополнительную память устройства, содержащий временные файлы, при удалении которых они только помечаются как удаленные, а в действительности не удаляются полностью, тем самым не освобождая место на устройстве.

Вместо вышеуказанного использования команды RUN на рис. 7 предлагается более эффективный способ, позволяющий не занимать пространство памяти лишними слоями.

```
FROM dedian:latest
WORKDIR /app
RUN git clone https://some.platypus.git && \
 cd platypus && \
 make && \
 mv ./binary /usr/bin/ && \
 cd .. && rm -rf platypus
```

Рис. 7. Эффективное использование команды RUN

При данном способе исходный код не попадает в сам образ, тем самым не сохраняется в памяти, так как он уже удаляется до завершения команды RUN.

Подводя итог, можно сказать о том, что представленные методы являются всего лишь частью от общего объёма существующих способов оптимизировать внедрение системы контейнеров Docker в туманные вычисления. Однако проанализированные методы помогают добиться значительных успехов в эффективном распределении и использовании программных ресурсов микрокомпьютеров. В дальнейшем децентрализованная система туманных вычислении продолжит охватывать все большие области покрытия

между ЦОДами и конечными устройствами, поэтому остро возникнут вопросы не только оптимизации микрокомпьютеров, но и их рационального расположения на местности.

Список используемых источников

1. Liu F. et al. A survey on edge computing systems and tools // Proceedings of the IEEE. 2019. T. 107. N 8. C. 1537–1562.

2. Ahmed A., Pierre G. Docker container deployment in fog computing infrastructures // 2018 IEEE International Conference on Edge Computing (EDGE). IEEE, 2018. C. 1–8.

3. Mao Y. et al. Resource management schemes for cloud-native platforms with computing containers of docker and kubernetes // arXiv preprint arXiv:2010.10350. 2020.

4. Docker optimization guide: 8 tricks to optimize your Docker image size // AugmentedMind. URL: https://www.augmentedmind.de/2022/02/06/optimize-docker-image-size/ (дата обращения 25.02.2023).

УКД 004.9
ГРНТИ 49.40.01

ОБЗОР МОДЕЛЕЙ ОЧКОВ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

А. И. Выборнова, А. А. Леонова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье приводится описание одних из популярных очков дополненной реальности разных производителей, а именно Epson, Rokid и Microsoft, и их анализ. Рассматриваются различные подходы разработки и создания AR очков. Выведены основные составляющие очков дополненной реальности необходимые для их создания актуальные на начало 2023 года.

AR-очки, дополненная реальность, очки дополненной реальности.

Технологии XXI века стремительно развиваются, охватывая всё больше сфер жизни. Одной из перспективных технологий сегодняшнего дня является технология дополненной реальности (AR), которая используется в медицине, решении бизнес-задач, образовании и различных других сферах.

Дополненная реальность – технология взаимодействия человека и компьютера, добавляющая цифровые объекты в физический мир. Системы AR основаны на трех принципах:

1. Объединение цифровой и физической реальности.

2. Взаимодействие в реальном времени цифровой и физической реальности.

3. Точное 3D-разграничение реальных и виртуальных объектов.

Для восприятия систем дополненной реальности необходимо специальное оборудование: очки или шлем. В данной статье рассмотрим подробнее какие существуют очки дополненной реальности, чем они схожи, и чем отличаются.

Обзор очков дополненной реальности

Epson Moverio – бинокулярные видеоочки, с дисплеями Si-OLED.

Данная модель очков Epson является четвертым поколением очков дополненной реальности и были выпущены в январе 2020 года.

Очки оснащены гибкими дужками и дополнительные носоупоры, что обеспечивает комфорт. Epson Moverio можно носить поверх очков для зрения [1].

Дисплей очков полностью прозрачен, через них видно всё происходящее вокруг, при этом можно использовать приложения дополненной реальности или воспроизводить 2D и 3D контент. Очки данной линейки оснащены технологией Si-OLED, которая обеспечивает цветопередачу высокого качества, четкое изображение с максимальным разрешением Full HD 1080p.

Данная модель очков дополненной реальности оснащена контроллером BO-IC400 работают под управлением ОС Android, платформа которой открывает широкие возможности для IT-разработчиков [1].

Ключевые характеристики умных очков Epson:

- Высокое разрешение – Full HD 1080p (1920×1080);
- Более широкий угол обзора (FOV) 34° – эквивалентно экрану диагональю 120 дюймов при просмотре с расстояния 5 м;
- Контрастность 100 000:1, благодаря чему достигается полная прозрачность;
- Удобство ношения с улучшенным распределением веса и опциональными носовыми упорами;
- Разъем USB-C для подключения к внешним устройствам;
- Бинокулярные прозрачные дисплеи Si-OLED.

Rokid Air – очки дополненной реальности, выпущенные в июле 2022 г., поддерживающие разрешение видео 4К, для звуковой поддержки которого предусмотрены 2 направленных HD динамика. Предоставляют для пользования 120-дюймовый виртуальный экран. Данная модель очков оснащена интеллектуальным голосовым управлением, а также управлениям жестами через интерфейс смартфона [2].

Rokid Air являются универсальными очками дополненной реальности, они совместимы со множеством устройств, например, смартфоны, игровые

консоли, планшеты и т. д., благодаря чему AR-очки удобны для повседневного использования.

Основные характеристики:

- 120-дюймовый экран высокой четкости с разрешением 4К;
- Оптический дисплей BirdBath с яркостью 1800 нит, контрастностью 100000:1 и углом обзора 43°;
- датчиками приближения и усовершенствованным 9-осевым (IMU, магнитометр);
- Распознавание голоса при помощи искусственного интеллекта;
- Регуляция фокуса для людей с плохим зрением;
- Сенсорная панель управления – подключенное устройство пользователя;
- HD динамики, создающие объемный звук;
- Легкие материалы, благодаря чему устройство весит 85 грамм.

Microsoft Hololens 2 – очки дополненной реальности, являются усовершенствованной моделью очков Microsoft Hololens 1 поколения, выпущены в ноябре 2019 года.

В Hololens 2 установлены три чипа: CPU, GPU и HPU (голографический процессор, отвечающий за правильный вывод голографических объектов). Внедрение данных чипов в очки делает их больше голографическим компьютером чем очками, по сути своей работы. Microsoft Hololens 2 оснащен 4 датчиками для отслеживания позиции головы, 2 камерами с инфракрасной подсветкой для фиксации направления взгляда, сенсором глубины для манипуляций над голограммами (1 МП), а также акселерометром, магнитометром и гироскопом [3].

Управление изображением в данной модели очков осуществляется при помощи рук, голограмму можно захватить пальцами, покрутить, изменить размер и многое другое. Управлять самой системой (приложениями, фотосьемкой и т. д.) можно при помощи голосовых команд, а также при помощи голосового помощника.

Разработчики утверждают, что такая модель очков виртуальной реальности предназначена не для обычного пользователя, а призвана помогать хирургам, сотрудникам фабрик и автосервисов, для тех, кому сложно интегрировать свой рабочий процесс в компьютер или смартфон.

Характеристики:

- Разрешение 2560×1440px;
- Угол обзора 65°;
- Дисплей – прозрачные голографические линзы
- Отслеживание головы 4-мя камерами видимого света;
- Отслеживание глаз 2-мя инфракрасными камерами;
- Управление голосом и жестами;

- Инерциальный модуль – акселерометр, гироскоп, магнитометр.

Заключение

Для наглядного сравнения, рассмотренных моделей очков дополненной реальности, основные характеристики AR-очков были вынесены в таблицу 1.

ТАБЛИЦА 1. Сравнение разных моделей AR-очков

Модель AR-очков / Параметры	Epson Moverio	Rokid Air	Microsoft Hololens 2
Дисплей	Si-OLED	BirdBath	Голографические линзы
Контрастность	100 000:1	100 000:1	
Угол обзора	34°	43°	65°
Разрешение	Full HD 1080 p	4K	2560×1440 px
Камеры	-	-	4 камеры видимого света; 2 инфракрасные камеры
Вес, г	119	85	566

Исходя из всего вышесказанного можно выделить несколько составляющих, с помощью которых можно создать идеальные очки дополненной реальности:

- Типоразмер обычных очков (как у очков для коррекции зрения);
- Тонкие дужки очков, не мешающие периферическому зрению;
- Поле зрения на уровне человеческого глаза (200° по горизонтали, 130° по вертикали);
- Мультипросмотровость (изображение видно при любом положении глаза);
- Мультицветность (вся палитра RGB);
- Разрешение, при котором наблюдатель не может различить отдельные пиксели;
- Отсутствие отслеживания глаз для переключения между различными видами (для разных направлений видения глаз);
- Отсутствие радужной окраски (появляется при использовании дифракционных и голографических оптических элементов).

Подводя итоги анализа очков дополненной реальности, становится очевидно, что все производители AR гарнитур стремятся к высокому качеству изображения, которое не будет уступать экранам смартфонов, но по размеру

они должны быть не больше, чем обычные очки для зрения, чтобы легко и практически незаметно интегрироваться в обычную жизнь человека. Еще одним важным аспектом является принцип управления данным девайсом, ведь многие производители уже выпускают и проектируют новые очки дополненной реальности для профессиональной деятельности человека, следовательно, необходимо, чтобы пользователь мог быстро и просто управлять AR очками голосом или простыми движениями рук.

Список используемых источников

1. Epson : сайт. URL: https://epson.ru/catalog/moverio/ (дата обращения 21.03.2023).
2. Rokid : сайт. URL: https://rokid.vizzion.ru/rokid-air (дата обращения 21.03.2023).
3. Microsoft : сайт. URL: https://www.microsoft.com/ru-ru/hololens/hardware (дата обращения 21.03.2023).

УДК 004.9
ГРНТИ 49.01

ВОСПРОИЗВЕДЕНИЕ ИЗОБРАЖЕНИЙ В ОЧКАХ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ: ТЕХНОЛОГИИ И УСТРОЙСТВА

А. И. Выборнова, Я. О. Нестерова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены основные области применения технологии дополненной реальности. Представлены типы технологии и дана их характеристика. Приведен обзор устройств, поддерживающих данную технологию и представленных на рынке на момент написания статьи. Обоснована актуальность проведения разработок в сфере дополненной реальности.

дополненная реальность, виртуальная реальность, AR очки, AR-контент, воспроизведение изображений.

Введение

В настоящее время наблюдается ежегодное увеличение числа пользователей технологиями AR (дополненная реальность) и VR (виртуальная реальность). По оценкам экспертов рынок AR и VR к 2025 году в среднем вырастет на 46 % по сравнению с 2020 годом.

Дополненная реальность – это технология, которая с помощью специализированных устройств позволяет накладывать виртуальные объекты

на объекты и среды реального мира, а также взаимодействовать реальным объектам с виртуальными [2]. В отличие от виртуальной реальности, которая воссоздает и заменяет всю реальную среду виртуальной, дополненная реальность только обогащает образ реального мира компьютерными изображениями и цифровой информацией.

Внутри устройства, создающего AR-контент, виртуальные 3D-изображения накладываются на объекты реального мира на основе их геометрических взаимосвязей [1]. Данное устройство вычисляет положение и ориентацию одних объектов в пространстве относительно других [4]. В результате комбинированное изображение проецируется на мобильные экраны, очки дополненной реальности, а также другие устройства, поддерживающие технологию дополненной реальности.

Технология дополненной реальности. Применение и типы

Существует четыре типа дополненной реальности:

1. AR на основе маркеров – это интерактивная система с использованием специальных маркеров. Как только пользователь подносит маркер к камере, то на экране устройства появляется виртуальный объект с эффектами, заданными определенным сценарием. Теоретически маркером может быть любой объект, но обычно выбирается черно-белый маркер простой формы, например, прямоугольник или квадрат. Такой выбор обоснован необходимостью быстро, в режиме реального времени, считывать маркеры вне зависимости от уровня освещенности, особенностей цветопередачи и вычислительной мощности используемого оборудования [3].

2. AR без использования маркеров. Принцип работы данной технологии основан на особом алгоритме распознавания, где на окружающею среду, снятую камерой, накладывается, так называемая, виртуальная «сетка». На этой сетке с помощью программных алгоритмов определяются некие опорные точки, по которым в дальнейшем находится точное место, к которому будет привязана виртуальная модель. Одно из главных преимуществ данной технологии заключается в том, что объекты, находящиеся в реальном мире, играют роль маркеров сами по себе и для них нет необходимости создавать специальные визуальные идентификаторы [3].

3. AR на основе проекции. Данная технология работает на основе проецирования искусственного света на физические поверхности для создания реалистичных объектов. То есть проекционные системы дополненной реальности проецируют виртуальные образы на физические модели, тем самым позволяя пользователям взаимодействовать с создаваемыми объектами [3].

4. AR на основе наложения. Отличительной особенностью данной технологии является частичная или полная замена исходного вида какого-либо

физического объекта. Ключевую роль в работе приложения играет распознавание объектов, так как невозможно заменить реальное изображение добавленным, если приложение не сможет определить объект и его расположение [3].

Обзор моделей очков дополненной реальности

Во многих современных устройствах уже поддерживается технология дополненной реальности. Это могут быть мобильные устройства, AR очки, AR контактные линзы, а также виртуальные дисплеи сетчатки глаза (VRD). Отдельное внимание хотелось бы уделить очкам виртуальной реальности и рассмотреть наиболее популярные их модели.

Google Glass. В 2013 году Google впервые представил концепт проекта Glass первого поколения. Внешне очки дополненной реальности мало чем отличались от очков для коррекции зрения. Существенным отличием являлись пятимегапиксельная камера, располагающаяся справа над глазом, и небольшой проектор. Также справа на дужке была размещена тач-панель для управления с помощью касаний. Основными техническими характеристиками очков Google Glass первого поколения являлись: 1 Гб оперативной памяти, встроенный накопитель на 16 Гб, аккумулятор емкостью 780 мАч, модуль Bluetooth 3 и Wi-Fi 802.11 b/g, а также акселерометр, гироскоп и магнитометр [7]. К недостаткам модели можно отнести высокую стоимость (порядка 1500$), отсутствие поддержки операционной системы Apple iOS, а также плохую автономность устройства. Кроме того, существенным минусом являлось голосовое управление, поддерживающее исключительно английский язык.

В 2017 году в продажу поступила вторая версия очков Google Glass Enterprise Edition. В процессе разработки данной модели были учтены все негативные отзывы владельцев очков первого поколения. В результате Glass Enterprise Edition стали легче своих предшественников и могли обходиться без подзарядки вдвое дольше за счет увеличения емкости аккумулятора. Также Google обновил аппаратное обеспечение очков, и технические характеристики стали следующими: 32 Гб постоянной памяти, процессор Intel Atom, ресиверы GPS и ГЛОНАСС, барометр и модуль Wi-Fi 802.11ac, работающий на частотах 2.4 и 5 ГГц [7].

На данный момент Google ведет работу над новым проектом, который имеет кодовое название Project Iris и скорее всего относится к классу устройств смешанной реальности, сочетающей в себе возможности виртуальной и дополненной реальности.

Microsoft HoloLens. В 2015 году корпорация Microsoft анонсировала очки дополненной реальности Microsoft HoloLens. Данная модель представляет собой головную гарнитуру. Устройство автономно, а время работы без

подзарядки варьируется от двух с половиной до пяти с половиной часов в зависимости от уровня нагрузки на процессор. К основным техническим характеристикам можно отнести: процессор Intel Atom X5-Z8100, 2 Гб оперативной памяти, встроенный накопитель объемом 64 Гб, видеопроцессор с 1024 Мб видеопамяти, а также голографический процессор (HPU) [6]. Над линзами очков располагаются четыре камеры, которые помогают отобразить картинку дополненной реальности, для каждого глаза выделено по две камеры – инфракрасная и обычная. В устройство встроены датчики, среди которых привычные для очков дополненной реальности гироскоп и акселерометр, а также датчик магнитных полей, который отвечает за корректное отображение голограмм. В дужки очков вмонтированы динамики, позволяющие слышать реалистичный звук и взаимодействовать с голосовым помощником, также через дужки выводится горячий воздух от работы системы.

В данный момент разработаны очки Microsoft HoloLens 2 поколения. Технически модель практически не отличается от своего предшественника, но немного видоизменен внешний вид, а также усовершенствованы некоторые функции. Важно отметить, что Microsoft HoloLens 2 может полностью отслеживать движение рук, это значительно упрощает управление объектами дополненной реальности.

Epson Moverio. В 2020 году компания Epson анонсировала выпуск нового поколения очков дополненной реальности Moverio, речь идет о моделях BT-40 и BT-40S. Рассмотрим их основные технические характеристики.

Модель Moverio BT-40 может подключаться к смартфонам, планшетам или ПК благодаря встроенному разъему USB Type-C, что позволяет использовать устройство в учебных целях, меняя его прошивку, а также в качестве дополнительного монитора [5]. Высокое разрешение воспроизводимого контента позволяет пользователю полностью окунуться в мир дополненной реальности.

Модель Moverio BT-40S оснащена специализированным пультом управления с интегрированной ОС Android, что позволяет пользователю устанавливать любые совместимые приложения. Также в данной модели присутствует тачскрин, возможность расширения памяти до 2 Тб, пыле и влагозащита IPX2, встроенные модули Wi-Fi и Bluetooth, GPS, компас, акселерометр, гироскоп, камера, фонарик, микрофон, аудио разъем Jack и высокопроизводительный аккумулятор, заряда которого хватает до 5 часов работы в режиме просмотра видео [5].

Данные модели активно применяются для разработки новых, а также улучшения старых приложений, использующих технологию дополненной реальности.

Помимо вышеперечисленных моделей очков дополненной реальности, на момент написания статьи в разработке находятся очки от компании Apple, технологии, используемые в которых, не раскрываются.

Заключение

Таким образом, видно, что многие корпорации осознают перспективность направления и стремятся занять нишу на рынке. Кроме того, с каждым годом растет количество областей применения технологии дополненной реальности, появляются новые устройства, инновационный функционал которых расширяет человеческие возможности.

Список используемых источников

1. Рочев А. А., Маколкина М. А. Развитие приложений и услуг дополненной реальности // Информационные технологии и телекоммуникации. 2018. Т. 6, N 3. С. 98–105.

2. Rauschnabel P. A. Virtually enhancing the real world with holograms: An exploration of expected gratifications of using augmented reality smart glasses. Psychology and Marketing. 2018. N 35. PP. 557–572.

3. Что такое дополненная реальность, или AR? // Microsoft. Dynamics 365: сайт. URL: https://dynamics.microsoft.com/ru-ru/mixed-reality/guides/what-is-augmented-reality-ar/ (дата обращения 12.03.2023).

4. Augmented reality (AR) // Techtarget: сайт. URL: https://www.techtarget.com/whatis/definition/augmented-reality-AR (дата обращения 12.03.2023).

5. Epson: сайт. URL: https://epson.ru/catalog/moverio/epson-moverio-bt-200/ (дата обращения 12.03.2023).

6. Microsoft: сайт. URL: https://www.microsoft.com/ru-ru/hololens (дата обращения 12.03.2023).

7. Google: сайт. URL: https://www.google.com/glass/start/ (дата обращения 12.03.2023).

УДК 004 519
ГРНТИ 20.01; 81.93.29

КОМПЛЕКСНАЯ МЕТОДИКА И АЛГОРИТМЫ СИНТЕЗА И ОЦЕНКИ РАЦИОНАЛЬНОСТИ ВАРИАНТОВ ПОСТРОЕНИЯ АРХИТЕКТУР ВЕДОМСТВЕННЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ КЛАССА «КИБЕРПОЛИГОН»

Б. В. Гавкалюк, М. Ю. Синещук, А. В. Шестаков

Санкт-Петербургский университет ГПС МЧС России

Статья посвящена вопросам методического и алгоритмического обеспечения процесса формирования ведомственных организационно-технических систем класса «киберполигонов». Рассматриваются процедуры синтеза организационно-технической системы с учетом распределения функций по компонентам ведомственного киберполигона в зависимости от принятого варианта построения архитектуры и стратегии ее поэтапного развития (совершенствования, модернизации). Исследуются процедуры оценки рациональности вариантов построения архитектур ведомственного киберполигона с учетом различного вклада критериев качества решений по построению таких систем из состава многовекторных групп критериев качества. Предлагается комплексная методика, которая может использоваться для широкого класса практических задач в прикладных научных исследованиях организационно-технических систем, их функциональных подсистем, проектировании и обосновании развития.

киберполигон, синтез, комплексная методика, алгоритмы.

Прикладные исследования организационно-технических систем класса «киберполигонов» проводятся по различным направлениям и отраслям экономики (энергетика, кредитно-финансовый сегмент), включая корпоративную инфраструктуру. Однако, несмотря на возрастающий практический интерес со стороны министерств и ведомств к их созданию и развитию на собственных информационных, телекоммуникационных и эксплуатационных ресурсах, должного освещения вопросы формирования системотехнических решений по построению ведомственных киберполигонов не получили. Наличие существенных ведомственных особенностей, как, впрочем, и специфика отраслей экономики, обусловливают объективную необходимость уточнения подходов к применению типовых организационно-технических решений для построения ведомственных киберполигонов [1]. Отсутствие регламентированного глоссария и концептуального единства

системотехнического облика немногочисленных многоцелевых киберполигонов обусловливает сосуществование различных терминологических сущностей, технических концепций киберполигонов, а также наполняет новым содержанием исследования проблематики построения архитектур ведомственных киберполигонов.

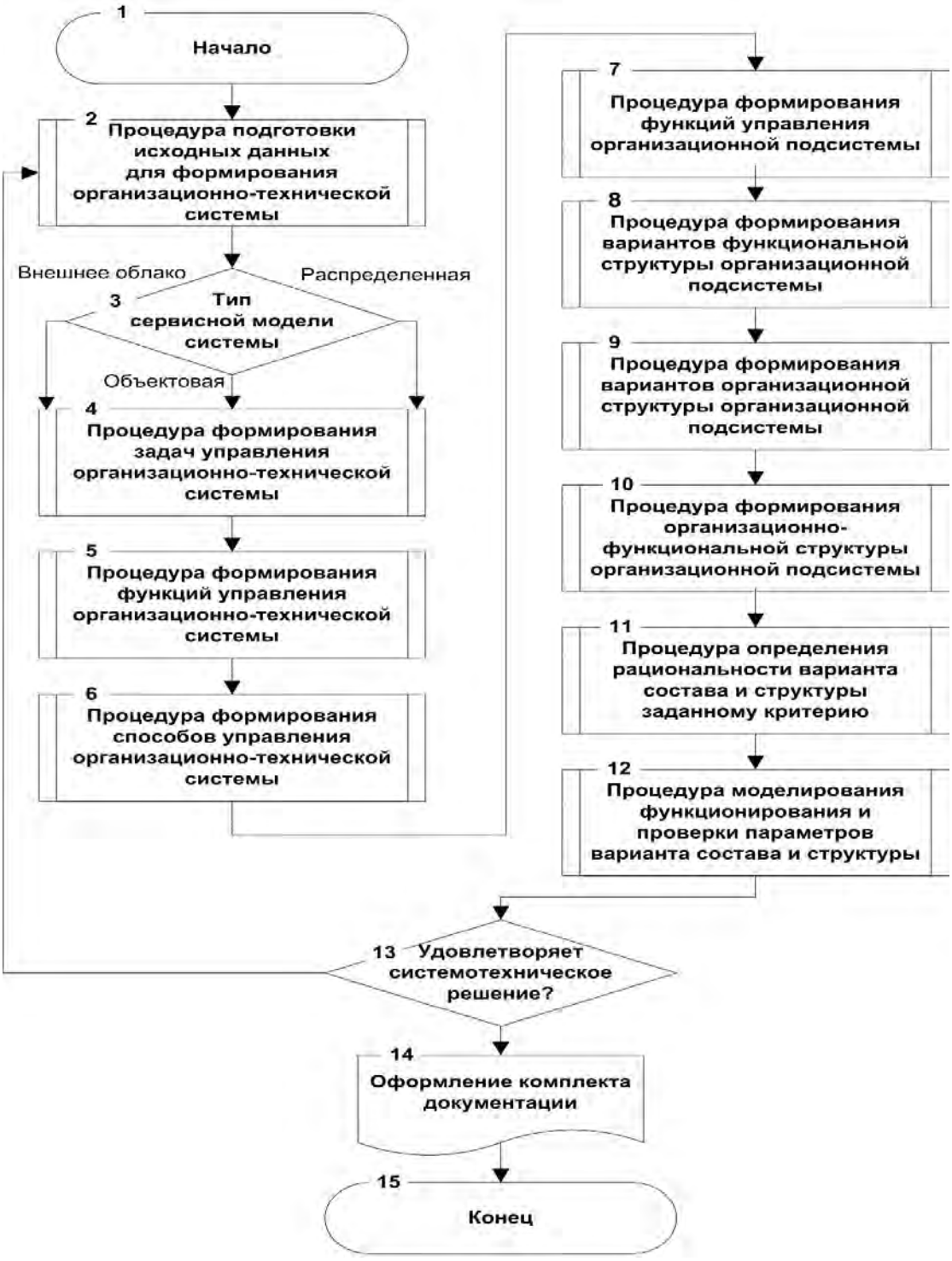


Рис. 1. Блок-схема комплексной методики синтеза и оценки рациональности варианта построения архитектуры ведомственного киберполигона

Ведомственный киберполигон представляет собой единую централизованную организационно-техническую систему в составе территориально-распределенных сегментов сил и средств, с сегментом управления на базе образовательного учреждения, уполномоченного по вопросам создания, развития и функционирования киберполигона, для организации и проведения кибертренировок и киберучений в рамках обучения, оперативной подготовки и переподготовки должностных лиц и сотрудников ведомства, территориальных органов и подведомственных организаций в области информационной и кибербезопасности, проведения исследований и информационной поддержки органов (центров) системы управления информационной безопасностью ведомства.

Комплексную методику синтеза и оценки рациональности вариантов построения архитектуры ведомственного киберполигона можно представить в виде блок-схемы процедур (рис. 1, см.выше).

Формирование архитектуры киберполигона, как организационно-технической системы, подразумевает использование процедур структурно-параметрического синтеза системотехнических решений по построению технической подсистемы (например, ориентированных на архитектуру автоматизированные системы в защищенном исполнении, как описано в пособии СПбГЭУ [2], или специального назначения, по материалам Военной академии связи [3]), а затем – и соответствующей организационной подсистемы (как показано в [4]). Технико-экономическая оценка должна осуществляться в процедуре выбора рационального варианта построения архитектуры с учетом этапности ее формирования.

Блок 2 предназначен для задания совокупности ограничений на параметры задач, функций, способы управления и актуализацию сведений баз данных, содержащих техническую и финансово-экономическую информацию применительно к трекам киберполигона. Трек киберполигона – совокупность организационных, функциональных, информационных и технических ресурсов субъектов в конкретной задаче: трек киберучений (кибертренировок), образовательный трек, трек исследования и тестирования по тематике кибербезопасности (табл. 1, см. ниже.).

Блок 3 – уточнение постановки задачи формирования архитектуры киберполигона в зависимости от принятого организационного решения по реализации его сервисной модели. Характеристики модели, используемые в комплексной методике, представлены в таблице 2 (см. ниже).

Блоки 4–10 представляют собой процедуры формирования различных сущностей архитектуры киберполигона. Основу процедур составляет реализация набора типовых алгоритмов, как описано, например, в [5]:

проверки соответствия очередного набора сущностей технической и организационной подсистем киберполигона заданным ограничениям;

отбраковки набора сущностей, не удовлетворяющих заданным ограничениям;

актуализации базы наборов сущностей, удовлетворяющих заданным ограничениям.

ТАБЛИЦА 1. Характеристики сервисной модели организационно-технической системы

Трек киберполигона	Задачи
Киберучений	Организация кибертренировок, киберучений и киберсоревнований по защите ИТ-инфраструктуры виртуальных территориальных органов и подведомственных организаций на основе групповых и индивидуальных оперативных задач ведомства и его подразделений, территориальных органов и организаций, в т. ч. центров кибербезопасности.
Образовательный	Обеспечение профориентированного обучения (самоподготовки, переподготовки, повышения квалификации) в подведомственных образовательных учреждениях в соответствии с ФГОС по направлению «Информационная безопасность», оперативная подготовка уполномоченных должностных лиц в области информационной безопасности ведомства и его подразделений, территориальных органов и организаций на основе компьютерного моделирования актуальных сценариев компьютерных атак, шаблонов фрагментов действующих инфраструктур, оценочных и методических средств, интегрированных с электронной информационной образовательной системой образовательных учреждений.
Исследования	Апробация и тестирование средств защиты информации (СЗИ) и технологий на основе эмулированных прообразов действующих информационных инфраструктур, реальных взаимодействующих информационных систем и инфраструктур, существующих и перспективных СЗИ, планируемых к оснащению объектов информатизации.

ТАБЛИЦА 2. Характеристики сервисной модели организационно-технической системы

Тип сервисной модели	Локация сервисов	Доступ	Управление сервисами	Организационная система
Внешнее облако	ЦОД Оператора	На контрактной основе	Нет	Оператор Киберполигона
Объектовая	ЦОД вуза	Без ограничений	Да	Локальная
Распределенная	По узлам сервисов трека	По расписанию	Да	Иерархическая

Особенностью процедур формирования функций и задач управления (блоки 4, 5 и 7) является выполнение алгоритма декомпозиции функций (задач) по трекам и компонентам инфологических моделей киберполигона на основе регламентированной модели центров обработки

данных (например, по ГОСТ Р 58812), либо поставщика телекоммуслуг (например, по ГОСТ Р 53633) с учетом реализации алгоритмов конфликтно-активного управления, предложенных Воронежским институтом ФСИН России [6].

Блоки 8–10 нужны для реализации распределенной сервисной модели киберполигона, и в отличие от традиционных алгоритмов формирования организационно-функциональных структур, основанных на «статических» первичных исходных данных [5], используют алгоритмы семплирования (упорядоченного сжатия и просеивания элементов структуры) модели графа технической подсистемы полномасштабного киберполигона до его первоочередного фрагмента. Методологической основой определения структурных параметров первоочередного фрагмента ведомственного киберполигона являются алгоритмы, изложенные в [4].

Блок 11 основан на оценке E_v показателя технико-экономической эффективности варианта построения архитектуры ведомственного киберполигона при одинаковых условиях его применения:

$$E_v = \underline{P_v} / C_v, \quad (1)$$

$$C_v = \sum_{i=1}^{r_v} C_i^{\text{разв}} + \sum_{i=1}^{r_v} C_i^{\text{обс}} + \sum_{i=1}^{r_v} C_i^{\text{об}} \ , \quad (2)$$

где P_v – интегральный показатель эффективности v-го варианта инфраструктуры киберполигона; C_v – величина финансовых ресурсов, затраченных на его создание $C_i^{\text{разв}}$, функционирование $C_i^{\text{обс}}$ и на обучение $C_i^{\text{об}}$ должностных лиц и персонала службы эксплуатации.

С учетом различной значимости функциональных задач треков используются алгоритмы формирования матрицы весовых коэффициентов «важности» каждой из функций киберполигона. Детализация процедуры представлена в авторской статье, подготовленной к публикации.

Блок 12 реализует не только алгоритмы локальной верификации и валидации отобранных вариантов организационной архитектуры и системотехнических решений, а также натурные проверки на действующих фрагментах, по результатам которых принимается решение либо об окончании выполнения процедур, либо корректировки исходных данных, в т. ч. ограничений.

Дальнейшее исследование направлено на разработку моделей и методов управления организационными проектами киберполигона.

Статья подготовлена в рамках выполнения в 2023 году прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР № 123030100017-2 и № 123030100009-7 от 01.03.2023.

Список используемых источников

1. Гавкалюк Б. В., Синещук М. Ю., Шестаков А. В. Инфологическая модель и критерии качества решений по построению ведомственных организационно-технических систем класса «киберполигон» // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2023. N 1 (65). С. 25–30.
2. Солодянников А. В. Информационная безопасность автоматизированных систем. СПб.: Изд-во СПбГЭУ, 2020. 108 с.
3. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства: Науч. монография / Под общ. ред. В. А. Липатникова. СПб.: ВАС, 2020. 716 с.
4. Введение в методологию обработки геопространственных данных генотипа телекоммуникаций : монография / А. В. Шестаков. Санкт-Петербург: ГУАП, 2016. 324 с.
5. Селифанов В. А., Селифанов В. В. Способ автоматизированного управления процессом структуры системы управления техническими системами и устройство для его осуществления. Пат. 2331097 Российская Федерация; заявитель и правообладатель Селифанов В.А. – № 2007103988/09, заявл. 01.02.2007, опубл. 10.08.2008.
6. Новосельцев В. И., Кочедыков С. С., Орлова Д. Е., Плющик К. А. Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / под ред. В. И. Новосельцева. М. : ИНФРА-М, 2023. 225 с.

УДК 004.71
ГРНТИ 49.33.29

АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ СЕТИ INFINIBAND

В. К. Гераськин, Е. Е. Ермолаев, Д. С. Кукунин, И. О. Федотов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием нейросетей, аналитики и big data появилась необходимость в высокопроизводительной сети с низкой задержкой для передачи большого массива данных. Одним из решений стала сеть InfiniBand, разработанная компанией InfiniBand Trade Association, которая основана на использовании специальных адаптеров и коммутаторов. InfiniBand – коммутационная компьютерная сеть, которая обеспечивает высокоскоростную связь между взаимосвязанными узлами. В данной работе выполнен анализ производительности сети и адаптеров mellanox на основе работы с различными типами трафика в рамках использования реального оборудования.

Infiniband, точка-точка, высокоскоростная сеть, компьютерная сеть, RDMA.

InfiniBand – высокоскоростная коммутационная компьютерная сеть, в состав которой входят серверы и рабочие станции, а также устройства хра-

нения и различные периферийные устройства. Каждый узел оборудован сетевым адаптером. Сферы применения InfiniBand: интеллектуальный анализ данных, deep learning и прогнозная аналитика [1].

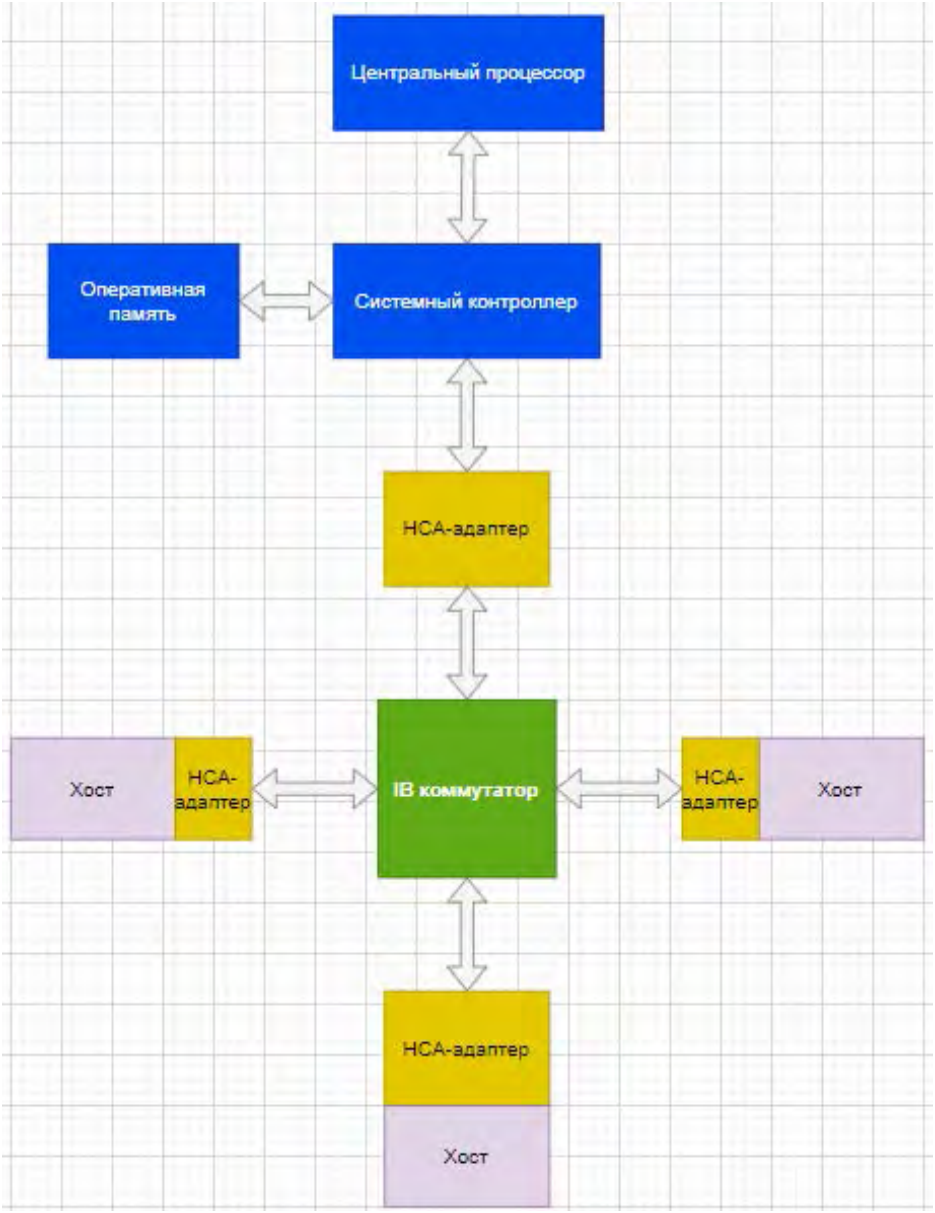


Рис. 1. Архитектура

По мере увеличения объема обрабатываемых данных, существующая шинная архитектура становится «бутылочным горлышком». Большинство таких систем посылают данные параллельно по задней шине. InfiniBand, напротив, использует последовательные каналы и шины с побитовой передачей данных. Это обеспечивает более эффективный обмен информацией между узлами.

Архитектура InfiniBand хорошо подходит для приложений, чувствительных к производительности [2] (рис. 1, см. выше). Ее низкие накладные

расходы снижают зависимость от ресурсов центрального процессора, высвобождая их для других операций. Она определяет несколько устройств, необходимых для коммуникации: канальный адаптер (HCA), коммутатор, маршрутизатор и менеджер подсети. В подсети должен быть хотя бы один канальный адаптер для каждого конечного узла и диспетчер подсети для настройки и обслуживания каналов. Все канальные адаптеры и коммутаторы должны иметь агент управления подсетью (*Subnet Management Agent,* SMA), необходимый для взаимодействия с диспетчером подсети [3].

Конечные узлы, такие как хосты и устройства, отправляют сообщения по каналам другим конечным узлам; сообщения маршрутизируются коммутаторами. Канальный адаптер (HCA) [3] обеспечивает интерфейс, с помощью которого хост-устройство может взаимодействовать с сетью (рис. 2)

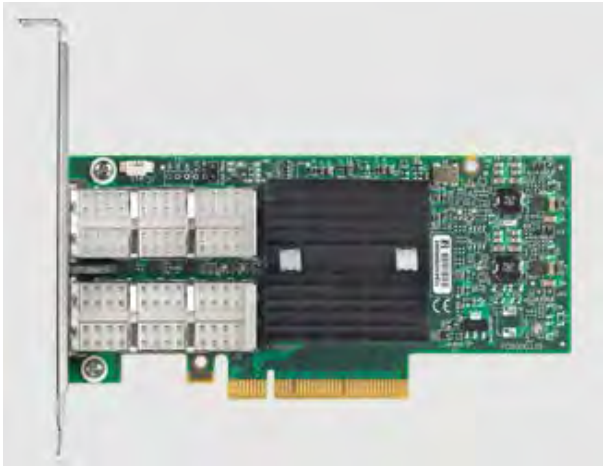


Рис. 2. 2-портовый адаптер HCA

Проведем сравнение InfiniBand с классической сетью Ethernet. В рамках тестирования использовались серверы с процессорами Intel Xeon 2.10Ghz, 16 vcpu. Операционная система: ubuntu 20.04. Тестировались встроенные Ethernet порты материнской платы 10 Гбит/с и Mellanox адаптер MT27600, скорость которого была искусственно зафиксирована на то же уровне 10 Гбит/с. Тестирование проводилось с использованием утилит iperf3 и qperf в которых устанавливались различные значения размера отправляемого пакета, а также количество параллельных потоков данных. Для тестирования джиттера и задержки использовался UDP трафик, в остальных случаях использовался TCP.

В основе сети Infiniband лежит технология RDMA (англ. *Remote Direct Memory Access* – удалённый прямой доступ к памяти), при котором передача данных из памяти удалённого компьютера в локальную память инициатора запроса производится непосредственно сетевым контроллером, при этом исключается участие CPU удалённого узла. [4] RDMA позволяет передавать данные без дополнительной буферизации и не требует активной работы ОС, библиотек или приложения на узле, к памяти которого производится обращение. Благодаря использованию RDMA, сеть позволяет освободить процессор от участия в обработке информации из ввода-вывода.

Если при однопотоковой передаче это мало заметно, то с увеличением количества параллельных потоков, загрузка процессора в случае с Ethernet

возрастает, особенно на стороне получателя. В то же время, как при использовании адаптера Mellanox нагрузка на процессор остается примерно на том же уровне (рис. 3).

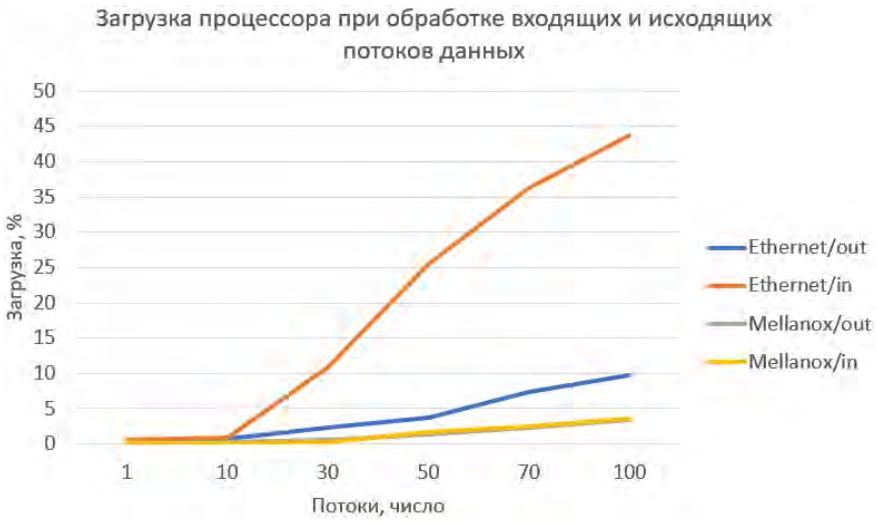


Рис. 3. График зависимости загрузки процессора от количества потоков данных

Вторым важным фактором оценки являются джиттер, который можно считать причиной задержки. В результате тестов с помощью утилит mtr и qperf были получены следующие результаты (рис. 4). Средний джиттер при использовании Ethernet составлял 13 мкс, когда как при использовании Mellanox всего 4 мкс. Задержка при увеличении размера передаваемого пакета в Ethernet значительно больше и возрастает быстрее.

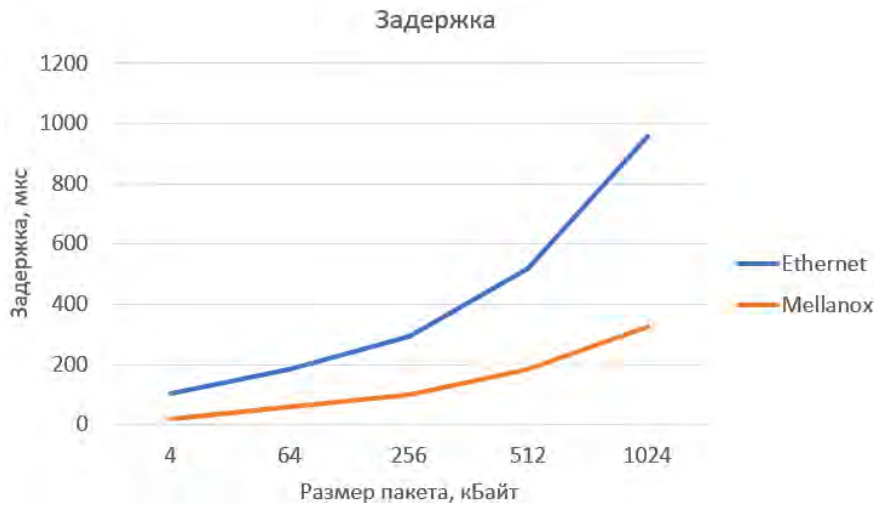


Рис. 4. График зависимости задержки от размера передаваемого пакета

Заключительный тест показывает пропускную способность двух сетей в зависимости от используемого размера передаваемого сообщения (пакета). Видно, что пропускная способность возрастает быстрее в случае с использованием карты Mellanox (рис. 5).

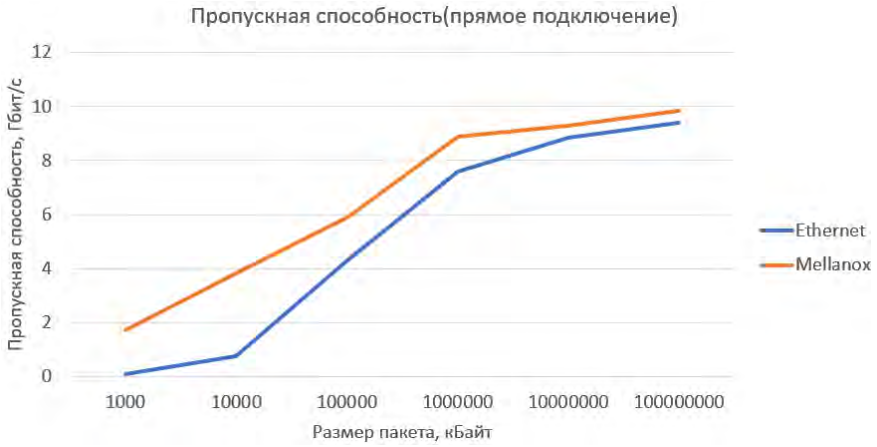


Рис. 5. График зависимости пропускной способности от размера передаваемого пакета

Из проведенных тестов видно, что сеть InfiniBand значительно превосходит классический Ethernet. Адаптеры Mellanox, обеспечивающие ее работу, позволяют работать с множественными потоками ввода-вывода, не нагружая процессор лишней работой. Работа с множественными потоками позволяет применять сеть InfiniBand в качестве сети в условиях, когда имеет место большое число параллельных потоков данных, будь то несколько работающих параллельно приложений или обычный переброс данных между хранилищем и клиентской машиной. В то же время сеть обеспечивает низкую задержку и высокую пропускную способность, превосходя таковые параметры у обычной сети ethernet на основе встроенных портов материнской платы, что делает ее хорошим выбором для чувствительных к задержкам приложений.

Список используемых источников

1. Paul Grun. Introduction to InfiniBand for End Users : InfiniBand Trade Association, 2010. 19 p.

2. Gregory F. Pfister. Aspects of the InfiniBand Architecture : CLUSTER, 2001. 5 p.

3. Гераськин В. К. Архитектура сети InfiniBand // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022). Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей : материалы конф. СПб. : СПбГУТ, 2023. 638 с.

4. An Integrated Tutorial on InfiniBand, Verbs, and MPI // IEEE Patrick MacArthur, Qian Liu, Robert D. Russell, Fabrice Mizero, Malathi Veeraraghavan, John M. Dennis. 2017. 14 p.

УДК 004.056
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ЗАЩИТЫ БЕСПРОВОДНОГО ТРАФИКА СЕТИ НА БАЗЕ WPA3

Е. Ю. Герлинг, Е. А. Зебзеев, А. Ю. Киструга

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Беспроводные сети являются неотъемлемой частью современных технологий. В частности, Wi-Fi – технология беспроводного подключения устройств к сети по стандартам семейства IEEE 802.11. Wi-Fi сети представляют собой наиболее распространенные компьютерные сети и используются по всему миру, как в частных домах, где предполагается подключение одного или нескольких устройств, так и в больших корпоративных сетях офисов крупных компаний, где количество подключенных устройств может измеряться сотнями. Одной из основных задач, стоящих перед данной технологией, является безопасная передача данных. Представленный в 2018 году стандарт WPA3 является последним на данный момент решением по обеспечению безопасности Wi-Fi сетей. В данной статье рассматриваются механизмы, применяемые в WPA3. Описан процесс аутентификации Simultaneous Authentication of Equals, называемый также SAE.

WPA3, SAE, OWE, информационная безопасность, администрирование сети.

Технологии беспроводной передачи данных, в частности Wi-Fi, используются повсеместно в современном мире. Wi-Fi сети используются как в малых частных сетях, где предполагается подключение одного или нескольких устройств, так и в больших корпоративных сетях офисов крупных компаний, где количество подключенных устройств может измеряться сотнями.

В составленном аналитиками IDC отчете за 2022 год говорится о том, что рынок WLAN вырос на 31 % по сравнению с предыдущим годом. Значительный рост объясняется увеличением спроса на продукцию, поддерживающую Wi-Fi 6. Так, например, лидером в сегменте точек доступа являются занимающие 82 % от всего дохода решения, поддерживающие Wi-Fi 6 [1].

Безопасности передачи данных всегда уделяется отдельное внимание, особенно в беспроводных сетях. Это связано с тем, что среда передачи является открытой, а передаваться могут, как персональные данные отдельного пользователя, так и конфиденциальная информация компании [2].

Актуальным стандартом безопасности Wi-Fi сетей является Wi-Fi Protected Access 3. В сертифицированных устройствах Wi-Fi 5 данный стан-

дарт не является обязательным, но для Wi-Fi 6 он является нативным. Следовательно, к безопасности современных WLAN стоит подходить с приоритетом использования данного стандарта [3].

По сравнению с предыдущим стандартом WPA3 имеет следующие основные особенности:

– Opportunistic Wireless Encryption (OWE);
– Simultaneous Authentication of Equals (SAE);
– 192-бит шифрование (опционально);
– Easy Connect (Device Provisioning Protocol, замена WPS).

OWE – это технология, призванная главным образом заменить уязвимый режим предварительного доступа с общим ключом (PSK) [4].

PSK используется в процессе четырехстороннего рукопожатия, в котором устройства вырабатывают ключи шифрования трафика. Основная проблема заключается в том, что, зная PSK и перехватив четырехстороннее рукопожатие, злоумышленник может самостоятельно вычислить ключи шифрования.

При OWE клиент и точка доступа (ТД) используют протокол обмена ключами Диффи-Хеллмана и получают общий секрет вместо PSK [5]. Пример процесса генерации общего секрета представлен на рис. 1.

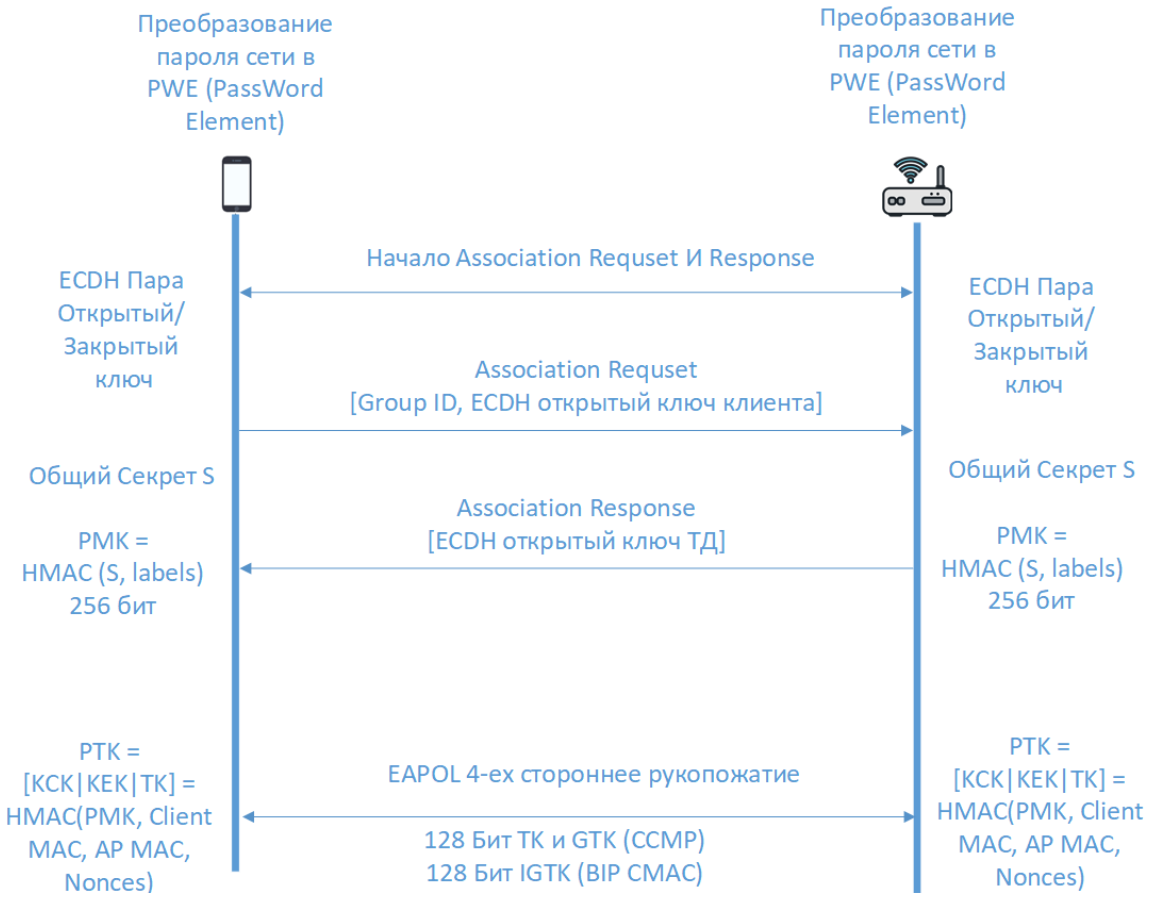


Рис. 1. Обмен сообщениям OWE

Основная идея – это передача открытых ключей Диффи-Хеллмана в сообщениях Assoc Req и Assoc Reg, после чего происходит выработка общего секрета, который используется при вычислении ключей шифрования.

Использование OWE обеспечивает защиту от атаки типа “MITM”, а также позволяет защитить фреймы управления, но из-за того, что протокол не предусматривает аутентификацию ТД, имеется уязвимость перед атаками типа “Honeypot” и “Evil Twin AP” [6].

Главной особенностью WPA3 является способность противостоять атакам по офлайн словарю на пароль сети Wi-Fi. В WPA2 использовалась аутентификация с предустановленным ключом PSK (*Pre shared key*), при которой для клиента и точки доступа формировался общий PMK (*Pairwise Master Key*). Парный мастер ключ генерировался по представленной ниже формуле:

$$PMK = PBKDF2\ (PassPhrase,\ SSID,\ ssidLength,\ 4096,\ 256),$$

где *PBKDF*2 – Password-Based Key Derivation Function 2, *PassPhrase* – ключ сети, *SSID* – идентификатор точки доступа, ssidLength – длина идентификатора, 4096 – количество итераций хеширования, 256 – длина ключа на выходе.

Стоить отметить, что PMK был общим для всех клиентов, а также была возможность легко получить его путем перехвата 4-ех стороннего рукопожатие [7].

WPA2 PSK считался безопасным до появления атаки с переустановкой ключа (*Key Reinstallation Attacks*, KRACK) [8]. В WPA3, взамен PSK, используется метод одновременной аутентификации равных (*Simultaneous Authentication of Equals*, SAE).

SAE основан на протоколе Dragonfly, а именно на методе Password Authenticated Key Exchange (PAKE) [9]. Данный протокол позволяет сгенерировать различные PMK для клиентов, которые будет невозможно получить даже если перехватить 4-ех стороннее рукопожатие.

Аутентификация SAE предназначена для случаев, когда аутентификация основана на пароле, который может быть распространен или получен потенциальным злоумышленником. С помощью SAE точка доступа в сети дополнительно аутентифицируется на основе статической пары открытого/закрытого ключей. Пример обмена сообщениями при использовании метода одновременной аутентификации равных приведен на рис. 2.

В первую очередь происходит преобразование пароля сети в ключевые значения Elliptic Curve Diffie-Hellman. ECDH – протокол, являющийся разновидностью протокола Диффи-Хеллмана, который использует шифрование на базе эллиптических линий, и позволяющий двум участникам, у каждого из которых есть пара из открытого и закрытого ключей в виде математический кривой, установить общий секрет по незащищенному каналу.

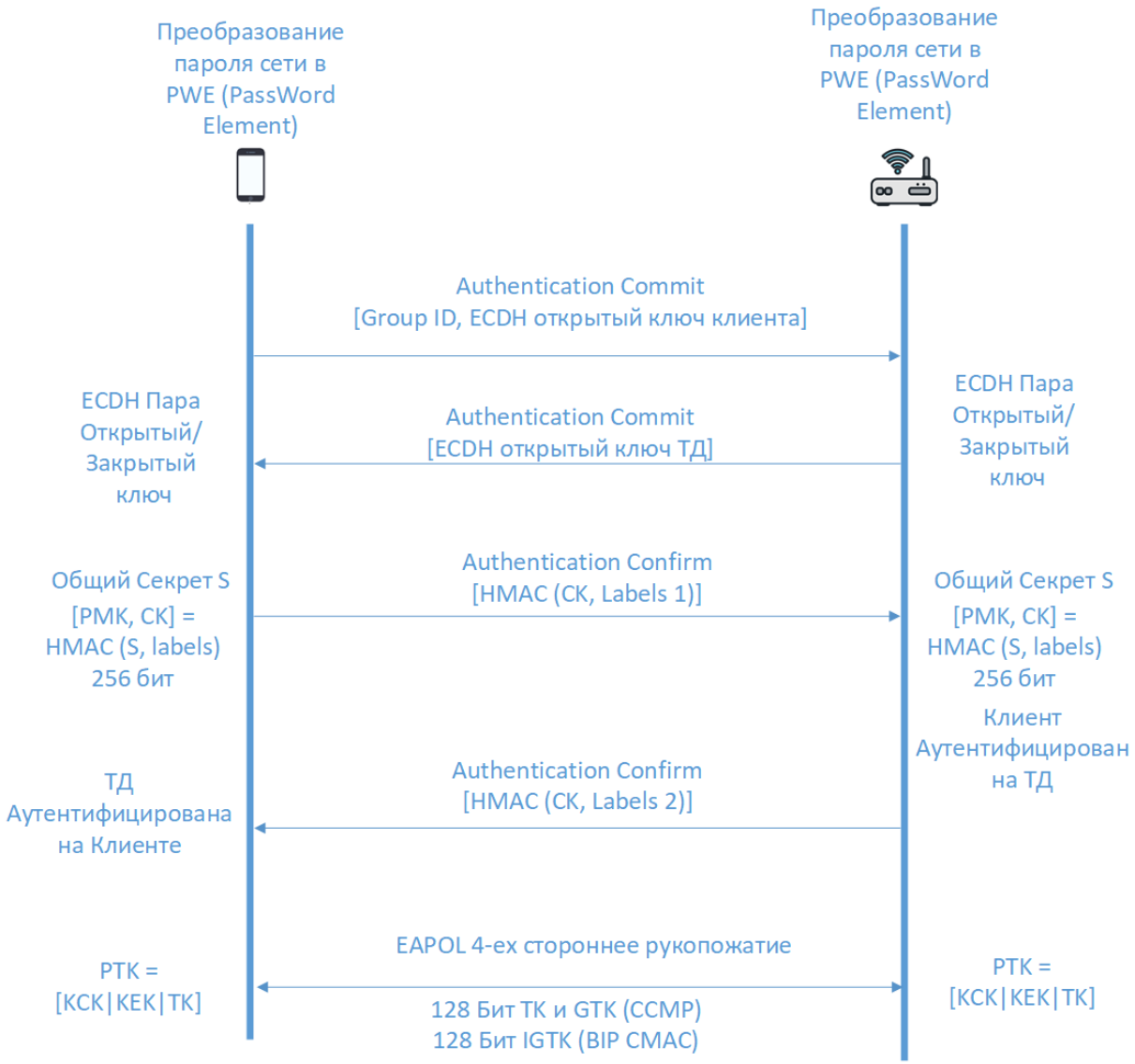


Рис. 2. Обмен сообщениям SAE

Следующий этап – это обмен сообщениями Auth Commit, стороны обмениваются открытыми ключами для генерации общего закрытого ключа. После этого происходит обмен сообщениям Auth Confirm, которыми стороны подтверждают, что они получили одинаковый общий секрет, путем отправки хэша.

Затем стороны вырабатывают PMK с использованием функции KDF-512. После того, как PMK сгенерирован, в процессе 4-ех стороннего рукопожатия он участвует в вычислении парного передаточного ключа PTK, аналогично WPA2.

Таким образом, в статье рассмотрены основные особенности защиты беспроводного трафика сети на базе WPA3. Описаны механизмы, применяемые в WPA3. Кроме того, приведен процесс аутентификации Simultaneous Authentication of Equals, называемый также SAE. Стандарт WPA3 позволяет

значительно улучшить безопасность WLAN по сравнению с предыдущими стандартами.

Список используемых источников

1. Enterprise WLAN market growth in fourth quarter of 2022 builds on 34% growth in third quarter of 2022 2021, According to IDC [Электронный ресурс]. URL: https://www.idc.com/getdoc.jsp?containerId=prUS50475523 (дата обращения 21.02.2023).

2. Дрепа В. Е., Кируга А. Ю., Ковцур М. М., Кузьмина О. И., Петров В. А. Исследование метода Fingerprinting для определения местоположения беспроводного клиента IEEE 802.11 // Заметки ученого. 2022. N 3–2. С. 137–141.

3. Крыщенко Н. И., Миняев А. А., Ковцур М. М. Обзор методических рекомендаций по конфигурированию защищённой WLAN сети // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция: материалы конф. Санкт-Петербург, 2022. С. 554–555.

4. Wi-FI Alliance, WPA3™ Specification Version 3.1, 2019.

5. RFC 8110, Opportunistic Wireless Encryption, 2017.

6. Ахрамеева К. А., Ворошнин Г. Е., Ковцур М. М. Исследование уязвимостей оборудования Mikrotik к атакам на беспроводные сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2021). Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 2. С. 57–63.

7. Kovtsur M. M., Muthanna A., Karelsky P., Kozmyan A., Voroshnin G., Al-Khafaji H. M. R. IPTV access methods with RADIUS-Server authorization // Journal of Information Technology Management. 2022. Т. 14. N 2. С. 80–89.

8. Mikrotik Юркин Д.Ю., Ворошнин Г.Е., Ковцур М.М., Мисливский Б.С. Исследование влияния атак Arpinject и Associationflood в беспроводных сетях на базе оборудования // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 1. С. 44–48.

9. RFC 7664, Dragonfly Key Exchange, 2015.

УДК 001.18
ГРНТИ 49.01.11

ИССЛЕДОВАНИЕ ВОПРОСОВ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ТЕОРИИ ЦИФРОВЫХ ДВОЙНИКОВ

В. Ю. Гойхман, В. Ю. Князева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время Международным союзом электросвязи ведется разработка стандартов в области применения цифровых двойников. Цифровой двойник – это представление физических объектов в цифровом мире в режиме реального времени. Данная

технология была использована во многих отраслях, ориентированных на интеллектуальное производство и "Индустрию 4.0". В данной статье рассматриваются вопросы практического применения теории цифровых двойников, а также определяются области применения теории цифровых двойников в инфокоммуникациях.

инфокоммуникации, искусственный интеллект, нейронные сети, цифровой двойник.

В современных условиях сети связи становятся все более сложными и масштабными, количество услуг увеличивается, и распространение новых сетевых приложений увеличивает сложность управления современными сетями. Таким образом, внедрение инноваций в области сетевых технологий, управление и эксплуатация будет становиться все более сложной задачей из-за высокого риска вмешательства в существующие сервисы и более высоких затрат на пробную версию внедрения. Для решения данной задачи в перспективе может быть использована технология цифрового двойника. Цифровой двойник позволит предварительно проверить изменения на нем с характеристиками из физической сети.

Цифровой двойник (Digital Twin, DT) – это представление физического объекта в цифровом мире в реальном времени. Концепция цифрового двойника предполагает взаимопроникновение цифровых и физических миров, т. е. процессы физической сети будут постоянно корректировать виртуальную модель, а результаты моделирования будут, в свою очередь, влиять на функционирование физической сети.

Задача данной статьи – выявить области практического применения теории цифровых двойников в инфокоммуникациях.

IETF (Инженерный совет Интернета) и ITU (Международный союз электросвязи) вводит понятие Digital Twin Networks (DTN), как виртуальное представление физической сети. Таким образом понятие DTN отличается от DT тем, что применяется в сфере телекоммуникаций и определяется ITU-T Y.3090. DTN реализует совместную эволюцию физического и виртуального пространства с помощью DT-моделирования, коммуникаций, вычислений и технологий обработки данных. Основным отличием по сравнению с традиционными системами управления сетью является интерактивное отображение виртуальной реальности. Таким образом, платформа DTN – это нечто большее, чем платформа эмуляции. DTN может использоваться для разработки различных расширенных сетевых приложений и оценки конкретного поведения (включая преобразование сети) перед фактической реализацией в физической сети, настройки сети для лучшей оптимизации поведения.

Архитектура DTN

DTN содержит четыре ключевые характеристики:

1) Данные являются краеугольным камнем для построения системы DTN. Сетевые данные, собранные из физической сети, могут храниться в DTN в качестве единого хранилища данных, которое может быть единственным источником достоверности и обеспечивать своевременную и точную поддержку моделей данными.

2) Интерактивное отображение используется для идентификации цифрового двойника и его объектов, и установления связи с физическими объектами или объектами другой DTN в реальном времени.

3) Различные модели данных, встроенные в сети цифровых двойников, могут быть спроектированы и гибко комбинированы для обслуживания сетевых приложений.

4) Стандартизированные интерфейсы между DTN и физической сетью, и DTN и сетевыми приложениями являются ключевыми факторами, которые могут эффективно обеспечить совместимость и масштабируемость системы DTN.

Международный союз электросвязи определяет трехуровневую архитектуру цифрового двойника (рис. 1) [2]:

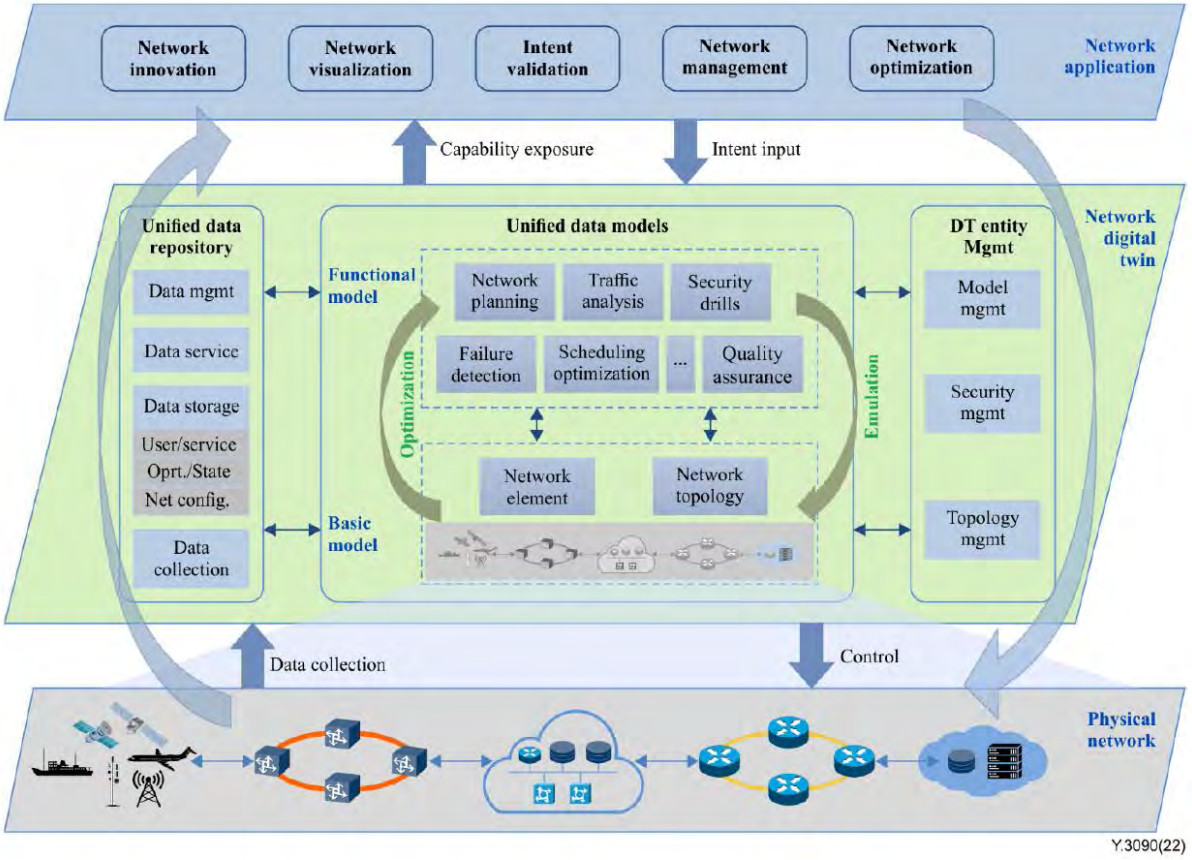


Рис. 1. Эталонная архитектура DTN (Y.3090)

1) Нижний уровень – это физический уровень. Все сетевые элементы, присутствующие в физических сетях, обмениваются сетевыми данными и управляются DTN. Физическая сеть объекта может содержать все инфраструктуры в сети или содержать только определенную инфраструктуру (например, ресурсы радиочастотного спектра, функциональные элементы пользовательского уровня в базовой сети и т. д.).

2) Средний уровень – это уровень цифрового двойника, который является ядром системы DTN. На данном уровне находится подсистема моделирования физических процессов, которая включает в себя унифицированное хранилище данных, унифицированные модели данных и управление объектами цифрового двойника.

3) Верхний уровень – это уровень сетевых приложений. Сетевые приложения передают требования на средний уровень для моделирования. После полной проверки уровень цифрового двойника сети отправляет обновления управления в сеть физического объекта.

Области практического применения:

1. Условия сложной эксплуатации и техническое обслуживание сети

В чрезвычайно больших масштабах традиционные сети начали трансформироваться в виртуализированную сеть, появилось много новых функций, которые делают эксплуатацию и обслуживание сети сложным. DTN может сочетать сбор данных, обработку больших данных и использование искусственного интеллекта для реализации оценки текущего состояния, диагностики прошлых проблем и прогнозирования будущих тенденций, а также предоставлять результаты анализа. Это поможет сети обеспечить прогнозируемое техническое обслуживание на основе текущего технического обслуживания.

2. Оптимизация сети

Поскольку эффективной платформы для моделирования не существует, традиционную оптимизацию сети приходится пробовать непосредственно в реальных сетях с долгосрочными затратами и высокой отдачей от обслуживания. Это также значительно увеличивает операционные расходы оператора сети. С помощью DTN возможное решение для оптимизации сети может быть полностью и быстро проверено с меньшими затратами. Технология цифрового двойника может применяться для оптимизации сети SDN для соответствия SLA при меняющейся нагрузке [3]. Цифровой двойник на базе графовых нейронных сетей (GNN, Graph neural network) реализует пользовательскую архитектуру нейронной сети (Neural Networks, NN) для передачи сообщений. Он явно определяет сетевые элементы и их отношения в своей внутренней архитектуре нейронной сети и учится рассуждать на основе этой графически структурированной информации. Цифровой

двойник был применен для оценки задержек на каждом пути в сетях, охватывающих широкий спектр топологий, конфигураций (маршрутизация и постановка в очередь) и уровней нагрузки. В результате цифровой двойник способен точно обобщать выборки из 106 сетей реального мира (из Internet Topology Zoo).

3. Ускорение сетевых инноваций и исследования сети

Реальная сетевая среда обычно недоступна для сетевых исследователей и для изучения инновационных методов. Вместо этого исследователям приходится использовать автономные платформы моделирования, что сильно влияет на реальную эффективность инноваций и значительно замедляет скорость их внедрения. DTN может генерировать виртуальный объект-двойник реальной сети, что поможет исследователям эффективно изучать сетевые инновации (например, новые сетевые протоколы, сетевые приложения AI / ML и т. д.) и поможет сетевым операторам быстро внедрять новые технологии с меньшими рисками. Сообществом ML предлагается алгоритм GNN для моделирования реляционно-структурированной информации [4]. Поскольку компьютерные сети в основном представлены в виде графиков, GNN предлагают преимущества для сетевого моделирования по сравнению с традиционными NN-архитектурами.

4. Мониторинг сети

DTN может получать массивные данные из сетевой инфраструктуры напрямую с помощью различных инструментов. Однако параметры сети (например, время завершения потока, сквозная задержка, доступная пропускная способность пути и т.д.) не могут контролироваться или измеряться непосредственно из физической сети. DTN может помочь клиентам или сетевым операторам косвенно оценивать или измерять параметры сети, анализируя массив данных из разных доменов на виртуальной платформе, а затем получать более полные измерения в сети.

5. Внедрение сети, основанной на намерениях (*Intent-Based Networks*, IBN)

Будущие сети, возможно, будут основаны на намерениях, где пользователи смогут вводить свои абстрактные "намерения" в сеть вместо подробных политик или конфигураций на сетевых устройствах. Ключевой особенностью сетевой системы, основанной на намерениях, является то, что намерение пользователя может быть гарантировано автоматически путем непрерывной корректировки политик и проверки ситуации в режиме реального времени. Чтобы снизить воздействие на реальную сеть, несколько ра-

ундов настройки и валидации лучше смоделировать на платформе DTN. Таким образом, DTN может стать важным средством быстрого и эффективного внедрения системы IBM.

6. Сетевая безопасность

С помощью платформы DTN тренировки по стратегии сетевой безопасности могут быть более эффективными (например, хакерские атаки, DDoS-атаки, вирусные атаки и т.д.) и полезными для заблаговременной разработки политики защиты безопасности и надежности физической сети.

Заключение

Таким образом, в статье была рассмотрена архитектура Digital Twin Network. В настоящее время определены следующие области использования цифровых двойников: эксплуатация и мониторинг сетей, оптимизация сети и сетевая безопасность, тестовая среда для IBN-сетей. Также цифровые двойники упростят проведение исследований технологий/протоколов.

Список используемых источников

1. Zhou C., Yang H., Duan X., Lopez D., Pastor A., Wu Q., Boucadair M., Jacquenet C. Digital Twin Network: Concepts and Reference Architecture [Электронный ресурс] // 2022 P. 5. URL: https://datatracker.ietf.org/doc/pdf/draft-irtf-nmrg-network-digital-twin-arch-02 (дата обращения 20.02.2023).

2. Recommendation ITU-T Y.3090. Digital twin network – Requirements and architecture [Электронный ресурс] // Series Y: Global information infrastructure, internet protocol aspects, next-generation networks, internet of things and smart cities. 2022. P. 17 URL: https://www.itu.int/rec/T-REC-Y.3090-202202-I/en (дата обращения 20.02.2023).

3. Ferriol-Galmes M., Suarez-Varela JPaillisse., J., Xiang Shi, Shihan Xiao, Xiangle Cheng, Barlet-Ros P., Cabellos-Aparicio A. Building a Digital Twin for network optimization using Graph Neural Networks [Электронный ресурс] // Computer Networks: электрон. научн. журн. 2022. N 217. P. 5. URL: https://www.sciencedirect.com/science/article/pii/S1389128622003681 (дата обращения 23.02.2023).

4. Almasan P., Ferriol-Galmes M., Paillisse J., Suarez-Varela J., Perino D., Lopez D., Perales A. A. P., Harvey P., Ciavaglia L., Wong L., Vishnu Ram, Shihan Xiao, Xiang Shi, Xiangle Cheng, Cabellos-Aparicio A., Barlet-Ros P. Digital Twin Network: Opportunities and Challenges [Электронный ресурс] // 2022. P. 4. URL: https://arxiv.org/pdf/2201.01144.pdf (дата обращения 25.02.2023).

UDK 004+004.93
GRNTI 20.53.19

POLYGRAPH SUBSYSTEM BASED ON ARTIFICIAL INTELLIGENCE

S. Goncharov, T. Ovodova

The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article presents the take on the future of lie detection. The complexity of usual polygraph procedures is an obstacle itself for implementing it into more criminal cases and everyday life situations. The author introduces a new artificial intelligence application to daily aspects of our lives that eliminates the human factor and makes the decision-making process much faster than it is today.

lie detection, polygraph procedures, new artificial intelligence application, Artificial Intelligence.

This article will present the view on the future of lie detection. It includes the usage of artificial intelligence in the form of neural network and basic human reflexes, such as pupil dilation. This reflex takes place in stressful situations, one of them concerns lying. The more severe the consequences of exposing a lie, the stronger the impact of this reflex.

Before diving into the specifics of how it works, we shall explain why it should exist in the first place. Mainly, the complexity of usual polygraph procedures is an obstacle itself for implementing it into more criminal cases and everyday life situations. For example, there is a lot of convictions that are proven to be based of false accusations. Up to 10 percent of the convicted in US prisons are actually not guilty [1]. In terms of everyday life, it would be great to have a powerful instrument to recognize lies in airports, for example. With this device, the guards will be able to recognize a lie in a matter of seconds if someone tries to carry something illegal with them. At the very least it would provide an extra level of confidence, which is never enough when it comes to security. Fast and reliable lie detection would also be helpful in civil cases where false accusations are very common. Thus, the introduction of artificial intelligence into such everyday aspects of our lives would eliminate the human factor and make the decision-making process much faster than it is now.

1. System development

The system's structure is divided into 2 modules. The first one is called "The CV (Computer Vision) module" and its task is to take a close-up picture of a person's eyes after he has answered a certain question, and then discover two circles:

the iris and the pupil. After that it calculates the ratio of their radii by simple division and passes it to the second module.

The second module is called “The AI (Artificial Intelligence) module”. Its task is to process the information given and, practically, to detect lies. To put it simply: we have a neural network, that is designed to work in a way like a human brain. We train it by “giving” it examples of what is a lie and what is not. These examples are the input data for the relationships explained earlier along with what should be output for each instance. These outputs are called “markers”. These markers contain values of either 0 or 1 (truth or lie respectively). Thus, the neutral network is trained by adjusting its parameters to match the correct output signal to a given input signal.

This solution is created using Python and TensorFlow, OpenCV, NumPy and Matplotlib libraries. MMU iris dataset has been used for training and performance testing. The whole working process of the first module relies heavily on OpenCV. It is a powerful tool for implementing computer vision and can easily detect circles and calculate their radiuses, which is the only thing needed from that module.

During designing the architecture of system’s neural network some of the conventional rules and tips have been used [2, 3]. By the nature of the system’s goal and requirements feedforward neural network is the most fitting solution for the second module. The input consists of 10 ratios and the output is of the only one so it is the most optimal to have only one hidden layer, ten input neurons, one output neuron and six hidden neurons. Designed architecture is presented on the fig. 1.

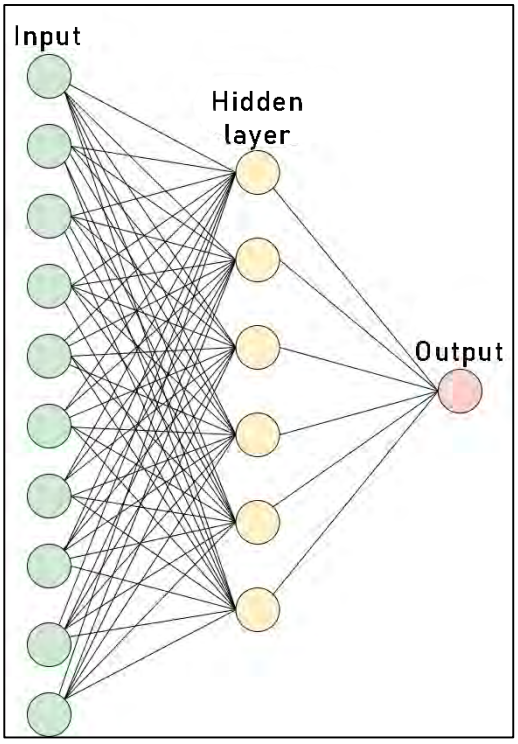


Fig. 1. Neural network’s architecture

As for activation functions, ReLU and sigmoid have been chosen for hidden and output layers respectively. ReLU is a great choice because of its simplicity and resistance to vanishing gradient that can slow down training process or even virtually disrupt it and make network perform significantly worse. Sigmoid is the most fitting choice for the output layer because in this case it basically smooths out given values and outputs a unit in range from 0 to 1. And this final value also tends to lean to either of these limits, which makes the decision making much easier. Graphs of these functions are presented on fig. 2 and 3 respectively to visualize their roles. In both cases abscissa represents the function’s input value and ordinate represents the value that it outputs.

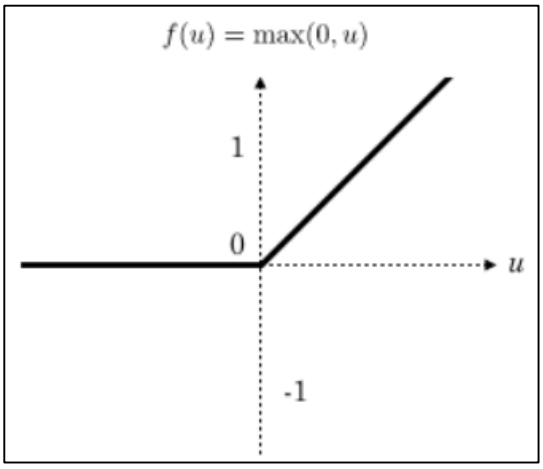


Fig. 2. ReLU graph

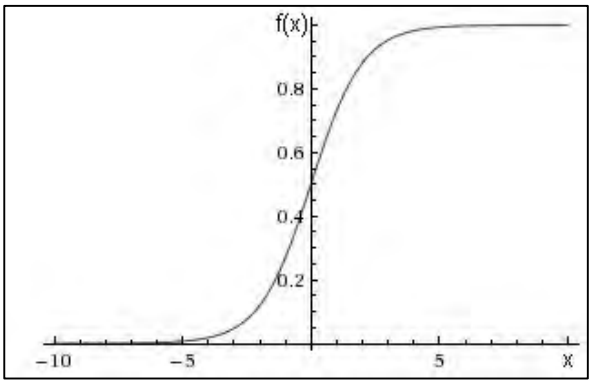


Fig. 3. Sigmoid graph

Training process is supervised and implements backpropagation for its versatility, speed and simplicity.

The network has been trained two times. First, with the sets of randomly generated numbers in certain limits for lie and truth accordingly (limits are necessary to simulate real values from photos). This includes 1000 numbers in total that have been divided in groups of 10 and labeled as mentioned above. Input order of these groups is randomized to avoid pattern thinking of the network. Difference in accuracy values for training and validation sets have indicated that no underfitting or overfitting had occurred.

After implementing the CV module into the system, the network then has been trained with real pictures instead of number sets. As expected, the accuracy decreased slightly compared to the original numbers, but still no anomalies were detected.

This two-step training process has been introduced in order to test overall network performance before implementing the CV module. It is necessary to fine-tune it or even completely redesign its architecture if any problems arise. Random numbers in first training sets have practically simulated real ratios that would have been used later.

2. System testing

22 sets of 10 photos each were used for testing (9 for lies and 13 for truth). Tests like this simulate real working experience so the input data consists of only pictures without any markers.

During the test the developed system has successfully identified all 9 sets of lies, but has wrongfully identified one of the sets of truth as lie as well. This performance brings it to the accuracy of roughly 95 % which is considered a good result for used amount of training data. In order to get better values, it is necessary to increase quality and quantity of training sets and fine-tune parameters of the CV module and neural network.

Developed system can be used as a part of a traditional polygraph system to ensure independency of the results as well as hold its own as an autonomous instrument of lie detection. The presented solution has great potential for use at airports and customs during inspections, in civil cases as a measure of truth and in other sectors where the use of a polygraph and similar technologies is justified. It is recommended to reconfigure and retrain neural network for individual scenarios in order to achieve its maximum accuracy and speed. It is also highly advised to frequently update training samples database since aforementioned accuracy, naturally, mainly depends on amount and quality of given input data.

References

1. Startling Wrongful Convictions Statistics: [Electronic resource] // The High Court. Text: digital. URL: https://thehighcourt.co/wrongful-convictions-statistics/ (reference date 28.02.2022).

2. Heaton J. Introduction to Neural Networks for Java. 2nd edit. Chesterfield: Heaton Research, Inc., 2008. (reference date 17.02.2022).

3. Machine Learning Mastery: [Electronic resource]. Text: digital. URL: https://machinelearningmastery.com. (reference date 20.02.2022).

The article is presented by Candidate of Philological Sciences, Associate Professor of the Department of Foreign and Russian Languages of SPbGUT E. A. Gorshkova.

УДК 004.056.5
ГРНТИ 81.93.29

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕХАНИЗМОВ КОНТРОЛЯ ПРАВАМИ ДОСТУПА В ОС LINUX

С. А. Горбань, А. В. Красов, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена изучению эффективности системы прав доступа. В статье рассмотрены особенности реализации и оценки системы прав доступа. Авторы статьи используют методы анализа, чтобы оценить результаты работы системы. Целью работы является проведение исследования, направленного на улучшение функционирования системы.

права доступа, ОС Linux, защищенность, администрирование.

Контроль правами доступа связан с определением разрешенных действий легитимных пользователей, посредничество при каждой попытке

пользователя получить доступ к ресурсу в системе. Определенная информационная технологическая инфраструктура может реализовывать системы контроля за правами к объектам системы. Для защиты файлов и каталогов операционные системы применяют механизм контроля доступа, а для управления доступом к таблицам и представлениям баз данных используются системы управления базами данных. Большинство коммерческих прикладных систем также оснащены механизмами контроля доступа, которые могут работать независимо от операционных систем и СУБД, на которых они установлены.

Часто цели системы контроля доступа формулируются как защита системных ресурсов от доступа неавторизованных или нежелательных пользователей. Однако, при большом количестве совместно используемых ресурсов, защита может стать проблемой. На самом деле, хорошо настроенная и эффективная система контроля доступа способствует совместному использованию ресурсов [1]. Достаточно тонкий механизм контроля доступа может обеспечить выборочный обмен информацией там, где в его отсутствие обмен может быть вообще считается слишком рискованным.

SELinux – инструмент безопасности для операционных систем Linux, дающая администраторам иметь полный контроль над предоставлением доступа к системе.

Утилита отвечает за контроль предоставления доступа к процессам, файлам и приложениям системы. Она основывается на наборах правил, которые указывают к чему можно или нельзя обращаться, при предоставлении доступа.

SELinux осуществляет проверку запроса на доступ к объекту с помощью кэша векторов доступа, где сохранены права доступа для субъектов и объектов. В случае, если кэш не содержит необходимой информации, SELinux обращается к серверу безопасности. Сервер проверяет контекст безопасности процесса или приложения и соответствующего файла на основе базы данных политик SELinux. Разрешение выносится в зависимости от результатов проверки.

Существует несколько вариантов настройки SELinux для обеспечения защиты вашей системы [2]. Наиболее распространенными среди них являются целевая политика и многоуровневая безопасность. При использовании целевой политики применяется настройка по умолчанию, которая охватывает широкий спектр процессов, задач и служб. Многоуровневая безопасность (MLS) может быть очень сложной и обычно используется только правительственными организациями.

Администратор может определить, на каком уровне должна работать система, посмотрев файл /etc/sysconfig/selinux. В файле будет раздел, показывающий, находится ли SELinux в разрешительном режиме, режиме принуждения или отключен, а также какая политика должна быть загружена.

SELinux основывается на типах и метках. Это означает, что все файлы и процессы маркируются и уже на основе меток происходит реализация политики, определенной в системе. Применений типов определяет может ли процесс получить доступ к файлу с определенным типом. Политика SELinux использует контексты в серии правил, которые определяют, как процессы могут взаимодействовать между собой и с другими системными ресурсами. По умолчанию политика SELinux запрещает взаимодействие, если правило явно не разрешает доступ [3].

Дискреционный контроль доступа в Linux является более распространенным чем мандатный. SELinux - представитель мандатной системы. Это дает определенные преимущества. Например, если в DAC у пользователя есть доступ root, то вы можете получить доступ к файлам любого другого пользователя. Но в системах MAC, таких как SELinux, существует административно устанавливаемая политика доступа. Даже если настройки DAC в вашем домашнем каталоге изменены, политика SELinux, не позволяющая другому пользователю или процессу получить доступ к каталогу, обеспечит безопасность системы.

Политики SELinux позволяют быть конкретными и охватывают большое количество процессов. С помощью SELinux можно вносить изменения для ограничения доступа между пользователями, файлами, каталогами и многим другим [4].

Процессы и файлы помечаются контекстом SELinux, который содержит дополнительную информацию, такую как пользователь SELinux, роль, тип и уровень. Для принятия решений по управлению доступом SELinux использует всю эту информацию. В Red Hat Enterprise Linux SELinux использует комбинацию Role-Based Access Control, Type Enforcement и Multi-Level Security для обеспечения надежной защиты [5].

На стенд с операционной системой Ubuntu 22.04.1 был установлен SELinux и выстроена система контроля правами доступа. Большинство компьютерных систем разработаны для использования несколькими пользователями. Привилегии означают, что разрешено делать пользователю. Общие привилегии включают доступ к файлам на чтение и редактирование, а также возможность изменять системные файлы. Повышение привилегий означает, что пользователь получает доступ к привилегиям, которые ему не полагаются. Эти привилегии могут быть использованы для удаления файлов, получения доступа к частной информации или установки вредоносных программ, таких как вирусы. Обычно такое происходит, когда система содержит ошибку, которая позволяет обойти меры защиты, или, когда ее проектные предположения о том, как она будет использоваться, оказываются неверными [6].

Были проведены атаки эксплойтами на развернутый стенд с SELinux. Анализ таблицы 1, показывает высокий уровень стойкости выбранной системы контроля доступа. В столбце с результатом – 0 это отрицательный исход атаки и 1 – положительный.

ТАБЛИЦА 1. Результат атак по эксплуатации уязвимостей.

Атака	Результат
Kernel exploits	0
Exploiting services root	0
Exploiting SUID Executables	0
Exploiting SUDO rights/user	0

В данной статье авторы рассмотрели одну из многих систем контроля правами к ресурсам и папкам, оценили ее устойчивость к атакам эксплойтами. Дальнейшим вектором исследования будет рассмотрение других утилит по настройке прав доступа и вывод единой системы оценки эффективности для рассматриваемых инструментов защиты информации.

Список используемых источников

1. Собель М. Г. Linux администрирование и системное программирование : учебник. 2-е изд. СПб. : Питер. 2011. 880 с.

2. Курячий Г. В., Маслинский К. А. Операционная система Linux: Курс лекций. Учебное пособие. М. : ALT Linux: Издательство ДМК Пресс, 2010. 348 с.

3. Негус К. Библия Linux. 10-е изд. СПб. : Питер, 2022. 928 с.

4. Казанцев А. А., Красов А. В., Катасонов А. И., Гельфанд А. М. Создание и управление security operations center для эффективного применения в реальных условиях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференцияи : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 590–595.

5. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Оценка рисков и угроз безопасности в среде «умный дом» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 316–321.

6. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 343–348.

УДК 681.7
ГРНТИ 49.46.29

РАЗРАБОТКА ОПТИКО-МЕХАНИЧЕСКОГО ТРАКТА ДЛЯ ДУПЛЕКСНОЙ ЛАЗЕРНОЙ КОСМИЧЕСКОЙ СВЯЗИ

Е. А. Горбуленко, Е. П. Меснянкин, С. Л. Потапов, Н. И. Потапова

АО «Научно-исследовательский институт оптико-электронного приборостроения»

В работе предложены различные варианты исполнения оптико-механического тракта для дуплексной лазерной космической связи (с общим приемо-передающим каналом и с раздельными каналами приема и передачи), приведены оценочные энергетические расчеты, оценочные расчеты массогабаритных характеристик, а также предложен вариант размещения функциональных узлов на борту космического аппарата для устройств с уменьшенными массогабаритными характеристиками для передачи больших объемов информации с высокими скоростями на расстояния от единиц до тысяч километров.

космическая лазерная связь, КОЛС, волоконно-оптическая линия связи, ВОЛС, оптико-механический тракт, дуплексная связь.

В настоящее время все более востребованы устройства, позволяющие осуществлять передачу больших объемов информации на значительные расстояния в космическом пространстве. Для обмена информацией в наземных условиях широкое применение получили волоконно-оптические линии связи (ВОЛС), где в качестве среды, в которой распространяется модулированное лазерное излучение, несущее информацию, используется оптическое волокно. Для обеспечения передачи информации через спутниковые системы связи необходимы соответствующие модули, работающие в космическом пространстве. Напрямую использовать при разработке этих устройств методы, лежащие в основе создания ВОЛС, нельзя, поскольку существует ряд особенностей, связанных с распространением лазерного излучения в свободном пространстве.

Важнейшими отличиями космических оптических линий связи (КОЛС) от ВОЛС являются следующие факторы:

1) наличие расходимости лазерного излучения при его распространении в свободном пространстве, приводящее к уменьшению дальности передачи информации;

2) отсутствие возможности использовать промежуточные усилители для обеспечения приема сигнала на больших расстояниях (для повышения

дальности возникает потребность в использовании мощных лазерных передающих устройств);

3) необходимость наведения терминалов КОЛС друг на друга в режиме приема-передачи информации, а также их сопровождения и компенсации уходов оптической оси при вибрациях носителя.

Анализ доступной в открытой печати информации [1] показал, что разработки в области создания КОЛС ведутся широким фронтом как за рубежом, так и в России. Европейское космическое агентство (ESA) разрабатывает систему межспутниковой космической лазерной связи EDRS (*European Data Relay System*). Аналогичные работы ведутся так же в США, Европе, Китае, Японии и Корее.

В России разработки ведутся множеством организаций, таких, как МГТУ им. Н.Э. Баумана, ИОФ РАН, МИФИ, ИТМО, СО РАН, МАИ, ООО «АРКОИРИС», НИИ Радио, НПК «Системы прецизионного приборостроения» [2, 3].

В работе рассматривались различные схемные решения КОЛС, из них было выбрано два наиболее перспективных, с точки зрения авторов: с общим приемо-передающим каналом и с раздельными каналами приема и передачи.

В рассматриваемых системах используется современная, промышленно выпускаемая элементная база: в качестве передающих и приемных устройств рабочего (информационного) лазерного излучения используются трансиверы, усиление выходной мощности обеспечивают оптоволоконные усилители, а за прием сигнала лазера наведения и допоиска (лазера-маяка) отвечают квадрантные фотоприемные устройства.

На рис. 1 приведена оптическая схема оптико-механического тракта (ОМТ) КОЛС с общим приемо-передающим каналом.

Передающий канал имеет два лазерных источника: рабочий (информационный), работающий на длине волны 1,55 мкм, и лазер-маяк, работающий на длине волны 1,06 мкм.

Излучение лазера-маяка от терминала первого абонента проходит через блок упреждения, отражается от светоделителя (6), расположенного под углом 45^{o}, затем отраженное излучение, проходит через дефлектор сопровождения (9) и дефлектор компенсации вибраций (10) и выходит через формирующий телескоп для облучения терминала второго абонента при его поиске. Сигнал от этого лазера-маяка регистрируется квадрантным фотоприемным устройством, находящимся на втором аналогичном терминале, от которого через блок управления сопровождением поступают сигналы на дефлектор сопровождения (9) – это необходимо для того, чтобы точно навестись на терминал абонента.

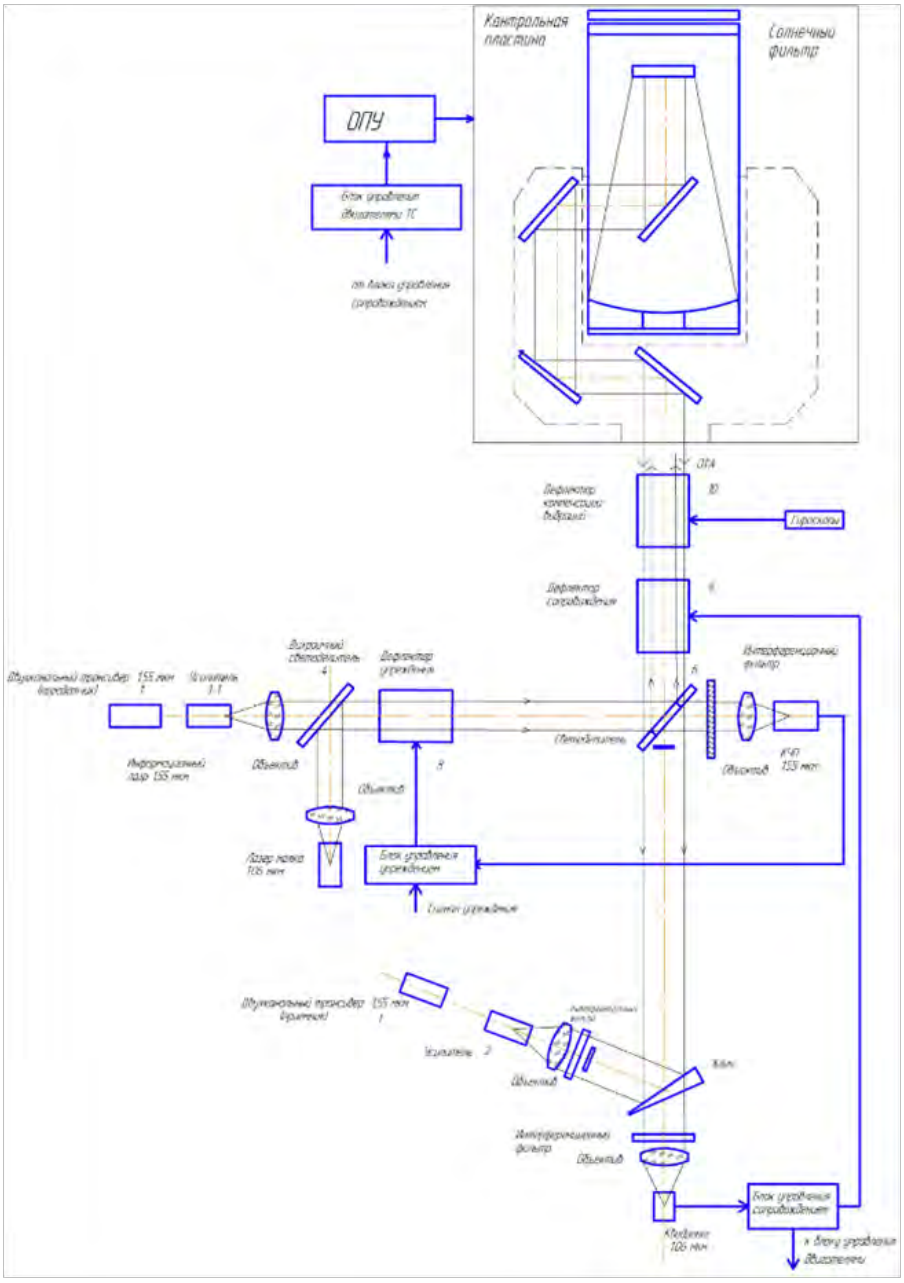


Рис. 1. Оптическая схема ОМТ КОЛС с общим приемо-передающим каналом

Рабочее лазерное излучение из двухканального трансивера (1) поступает в оптоволоконный усилитель (1-1), проходит блок упреждения, который с применением дефлектора упреждения (8) и блока управления упреждением организует систему допоиска объекта (излучение попадает на координатно-чувствительный приемник (КЧП), который используется для контроля угла поворота дефлектора). Одним из важных элементов в приемо-передающем тракте является светоделитель (6), имеющий в центре зеркальное покрытие с коэффициентом отражения близким к 100 %, а по окружности просветляющее покрытие, обеспечивающее пропускание практически 100% излучения для длин волн 1,06 мкм и 1,55 мкм. Пройдя

через дефлектор сопровождения (9) и дефлектор компенсации вибраций (10), излучение выходит через формирующий объектив для передачи информации абоненту.

Принятый сигнал рабочего излучения от абонента на втором терминале проходит путь сигнала лазера-маяка до оптического клина, после отражения от которого рабочее излучение попадает в оптоволоконный усилитель (2), а затем информация регистрируется приемником двухканального трансивера (1).

Были проведены оценочные расчеты мощности сигнала на фотоприемнике для установления возможности приема сигнала на расстоянии 4000 км при использовании типовых характеристик коммерческих образцов трансиверов и усилителей.

Исходные данные, которые использовались для проведения оценочных расчетов, приведены в таблице 1.

ТАБЛИЦА 1. Исходные данные для оценочных расчетов

Параметр	Значение	Единицы измерения
Длина волны передатчика трансивера (λ)	1,55	мкм
Мощность передатчика трансивера ($P_{зг}$)	1	мВт
Мощность передатчика «маяка» (P)	1	Вт
Пропускание модулятора ($\gamma_м$)	0,7	б/р
Коэффициент усиления усилителя (M)	1000	б/р
Потери в мультиплексоре при оценках (γ_1)	0,63	б/р
Пропускание при согласовании волокно – передающий тракт (γ_2)	0,5	б/р
Пропускание телескопической системы (τ)	0,7	б/р
Диаметр передаваемого излучения на выходе (диаметр объектива в режиме «передача») (D_1)	57; 71; 80; 100	мм
Эквивалентный диаметр объектива в режиме «приема» (D_2)	57; 71; 80; 100	мм
Дистанция (L)	4000	км
Пропускание при согласовании приемный тракт – приемник (γ_3)	0,5	б/р
Потери в демультиплексоре при оценках (γ_4)	0,63	б/р
Коэффициент усиления усилителя приемника (M_1)	1000	б/р
Расходимость излучения лазера-маяка (φ)	3	угл. мин.

**б/р – безразмерная величина*

Потери на трассе при передаче данных можно определить следующим образом:

$$k_1 = \left[D_2 / (L \cdot \theta)\right]^2, \quad (1)$$

где $\theta = 2{,}44 \cdot \lambda / D_1$ – расходимость рабочего излучения (полный угол).

Потери на трассе для излучения лазера-маяка оценивались по выражению (2):

$$k_2 = \left[D_2 / (L \cdot \varphi) \right]^2 \quad (2)$$

Принятая мощность сигнала рабочего излучения на приемнике равна:

$$P_{\text{пр}} = P_{\text{ЗГ}} \cdot \gamma_M \cdot M \cdot \gamma_1 \cdot \gamma_2 \cdot k_1 \cdot \tau^2 \cdot \gamma_3 \cdot M_1 \cdot \gamma_4 . \quad (3)$$

Принятая мощность сигнала от лазера-маяка квадрантным приемником составит:

$$P_M = P \cdot \gamma_M \cdot \gamma_2 \cdot k_2 \cdot \tau^2 \cdot \gamma_3 \quad (4)$$

Диаметр полной выходной апертуры телескопической системы определяется диаметром передаваемого излучения на выходе (D_1) и равен:

$$D = D_1 \cdot \sqrt{2} \quad (5)$$

Результаты проведенных оценочных расчетов представлены в таблице 2.

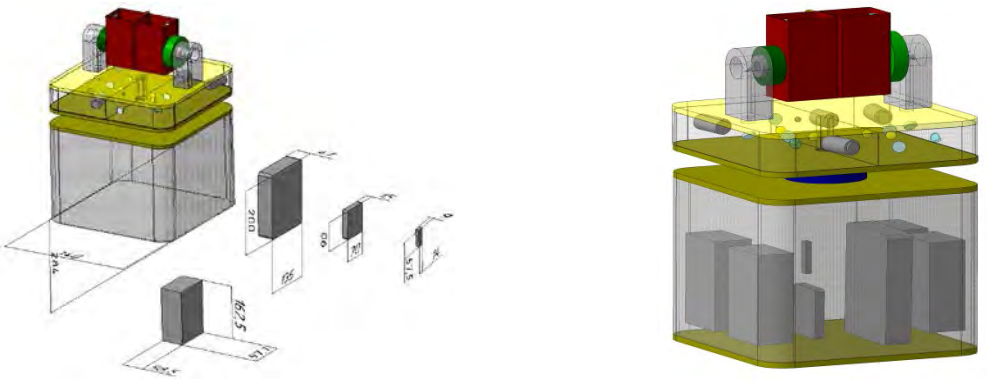
ТАБЛИЦА 2. Результаты оценочного расчета

D_1, D_2, мм	D, мм	$P_{пр}$, мкВт (данные)	$P_{пр}$, дБм (данные)	$P_м$, пВт (лазер-маяк)
1	2	3	4	5
100	141	9,9	–20,0	70,0
80	113	4,1	–23,9	45,0
71	100	2,5	–26,0	35,5
57	81	1,0	–29,8	22,9

В таблице 2 в столбце 4 приведены результаты расчетов величины принятой мощности рабочего излучения в пересчете на дБм. На основе расчетов и проведенного анализа можно сделать вывод, что приемники трансиверов имеют чувствительность близкую к необходимой для приема сигнала на заданном расстоянии, которая может достигать –35 дБм [4].

Оптические схемы приемного и передающего каналов КОЛС с раздельными каналами идентичны по функциональному действию и элементной базе схемам КОЛС с общим приемо-передающим каналом, но вариант исполнения с раздельными приемным и передающим каналами позволяет разнести функциональные узлы так, чтобы избежать большей части рассеянного излучения (исключить возможность попадания из передающего канала в приемный канал). Однако за счет этого могут увеличиться массогабаритные характеристики КОЛС. Это необходимо учитывать при оценочном расчете и выборе оптимального схемного решения КОЛС.

Проведенный оценочный расчет габаритных размеров терминала показал (см. рис. 2), что габаритные размеры терминала с учетом размещения функциональных узлов остаются небольшими (350 х 350 х 600 мм), что должно позволить разместить данный терминал на космическом носителе.



а) б)

Рис. 2. Результаты оценки габаритных размеров терминала:
а) размеры терминала и функциональных блоков; б) примерная компоновка функциональных блоков в терминале

В заключение следует отметить, что для окончательного выбора варианта исполнения ОМТ КОЛС необходимо проведение макетирования основных узлов и проведение сравнительного анализа, при которых будут оценены энергетические и массогабаритные характеристики системы в зависимости от требований к КОЛС.

Список используемых источников

1. Казанцев С. Г. Лазерные технологии для телекоммуникационной платформы малого космического аппарата // Вопросы электромеханики. Труды ВНИИЭМ. 2018. Т. 163, N 2. С. 29–47.

2. Широбакин С. Е., Крюкова И. В., Чуковский Н. Н., Тананаев Г. Ю. Новая концепция построения бортовой аппаратуры межспутниковых оптических линий связи. // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2008. N 2. С. 122–127.

3. Межспутниковые лазерные системы передачи информации [Электронный ресурс]. URL: https://npk-spp.ru/activity/mezhsputnikovye-lazernye-sistemy-peredachi-informatsii/ (дата обращения 14.02.2023).

4. Оптический трансивер LS48-A3L-TC-N [Электронный ресурс]. URL: https://componentltd.ru/catalog/sfp-moduli/opticheskiy-transiver-ls48-a3l-tc-n/ (дата обращения 15.02.2023).

УДК 654.739
ГРНТИ 49.33.29

ОБЗОР И СИСТЕМАТИЗАЦИЯ ПРОГРАММНЫХ СРЕДСТВ, ИСПОЛЬЗУЕМЫХ ДЛЯ РАССЛЕДОВАНИЯ КИБЕРАТАК

М. Д. Горда[1], А. А. Чечулин[1,2]

[1]Санкт-Петербургский федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Несмотря на совершенствование различных средств защиты информации, с каждым годом наблюдается всё больший рост количества киберпреступлений, часть из которых не удается обнаружить или предотвратить в момент проведения. Такие киберпреступления являются объектом исследования для киберкриминалистов. В рамках расследования специалисты используют различное специализированное программное обеспечение, которое позволяют отследить место и время совершения преступления, а, иногда, и самого преступника. В статье будет представлен обзор и систематизация современных программных средств компьютерной криминалистики, а также проанализированы их достоинства и недостатки.

форензика, компьютерная криминалистика, расследование киберпреступлений.

На этапе планирования различных видов кибератак, потенциальным преступникам необходимо изучить информацию о теоретической и практической части проведения атак. Для того, чтобы найти все необходимые данные, скачать специальные утилиты и инструкции к ним, хакеры используют веб браузеры. Поэтому одной из важнейших задач кибер-криминалиста является нахождение доказательств посещения различных веб ресурсов потенциальным подозреваемым. Для этого эксперты пользуются специальными утилитами [1] для обнаружения следов посещения пользователем искомых ресурсов.

Для того, чтобы понять, как проходит данный этап расследования киберпреступлений необходимо изучить и систематизировать программные средства [2], использующиеся специалистами, а также проанализировать функционал утилит.

Практической ценностью доклада является нахождение оптимального программного средства для расследования рассматриваемого этапа работы кибер-криминалиста.

Одним из типичных представителем данных утилит является программное обеспечение Browser History Examiner, которое позволяет соби-

рать и анализировать информацию о поисковых запросах браузера, посещённых веб страниц, а также об аккаунтах пользователя. Приложение устанавливается в операционную систему и собирает все необходимые данные для предоставления отчёта, затем, собранные данные можно представить в виде PDF файла. Также функционал программного обеспечения позволяет определять интернет-активность пользователя браузера и временные интервалы использования, фильтровать полученные данные по ключевым словам, диапазонам дат и времени, собирать необходимые данные как локально, так и удалённо по сети, восстанавливать удалённую историю веб-браузера из теневых копий, просматривать кэшированные веб страницы в том состоянии, в котором их видел пользователь, просматривать адреса электронной почты, автоматически извлекаемые из истории браузера. Browser History Examiner может анализировать необходимые данные из следующий браузеров: Google Chrome, Microsoft Edge. Mozilla Firefox, Internet Explorer 10/11 версии, Safari. Недостатками ПО являются: платное лицензирование на основе годовой подписки, возможность установки только на OS Windows.

Аналогичным функционалом оснащено программное обеспечение Web Historian, которое позволяет просматривать структуру директорий на наличие файлов истории активности браузеров: Internet Explorer, Mozilla Firefox, Opera, Safari. После загрузки исходных данных в программное обеспечение, криминалист может произвести следующие действия: просмотр списка URL адресов, на которые переходил пользователь, анализ cookie файлов, оставшихся после посещения веб страниц, просмотр истории форм веб страниц в том виде, как их видел пользователь, просмотр загрузок пользователя, которые он производил с веб страниц, в процессе их посещения. Также ПО Web Historian позволяет просматривать информацию в виде графиков и статистических данных за указанный период времени. В отличие от Browser History Examiner, данное ПО предоставляет возможность вывода отчётов в формате Excel, HTML, XML и CSV. К недостаткам можно отнести то, что в результате работы ПО формируется множество html файлов, которые необходимо обрабатывать вручную.

Также при необходимости извлечения и анализа данных браузера специалист в области информационной безопасности может воспользоваться утилитой Forensic Tool Kit (FTK). Она позволяет собирать необходимые данные из браузеров Google Chrome, Microsoft Edge. Mozilla Firefox, Internet Explorer 10/11 версии, Safari. Преимуществом данного ПО является просмотр кэшированных страниц в интерфейсе, подобному браузеру. Из преимуществ ПО представлены: просмотр истории посещений веб страниц пользователем, просмотр и экспорт кэшированных страниц в формате HTML. Недостатками программного обеспечения является тот факт, что для каждого случая активности представлен отчёт в виде отдельной таблицы, что усложняет экспорт данных в едином виде.

Утилита Hack Browser Data Tool является программным инструментом с открытым кодом, который позволяет получить данные паролей, закладок, историю посещений web-страниц пользователем компьютера, а также данные кредитных карт, сохраненных в браузере для удобной оплаты. Отличительной чертой данной утилиты является количество поддерживаемых браузеров, а также их beta и dev версий, что является несомненным преимуществом над другими программными средствами: Google Chrome (+ beta версия), Microsoft Edge, 360 Speed, QQ, Brave, Opera, Opera GX, Yandex, Firefox (+ beta, dev, ESR версии). Несмотря на то, что данный программный продукт необходимо устанавливать в исходную систему, он является кроссплатформенным и поддерживает операционные системы: Windows, MacOS, Linux. В результате работы программы, криминалист получает систематизированный список csv файлов с информацией об закладках, историей браузера, файлах cookie и сохранённых паролей пользователя.

Среди преимуществ Hack Browser Data Tool представлены: ПО поддерживает работу в большем количестве браузеров, среди которых есть бета версии и версии для разработчиков, Hack Browser Tool является продуктом с открытым исходным кодом. К недостаткам данного программного обеспечения можно отнести: сравнительно ограниченный и специфический функционал и отсутствие графического интерфейса (работа в программе реализована через командную строку).

Как и Hack Browser Data Tool, утилита Hindsight является программным продуктом с открытым кодом. Она является бесплатным инструментом для анализа информации, полученной из браузеров на базе движка Chromium. Среди поддерживаемых браузеров есть такие как: Google Chrome, Yandex, Opera, Chromium, Safari.

В отличие от Hack Browser Data Tool, Hindsight имеет графический интерфейс для взаимодействия с пользователем, который работает на основе web сервера, локально устанавливаемого в ОС компьютера. Утилита может анализировать URL-адреса, историю загрузок, записи кэша, закладки, записи автозаполнения, сохраненные пароли, настройки, расширения браузера, HTTP-файлы cookie и записи локального хранилища (файлы cookie HTML5). После извлечения данных из каждого файла они сопоставляются с данными из других файлов истории и помещаются на временную шкалу. Единственное поле, которое необходимо заполнить – это путь к профилю пользователя, затем утилита соберёт данные из установленных браузеров и сохранит отчёт в формате csv, который затем может анализировать криминалист. Преимуществами данного программного продукта является большой выбор поддерживаемых браузеров, а также графический интерфейс.

В качестве программного обеспечения для анализа накопителей или их отдельных разделов используют специальные Live CD/USB дистрибутивы, которые содержат специальные утилиты для анализа и расследования

информации, полученной из браузеров. К примеру, в популярном у криминалистов Live дистрибутиве Kali Linux Forensics Mode [3] встроена утилита Dumpzilla, которая позволяет выгружать необходимую информацию из веб-браузеров подозреваемого.

Среди преимуществ данного программного обеспечения представлены следующие возможности: извлечение файлов cookie, получение пользовательских настроек браузера, а именно: разрешения домена, настройки прокси и т. д., просмотр загрузок и веб форм, содержащие поисковые запросы пользователя, визуализация и извлечение кэша HTML5, а также «эскизов» посещённых сайтов, извлечение сохранённых паролей в браузере, а также данных текущего сеанса: веб-сайты, URL-адреса ссылок и текст, используемый в формах, визуализация живого пользовательского сёрфинга, просмотр SSL сертификатов, добавленных в качестве исключения.

Недостатками данного программного обеспечения являются ограниченное число поддерживаемых браузеров, а также отсутствие web интерфейса при взаимодействии с ним.

Сравнительный анализ программных средств для экспертизы доказательств, которые может получить криминалист при анализе web браузеров, представлен в таблице 1 (см. на след. стр.).

Среди описанных программных продуктов для анализа web-браузеров представлены как утилиты с широким функционалом, так и очень ограниченные в использовании. Несмотря на это, невозможно определить, какое из программных средств будет использовать специалист, когда перед ним будет стоять та или иная задача.

Также представленные программные продукты не всегда могут иметь нужный функционал сбора, анализа данных или необходимый формат вывода данных, так как одной из важнейших частей расследования киберпреступлений является формирование и представление отчёта в понятном для получателя виде [4].

Исходя из этого можно сделать вывод, что универсального программного средства для сбора и анализа данных из web-браузеров на данный момент не существует, исходя из специфичности задач, которые данное ПО помогает реализовать эксперту-криминалисту [5].

Исследование выполнено за счет гранта Российского научного фонда No 18-71-10094, https://rscf.ru/project/18-71-10094/».

Список используемых источников

1. 15 лучших и бесплатных инструментов компьютерного криминалиста [Электронный ресурс] // URL: https://habr.com/ru/company/tomhunter/blog/660773/ (дата обращения 19.01.2023).

2. Keith J. Jones, Rohyt Belani. Экспертиза web-браузеров, часть 1 [Электронный ресурс] // URL: https://www.securitylab.ru/analytics/216398.php (дата обращения

18.01.2023).

3. Отдел расследования инцидентов: Наша подборка программ для проведения forensic-расследований [Электронный ресурс] // URL: https://xakep.ru/2011/04/21/55219/ (дата обращения 17.01.2023).

4. Kolomeec M., Gonzalez-Granadillo G., Doynikova E., Chechulin A., Kotenko I., and Debar H. Choosing models for security metrics visualization // Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag. Vol. 10446. PP. 75–87.

5. Проноза А. А., Виткова Л. А., Чечулин А. А., Котенко И. В., Сахаров Д. В. Методика выявления каналов распространения информации в социальных сетях // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2018. Т.14, N 4. С. 362–377.

ТАБЛИЦА 1. Анализ программных средств

Утилита Параметр	Browser History Examiner	Web Historian	Forensic Tool Kit	Hack Browser Tool	Hindsight	Dumpzilla
Лицензирование	Годовая подписка 279$	Свободное ПО	Свободное ПО	Свободное ПО с открытым кодом	Свободное ПО с открытым кодом	Свободное ПО с открытым кодом
Возможность извлечения данных	+	-	+	+	+	+
Формат вывода	PDF	HTML, XML, CSV.	HTML	CSV	CSV	WEB
Фильтры по категориям	Фильтр по дате и времени, по ключевым словам и категориям страниц	Фильтр по дате и времени, по ключевым словам	Фильтр по дате и времени	Фильтр по любому текстовому параметру	Фильтр по временной шкале	Фильтр по любому текстовому параметру
Поддерживаемые браузеры	Chrome, Edge. Firefox, Explorer 10/11, Safari	Explorer, Firefox, Opera, Safari	Chrome, Edge. Firefox, Explorer 10/11, Safari	Chrome, Edge, 360 Speed, QQ, Opera, Yandex, Firefox	Браузеры, основанные на Chromium	Chrome, Firefox, IE и Edge
Восстановление из теневых копий	+	-	-	+	-	-
Извлечение данных удалённо	+	-	-	-	-	-
Просмотр кэшированных страниц	+	+	+	-	-	+
Просмотр загрузок пользователя	+	-	+	-	-	+

УДК 621.391.6
ГРНТИ 49.44.01

МОНИТОРИНГ ФИЗИЧЕСКОЙ СРЕДЫ ОПТИЧЕСКОЙ СЕТИ ДОСТУПА

Н. И. Горлов

Сибирский государственный университет телекоммуникаций и информатики

Статья посвящена вопросам мониторинга в физических средах оптических сетей доступа. Обосновано применение технологии, основанной на принципах рассеяния Мандельштама – Бриллюэна. Представлены расчетные соотношения, позволяющие оценить основные функциональные возможности бриллюэновской рефлектометрии во временной области. Проанализирована возможность проведения мониторинга физических каналов древовидной топологии оптической сети доступа методом анализа Бриллюэна во временной области с помощью конечных отражений.

мониторинг, пассивная оптическая сеть, физическое напряжение, рассеяние Бриллюэна, метод конечных отражений.

Введение

Число пользователей услуг *fiber to the home* (*FTTH*) быстро растет, и операторы связи прилагают усилия для снижения затрат на техническое обслуживание, связанных с огромным количеством оптического оборудования. Для предоставления услуги FTTH в оптической сети доступа обычно используется пассивная оптическая сеть (*passive optical network – PON*), которая уменьшает требования к оптическому кабелю и обслуживающему его оборудованию провайдера. Однако, при этом возникает проблема диагностики, связанная с дистанционным мониторингом параметров PON.

Традиционная оптическая рефлектометрия во временной области (*Optical Time Domain Reflectometer – OTDR)* уже нашла практическое применение в качестве технологии дистанционного тестирования. Однако, когда в сети доступа установлен оптический разветвитель, сигналы обратного рассеяния от разветвленных волокон за разветвителем перекрываются на магистральном волокне. По этой причине определить неисправность в отдельно взятой ветви древовидной топологии с несколькими разветвителями и абонентскими узлами из центрального офиса с помощью OTDR становится проблематичным. В этой связи сокращение операций по техническому обслуживанию, осуществляемое за счет использование дистанционного тестирования OTDR, остается ограниченным. С другой стороны, в большинстве широко используемых оптоволоконных сетей FTTH используются PON с наружным разветвителем. Все перечисленное

выше обуславливает острую необходимость разработки технологии удаленного тестирования за пределами разветвителя для нужд телекоммуникационной отрасли. Передаточные и механические параметры оптических волокон, используемых в PON, являются основой для разработки технологии. При этом важно исследовать их для практического применения.

1. Основы бриллюэновского оптического анализа во временно области

Оптический метод измерения, использующий рассеяние Бриллюэна, представляет собой метод, который использует линейную зависимость сдвига частоты Бриллюэна (BFS) от изменения температуры или деформации. Для определения BFS используется пиковая частота спектра усиления Бриллюэна (BGS), наблюдаемая с помощью функции подгонки. Рассеяние Бриллюэна – это неупругое рассеяние фотонов акустическими фононами. Сдвиг частоты Бриллюэна определяется соотношением

$$\nu_{\text{в}} = \frac{2nV_A}{\lambda_u}, \quad (1)$$

где υ_B – сдвига частоты Бриллюэна; n – показатель преломления материала сердцевины; V_A – скорость акустической волны; λ_u– длина волны света накачки.

Для оптического волокна из кремнезема (показатель преломления $n = 1{,}45$), при скорости звука $V_A = 5{,}96$ км/с сдвиг частоты, вызванный рассеянием Бриллюэна в полосе длин волн 1,55 мкм, составляет приблизительно 11.1 ГГц [2].

Методы измерения по Бриллюэну отслеживают линейное увеличение *BFS*, которое происходит при повышении температуры [3] или растягивающей деформации [4]. Эта зависимость обусловлена зависимостью акустической скорости в оптическом волокне от температуры и деформации.

Уравнения (2) и (3) выражают зависимость *BFS* от температуры и деформации при растяжении соответственно:

$$\nu_{\text{в}}(t) = \nu_{\text{в}}(t)[1 + C_t(t - t_r)], \quad (2)$$

$$\nu_{\text{в}}(\varepsilon) = \nu_{\text{в}}(0)[1 + C_s\varepsilon]. \quad (3)$$

Здесь t – температура, t_r – исходная температура, а ε – деформация при растяжении.

C_t и C_s являются линейными коэффициентами для изменений температуры и деформации1.10 МГц/℃ и 0.0483 МГц/$\mu\varepsilon$, соответственно, при длине волны 1553.8 нм [5].

Поскольку изменения температуры и деформации не могут быть измерены отдельно, изменение BFS $\delta V_{\text{В}}$ иногда выражается уравнением:

$$\delta\nu_{\text{в}}(t, \varepsilon) = C_t\delta t + C_{\varepsilon}\delta\varepsilon. \quad (4)$$

Здесь δ_t и δ_ε представляют собой изменения температуры и деформации соответственно. На практике для компенсации изменений температуры или деформации, не предназначенных для измерения, подготавливается эталонное оптическое волокно или эталонные данные.

Для определения BFS применяется подгонка к полученным BGS. BGS имеет форму, которая может быть аппроксимирована функцией Лоренца с центральной частотой V_B и шириной спектра на уровне 0,5 относительно максимума ΔV_B . В случае квадратурной подгонки погрешность измерения BFS может быть оценена с помощью уравнения [5].

$$\sigma_\nu(z) = \frac{1}{SNR(z)}\sqrt{\frac{3}{4}\delta * \Delta\nu_\text{в}}. \quad (5)$$

Здесь *SNR*(z) – отношение сигнал/шум (SNR) пика BGS в координате z, a, δ – шаг выборки частоты ($\delta \ll \Delta V_\text{B}$).

Уравнение (5) показывает, что обнаруживаемый минимум изменение BFS уменьшается обратно пропорционально SNR измеренного распределения BGS и увеличивается пропорционально квадратному корню из шага выборки частоты δ.

Бриллюэновский оптический анализ во временной области (BOTDA) измеряет интенсивность бриллюэновского рассеяния как функцию времени. Когда скорость отклика фотоприемника достаточно высока, пространственное разрешение соответствует ширине импульса света накачки.

Пространственное разрешение δz выражается уравнением [4]:

$$\delta z = \frac{\nu W_u}{2}. \quad (6)$$

Здесь V – групповая скорость света в оптическом волокне, а W_u – ширина импульса света накачки. Пространственное разрешение стандартного BOTDA ограничено 1 м. Это связано с тем, что время жизни фонона составляет около 10 нс, и трудно реализовать ширину импульса накачки менее 1 м.

2. Анализа Бриллюэна с помощью конечных отражений (ERA-BA)

Недавно был предложен анализ Бриллюэна с помощью конечного отражения (ERA-BA), которые могут измерять индивидуальные характеристики разветвленных волокон на основе BOTDA [5]. ERA-BA измеряет характеристики разветвленного волокна, анализируя коэффициент усиления по Бриллюэну, вызванный столкновением между импульсом накачки и зондирующим импульсом, отраженным от дальнего конца ответвления. Метод измерения разветвленных волокон ERA-BA позволяет проводить удаленное тестирование всех оптических сетей доступа, которые включают разветвленные волокна, и значительно сокращает количество операций на месте. Можно ожидать, что это обеспечить высококачественное техническое обслуживание чрезвычайно крупных сетевых объектов при низких затратах

и с небольшой рабочей силой. Рис. 1 представляет собой схематическую иллюстрацию, показывающую принцип работы ERA-BA.

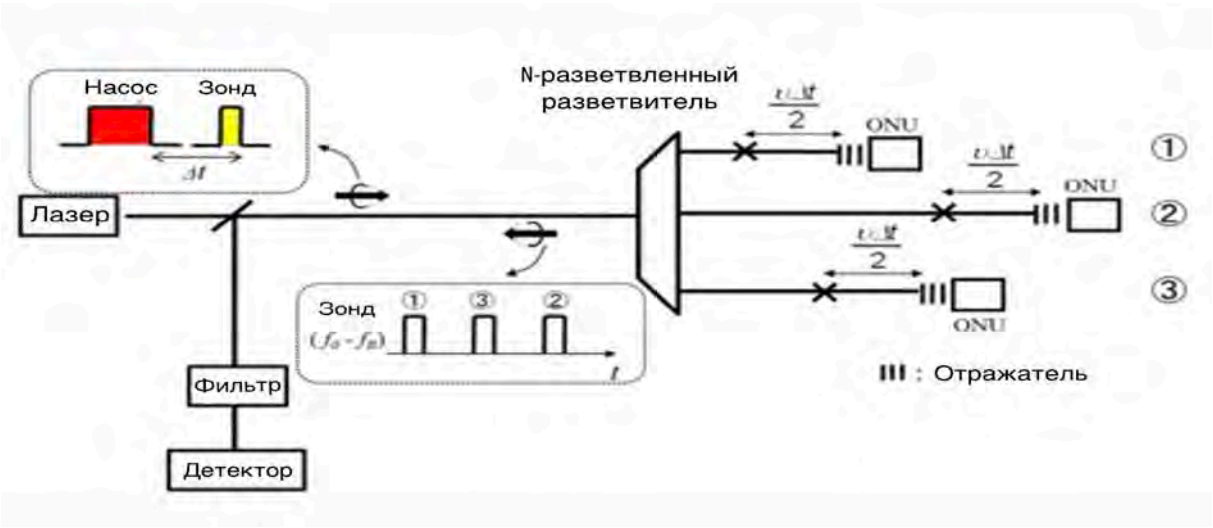


Рис. 1. Схематическая иллюстрация принципа ERA-BA

ERA-BA – это оптический метод измерения, который измеряет характеристики каждого разветвленного волокна со стороны магистрального волокна. Здесь характеристиками являются оптические потери, а также изменения температуры и деформации. Характеристики разветвленного волокна измеряются с помощью анализа усиления Бриллюэна с использованием столкновения между импульсом накачки и зондирующим импульсом, возвращающимся с дальнего конца ответвления. Зависимость интенсивности усиления по Бриллюэну на мощности насоса полезно для измерения потерь в ответвлениях. Между тем, BFS, который изменяется в зависимости от изменений температуры и деформации, измеряется для определения оптического волокна с разветвленной топологией волокна.

Чтобы вызвать столкновение тестовых импульсов в разветвленных волокнах, нам нужен оптический фильтр, который отражает пробный импульс на дальнем конце разветвленного волокна. Импульс накачки запускается после зондирующего импульса с временной задержкой Δtдля столкновения в положении $V\Delta t/2$ от дальнего конца. Измерение распределения возможно путем последовательного изменения времени задержка Δt. Чтобы эффективно генерировать дальнее отражение в существующей сети доступа, мы можем использовать тестовый фильтр отсечки света, как рекомендовано в ITU–T L.66.

С другой стороны, при зондировании с разветвленным волокном мы можем использовать фильтр FBG или фильтр полного отражения, рассчитанный на длину волны зонда.

Разница во времени обратного хода возвращенных зондирующих импульсов, вызванная разной длиной разветвленных волокон, используется для определения сигналов от разветвленного волокна. Чтобы идентифицировать разветвленные волокна, нам, по крайней мере, нужна разница в длине разветвления δL, выраженная по уравнению

$$\delta L = \frac{\nu W_r}{2}, \quad (7)$$

где W_r – это длительность зондирующего импульса.

Для телекоммуникационных сетей, поскольку разветвленное волокно длины случайным образом различаются на несколько метров, целевая производительность разрешения идентификации волокна должна быть равна или превышать это значение.

При распознавании разветвленных волокон разность длин ответвлений может быть произвольно установлена с помощью дополнительного волокна задержки. Пространственное разрешение может быть определено уравнением (7) с использованием ширины импульса накачки, как в обычном BOTDA.

Заключение

Проанализированный в докладе метод проведения мониторинга физических каналов древовидной топологии пассивной оптической сети методом анализа Бриллюэна во временной области с помощью конечных отражений в достаточной степени соответствует критериям обслуживания оптоволоконного кабеля для тестирования волокна в процессе эксплуатации в сетях доступа *ITU–T L.66*, (2007).

Список используемых источников

1. Tateda M., Tanaka S. and Sugawara Y. // Appl. Opt., 19, 770, 1980.

2. Agrawal G. P. Nonlinear Fiber Optics 4th edition, Academic Press, (2007).

3. Kurashima T., Horiguchi T., and M. Tateda M. Thermal effects on Brillouin frequency shift in jacketed optical silica fibers // Appl. Opt. 1990. Vol. 29, No.15. PP. 2219–2222.

4. Horiguchi T., Kurashima T.and Tateda M. Tensile strain dependence of Brillouin frequency shift in silica optical fibers // IEEE Photon. Tech. Lett. 1989. Vol. 1, No. 5. PP. 107–108.

5. Soto M. A. and Thévenaz L. Modeling and evaluating the performance of Brillouin distributed optical fiber sensors // Opt. Express. 2013. Vol. 21, No. 25. PP. 31347–31366.

УДК 621.372.8: 621.396: 621.315
ГРНТИ 47.13.85

КЛАССИФИКАЦИЯ И ОБЛАСТЬ ПРИМЕНЕНИЯ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ НА ПРИНЦИПЕ РАССЕЯНИЯ МАНДЕЛЬШТАМА-БРИЛЛЮЭНА

Н. И. Горлов

Сибирский государственный университет телекоммуникаций и информатики

Статья посвящена классификации и области применения волоконно-оптических датчиков на принципе рассеяния Мандельштама-Бриллюэна. В нем представлена математическая модель процесса получения измерительной информации по результатам анализа спектра обратно рассеянного сигнала. Особый интерес представляют волоконно-оптические датчики для контроля целостности трубопровода и для охраны/ограждение по периметру.

оптическое волокно, волоконно-оптический датчик, рассеяние Мандельштама–Бриллюэна, бриллюэновский сдвиг частоты.

Введение

Волоконно-оптический датчик в общем случае состоит из подводящего волоконно-оптического кабеля и преобразователя сигналов. При этом оптическое волокно используется одновременно в качестве чувствительного элемента и линии передачи данных. Датчики преобразуют измеряемые величины, такие как деформация, температура, давление из физического мира в сигналы, которые могут быть считаны в электронной форме.

1. Постановка проблемы

Рассеяние Бриллюэна приводит к появлению двух дополнительных частот по обе стороны от центральной частоты спектра зондирующего сигнала (рис. 1, см. ниже).

На рис. 1 используются следующие обозначения: λ_0 – центральная длина волны импульса накачки; T – температурное воздействие на оптическое волокно; ε – параметр деформации.

Частота υ_B линий Бриллюэна определяется условием согласования акустического и оптического волновых фронтов [1]. Она определяется соотношением

$$\upsilon_B = 2n_1 \frac{V_A}{\lambda}\left(\frac{1}{2}\theta\right), \quad (1)$$

где n_1 – эффективный коэффициент преломления; V_A – акустическая скорость; θ – угол между лучами рассеянного и падающего потока.

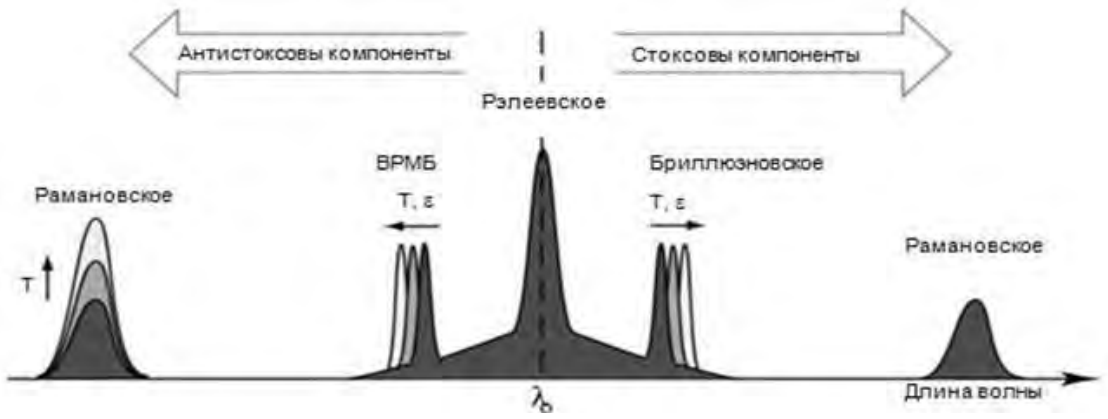


Рис. 1. Спектры обратнорассеянных сигналов

Спектр сигнала бриллюэновского рассеяния сдвинут приблизительно 10 ГГц, в то время как спектр комбинационного рассеяния на 13 ТГц. При этом ширина спектра рассеяния Бриллюэна значительно меньше, чем у комбинационного рассеяния. Все эти количественные различия сделали рассеяние Бриллюэна гораздо более универсальным, чем комбинационное рассеяние для распределенного зондирования.

Соотношения между сдвигом частоты и интенсивностью сигнала бриллюэновского рассеяния в зависимости от температуры и деформации удобно выразить матрицей 2 × 2 [2]

$$\begin{bmatrix}\Delta\upsilon_B\\ \Delta I_B\end{bmatrix}=\begin{bmatrix}C_{\upsilon_B\varepsilon} & C_{\upsilon_B T}\\ C_{I_B\varepsilon} & C_{I_B T}\end{bmatrix}. \quad (2)$$

В этой матрице приняты следующие обозначения: $C_{\upsilon_B\varepsilon}$, $C_{\upsilon_B T}$ – коэффициенты сдвига частоты; $C_{I_B\varepsilon}$, $C_{I_B T}$ – коэффициенты интенсивность.

Эти коэффициенты характеризуют изменения частоты и интенсивности от деформации Δε и температуры ΔT и могут быть определены экспериментально для конкретного типа оптического волокна.

При условии, что определитель этой матрицы отличен от нуля, его можно инвертировать, чтобы измеренные изменения частоты и интенсивности можно было использовать для определения температуры и деформации относительно некоторой базовой линии следующим образом:

$$\begin{bmatrix}\Delta\varepsilon\\ \Delta T\end{bmatrix}=\frac{1}{|C_{\upsilon_B\varepsilon}C_{I_B T}-C_{I_B\varepsilon}C_{\upsilon_B T}|}\begin{bmatrix}C_{I_B T} & -C_{\upsilon_B T}\\ -C_{I_B\varepsilon} & C_{\upsilon_B\varepsilon}\end{bmatrix}. \quad (3)$$

Значения коэффициентов чувствительности для типичных одномодовых волокон представлены ниже:

$$\begin{bmatrix} C_{\upsilon_B\varepsilon} & C_{\upsilon_B T} \\ C_{I_B\varepsilon} & C_{I_B T} \end{bmatrix} = \begin{bmatrix} 0{,}046\ \text{Мгц/мк}\varepsilon & 1{,}07\ \text{МГц/К} \\ -8\cdot 10^{-4}\%/\text{мк}\varepsilon & 0{,}36\%/\text{К} \end{bmatrix}.$$

2. Классификация датчиков

Оптоволоконные датчики выполняют функции мониторинга внешних факторов и передачи сигнала. По характеру влияния внешних факторов на параметры информационного сигнала они классифицируются по признакам модуляции интенсивности, фазы, поляризации и частоты. По принципу функционирования классифицируемые датчики делятся на два вида [2]:

– датчики, функционирующие во временной области;

– датчики, в которых используется зондирующий сигнал с частотной модуляцией.

Все датчики предполагают ввод зондирующего сигнала либо с одного конца оптического волокна (*Brillouin Optical Time-Domain Reflectometry* – BOTDR) [3], либо с обоих концов (*Brillouin optical time-domain analysis* – BOTDA [4]). Методы зондирования оптического волокна на основе рассеяния Бриллюэна представлены в таблице 1.

ТАБЛИЦА 1. Методы зондирования оптического волокна на основе рассеяния Бриллюэна

Схема зондирования	Временная область	Частотная область	Корреляционная область
Зондирование с одного конца	Бриллюэновский оптический рефлектометр во временной области (BOTDR)	Бриллюэновский оптический рефлектометр в частотной области (BOFDR)	Бриллюэновский оптический рефлектометр в корреляционной области(BOCDR)
Зондирование с двух концов	Бриллюэновский оптический анализатор во временной области (BOTDA)	Бриллюэновский оптический анализатор в частотной области (BOFDA)	Бриллюэновский оптический анализатор в корреляционной области (BOCDA)

В схеме зондирования с одного конца происходит инжекция оптической волны накачки в тестируемое волокно с последующим детектированием обратного сигнала спонтанного рассеянного Бриллюэна. В схеме зондирования с двух концов достигается режим стимулированного рассеяния Бриллюэна. Рассматривая области взаимодействия оптических волн можно выделить три подкатегории: временная область, частотная область и корреляционная область. В методе временной области достигается высокое отношение сигнал/шум, большое расстояние зондирования, но пространственная разрешающая способность остается низкой. В методе частотной области достигается высокая чувствительность и широкий диапазон зондирования. Метод корреляционной области обеспечивает высокую пространственную

разрешающую способность, но он подходит для зондирования точек с высокой частотой дискретизации.

Для улучшения метрологических характеристик датчиков существует множество методов: оптическое усиление, когерентное детектирование, самогетеродинное обнаружение, мультиплексирование с разделением по времени, мультиплексирование с частотным кодом, дифференциальное усиление Бриллюэна, мультиплексирование зонда с накачкой по времени и частоте.

Для измерения дифференциального бриллюэновского усиления вместо самого бриллюэновского усиления был предложен метод дифференциального бриллюэновского оптического анализа во временной области (DPP-BOTDA), который обладает высоким пространственным разрешением. В этом методе используются два разных зондирующих импульса, отличающихся небольшой разницей в длительности. Дифференциальный спектр усиления получается путем вычитания двух спектров усиления Бриллюэна, а пространственное разрешение определяется разностью длительностей зондирующих импульсов.

Датчики OTDR на основе мультиплексирования с разделением длин волн, в которых зондирующий сигнал содержит несколько длин волн с малым интервалом между ними, имеют высокое соотношение сигнал/шум. Однако, в этих датчиках существует реальная опасность возникновения продуктов нелинейного преобразования. Поэтому в датчиках этого типа используется мультиплексирование с различной задержкой во временной области и неравномерный частотный интервал.

3. Основные области применения

Ниже описываются основные области применения распределенных датчиков на принципе рассеяния Бриллюэна:

1. Телекоммуникации. Одним из первых применений распределенного тензодатчика был мониторинг установки многоволоконных кабелей в каналах, где часть усилий, передаваемых кабелю, передается волокнам. Эта работа продемонстрировала деформацию волокон порядка 0,06 %, что все еще значительно ниже уровня, при котором статическая деформация ухудшила бы срок службы большинства волокон. Однако, это показало, что, несмотря на использование конструкции кабеля с прорезями, предназначенной для изоляции волокон от напряжения на кабеле, часть усилий все же передается на волокна.

2. Энергетические кабели. BOTDR был предложен для мониторинга воздушных линий электропередачи. Провода заземления, которые проходят над фазными проводниками в высоковольтных линиях передачи, все чаще включают оптические волокна для связи. Кроме этого, провода заземления с оптической поддержкой известны как оптический провод заземления.

Требуемая информация – это температура и связанная с ней деформация, вызванная тепловым расширением. Последнее привело бы к деформации волокон внутри оптического провода заземления, поскольку они соединены с проволокой.

3. Гражданское строительство. В гражданском строительстве мониторинг изменений размеров конструкции может обеспечить раннее предупреждение о начинающемся разрушении. Используются многие существующие методы, такие как тензодатчики и хрупкие контрольные пластины, но в крупномасштабных конструкциях установка достаточного количества точечных датчиков является дорогостоящей и подверженной поломке. Кроме того, детали, вызывающие озабоченность, могут быть недоступны для осмотра. Таким образом, распределенное волоконно-оптическое зондирование может восполнить этот пробел.

4. Охрана/Ограждение по периметру. Большинство волоконно-оптических систем обнаружения вторжений основаны на акустических сигналах. Однако существуют примеры квазистатического напряжения, создаваемого волокном в результате присутствия постороннего, используемого непосредственно для обнаружения вторжения. Для этого приложения требуется быстрое обнаружение, и измерение обновлялось с интервалом в 1,5 секунды для предполагаемого уровня деформации 0,01 %. В реальном приложении датчик может использоваться, например, для определения деформации грунта.

Заключение

Волоконно-оптические датчики на эффекте рассеяния Бриллюэна позволяют производить измерения широкого спектра параметров с достаточно высокой точностью и пространственной разрешающей способностью. Последние публикации по вопросам оптического зондирования свидетельствуют о расширении функциональных возможностей проанализированных датчиков.

Список используемых источников

1. Heiman D., Hamilton D. S., Hellwarth R. W. Brillouin scattering measurements on optical glasses // Phys. Rev. B 1979, 12. PP. 6583–6585.

2. Zhang H., Zhou D., Wang B., Xu P., Li H., Dong Y. “Recent Progress in Fast Distributed Brillouin Optical Fiber Sensing” // Appl. Sci. 2018, 8, 1820; doi:10.3390/app8101820.

3. Zhou D., Dong Y., Wang B., Pang C., Ba D., Zhang H., Lu Z., Li H., Bao X., “Single-shot BOTDA based on an optical chirp chain probe wave for distributed ultrafast measurement” // Light Sci. Appl. 2018, 7, 32. PP. 574–579.

4. Bao X., Chen L., “Recent Progress in Brillouin Scattering Based Fiber Sensors” // Sensors. 2011. 11, No 2. PP. 102–117.

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ РАБОЧИХ ХАРАКТЕРИСТИК АЛГОРИТМА 2D-MUSIC ДЛЯ ЧАСТОТНОГО ДИАПАЗОНА FR2 В СЕТЯХ МОБИЛЬНОЙ СВЯЗИ НОВОГО ПОКОЛЕНИЯ

И. В. Гришин, А. Ю. Казакова, Д. В. Окунева

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлен анализ метода обработки поля в раскрыве плоской антенной решетки 2D-MUSIC, позволяющий определить направление приема сигналов, поступающих от пользовательских устройств, работающих в миллиметровом диапазоне длин волн в сверхплотных сетях и разнесённых по угловым координатам друг от друга на интервал меньший релеевского интервала разрешения. Приведенные результаты эксперимента, позволяют оценить рабочие характеристики рассматриваемого метода.

2D-MUSIC, азимут, угол места, абонентский терминал, антенная решетка.

Одним из основных показателей эксплуатационных характеристик сети нового поколения согласно рекомендациям Международного союза электросвязи является увеличение пропускной способности сети более чем на порядок. Эффективным решением, позволяющим добиться такого резкого скачка в скоростях передачи данных конечным пользователям, является переход в миллиметровый диапазон длин волн FR2. Следует учитывать, что для передачи данных в диапазоне FR2 характерны значительные потери на трассе: как в открытом пространстве, так и обусловленные отражением и рассеянием. В связи с этим в [1] отмечается, что в случае предоставления услуг беспроводного абонентского доступа в диапазоне FR2 рядом преимуществ обладают системы передачи данных низкой мощности и малого радиуса действия. Также в миллиметровом диапазоне антенные элементы могут быть интегрированы в малый форм-фактор, что позволяет задействовать технологию формирования трехмерной диаграммы направленности с целью компенсации высоких потерь при распространении радиоволн.

Для формирования требуемой диаграммы направленности антенная решётка базовой станции должна располагать сведениями о количестве абонентских терминалов, находящихся в пределах соты, и их координатах.

Наибольшую популярность при определении направления на источник сигнала получили подпространственные методы, такие как ESPRIT

и MUSIC. Целью данной работы является анализ рабочих характеристик модифицированного алгоритма 2D-MUSIC для систем беспроводной связи, работающих в диапазоне FR2 и использующих прямоугольные антенные решётки URA.

Математическая модель канала MIMO для одного абонентского терминала, передающего символ с номером t в передаваемой последовательности, может быть описана выражением:

$$\dot{\mathbf{H}}(t)=\sum_{l=1}^{L}\dot{h}_l(t)\sqrt{N_T N_R}\,\dot{\mathbf{a}}_R\left(\theta_{R,l}(t),\varphi_{R,l}(t)\right)\dot{\mathbf{a}}_T^H\left(\theta_{T,l}(t),\varphi_{T,l}(t)\right), \quad (1)$$

где t – номер передаваемого символа, L – количество путей распространения радиоволн, $\dot{h}_l(t)=\left|\dot{h}_l(t)\right|\exp\left(j\psi_l(t)\right)$ – комплексный отклик радиоканала для l-го пути распространения, $\psi(t)$ – параметр, определяющий время распространения фронта волны до точки наблюдения из произвольной точки раскрыва, N_R, N_T – количество элементов в антенных решётках (АР) базовой станции (БС) и абонентского терминала (АТ), $[\ ]^H$ – эрмитово сопряжение, $\dot{\mathbf{a}}_{R,l}\left(\theta_{R,l}(t),\varphi_{R,l}(t)\right)$, $\dot{\mathbf{a}}_T\left(\theta_{T,l}(t),\varphi_{T,l}(t)\right)$ – комплексные векторы отклика АР БС и АТ, определяемые как:

$$\dot{\mathbf{a}}_R\left(\theta_{R,l}(t),\varphi_{R,l}(t)\right)=N_R^{-1/2}\exp\left(-j\mathbf{x}_R^T\boldsymbol{\beta}\left(\theta_{R,l}(t),\varphi_{R,l}(t)\right)\right),$$

$$\dot{\mathbf{a}}_T\left(\theta_{T,l}(t),\varphi_{T,l}(t)\right)=N_T^{-1/2}\exp\left(-j\mathbf{x}_T^T\boldsymbol{\beta}\left(\theta_{T,l}(t),\varphi_{T,l}(t)\right)\right),$$

где $\theta_{R,l}(t)$, $\theta_{T,l}(t)\in\left[-\pi/2 \quad \pi/2\right]$ – угол места направления приёма/ передачи сигнала для l-го пути распространения, $\varphi_{T,l}(t)$, $\varphi_{T,l}(t)\in\left[-\pi/2 \quad \pi/2\right]$ – азимутальный угол направления приёма/ передачи сигнала для l-го пути распространения, $\mathbf{x}_R=\left[\mathbf{x}_{R,1}\ \mathbf{x}_{R,2}\ldots\ \mathbf{x}_{R,N_R}\right]$ – матрица декартовых координат элементов АР стороны приема (где $\mathbf{x}_{T,n}=\left[x_{T,n},\ y_{T,n},\ z_{T,n}\right]^T$, $n\in 1\ldots N_T$,), $\mathbf{x}_T$ определяется аналогично $\mathbf{x}_R$, $\boldsymbol{\beta}\left(\theta_{R,l}(t),\varphi_{R,l}(t)\right)$, $\boldsymbol{\beta}\left(\theta_{T,l}(t),\varphi_{T,l}(t)\right)$ – векторные волновые числа для АР БС и АТ, определяемые согласно выражению (с целью сокращения записи аргумент времени опущен):

$$\boldsymbol{\beta}\left(\theta_{R,l},\varphi_{R,l}\right)=2\pi\lambda^{-1}\left[\sin\left(\theta_{R,l}\right)\cos\left(\varphi_{R,l}\right),\ \sin\left(\theta_{R,l}\right)\sin\left(\varphi_{R,l}\right),\ \cos\left(\theta_{R,l}\right)\right]^T$$

$$\boldsymbol{\beta}\left(\theta_{T,l},\varphi_{T,l}\right)=2\pi\lambda^{-1}\left[\sin\left(\theta_{T,l}\right)\cos\left(\varphi_{T,l}\right),\ \sin\left(\theta_{T,l}\right)\sin\left(\varphi_{T,l}\right),\ \cos\left(\theta_{T,l}\right)\right]^T.$$

Как было указано выше, для систем, работающих в диапазоне FR2, наилучшим является сценарий, при котором радиус соты является малым и ограничивается несколькими десятками метров. В таком случае можно

сделать допущение о распространении сигналов в условиях прямой видимости и $L = 1$, что позволяет опустить индекс l в последующих выражениях. В таком случае принимаемый БС сигнал, представляющий аддитивную смесь сигналов, переданных M АТ, и аддитивного белого гауссового шума (АБГШ) может быть представлен выражением:

$$\dot{\mathbf{y}}(t) = \dot{\mathbf{w}}^H \dot{\mathbf{H}}(t) \dot{\mathbf{F}} \dot{\mathbf{s}}(t) + \dot{\mathbf{n}}(t) = \dot{\mathbf{A}}(t) \dot{\mathbf{s}}(t) + \dot{\mathbf{n}}(t), \quad (2)$$

где $\dot{\mathbf{F}} = [\dot{\mathbf{f}}_1 \ldots \dot{\mathbf{f}}_m \ldots \dot{\mathbf{f}}_M]^T$, $\dot{\mathbf{f}}_m \in \mathbb{C}^{N_T \times 1}$ – вектор формирования луча АР m-го АТ, $\dot{\mathbf{w}} \in \mathbb{C}^{N_R \times 1}$ – комплексный вектор весовых коэффициентов АР БС, – вектор сигнала, переданных M АТ , $\dot{\mathbf{n}}(t)$ – вектор АБГШ, присутствующий на элементах АР с нулевым средним и дисперсией σ^2., $\dot{\mathbf{s}} \in \mathbb{C}^{N_T \times 1}$ – вектор линейной комбинации переданных сигналов от M АТ, $\dot{\mathbf{A}}(t) = \dot{\mathbf{w}}^H \dot{\mathbf{H}}(t) \dot{\mathbf{F}}$.

С целью вычисления количества источников излучения, в качестве которых выступают АТ, и определения их угловых координат должна быть найдена ковариационная матрица сигнала $\dot{\mathbf{y}}(t)$, которая согласно (2) будет иметь вид:

$$\begin{aligned} \dot{\mathbf{R}} &= E\left\{\dot{\mathbf{y}}(t)\dot{\mathbf{y}}^H(t)\right\} = \dot{\mathbf{A}} E\left\{\dot{\mathbf{s}}(t)\dot{\mathbf{s}}^H(t)\right\}\dot{\mathbf{A}}^H + E\left\{\dot{\mathbf{n}}(t)\dot{\mathbf{n}}^H(t)\right\} = \\ &= \dot{\mathbf{A}}\dot{\mathbf{R}}_S\dot{\mathbf{A}}^H + \sigma^2\mathbf{I}_{N_R} = \dot{\mathbf{U}}_S\dot{\mathbf{E}}_S\dot{\mathbf{U}}_S^H + \sigma^2\dot{\mathbf{U}}_n\dot{\mathbf{U}}_n^H(t) = \dot{\mathbf{U}}_R\dot{\mathbf{E}}_R\dot{\mathbf{U}}_R^H \end{aligned} \quad (3)$$

где $\mathbf{E}_R = diag\left\{e_1, e_2, \ldots, e_{N_R}\right\}$, $e_1 \geq e_2 \geq \ldots \geq e_{N_R-1} \geq e_{N_R} \geq 0$ – матрица собственных значений $\dot{\mathbf{R}}$, $\dot{\mathbf{U}}_R = \left[\dot{\mathbf{u}}_1, \dot{\mathbf{u}}_2, \ldots, \dot{\mathbf{u}}_{N_R}\right] = \left[\dot{\mathbf{U}}_S, \dot{\mathbf{U}}_n\right]$ – матрица собственных векторов, $E\left\{\dot{\mathbf{n}}(t)\dot{\mathbf{n}}(t)^H\right\} = \sigma^2\mathbf{I}_{N_R}$ – ковариационная матрица АБГШ, $\mathbf{I}_{N_R}$ – единичная матрица размерности N_R, $\dot{\mathbf{E}}_S = \dot{\mathbf{E}}_R - \sigma^2\mathbf{I}_{N_R}$ – матрица собственных значений полезного сигнала. Матрица $\dot{\mathbf{U}}_S$, состоящая из $\hat{M}$ собственных векторов $\dot{\mathbf{R}}$ определяет сигнальное подпространство, $\dot{\mathbf{U}}_n$ – матрица из $N_R - \hat{M}$ собственных векторов $\dot{\mathbf{R}}$ определяет подпространство шумов [2].

Значение величины оценки количества АТ $\hat{M}$ определяется количеством собственных значений, для которых справедливо условие $e_1 \geq e_2 \geq \ldots \geq e_{\hat{M}} \geq \sigma^2$. Такая оценка может быть произведена согласно информационному критерию Акаике [3, 4], при котором ищется минимум функции вида:

$$AIC(\hat{M}) = -T \cdot \left(N_R - \hat{M}\right) \ln \left[\frac{\prod_{i=\hat{M}+1}^{N_R} e_i^{\left(N_R - \hat{M}\right)^{-1}}}{\left(N_R - \hat{M}\right)^{-1} \sum_{i=\hat{M}+1}^{N_R} e_i} \right] + \hat{M} \cdot \left(2N_R - \hat{M}\right), \quad (4)$$

В таблице 1 приводятся результаты эксперимента по определению количества АТ $\hat{M}$ согласно критерию (4) для M = 14 и различных значений сигнал/шум SNR, дБ и количества элементов у АР N_R.

ТАБЛИЦА 1. Оценка количества АТ согласно критерию Акаике

Параметр	Значение								
Кол-во АТ:	14								
Кол-во элементов у АР АТ:	4								
Кол-во элементов у АР БС:	256	64	16	256	64	16	256	64	16
Отношение сигнал/шум, дБ:	25.6	26	27.3	16	16	16	–3.9	–3.4	–3.7
Кол-во обнаруженных АТ:	12	11	15	12	10	15	10	6	15

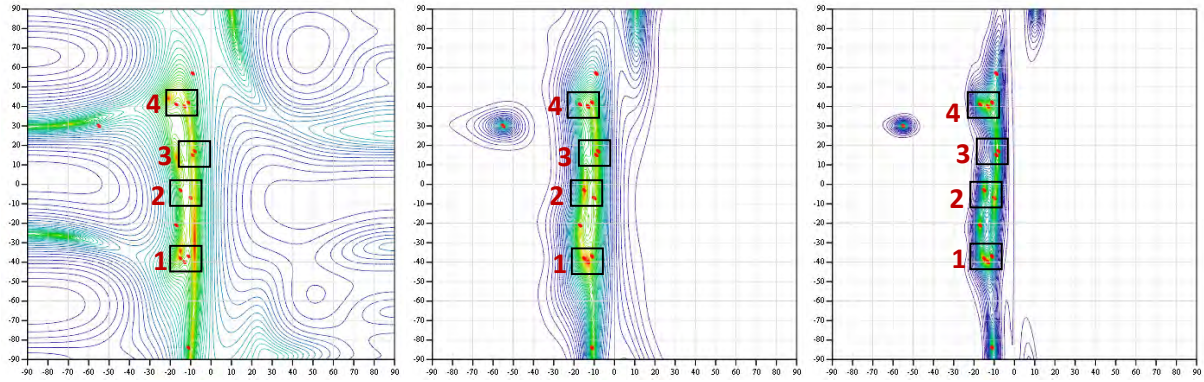
Как показывают приведённые в таблице 1 данные, АБГШ оказывает существенное влияние на точность расчётов. Не менее важное влияние оказывает количество элементов АР. Так для N_R = 16 оценка $\hat{M} > M$ вне зависимости от значения величины SNR.

Векторы отклика антенной решётки являются ортогональными подпространству шума. Данный факт позволяет определить угол места и азимут источников излучения путем нахождения функции пространственного спектра:

$$S(\hat{\theta}_{R,p}, \hat{\varphi}_{R,p}) = \frac{1}{\dot{\hat{\mathbf{a}}}_{R,p}^H(\hat{\theta}_{R,p}, \hat{\varphi}_{R,p}) \dot{\mathbf{U}}_n \dot{\mathbf{U}}_n^H \dot{\hat{\mathbf{a}}}_{R,p}(\hat{\theta}_{R,p}, \hat{\varphi}_{R,p})}, \quad (5)$$

где $\hat{\theta}_{R,p}, \hat{\varphi}_{R,p}$ – оценки углов положения и азимута, $\dot{\hat{\mathbf{a}}}_{R,p}(\hat{\theta}_{R,p}, \hat{\varphi}_{R,p})$ – оценка вектора отклика элементов плоской эквидистантной АР базовой станции. С целью определения точностных характеристик алгоритма 2D-MUSIC был проведен ряд вычислительных экспериментов. Результаты одного из экспериментов, характерные для других экспериментов, приведены в виде графиков изолиний спектра, а также сведены в таблицу 2 (см. на след. стр.). На графиках изолиний области 1–4 соответствуют данным, представленным в ячейках таблицы 2, выделенных серым (обл. 1), зелёным (обл. 2), голубым (обл. 3) и коричневым (обл. 4) цветами соответственно. Выделение цветом ячеек в таблице осуществляется в случае отсутствия между двумя пиками пространственного спектра сигнала в области координат реального местоположения АТ провала величиной не менее 5 дБ [4], что означает то, что

вопрос о разрешении данных источников сигналов не решён. Угловые координаты реальных местоположений АТ на рис. 1 обозначены красным цветом.



а) б) в)

Рис. 1. Изолинии пространственного спектра N_R = 256
а) SNR = –4 дБ; б) SNR = 16 дБ; в) SNR = 26 дБ

Как видно из таблицы 2, для наилучших условий приёма сигналов АР с 256 элементами при соотношении сигнал/шум 26 дБ количество обнаруженных максимумов $S(\hat{\theta}_{R,p},\hat{\varphi}_{R,p})$, рассчитанных согласно (5) с шагом перебора в 1° по углу места и азимуту, составило 10. Это не соответствует оценке количества АТ $\hat{M}$, рассчитанной методом Акаике (табл. 1) $\hat{M}$ =12 (при действительном количестве АТ– 14). Для АР с 16 и 64 элементами количество максимумов, в свою очередь, составило 5 ($\hat{M}$ =15) и 9 ($\hat{M}$ =11) соответственно. На примере узлов 9 и 11 видно, что разрешение узлов, разнесённых по угловым координатам менее чем на 5°, оказывается невозможным. Для случаев обнаруженных АТ среднеквадратическое отклонение оценок угловых координат как по углу места, так и по азимуту составляет σ_{ang} = 2°. Данный факт приводит к необходимости уменьшения шаг перебора и проведения повторных расчётов спектра $S(\hat{\theta}_{R,p},\hat{\varphi}_{R,p})$ в области найденных максимумов. Для данного случая границы области поиска в точке локального максимума брались равными ±5° по азимуту и углу места, шаг перебора по азимуту и углу места составил 0,25°. Результаты эксперимента для источников сигнала (1 и 2) с координатами: $\theta_{T,1}$= –13,4°, $\varphi_{T,1}$= –39,7°; $\theta_{T,2}$= –11,4°, $\varphi_{T,2}$= –36,7° (см. табл.1) –приведены в виде графиков изолиний для соотношения сигнал/шум равного 26 дБ (рис. 2). Как видно из представленных графиков, разрешение АТ для сигналов, передаваемых в FR2 диапазоне, при шаге перебора в 0,25° оказывается возможным для источников с угловым разносом не меньшим чем 2° для антенн с $N_R \geq 256$ и большим 4° для антенн с $N_R \geq 64$ при значениях сигнал/ шум SNR ≥ 20 дБ.

ТАБЛИЦА 2. Значения оценок угловых координат абонентских терминалов

АТ	1	2	3	4	5	6	7	8	9	10	11	12	13	14
θ°	–13,4	–11,4	–17,2	–54,9	–10,6	–15,3	–9,4	–8,8	–14,8	–16,9	–9,7	–10,6	–8,5	–13,2
φ°	–39,7	–36,7	–21,1	30,1	–83,5	–38,1	14,9	57,4	–2,6	41,4	–7,1	41,6	16,8	40
Количество элементов АР БС N_R=16; SNR= –4 дБ														
χ°	–13	–13	–14	–	–12	–13	–11	–	–9	–16	–9	–	–11	–15
ψ°	–33	–30	–24	–	–77	–31	22	–	4	38	0	–	24	37
S, дБ	–1,7	–1,4	–0,9	нет	–2,4	–1,5	–2,2	нет	–2,5	–2,5	–2,6	нет	–2,2	–2,4
Количество элементов АР БС N_R=64; SNR= –4 дБ														
χ°	–12	–12	–11	–52	–8	–12	–11	–9	–12	–10	–12	–8	–10	–8
ψ°	–33	–33	–24	28	–77	–33	12	54	0	38	0	39	14	37
S, дБ	–0,1	–0,1	–0,3	–2,4	–0,6	–0,1	–0,7	–1,5	0	–1,1	0	–1	–0,7	–0,9
Количество элементов АР БС N_R=256; SNR= –4 дБ														
χ°	–11	–11	–15	–53	–9	–11	–6	–10	–13	–10	–13	–10	–6	–10
ψ°	–38	–38	–19	32	–81	–38	18	54	–1	43	–1	43	18	43
S, дБ	0	0	–0,8	–1,8	–0,9	0	–1	–2	–0,1	–1	–0,1	–1	–1	–1
Количество элементов АР БС N_R=16; SNR=16 дБ														
χ°	–11	–12	–12	–51	–8	–11	–12	–	–12	–10	–12	–7	–6	–7
ψ°	–43	–30	–15	33	–77	–41	12	–	–6	43	–10	39	24	39
S, дБ	–1,5	–1,6	–1,3	–1,8	–1,6	–1,6	–2,6	нет	–1,5	–2,7	–1,3	–0,9	–2,6	–0,9
Количество элементов АР БС N_R=64; SNR=16 дБ														
χ°	–12	–12	–15	–53	–9	–12	–7	–10	–13	–10	–13	–9	–7	–8
ψ°	–37	–37	–24	32	–81	–37	22	54	–1	43	–1	41	24	37
S, дБ	0	0	–1	–1,8	–1,3	0	–1,1	–2,3	–0,3	–1,2	–0,3	–1	–1	–0,9
Количество элементов АР БС N_R=256; SNR=16 дБ														
χ°	–13	–13	–15	–53	–9	–13	–6	–8	–13	–11	–13	–11	–7	–11
ψ°	–36	–36	–19	32	–81	–36	18	54	–1	42	–1	42	24	42
S, дБ	0	0	–0,6	–0,7	–1,5	0	–1,3	–2	–0,5	–0,1	–0,5	–0,1	–1,2	–0,1
Количество элементов АР БС N_R=16; SNR=26 дБ														
χ°	–6	–6	–12	–	–	–12	–	–	–12	–12	–12	–12	–	–12
ψ°	–40	–40	–14	–	–	–40	–	–	–6	42	–8	42	–	42
S, дБ	0	0	–2,3	нет	нет	–2,1	нет	нет	–1,8	–1,9	–1,5	–1,9	нет	–1,9
Количество элементов АР БС N_R=64; SNR=26 дБ														
χ°	–12	–12	–15	–53	–9	–12	–7	–10	–13	–11	–13	–11	–7	–11
ψ°	–37	–37	–19	32	–81	–37	12	54	–1	43	–1	43	14	43
S, дБ	0	0	–0,7	–1,7	–1,9	0	–1	–2,6	–0,1	–1,1	–0,1	–1,1	–1,1	–1,1
Количество элементов АР БС N_R=256; SNR=26 дБ														
χ°	–13	–13	–15	–53	–9	–13	–6	–7	–8	–11	–8	–11	–7	–11
ψ°	–36	–36	–19	32	–81	–36	18	58	–6	42	–6	42	24	42
S, дБ	–0,2	–0,2	–0,8	–0,6	–1,7	–0,2	–1,5	–1,4	–0,7	0	–0,7	0	–1,4	0

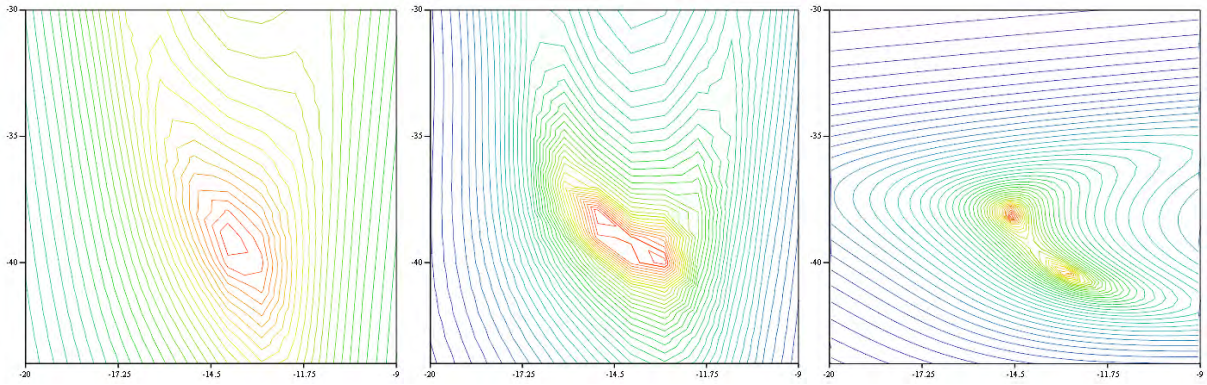


Рис. 2. Изолинии пространственного спектра SNR = 26 дБ, шаг – 0,25°
а) N_R = 16; б) N_R = 64; в) N_R = 256

Список используемых источников

1. Рекомендация МСЭ-R P.1411-11 «Данные о распространении радиоволн и методы прогнозирования для планирования наружных систем радиосвязи малого радиуса действия и локальных радиосетей в диапазоне частот от 300 МГц до 100 ГГц».

2. Баланис К. А., Иоанидес П. И. Введение в смарт-антенны / ред. В. В. Попов, М. Д. Парнес ; пер. К. В. Юдинцев. М. : РИЦ Техносфера, 2012. 200 с.

3. Madisetti V., Williams D. (ed.). Digital Signal Processing Handbook. CRC Press, 1997. 1776 p.

4. Ратынский М. В. Адаптация и сверхразрешение в антенных решетках. М. : Радио и связь, 2003. 197 с.

УДК 656.7.025
ГРНТИ 55.47.07

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ СТЕРЕОЗРЕНИЯ В БПЛА

И.С. Гурьянов, И. А. Кайсина

Ижевский государственный технический университет им. М. Т. Калашникова

В статье представлен обобщенный обзор БПЛА различного типа, перечислены типы полезных нагрузок и современные технологии. Выделено, что перспективным направлением развития отрасли считается повышение автономности БПЛА. Важной частью повышения автономности, в том числе в замкнутых пространствах может быть применение стереозрения. В статье предполагается, что стереозрение будет использоваться для обнаружения объектов и измерения расстояния до них с целью предотвращения столкновений. Представлен стенд для проведения дальнейших испытаний алгоритмов стереозрения.

беспилотный летательный аппарат, стереозрение, автономность.

Беспилотный летательный аппарат (далее БПЛА) – летательный аппарат, выполняющий полет без пилота (экипажа) на борту и управляемый в полете автоматически, оператором с пункта управления или сочетанием указанных способов [1]. По типу все БПЛА можно разделить на 5 групп:

– с жестким крылом,
– с гибким крылом,
– с машущим крылом,
– с вращающимся крылом,
– аэростатические [2].

По разнообразию конструкции существует 4 основных типа беспилотных летательных аппаратов:

- мультироторные (рис. 1),
- беспилотник самолетного типа (рис. 2),
- однороторный дрон – беспилотный вертолет (рис. 3),
- гибридные дроны (рис. 4).

Рис. 1. Мультикоптерный дрон

Рис. 2. Беспилотник с неподвижным крылом

Рис. 3. Однороторный дрон

Рис. 4. Гибридный дрон

Наиболее востребованными являются следующие области применения БПЛА: чрезвычайные ситуации (пожары, наводнения, поиск людей), мониторинг (электростанций (АЭС), нефтегазопроводы, сельское хозяйство, электросети, земельные ресурсы, лесные ресурсы, водные ресурсы, инфраструктуры, дороги, ЖД линии, месторождения), безопасность (охрана государственных границ, охрана объектов и людей) и аэрофотосъемка (геокалькулятор, геодезические работы, картографические работы, авиаучет) [3, 4, 5, 6, 7].

Отдельно стоит выделить, что в настоящее время одним из перспективных направлений является повышение автономности полета БПЛА в том

числе в замкнутых пространствах. Для обеспечения автономного полета могут использоваться различные технологии, такие как искусственный интеллект для обнаружения объектов интереса, системы технического зрения (СТЗ) и другие.

Используемые технологии в БПЛА

Основным источником развития робототехнических систем, в том числе и БПЛА и систем искусственного интеллекта является усовершенствование вычислительной техники, устройств и сенсоров, позволяющих получать информацию об окружающей среде. Этот процесс неразрывно связан с развитием программного обеспечения (далее ПО) бортовых процессоров, которые используются при управлении БПЛА.

Беспилотники оснащаются датчиками и полезными нагрузками, адаптированными к конкретным задачам. Это специализированное оборудование имеет широкий спектр технических характеристик и применений, что делает его подходящей альтернативой ручным инспекциям во многих отраслях. Термин «полезная нагрузка» в отношении БПЛА, самолетов, вертолетов, космических аппаратов в широком понимании означает количество, тип и массу оборудования, ради которого создается или запускается аппарат. Простыми словами, это оборудование, перевозимое беспилотником для выполнения конкретной миссии или задачи. В случае БПЛА чаще всего это визуализирующее оборудование: камеры, тепловизоры, дальномеры или датчики для осмотра, оценки ситуации, активов, местоположения [8].

Можно выделить следующие типы полезных нагрузок:

- Фото и видеокамеры, являются одними из самых распространенных полезных нагрузок и необходимы для осуществления мониторинга.
- Лидарные датчики для коммерческих БПЛА – это датчики, предназначенные для отправки быстрых лазерных импульсов на землю для создания 3D-карты и сбора передовых геопространственных и топографических картографических данных.
- Инфракрасные и тепловые датчики для промышленных дронов имеют еще более широкий спектр применения. Тепловые датчики могут использоваться для обнаружения утечек тепла или воды в трубопроводной системе, для выявления коррозий, дефектов, теплопотери строительных объектов, для поиска людей и спасения пропавших на открытых участках, для разведки, для выявления очагов возгорания и другого.
- Специализированные магнитометры используются для измерения интенсивности одной или нескольких составляющих магнитного поля.
- УФ-камеры представляют собой оптико-электронное устройство, предназначенное для наблюдения объектов, излучающих или отражающих излучение в ультрафиолетовом солнечно-слепом диапазоне спектра.

• Датчики обнаружения излучения, промышленные БПЛА могут в качестве полезной нагрузки переносить датчики обнаружения радиации в районы, которые считаются слишком опасными для отправки туда групп людей).

На основе данных, получаемых с полезных нагрузок, в том числе с фото и видеокамер могут быть применены различные методы и алгоритмы автоматизации процесса, например, посадки аппарата. При этом отдельной важной проблемой при обеспечении безопасности полета является сохранность беспилотника, в том числе с использованием стереозрения. Эта технология служит для управления БПЛА и предотвращения столкновения с какими-либо объектами. Применение стереозрения позволяет получать данные о глубине изображения, определять расстояние до объектов и их геометрический объем, строить трехмерную картину окружающего мира [8].

Тестовый стенд для реализации стереозрения

Под стереозрением понимают систему технического зрения (далее –СТЗ) на базе двух видеокамер, разнесенных на некоторое расстояние друг от друга. Компьютерные алгоритмы на базе нейронных сетей, сравнивая в режиме реального времени картинки с этих камер, могут вычислять не только объекты в трехмерном пространстве, но и расстояние до них, а также распознавать их геометрические формы. Добиться этого можно за счет анализа «смещения» видимых объектов относительно центральной оси «зрения», как это происходит с человеческими глазами (рис. 5).

Рис. 5. Стереозрение

Алгоритмы стереозрения и методы находят применение при решении задач автономности БПЛА, например, на складах и других закрытых помещениях [9, 10, 11].

С целью дальнейшего тестирования алгоритмов стереозрения был собран тестовый стенд, который включает: в качестве микрокомпьютера – Rasspberry Pi 3, в качестве видеокамер – и 2 Raspberry pi камеры. На микрокомпьютер установлена операционная система Ubuntu Mate 16, язык для реализации скриптов Python.

Для тестирования алгоритмов стереозрения сформирована последовательность действий:

1. Собран корпус для стереокамер, камеры расположены на фиксированном расстоянии друг от друга – это базовая линия. Важно чтобы она всегда оставалась неподвижной.

2. Далее подключены камеры и запущены камеры.

3. Выполнена стереокалибровка, исправления.

4. Сопоставлено правое и левое представления камер.

5. Получена на выходе карта несоответствий, где различия соответствуют различиям в плоскости изображения для одного и того же рассматриваемого.

6. За счет триангуляции получена карта глубины [12, 13, 14].

Собранный стенд послужит основой для тестирования алгоритмов стереозрения.

Заключение

В статье представлен обобщенный обзор БПЛА различного типа, перечислены типы полезных нагрузок и современные технологии. Выделено, что перспективным направлением развития отрасли считается повышение автономности БПЛА. Важной частью повышения автономности, в том числе в замкнутых пространствах может быть применение стереозрения. В статье предполагается, что стереозрение будет использоваться для обнаружения объектов и измерения расстояния до них с целью предотвращения столкновений. Представлен стенд для проведения дальнейших испытаний алгоритмов стереозрения.

Список используемых источников

1. Википедия. Беспилотный летательный аппарат. URL: Беспилотный летательный аппарат - Википедия (turbopages.org) (дата обращения 15.01.2023).

2. Типы беспилотных летательных аппаратов. Обзор: [Электронный ресурс]. URL: Типы беспилотных летательных аппаратов. Обзор. (aviatest.aero) (дата обращения 15.01.2023).

3. Кучерявый А. Е., Владыко А. Г., Киричек Р. В. Теоретические и практические направления исследований в области летающих сенсорных сетей // Электросвязь. 2015. N 7. С. 9.

4. Бондарев А. Н., Киричек Р. В. Обзор беспилотных летательных аппаратов общего пользования и регулирования воздушного движения БПЛА в разных странах //Информационные технологии и телекоммуникации. 2016. Т. 4. N 4. С. 13.

5. Киричек Р. В., Парамонов А. И. Беспилотный летательный аппарат как система массового обслуживания // Электросвязь. 2015. N 7. С. 16–19.

6. Думин Д. И. и др. Применение установленных на БПЛА систем обнаружения GSM-устройств для поиска пострадавших в результате ЧС // Информационные технологии и телекоммуникации. 2018. Т. 6. N 2. С. 62–69.

7. Маколкина М. А. и др. Исследование взаимодействия приложений дополненной реальности и методов управления БПЛА // Информационные технологии и телекоммуникации. 2016. Т. 4. N 2. С. 33–42.

8. Полезная нагрузка и датчики: [Электронный ресурс]. URL: Что такое промышленные БПЛА - DJI Гид покупателя (djimsk.ru) (дата обращения 15.01.2023).

9. Обход препятствий подвижными техническими средствами с использованием стереозрения: [Электронный ресурс]. URL: Обход препятствий подвижными техническими средствами с использованием стереозрения – тема научной статьи по компьютерным и информационным наукам читайте бесплатно текст научно-исследовательской работы в электронной библиотеке КиберЛенинка (cyberleninka.ru) (дата обращения 17.01.2023).

10. Разработка системы стереозрения для мобильного робота [Электронный ресурс]. URL: Разработка системы стереозрения для мобильного робота – тема научной статьи по компьютерным и информационным наукам читайте бесплатно текст научно-исследовательской работы в электронной библиотеке КиберЛенинка (cyberleninka.ru) (Дата обращения 18.01.2023).

11. Система дистанционного автоматического управления БПЛА на основе технического зрения [Электронный ресурс]. URL: Титков_И.П. (bmstu.ru) (дата обращения 19.01.2023).

12. Разработка модели определения глубины пространства для задач детектирования препятствий беспилотного летательного аппарата [Электронный ресурс]. URL: РАЗРАБОТКА МОДЕЛИ ОПРЕДЕЛЕНИЯ ГЛУБИНЫ ПРОСТРАНСТВА ДЛЯ ЗАДАЧ ДЕТЕКТИРОВАНИЯ ПРЕПЯТСТВИЙ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА - Современные наукоемкие технологии (научный журнал) (top-technologies.ru) (дата обращения 19.01.2023)

13. Машинное стереозрение для новичк.ов:две камеры Raspberry Pi и Python: [Электронный ресурс]. URL: Машинное стереозрение для новичков: две камеры Raspberry Pi и Python / Хабр (habr.com) (дата обращения 19.01.2023).

14. Основы стереозрения: [Электронный ресурс]. URL: Основы стереозрения / Хабр (habr.com) (дата обращения 19.01.2023).

УДК 004.056
ГРНТИ 81.93.29

ПОДХОДЫ К ИСПОЛЬЗОВАНИЮ EBPF ДЛЯ МОНИТОРИНГА СЕТЕЙ

А. Далех Аль-Магсуси

Национальный исследовательский университет ИТМО

У многих поставщиков облачных услуг возникают проблемы при мониторинге сети с помощью популярных инструментов мониторинга, основанных на eBPF, использующих Kubernetes и работающих в различных версиях ядра. Несмотря на сложности с совместимостью eBPF может использоваться для мониторинга в случаях, в которых традиционные инструменты терпят неудачу. Тем не менее, у многих отсутствует понимание сложности, ограничений и потенциальных рисков использования данной технологии. Кроме того, только небольшое количество компаний

в настоящее время предлагают готовые к использованию продуктов. В данной работе будут представлены результаты использования технологии eBPF и ряд выводов, которые были получены в результате проведенных экспериментов.

кибер-атаки, аномальные данные, системы контейнеризации, ebpftrace.

Технология eBPF позволяет организовать оперативный и подробный мониторинг процессов систем оркестрации, например, в Kubernetes. Поскольку масштабируемость Kubernetes зависит от возможности добавлять или удалять контейнеры, то нет гарантии что конкретный контейнер будет работать постоянно. А поскольку контейнеры создаются и уничтожаются по желанию пользователя, то возможно, что агенты, размещенные в конкретном контейнере, не будут работать. При этом, система мониторинга, основанная на eBPF работает на операционной системы и оттуда позволяет отслеживать всю активность. Проведенный анализ показал, что технология eBPF позволяет быстро собирать сетевые данные в ОС Linux и при этом экономно использовать центральный процессор. Правила сбора данных в технологии eBPF по умолчанию статичны. Они могут стать более адаптивными с помощью, например, Cilium, проекта с открытым исходным кодом, позволяющего осуществлять управление правилами eBPF. Cilium позволяет автоматически настраивать правила eBPF на основе анализа пакетов сетевого трафика [1]. Поскольку код eBPF реализован непосредственно в ядре ОС Linux, это упрощает мониторинг системных операций, так как они выполняются именно ядром. Некоторые приложения eBPF могут запускаться в результате системных событий. Мониторинг в ядре ОС более надежен, поскольку программы eBPF проверяются на наличие ошибок, таких как бесконечные циклы.

В наши дни расширенный пакетный фильтр Беркли (eBPF) является методом перехвата маршрута выполнения системных вызовов в Linux. Это связано с тем, что eBPF может эффективно выполнять программы, передаваемые из пользовательского пространства в ядро. крошечные определяемые пользователем приложения к доступным точкам трассировки ядра и точкам входа и выхода процедур ядра. Связанные программы создаются и запускаются на виртуальной машине в ответ на такие события, как отправка точки трассировки или возврат указанной процедуры ядра. Помимо фильтрации данных, эти программы могут сохранять состояние в структурах данных между вызовами зонда и использовать кольцевые буферы для передачи событий из ядра в пространство пользователя, где они могут быть собраны внешним приложением.

Когда происходит взаимодействие клиента и сервера, новое сетевое соединение формируется независимо от используемого языка программирования. Такое соединение определяется парой IP-адресов и номеров портов. Одна из пар представляет собой клиента. в то время как другая представляет

сервер. При этом в ядре Linux создается новая структура данных struct sock с локальными и удаленными адресами и портами. Поле локального адреса в подключающемся клиенте должно соответствовать полю удаленного адреса на принимающем сервере и наоборот.

Из-за того, что файловые дескрипторы не имеют значения вне контекста процесса, информация, необходимая для идентификации связанных процессов, не может быть собрана путем непосредственного перехвата системных вызовов. Системные вызовы connect и inet csk accept являются функциями ядра, которые управляют структурами, содержащими соответствующие данные. Перехватывая вызовы, а также событие CONNECT можно передать сведения о сетевых соединениях в пространство пользователя.

Чтобы уменьшить объем информации, которая должна быть передана в пользовательское пространство для создания взвешенного графа связи, также предлагается использовать eBPF, но при этом обработка данных должна происходить внутри ядра операционной системы в рамках ограниченных возможностей пространства ядра.

Чтобы программа, основанная на технологии eBPF перенаправляла событие из ядра в пространство, она должна сначала создать необходимую структуру данных и сохранить ее в кольцевом буфере, который связывает программу в ядре с внешним приложением в пространстве пользователя. При этом, при переполнении этого буфера происходит перезапись старых событий новыми, что увеличивает скорость потери данных при заполнении кольцевого буфера. Потери растут по мере увеличения пропускной способности.

Существующие системы мониторинга могут либо выполнять трассировку на уровне системы, которая показывает и измеряет, как взаимодействуют различные части распределенной системы, либо собирать информацию об использовании ресурсов в пространстве пользователя таким образом, который не зависит от приложения [2]. Метод, основанный на eBPF, предлагает баланс между традиционными способами мониторинга, уделяя большое внимание правильному анализу данных, которые перемещаются как между элементами сети, так и между процессами [3].

Список используемых источников

1. Ларин Д. В., Гетьман А. И. Средства захвата и обработки высокоскоростного сетевого трафика // Труды Института системного программирования РАН. 2021. Т. 33, N 4. С. 49–68,

2. Филиппов И. В. Исследование и разработка систем программирования масштабируемых высокопроизводительных сетевых функций в облачных инфраструктурах : дис. … канд. техн. наук : 05.13.11 / Филиппов Илья Викторович. Москва, 2019. 107 с.

3. Kotenko I., Levshun D., Chechulin A. Event correlation in the integrated cyber-physical security system // The 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, May 2016. PP. 484–486.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. А. Чечулиным.

УДК 004.051
ГРНТИ 20.53.23

АНАЛИЗ ВЛИЯНИЯ MPLS НА РАБОТУ IPSEC В СЕТИ СЕРВИС-ПРОВАЙДЕРА ПРИ ИСПОЛЬЗОВАНИИ ОТЕЧЕСТВЕННОГО СЕТЕВОГО ОБОРУДОВАНИЯ

Р. И. Дементьев, Д. Я. Держко, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На текущий момент времени остро стоит проблема импортозамещения в российских IT компаниях. В данной статье рассматриваются аспекты влияния многопротокольной коммутации по меткам на быстродействие IPsec-туннеля на примере оборудования компании «Eltex». Представлен сегмент сети и проведены базовые тесты производительности. В дальнейшем планируются исследования в области реализации сервисов MPLS VPNL3, MPLS VPN L2 и MPLS TE.

*информационная безопасность, импортозамещение, производительность, отказоустойчивость, MPLS, IPsec, маршрутизация***.**

Введение

В настоящее время в сетях сервис-провайдеров повсеместно используется технология многопротокольной коммутации по меткам (англ. Multiprotocol label switching) [1]. В концепции технологии MPLS используется понятие метки (label), которая встраивается граничным MPLS-маршрутизатором между заголовками канального и сетевого уровня модели OSI. Использование меток дает унификацию – возможность инкапсулировать через сеть сервис-провайдера большое количество протоколов: Ethernet, HDLC, Frame Relay, IPv4, IPv6 и др. На базе технологии MPLS работает множество сервисов: MPLS VPNL3, MPLS VPNL2, MPLS Traffic Engineering [2].

Исходя из указа президента РФ [3], необходимо подготовить отечественные КИИ к полному переходу на отечественное оборудование уже в 2025 году.

Прослеживается острая необходимость в проведении актуальных тестов современных технологий на базе отечественных решений с выявлением особенностей реализации.

Полученные результаты можно будет использовать для создания учебных пособий и обучающих программ для работников предприятий и студентов.

Цель исследования и ее выполнение

Цель данного исследования – проверить влияние MPLS на производительность IPsec VPN, настроенного между двумя устройствами клиентов (на базе ОС Linux Ubuntu). Она достигается построением двух защищенных туннелей через сеть сервис-провайдера.

Многопротокольная коммутация по меткам представляет собой технологию маркировки сетевых пакетов, время сходимости которой зависит от протокола динамической маршрутизации – BGP, OSPF или IS-IS [4].

Разработка сегментов ИВС

Разработка сегментов информационной вычислительной сети (ИВС) [5, 6, 7] проводилась на физическом оборудовании, предоставленном кафедрой ЗСС университета СПбГУТ. Модель топологии сети отражает клиентов сетевых услуг, которые связаны через сеть сервис-провайдера. Для маршрутизации использовался протокол IS-IS, так как его реализация представляла практический интерес в рамках составления программы обучения для кафедры ЗСС. В таблице 1 отражены роли, выполняемые устройствами в сети.

ТАБЛИЦА 1. Роли, выполняемые узлами в проектируемой сети

Имя узла	Роль
P1	Внутренние маршрутизаторы сети оператора
P2	
P3	
PE1	Граничные маршрутизаторы со стороны оператора
PE2	
PC1	Клиенты сетевых услуг
PC2	

На рис. 1 представлена топология, реализуемая в рамках опыта.

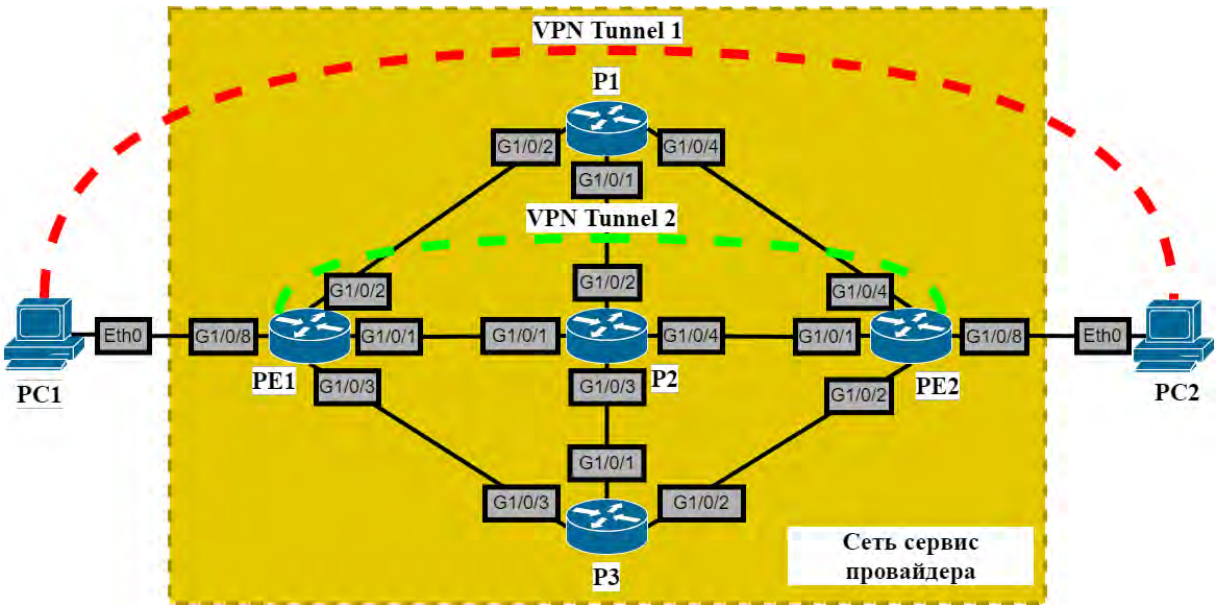


Рис. 1. Топология проектируемой сети

Проведение проверок

Для демонстрации работы оборудования применялась утилита «Iperf», позволяющий наглядно отразить скорость шифрованного трафика IPsec VPN между оконечными устройствами в туннельном режиме [8]. В качестве параметров для сравниваемых туннелей были заданы: «aes128-sha1-modp2048».

Для наглядного представления часть результатов эксперимента выведена в таблице 2.

ТАБЛИЦА 2. Результат выполнения команд по отправке информации

Команда на получателе	Отправитель/ получатель	Результат выполнения команды
Транспортный протокол TCP		
.\iperf3.exe -s -f k -p 5201	PC1/PC2	Connecting to host 192.168.42.1, port 5201 [6] local 192.168.42.10 port 50980 connected to 192.168.42.1 port 5201 [ID] Interval Transfer Bitrate Retr Cwnd [6] 0.00-0.10 sec 875 KBytes 71644 Kbits/sec 0 60.0 KBytes [6] 0.10-0.21 sec 1.75 MBytes 136990 Kbits/sec 0 150 KBytes - [6] 109.30-109.49 sec 896 KBytes 37890 Kbits/sec 0 1.83 MBytes [6] 109.49-109.50 sec 1.75 MBytes 5860305 Kbits/sec 0 1.83 MBytes - [ID] Interval Transfer Bitrate Retr

Команда на получателе	Отправитель/ получатель	Результат выполнения команды
Транспортный протокол TCP		
		[6] 0.00-109.50 sec 2.00 GBytes 156907 Kbits/sec 762 sender [6] 0.00-109.54 sec 2.00 GBytes 156706 Kbits/sec receiver

Рассмотрены несколько ситуаций для VPN tunnel 1. В первой отображена скорость передачи трафика объемом 2 Гб, с использованием протокола TCP. Во втором случае использовался протокол UDP. Для увеличения достоверности результата трафик был отправлен три раза для каждой ситуации. Эксперимент был повторен также и без использования технологии MPLS. Стоит отметить, что информация передавалась в зашифрованном виде, что обеспечило безопасность данных. На основании полученных результатов были построены графики пропускной способности в зависимости от времени, которые показаны на рис. 2 и рис. 3 (см. ниже).

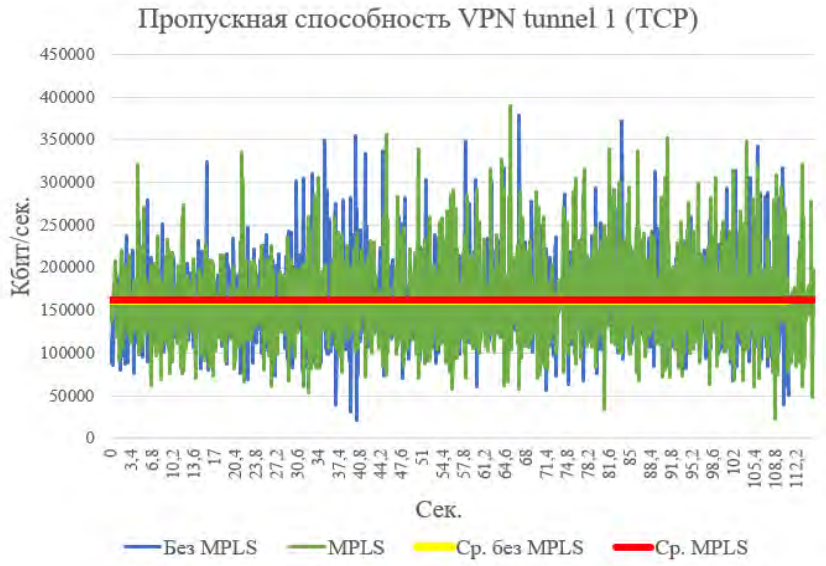


Рис. 2. Пропускная способность VPN Tunnel 1 (Протокол TCP)

На основании полученных результатов, можно сделать вывод, что технология MPLS при построении VPN туннелей на клиентских устройствах влияет на время передачи трафика. Средняя суммарная пропускная способность для различных транспортных протоколов без MPLS – 117 Мбит/с, с MPLS – 110 Мбит/с.

Явно видно, что она не оказала существенного влияния на пропускную способность шифрованного трафика при использовании протокола TCP. При использовании протокола UDP происходит выравнивание значений для пропускной способности, однако среднее время передачи значительно увеличивается.

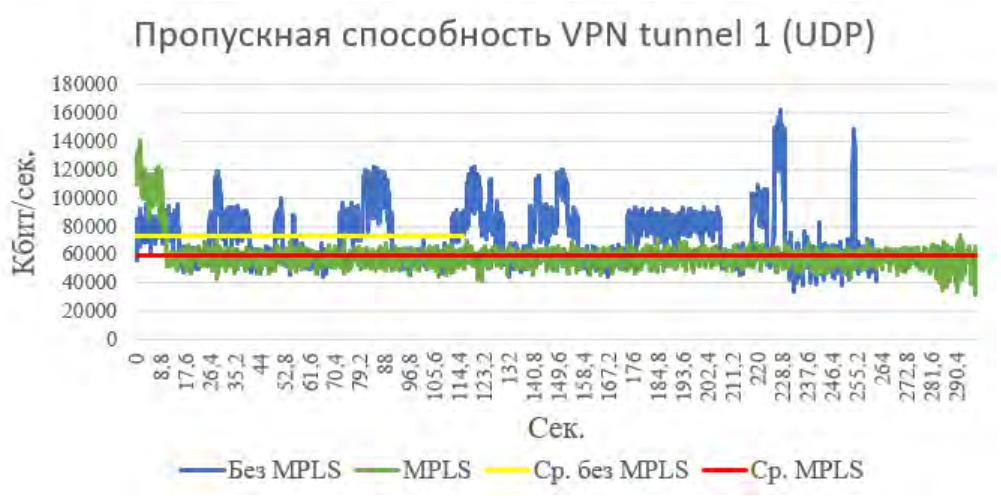


Рис. 3. Пропускная способность VPN Tunnel 1 (Протокол UDP)

В рамках альтернативного исследования VPN tunnel 2 была проверена пропускная способность трафика при использовании протоколов MPLS и IPsec на сетевых устройствах «ESR-200», а также проведены аналогичные тесты. Средняя суммарная пропускная способность составила 385 Мбит/с для 2 Гб шифрованного трафика.

Наиболее эффективным оказалось построение VPN туннелей через сетевые устройства, так как они являются более производительными и не нагружают абонентские устройства дополнительными задачами по обработке трафика.

В целом, технология MPLS была успешно реализована в рамках учебного сетевого оборудования. Появилась возможность организовать сервис MPLS L3VPN.

Выводы

Очевиден вывод, что технология многопротокольной коммутации по меткам может быть реализована на отечественном оборудовании. Эффективнее организовывать VPN туннели через сетевые устройства. Технология MPLS явно влияет на характеристики пропускной способности при передаче шифрованного трафика с использованием протокола UDP.

Явно стоит задача реализация дополнительных механизмов обеспечения безопасности при использовании технологии MPLS. А также необходимо провести тесты сети с абонентами, использующими различные протоколы.

Существует потенциал для проведения тестов сходимости. Все задачи моделирования выполнены.

Список используемых источников

1. Гольдштейн А. Б., Яновский Г. Г. Исследование механизма туннелирования мультимедийного трафика в сети MPLS. СПб. : СПбГУТ, 2004.

2. Карельский П. В., Ковцур М. М., Рязанцев К. С. Разработка проекта модернизации сети провайдера с внедрением сервисов на базе MPLS // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 446–450.

3. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

4. Гольдштейн А. Б., Гольдштейн Б. С. Технология и протоколы MPLS. СПб. : БХВ-Санкт-Петербург, 2005. 304 с.

5. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. N 3 (75). С. 34–42

6. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе ipv6 // Защита информации. Инсайд. 2020. N 1 (91). С. 51–57.

7. Красов А. В., Лосин Е. П., Ушаков И. А. Проблема безопасности передачи групповых рассылок в IP-сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 3. С. 295–301.

8. Платонов А. П., Сидельников Д. И., Стрижов М. В., Сухов А. М. Критерии качества Интернет-соединений // Телекоммуникации. 2007. N 8. С. 24–27.

УДК 654.739
ГРНТИ 49.33.29

НЕКОТОРЫЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ПЕРЕДАЧИ ТРАФИКА 3D-ВИДЕОИЗОБРАЖЕНИЙ

Н. А. Демидов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассмотрены различные области использования 3D-видеоизображений и обоснована актуальность изучения особенностей данного вида трафика. Представлены некоторые результаты исследования трафика 3D-видеоизображений. Описана экспериментальная составляющая исследования. Обозначены проблемы, требующие решения для получения качественного голографического видеоконтента. Предложены для обсуждения стратегические направления дальнейших этапов в программе эксперимента.

голографические технологии, цифровая голография, трафик 3D изображений, трафик 3D видеопотока, трафик видеопотока, передача данных, сети связи.

Актуальность исследования характеристик и свойств параметров трафика 3D видеоизображений может быть подтверждена экспоненциально-возрастающим количеством инновационных приборов, оборудования, услуг связи, которые базируются на достижениях в сфере голографических технологий.

Проведенный анализ исследований, рассматривающих вариативность использования голографических технологий, позволил сделать определенную структуризацию областей их применения. К первой группе были отнесены сферы деятельности, где 3D визуализация активно используется. Вторую, составили направления, в сфере которых ведется внедрение или разработки проектов с использованием 3D видео. Следующая группа представляет собой области потенциально позитивные к разработкам инновационных продуктов на основе голографических технологий, в них решение многих задач невозможно без уникальных методов, которые дает голография.

Сферы деятельности, где 3D визуализация активно используется. Это, в первую очередь, восстановительная хирургия, протезирование, где большое значение имеет предоперационное планирование, в рамках которого наиболее эффективным является использование трехмерных методов визуализации. Данная методика повышает точность оперативного вмешательства, позволяет проводить оперативное вмешательство с минимальной степенью травматичности, снижает вероятность последующих осложнений, что подтверждается многочисленными клиническими примерами [1].

Протезирование получило новую возможность для развития. Альтернативой выполнения биологических реконструктивных и калечащих операций стало индивидуальное протезирование с помощью 3 D технологий [2].

На основе голографических технологий формируют новые подходы в робототехнике, станкостроении, машиностроении. Так, в машиностроении на основе 3D-моделей проводят моделирование движения промышленных роботов [3].

Для экспериментальной отработки бортовых полетных операций, выполняемых с помощью антропоморфных роботов, используют виртуальные 3D модели [4].

В ходе производства ситуационных баллистических экспертиз в криминалистике применяется технология лазерного 3D-сканирования для последующей работы с 3D-моделью, что предоставляет возможность, как следователю, так и эксперту возвращаться на место происшествия, где все детали, начиная от мельчайших следов, заканчивая погодными условиями, не подвергаются изменениям [5].

Внедрение и разработка новых проектов с использованием голографических технологий ведется в целом спектре отраслей военно-промышленного комплекса. Разнообразные тренажеры и симуляторы для обучения и формирования навыков становятся все более совершенными.

В образовании, как средство для повышения его качества, начинают использовать трехмерные изображения, однако, 3D-видео еще не получило широкого распространения.

В начальной стадии находится применение виртуальных 3D-моделей для изучения и популяризации крупномасштабных научно-технических объектов [6].

К потенциально перспективным, в рамках инновационных продуктов на основе голографических технологий, можем отнести музейное дело, разнообразные рекреационные направления (отдых и развлечения). Новое направление в развитии музейного дела, например, обеспечило создание ультрареалистичной полноцветной трехмерной копии артефакта, изображение которого, в экспозиции музея, практически неотличимы от воссозданного объекта [7]. Вместе с тем, создание в музейном пространстве, например, батальных сцен в 3D-видео формате, находится на уровне идей и возможных проектов.

Необходимость внедрения новых способов визуализации объектов на основе голографических технологий, создает потребность в исследовании свойств нового вида трафика, передающего 3D видеопоток в режиме реального времени [8].

Важность и актуальность проблемы подчеркивает значительное число исследований, посвященных изучению характеристик видео-трафика, мультимедийного трафика, трафика 3D-изображений, моделированию трафика в условиях развития сетей связи.

Фундаментальные основы заложены и развиваются в исследованиях Р. В. Киричека, А. Е. Кучерявого, М. А. Маколкиной, А. И. Парамонова, А. Н. Степутина, О. И. Шелухина.

Исходя из положения о том, что для экспериментального исследования необходимо создать условия для воспроизведения явления с минимальным внешним воздействием, на модели, отличающейся простотой в использовании. Была разработана и апробирована модель для наблюдения за поведением трафика, с целью проверки определенных сформулированных предположений.

На рис. 1 представлена структурная схема модели для мониторинга исследуемого трафика.

Эксперимент подразумевал исследование передачи изображения одного движущегося объекта на однотонном фоне и передачи двух объектов в движении на том же однотонном фоне, с последующим сравнением.

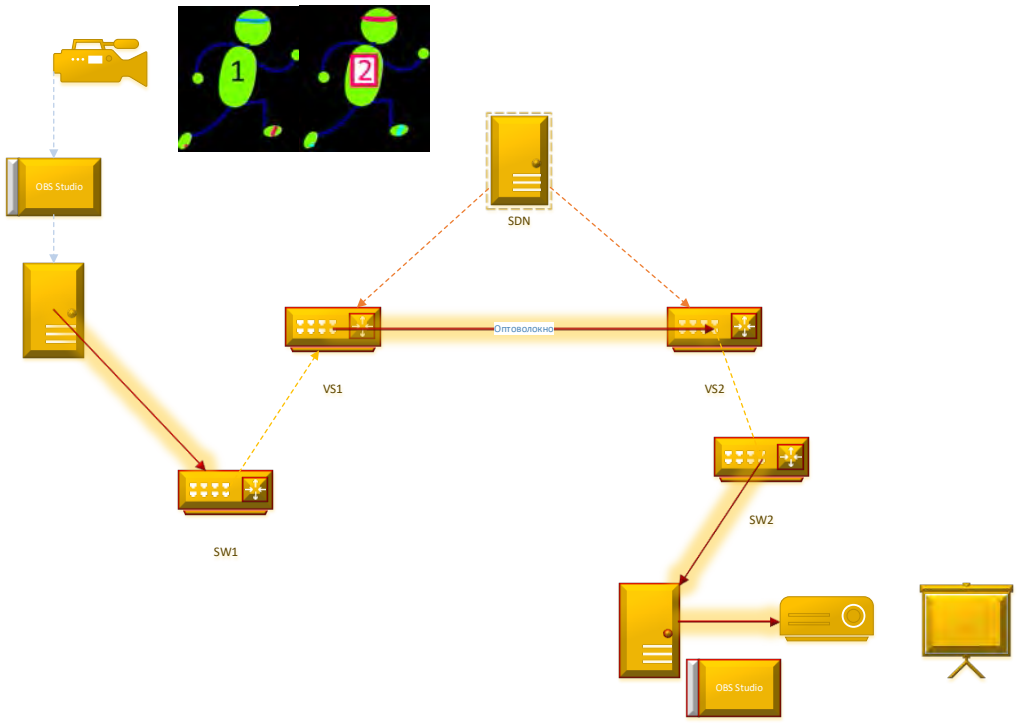


Рис. 1. Структурная схема модели для экспериментального исследования

Для создания трафика 3d видеопотока на первом этапе, была использована камера RGB-D, которая фиксировала одного человека в движении. Трансляцию и воспроизведение осуществляли с помощью приложения OBS Studio.

В модели, в сеть передачи данных вошли два коммутатора, на которых были реализованы виртуальные коммутаторы с поддержкой openflow. Наблюдение трафика на принимающем коммутаторе осуществляли с помощью виртуального сервера с технологией SDN.

Результаты мониторинга последовательно представлены на рис. 2 и 3.

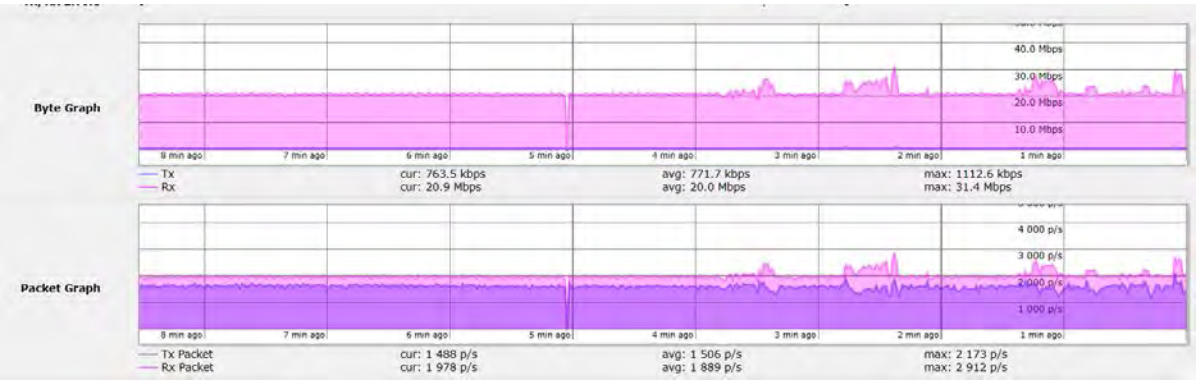


Рис. 2. График мониторинга при передаче одного подвижного объекта на зеленом фоне

Для передачи двух подвижных объектов на зеленом фоне потребовалось в двое больше пропускной способности, это можно наблюдать на рис. 3.

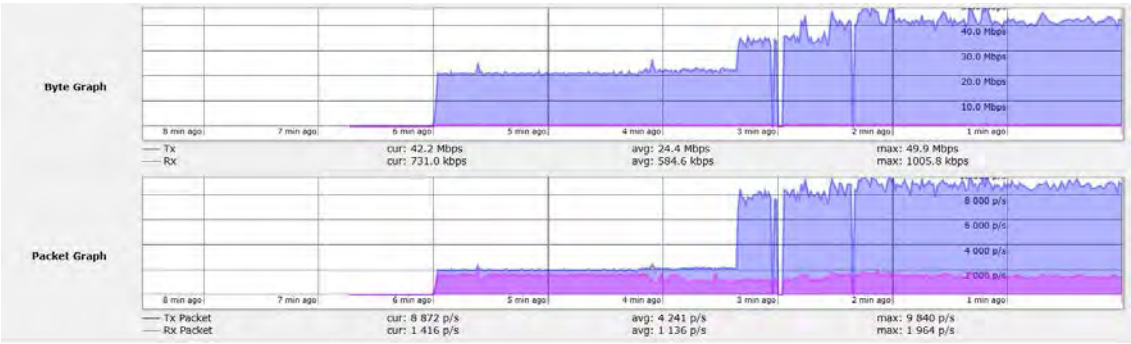


Рис. 2. Графики мониторинга при передаче двух подвижных объектов на зеленом фоне

На рис. 3 можно отметить, что начало передачи требует 20 Мбит/с пропускной способности. Это происходит в связи с тем, что объекты начинали движения плавно. Для передачи 3d видеопотока, движущегося человека с высокой скоростью, в ускоренном темпе движения, хаотично, требовалось свыше 40 мегабит в секунду.

В результате экспериментального исследования была подтверждена рабочая гипотеза о необходимой пропускной способности для передачи трафика 3d видеопотока.

Разработанные, для экспериментального исследования, модели, могут быть использованы для мониторинга поведения трафика при передаче данных, с последующим анализом взаимозависимостей различных свойств трафика 3D видеопотока в режиме реального времени.

Перспективным направлением дальнейшего исследования может быть проведение сравнительного анализа передачи трафика 3D-видеопотока с помощью технологии SDN и Openflow и без их использования.

Список используемых источников

1. Тарасенко С. В., Загорский С. В. Использование навигационных хирургических шаблонов при дентальной имплантации у пациентов с частичной вторичной адентией // Клиническая стоматология. 2018. N 4 (88). С. 18–21.

2. Jungo Imanishia, Peter FM Choong. Three-dimensional printed calcaneal prosthesis following total calcanectomy. International Journal of Surgery Case Reports. 2015. N 10. PP. 83–87.

3. Крахмалев О. Н., Петрешин Д. И. Моделирование движения промышленных роботов в программном комплексе «Универсальный механизм» на основе 3D-моделей // Транспортное машиностроение. 2014. N 4 (44). С. 52–57.

4. Sokhin I. G., Burdin B. V., Mikhaylyuk M. V., Torgashev M. A. The usage of virtual 3D models for experimental exercising the flight operations performed with the help of anthropomorphic robots // Robototekhnika i tekhnicheskaya kibernetika. 2013, No. 1. PP. 42–46.

5. Кудряшов Д. А. Комплексный подход при использовании современных экспертных технологий в ходе производства ситуационных баллистических экспертиз // Вестник экономической безопасности. 2022. N 5. С. 116–121.

6. Леонов А. В. Применение 3D-технологий в истории науки и техники. 3D-модель как историко-технический источник // В сб.: Междисциплинарные методы в изучении

истории науки и техники: Материалы науч. конф., Москва, 27 мая 2015 г. / Отв. ред. Ю.М. Батурин. М. : ИИЕТ РАН, 2015. С. 42–45.

7. Готовчиц В. А. Голографические технологии в музейном пространстве // Республиканская научно-практическая интернет-конференция молодых исследователей MediaLex-2018. Брест, 2018. С. 56–60.

8. Шыпота Н. А. Анализ особенностей голографических сетевых приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С.688–692.

9. Волков А. Н., Мутханна А. С. А., Кучерявый А. Е. Сети связи пятого поколения: на пути к сетям 2030 // Информационные технологии и телекоммуникации. 2020. Т. 8. N 2. С. 32–43.

10. Городецкий С. С., Беляков В. А. Перспективы использования виртуальной реальности и 3d-технологий в военно-прикладных целях // HOMO CYBERUS. 2018. N 2 (5). С 35–39.

11. Кучерявый А. Е., Парамонов А. И., Тарасов Д. В. Особенности видеотрафика для сетей связи следующего поколения // Электросвязь. 2010. N 2. С. 37–43.

12. Парамонов А. И. Разработка и исследование комплекса моделей трафика для сетей связи общего пользования : дис. … д-ра техн. наук : 05.12.13 / Парамонов Александр Иванович. СПб., 2014. 325 с.

13. Парамонов А. И., Сенькина Н. С. Проблемы развития инфокомму- никационных услуг и их влияние на перераспределение трафика // Информационные технологии и телекоммуникации. 2016. Том 4. N 1. С. 46–54.

14. Шелухин О. И., Осин А. В. Мультифрактальные свойства трафика реального времени // Электротехнические и информационные комплексы и системы. 2006. Т. 2. N 3. С. 36–43.

Статья представлена научным руководителем, профессором кафедры ССиПД СПбГУТ, доктором технических наук, доцентом М. А. Маколкиной.

УДК 621.396.4
ГРНТИ 50.37.03

СОВРЕМЕННОЕ СОСТОЯНИЕ МЕТОДОВ АНАЛИЗА ЭФФЕКТИВНОСТИ СИСТЕМ ХРАНЕНИЯ И РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

А. Е. Деркач, А. В. Михайличенко, И. Б. Паращук

Военная орденов Жукова и Ленина Краснознаменная академия связи
им. Маршала Советского Союза С. М. Буденного

Рассмотрены состояние, условия и особенности применения современных методов анализа эффективности функционирования таких сложных информационно-техни-

ческих систем, которыми являются системы хранения информации и резервного копирования для центров обработки данных. Предложены варианты формулировки классификационных признаков для идентификации таких методов, к которым могут быть отнесены: тип показателя эффективности, класс априорной неопределенности процесса функционирования систем, зависимость показателя эффективности от времени, а также способ оценивания эффективности систем такого класса.

анализ эффективности, метод, показатель эффективности, система хранения и резервного копирования, центр обработки данных, требования, метод, классификационный признак.

В связи с продолжающимся эволюционным развитием средств и комплексов обработки и хранения информации, основанных на современных технологиях, например, «облачных» вычислениях (Cloud Computing), «туманных» вычислениях (Fog Computing) или «граничных» вычислениях и хранении данных (Edge Computing), а также в связи усложнением алгоритмов обработки данных и ужесточением условий функционирования, значительно возросла актуальность проблемы обоснования методов анализа эффективности функционирования яркого представителя подобных объектов – центров обработки данных (ЦОД) и их ключевых компонентов: серверного комплекса, системы хранения данных и резервного копирования, сетевой инфраструктуры, инженерной системы и системы безопасности.

При этом система хранения данных (СХД) и резервного копирования (РК) является ядром, технологическим фундаментом современных ЦОД, что подчеркивает ее значимость в архитектуре дата-центров и вклад в общую эффективность функционирования объектов такого класса [1, 2].

Подобная система включает консолидирующие дисковые массивы, сеть хранения данных, а также подсистему резервного копирования и аварийного восстановления данных [3, 4, 5, 6, 7].

Актуальность проблемы обоснования специальных методов анализа эффективности функционирования СХД и РК для ЦОД, помимо прочего, связана с трудностями выбора конкретного метода. Обоснование выбора того или иного метода анализа эффективности СХД и РК связано с целями данного анализа в конкретной ситуации, нацелены, в основном, на оказание помощи исследователям при выборе того или иного метода и опирается на характерные признаки этих современных методов, каждый из которых обладает определенным классификационным признаком [8, 9].

В роли таких признаков могут быть обозначены: тип показателя эффективности (ПЭ), класс априорной неопределенности процесса функционирования СХД и РК, степень изменения значений ПЭ во времени, уровень зависимости ПЭ от значений параметров, входящих в него, а также математический подход к оценке (способ оценивания) ПЭ СХД и РК для

ЦОД. Эти признаки коррелированы между собой, поскольку, по сути, воспроизводят различные свойства одних и тех же методов анализа эффективности систем хранения данных и резервного копирования.

Первичным классификационным признаком принято считать вид процесса (операции), эффективность которой необходимо анализировать. С учетом того факта, что под целенаправленным процессом принято понимать упорядоченную совокупность взаимосвязанных операций или действий, реализующих достижение конкретного результата (цели), выделяют три вида процесса (операции), отличающихся характером связей между исходом данного процесса (операции) и решением проблемы, на которую он нацелен. Очевидно, что можно выделить три вида процессов (операций), и, соответственно три группы методов анализа эффективности: вероятностные (стохастические), детерминированные и неопределенные (нечеткие). Более того, методы, используемые для описания вышеперечисленных типов процессов (операций), по сути, определяют классификационный признак, характеризующий класс априорной неопределенности процесса функционирования СХД и РК. При этом в вероятностных методах признаком эффективности процесса функционирования СХД и РК, т.е. степени его приспособленности к достижению цели функционирования в условиях фактического воздействия случайных факторов, служит вероятность достижения цели процесса (операции) [10, 11].

Использование детерминированных методов предлагается рассматривать лишь как некоторые приближения стохастических, рациональность и математическая корректность их использования должна быть обоснована в каждом конкретном случае анализа эффективности процесса функционирования СХД и РК. Особого внимания, на наш взгляд, заслуживают неопределенные (нечеткие) методы, причем, как и в классической постановке, принято различать три ключевых уровня априорной неопределенности, описывающей степень неполноты априорного задания вероятностных характеристик случайных процессов, протекающих в СХД и РК. Речь идет либо о полном априорном задании распределений вероятностей таких случайных процессов, либо о параметрической априорной неопределенности, либо, когда априорная неопределенность о значениях вероятностных распределений для случайных процессов, протекающих в СХД и РК, носит непараметрический характер. Практика показывает, что с учетом все более возрастающего количества факторов, воздействующих на СХД и РК в современных условиях, с учетом небольшого объема экспериментальных наблюдений, особенно для вновь разрабатываемых СХД и РК, все чаще при анализе эффективности функционирования прибегают к методам, учитывающим нечеткую (размытую) априорную неопределенность о значениях вероятностных характеристик случайных процессов, протекающих в СХД

и РК. Для учета такого вида неопределенности зачастую предлагается воспользоваться методами анализа эффективности, включающими методологические и математические инструменты теории нечетких множеств, искусственный нейронных сетей, нейро-нечетких сетей, элементы теории игр и теории катастроф. Одним их возможных классификационных признаков принято считать степень зависимости разнообразных параметров, входящих в комплексный (векторный) ПЭ функционирования СХД и РК, причем, обычно рассматривают методы анализа эффективности, характеризующиеся либо линейной, либо нелинейной зависимостью этих параметров (компонент) показателя эффективности [12, 13].

Методы анализа эффективности функционирования СХД и РК можно также различать по степени изменения значений ПЭ во времени: методы статического и динамического анализа. Методы статического анализа предполагают предварительный сбор статистики о параметрах состояния СХД и РК на различных временных интервалах (их иногда называют этапами локальной стационарности), а затее ее обработку и оценку. Методы динамического анализа применимы для оценки динамического (текущего, пошагового) характера изменений значений показателей качества (ПК) СХД и РК в процессе их функционирования, вариаций, вызванных динамикой изменениями структуры, режимов и условий их функционирования. Они нацелены на расчет оценочных значений этих ПК СХД и РК в онлайн-формате, почти в реальном масштабе времени. Для этого используют методы стохастического оценивания выборочных значений ПК СХД и РК, а также вид плотности распределения вероятностей (ПРВ) таких значений.

По типу показателя эффективности (критерия эффективности) принято различать скалярный анализ по частному критерию, анализ по интегральному критерию «эффект-затраты» и многокритериальный анализ эффективности функционирования СХД и РК.

По выбранному математическому подходу к оценке (способу оценивания) ПЭ СХД и РК для ЦОД принято различать методы компромисса, методы рандомизации и формальные методы. Методы компромисса основаны на построении компромиссных множеств (множеств Парето).

В основе методов рандомизации лежит замена детерминированных требований к результатам функционирования СХД и РК для ЦОД (или показателей качества СХД и РК для ЦОД) их рандомизированными копиями, в основе анализа лежат критерии пригодности и оптимальности [10].

Формальные методы могут быть точными и приближенными, они включают аналитические способы оценки, численные способы, способы статистического имитационного моделирования и статистические испытания.

Таким образом, изучение классификационных признаков и детальное исследование особенностей современных методов анализа эффективности

СХД и РК показывают, что все эти методы имеют свои преимущества, но не свободны от недостатков. Сочетание этих достоинств и недостатков определяет пригодность конкретных методов для анализа эффективности реальной СХД и РК в конкретной ситуации. Использование того или иного метода зависит от многих условий, в том числе от целей, стоящих перед исследователем и имеющихся исходных данных.

Список используемых источников

1. Прохоров А. Н., Рахматуллин С. С. Центры обработки данных. Анализ, тренды, мировой опыт. Изд. первое. М. : ООО «АльянсПринт», 2021. 416 с.

2. Румянцев Ю.В., Акулов С.В., Гурова В.А. Центры обработки данных. М. : Изд. «Русатом – цифровые решения». 2020. 40 с.

3. Бережной А. Н. Сохранение данных: теория и практика. М. : ДМК Пресс, 2016. 317 с.

4. Сомасундарам Г., Шривастава А. От хранения данных к управлению информацией. 2-е изд. СПб. : Питер, 2016. 544 с.

5. Парфенов Ю.П. Постреляционные хранилища данных: учеб. пособие. Екатеринбург: Изд-во Урал. ун-та, 2016. 120 с.

6. Паращук И. Б., Крюкова Е. С., Михайличенко Н. В. Многопараметрические системы хранения данных, дата-центры и электронные библиотеки: способ контроля параметров технического состояния и анализа качества // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1 \ СПОИСУ. СПб., 2020. С. 102–104.

7. Ананченко И. В., Зудилова Т. В., Хоружников С. Э. Средства резервного копирования, восстановления, защиты данных в операционных системах Windows. СПб. : Университет ИТМО, 2019. 50 с.

8. Колос Н. В., Ожог С. В., Иовлева О. В. Исследование методических подходов к оценке эффективности ИТ-проектов // Вестник Белгородского университета кооперации, экономики и права. 2017. Вып. 6 (67). С. 70–80.

9. Паращук И. Б. Методы анализа эффективности функционирования радиотехнических систем и направления их совершенствования // Зарубежная радиоэлектроника. 2000. N 2. С. 67–72.

10. Петухов Г. Б. Основы теории эффективности целенаправленных процессов. Часть 1. М. : МО СССР, 1989. 660 с.

11. Анисифоров А. Б., Анисифорова Л. О. Методики оценки эффективности информационных систем и информационных технологий в бизнесе: учебное пособие. СПб. : СПб государственный политехн. университет, 2014. 97 с.

12. Надежность и эффективность в технике. Том 3. Эффективность технических систем / Под ред. В. Ф. Уткина и Ю. В. Крючкова. М. : Машиностроение, 1988. 328 с.

13. Терентьев В. М., Санин Ю. В. Анализ эффективности функционирования автоматизированных сетей многоканальной радиосвязи. СПб. : ВАС, 1992. 80 с.

УДК 004.7
ГРНТИ 49.33.29

ПАРАМЕТРЫ В SDN ДЛЯ ПРОГНОЗИРОВАНИЯ СЕТЕВЫХ СОБЫТИЙ

Ю. С. Дмитриева, В. С. Елагин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается протокол управления и конфигурации сетевых элементов SDN. Протокол OF-Config является сопутствующим протоколом OpenFlow, динамически поддерживает взаимодействие контроллера и коммутатора OpenFlow. Благодаря применению протокола OF-Config и изменению параметров можно избежать перегрузки и отказа сети. Анализу этих параметров посвящена данная статья.

SDN, программно-конфигурируемая сеть, OpenFlow, OF, OF-Config.

Введение

Основной проблемой сети передачи данных является динамический характер сетевых приложений и их среды. Требования к производительности передаваемых потоков данных могут меняться со временем. Для эффективной работы приложений базовая сеть должна быть достаточно гибкой, чтобы динамически меняться в ответ на любые изменения в требованиях приложений и их окружений. В традиционной сети операторы вручную настраивают сетевые устройства для различных приложений. Это затрудняет управление и оптимизацию сети, что может привести к ошибкам в сети. Программно-конфигурируемая сеть решает эти проблемы. Рассмотрим протокол OF-Config (протокол конфигурации SDN) и параметры прогнозирования сети: очередь, коммутаторы OpenFllow (коммутаторы OF), порты.

Организация трафика в SDN

В традиционной сети управляют трафиком маршрутизаторы и коммутаторы. Пересылка данных и решения маршрутизации выполняются в одном и том же устройстве. В программно-конфигурируемой сети (от англ. *Software-Defined Network*, SDN) коммутатор OF разделяет эти две функции. Он выполняет пересылку данных, а решения маршрутизации выполняет отдельный контроллер. Открытый расширяемый протокол OF устанавливает соединение между контроллером и коммутатором [1, 2].

В программно-конфигурируемой сети реализован механизм маршрутизации, в котором протоколы динамически меняются в зависимости от состояния сети для повышения эффективности использования ресурсов, избегая сбоев и перегрузок, и улучшения качества обслуживания.

Контроллер с помощью протокола OpenFlow (протокола OF) добавляет, обновляет и удаляет записи в таблице потоков; запрашивает у коммутатора собранную статистику и характеристики, а также конфигурирует коммутатор и его порты.

Логический коммутатор OF состоит из каналов OpenFlow к внешнему контроллеру, таблиц потоков (*flow tables*) и групповой таблицы (*group table*), которые пересылают пакеты (рис. 1). Таблица потоков в коммутаторе содержит набор записей для управления потоками; запись потока состоит из полей соответствия, счетчиков и набора инструкций для соответствующих пакетов [3].

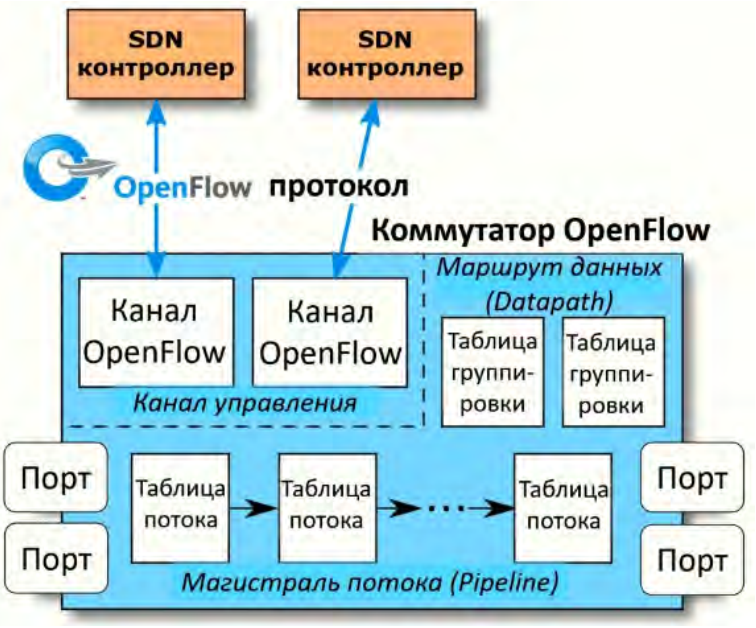


Рис. 1. Базовая архитектура коммутатора OpenFlow

Протокол конфигурации SDN, в отличие от протокола OF, разработан для решения задач более высокого уровня: созданию сетевой среды, конфигурации коммутаторов и принятию решений, например, о закрытии или открытии отдельных портов [4, 5].

На рис. 2 представлена схема взаимодействия протокола OpenFlow и операционного контекста (operational context). Протокол конфигурации SDN позволяет удаленно конфигурировать обмен данными, например, формирование таблицы переадресации и решений относительно действий протокола OF.

Схемы протокола конфигурации SDN (рис. 3):

•Логический коммутатор OF – схема узла передачи данных OF. Протокол конфигурации SDN выполняет конфигурацию логического коммутатора OF для взаимодействия контроллера OpenFlow (контроллер OF) и управления по протоколу OF;

•OF-совместимый коммутатор – физический или логический сетевой элемент, ресурсы которого (порты, очереди и пр.) выделены одному или нескольким логическим коммутаторам OF. Протокол конфигурации SDN динамически назначает ресурсы OF-совместимого коммутатора размещенным на нем логическим коммутаторам OF;

•Точка конфигурации OF – источник сообщений конфигурации SDN для OF-совместимых коммутаторов [6].

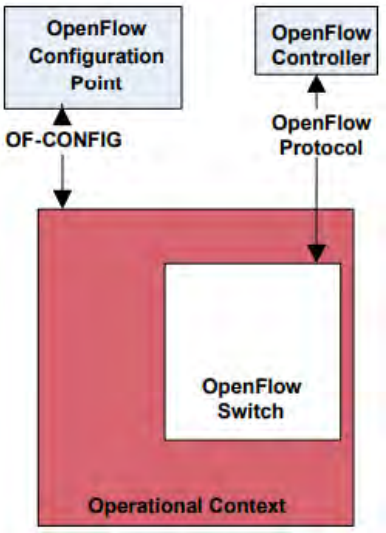


Рис. 2. Схема взаимодействия протокола OpenFlow и операционного контекста (operational context)

Протокол конфигурации SDN работает совместно с протоколом OF, динамически поддерживает связь контроллера OF и коммутатора OF.

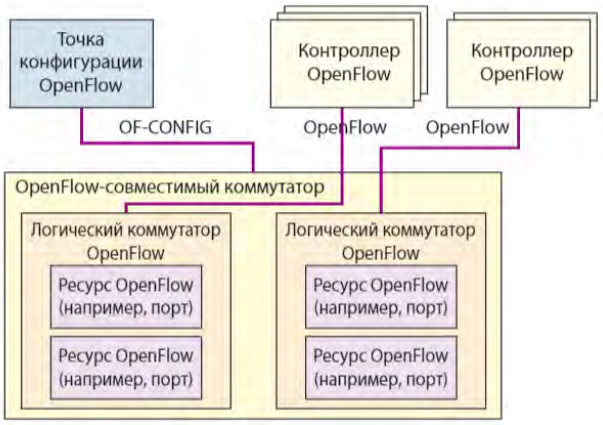


Рис. 3. Архитектура протокола конфигурации SDN

Порты OF коммутатора

Протокол OF содержит методы для конфигурирования ограниченного числа параметров портов коммутаторов OF.

Существуют следующие параметры конфигурации портов:

- admin-состояние (*admin-state*);
- нет приема (*no-receive*);
- нет входящих пакетов (*no-packetin*);
- не переадресовывать (*no-forward*).

Сетевым интерфейсом для передачи пакетов между обработкой OF и остальной сетью является Порт-OF. Коммутаторы OF логически подключаются друг к другу через порт OF. OF коммутатор поддерживает три типа OF портов:

- Физический порт, который соответствует аппаратному сетевому интерфейсу.
- Логический порт, который не соответствуют напрямую аппаратным интерфейсам коммутатора.
- Зарезервированный порт выполняет специальное действие по пересылке пакета. Зарезервированные порты: all, any, controller, local, table, in_port, unset. Порт controller представляет собой канал связи с контроллером OF.

У портов существует четыре набора характеристик: поддерживаемые, текущие, анонсированные, и анонсированные партнером. Текущий, поддерживаемый и анонсированный партнером набор характеристик содержит статусную информацию и не требуют конфигурирования. Протокол конфигурации SDN 1.2 обеспечивает конфигурирование анонсированных характеристик следующими параметрами:

- скорость (*speed*);
- дуплексный режим (*duplex-mode*);
- проводная среда (*copper-medium*);
- волоконная среда (*fiber-medium*);
- автоматическое согласование (*auto-negotiation*);
- пауза (*pause*);
- асимметричная пауза (*asymmetric-pause*).

Логические порты поддерживают передачу метаданных контроллеру. Настройку логических портов, ограниченную небольшим числом туннелей, которые могут использоваться в сценариях информационного центра типа виртуализации сети поддерживает протокол конфигурации SDN 1.2.

Туннель (логический порт)

Логический порт OF поддерживает специфический метод инкапсуляции. Ему соответствует оконечная точка туннеля. Создание виртуальных сетей путем инкапсуляции является общим случаем использования туннелей. Например, инкапсуляция трафика уровня 2 (*Ethernet*) в пакетах уровня 3 (IP). Протокол конфигурации SDN осуществляет связь логических портов OF с конкретным типом туннеля и соответствующими параметрами туннеля.

Элемент «tunnel» имеет тип туннеля и существует, если порт является логическим, который представляет собой конец туннеля. Существуют следующие виды туннелей: IPinGRE, VxLAN и NVGRE, имеющие общий

набор элементов: адреса начальной (“*local”*) и конечной точки туннеля (“*local-XXX-address*” и “*remote-XXX-address*”) для типов адресов IPv4, IPv6 и MAC.

Очередь

Механизм, позволяющий управлять приемом и передачей пакетов это очередь. OF-Config 1.2 обеспечивает средства для конфигурирования трех параметров в очереди:

- Минимальная скорость (*min-rate*);
- Максимальная скорость (*max-rate*);
- Эксперементальная (*experimenter*).

Выводы

С помощью протокола OF-Config в программно-конфигурируемой сети изменяем сетевые элементы такие как порты, очереди, чтобы избежать перегрузки и отказа сети. Список параметров, влияющих на поведение сети получен при прогнозировании. Для более точного прогноза необходимо рассмотреть протоколы мониторинга SDN с помощью которых можно получать параметры сети. Следующая статья будет посвящена анализу и разработке такого протокола.

Список используемых источников

1. Дмитриева Ю. С., Елагин В. С. Модели и характеристики сетевых SDN ресурсов // Вестник связи. 2020. N 6. С. 35–40.

2. Смелянский Р. Л. Программно-конфигурируемые сети // Открытые системы. 2012. N 9. URL: http://www.osp.ru/os/2012/09/13032491/

3. ONF Specification // Open network foundation.2015. URL: https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.

4. OF-CONFIG 1.2 | OpenFlow Management and Configuration Protocol. URL: https://opennetworking.org/wp-content/uploads/2013/02/of-config-1.2.pdf.

5. ONF OpenFlow Management and Configuration protocol (OF-CONFIG), version 1.2 – 2014.

6. Ефимушкин В. А., Ледовских Т. В., Корабельников Д. М., Языков Д. Н. Сравнительный анализ архитектур и протоколов программно-конфигурируемых сетей // Электросвязь. 2014. N 8. С. 9–14.

УДК 621.396.4
ГРНТИ 50.37.03

ПРОБЛЕМЫ ЦЕЛЕУКАЗАНИЯ ДЛЯ НЕСКОЛЬКИХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ СТРАТЕГИЙ РОТАЦИИ И КЛАСТЕРНОГО ПОДХОДА

М. Е. Дмитриенко, В. В. Ерыгин, М. Р. Семкина

Военная орденов Жукова и Ленина Краснознаменная академия связи
им. Маршала Советского Союза С. М. Буденного

В данной статье рассматриваются проблемы назначения целей оружию для системы обороны для противодействия многочисленным объектам, сосредоточенным в узкой области, таким как ракетные угрозы на малой высоте или рои беспилотных летательных аппаратов. Два алгоритма назначения целей оружия - стратегия с фиксированным вращением и стратегия ротации — предлагаются на основе этой формулировки.

назначение цели оружию, вероятность поражения, множество воздушных объектов, оперативная стратегия, моделирование.

Назначение цели оружию (НЦО) или же целеуказание – это проблема назначения перехватчиков (т. е. средств защиты) соответствующим образом для противодействия выявленным угрозам. За последние десятилетия эта проблема обострила свою актуальность для систем с автономной поддержкой принятия решений в интересах противовоздушной обороны [1]. Конечной целью НЦО является минимизация ожидаемого ущерба для потенциала собственной силы, что называется НЦО на основе сохранения потенциала [2]. Если нет необходимости учитывать затраты, то может быть принята целевая НЦО, которая сводится к минимуму ожидаемой живучести целей противника после применения средств поражения. Точечная защита от наземных целей является примером НЦО на основе целей. Существует две категории НЦО: статическое НЦО и динамическое НЦО [2]. Статическое НЦО рассматривает временную задачу защиты на одном этапе; динамическое НЦО принимает последовательность решений за несколько этапов, на каждом из которых учитывается фактические ограничения: временные окна для пар оружия и целей.

Первая проблема с НЦО заключается в том, чтобы ее действие (время принятия решения) было как можно ближе к реальному времени, и сводится к минимуму время реакции на цели или же уменьшения времени в контуре

управления оружием. Однако, НЦО хорошо известна как *NP* -полная проблема, что означает, что вычислительная сложность экспоненциально растет по мере увеличения размера проблемы (т. е. увеличивается количество угроз и перехватчиков). Предыдущие исследования, особенно касающиеся статических алгоритмов НЦО, были в значительной степени сосредоточены на решении вычислительной сложности общих задач НЦО. За последние десятилетия были разработаны сложные методы поиска и эвристические методы для решения общих задач НЦО, такие как Лагранжева релаксация [3], точная и эвристическая или оптимизация муравьиной колонии [4], оптимизация роя частиц [5], генетические алгоритмы [6], поиск перестановок и табу [7], поиск по переменному соседству, поиск гармони, гибридная дискретная оптимизация серого волка [8] и алгоритмы жадной максимизации [9]. Из этих методов алгоритмам жадной максимизации уделяется значительное внимание из-за их преимуществ по эффективности во времени.

Вторая проблема, касающаяся НЦО, заключается в том, что задача НЦО должна максимально точно отражать реальную ситуацию взаимодействия без увеличения сложности задачи, чтобы разработанный алгоритм был полезен на практике [10]. Ученые обнаружили, что фактическое время стрельбы перехватчика является одним из существенных факторов, влияющих на вероятность поражения (ВП). Затем они сформулировали временную задачу НЦО, рассмотрев зависящей от времени выигрыш, чтобы определить закономерность более подходящего времени стрельбы перехватчика. Был предложен двухэтапный подход к решению динамических задач НЦО, первым шагом которого было назначение перехватчиков целям, а вторым шагом было определение последовательности времени стрельбы. Другие предложили иерархически разложенный двухэтапный алгоритм для определения назначения каждого перехватчика и времени стрельбы путем моделирования изменения вероятности поражения в зависимости от времени как выпуклой функции. Так же был предложен новый алгоритм назначения оружия целям, чтобы гарантировать желаемою ВП. Они предложили алгоритм НЦО, основанный на времени, используя простое предположение о ВП для доступного времени поражения. Исследования рассматривали ВП в соответствии с временем до вылета, линией визирования и расстоянием промаха между перехватчиком и целью для перехватчика в полете. Однако ни одно исследование не было направлено на улучшение ВП путем определения того, как бороться с конкретными факторами, влияющими на ВП перед запуском.

В последнее время защита от площадных целей, которые представляют собой множественные цели, сосредоточенные в узкой области, такие как ракетные угрозы на малой высоте или рои дронов, стала важной проблемой, и алгоритм НЦО для этого типа взаимодействия пользуется большим спросом. Поскольку системы защиты от ракетных угроз на малых высотах или

стаи дронов потребляют большое количество перехватчиков во время боя, каждый перехватчик обычно имеет небольшие размеры и разрабатывается с использованием недорогих деталей; следовательно, такие перехватчики по своей сути обладают меньшей маневренностью, чем другие перехватчики. Из-за этой характеристики ВП могут значительно варьироваться в зависимости от относительной геометрии взаимодействия между целью и пусковой установкой (т. е. ошибки курса между углом ориентации пусковой установки и углом подхода к цели) в этом конкретном типе взаимодействия. Кроме того, ошибки начального курса могут оказать негативное влияние на взаимодействие, поскольку большая ошибка начального курса для перехватчика, назначенного цели, может повлиять на весь курс. Кроме того, поскольку количество целей, которые должны быть поражены, в таком случае очень велико, эффективная работа пусковой установки имеет решающее значение. Соответственно, алгоритм НЦО должен учитывать эти факторы, чтобы обеспечить практическое решение. К сожалению, существующие методы не могут обеспечить практических решений НЦО для этого типа поражения, поскольку ухудшение ВП из-за ошибок курса обычно не учитывается для нескольких целей.

Мотивированное этими наблюдениями, это исследование было направлено на изучение и предложение подходящих алгоритмов НЦО для систем обороны для противодействия угрозам с использованием ракет на малых высотах или роев дронов. Сначала были рассмотрены две стратегии для исследования эффективности поражения относительно изменения ВП из-за ошибки курса: стратегия с фиксированным вращением (ФВ) и стратегия вращения (СВ). Стратегия ФВ фиксирует угол ориентации пусковой установки на определенном значении во время боя, а стратегия СВ поворачивает угол ориентации пусковой установки, чтобы выровнять его с углом подхода к цели. Стратегию ФВ можно рассматривать как обычный метод. Для реализации этих стратегий сначала было смоделировано изменение ВП в соответствии с изменениями ошибок курса. На основе этой модели затем были сформулированы задачи НЦО, соответствующие двум стратегиям, с использованием структуры смешанного целочисленного линейного программирования (СЦЛП). Стратегия ФВ была направлена на минимизацию времени реакции на цель, но ВП может ухудшиться из-за несоответствия между углом ориентации пусковой установки и углом подхода к цели (т. е. ненулевой ошибкой курса). И наоборот, при стратегии СВ может произойти потеря времени реакции на цель, поскольку выравнивание требует дополнительного времени. Однако более высокая ВП может быть достигнута за счет минимизации ухудшения ВП из-за ошибки курса. В результате в стратегии ФВ количество целей, которые могут быть поражены, увеличивается, но ВП

против каждой цели уменьшается. С другой стороны, в стратегии СВ количество целей, которые могут быть поражены, уменьшается, но ВП против каждой цели увеличивается.

Кроме того, это исследование дополнительно расширило две стратегии для повышения эффективности взаимодействия с несколькими целями с использованием нового метода НЦО на основе кластеризации (КНЦО). Предлагаемый метод группирует несколько целей в подмножества перед выполнением НЦО. Затем вычисляется начальный угол ориентации каждой пусковой установки, используя информацию о центроиде каждого кластера относительно каждой пусковой установки. Более конкретно, вектор расстояния, отражающий характер проблемы, путем кластеризации целей для инициализации угла ориентации пусковой установки. Вектор расстояния представляет относительную взаимосвязь между целью и несколькими пусковыми установками; поэтому цели, подходящие для поражения одной и той же пусковой установкой, могут быть назначены одному и тому же кластеру на основе вектора расстояния. Затем угол ориентации пусковой установки можно определить по целям, включенным в кластер.

Стоит отметить, что предлагаемый метод инициализации может помочь уменьшить потери ВП из-за ошибок курса в стратегии ФВ и сократить время реакции в стратегии СВ.

Список используемых источников

1. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений // Радиотехнические и телекоммуникационные системы. 2017. № 2. С. 41−49.

2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 6. С. 46−51.

3. Чуднов А. М. Курашев З. В. Особенности оптимизации распределения информационных потоков в неоднородных сетях связи, Труды академии. Научно-технический сборник № 94. Итоги науки и техники. СПб. : ВАС, 2016. Инв. № 8478. С. 244−249.

4. Manne A. S. ‘‘A target-assignment problem,’’ Oper. Res., 1957. Vol. 6. No. 3. PP. 346–351.

5. Roux J. and Van Vuuren J. ‘‘Threat evaluation and weapon assignment decision support: A review of the state of the art,’’ ORiON, Dec. 2007. Vol. 23. No. 2. PP. 151–187.

6. Ni M., Yu Z., Ma F., and Wu X. ‘‘A Lagrange relaxation method for solving weapon-target assignment problem,’’ // Math. Problems Eng., Nov. 2011. Vol. 2011. Art. No. 873292.

7. Lee Z. J., Lee C. Y., and Su S. F. ‘‘An immunity-based ant colony optimization algorithm for solving weapon–target assignment problem,’’ // Appl. Soft Comput., 2002. Vol. 2. No. 1, Pp. 39–47.

8. Zhou Y., Li X., Zhu Y., and Wang W., ‘‘A discrete particle swarm optimization algorithm applied in constrained static weapon-target assignment problem,’’ // Proc. 12th World Congr. Intell. Control Autom. (WCICA), Jun. 2016, PP. 3118–3123.

9. Bisht S. ‘‘Hybrid genetic-simulated annealing algorithm for optimal weapon allocation in multilayer defence scenario,’’ Defence Sci. J., May 2004. Vol. 54. No. 3. PP. 395–405.

10. Blodgett D. E., Gendreau M., Guertin F., Potvin J.-Y., and Seguin R. ‘‘A Tabu search heuristic for resource management in naval warfare,’’ J. Heuristics, Mar. 2003. Vol. 9. No. 2. PP. 145–169.

11. Wang J., Luo P., Hu X., and Zhang X. ‘‘A hybrid discrete grey wolf optimizer to solve weapon target assignment problems,’’ Discrete Dyn. Nature Soc., Nov. 2018. Vol. 2018. Art. No. 4674920.

12. Wang Z., Wang X., Liang Y., and Pan Q. ‘‘Weapon target assignment leveraging strong submodularity,’’ in Proc. IEEE Int. Conf. Inf. Autom. (ICIA), Aug. 2013, PP. 74–79.

13. Xin B., Chen J., Peng Z., Dou L., and Zhang J. ‘‘An efficient rulebased constructive heuristic to solve dynamic weapon-target assignment problem,’’ IEEE Trans. Syst., Man, Cybern., A, Syst. Humans, May 2011. Vol. 41. No. 3. PP. 598–606.

УДК 621.396.4
ГРНТИ 50.37.03

ПРИМЕНЕНИЕ МИКРОКОАКСИАЛЬНЫХ ВИНТОКРЫЛЫХ МАШИН В ВОЕННЫХ ДЕЙСТВИЯХ: ОБЗОР, КЛЮЧЕВЫЕ ТЕХНОЛОГИИ И СЦЕНАРИИ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ.

М. Е. Дмитриенко[1], **В. В. Ерыгин**[1], **Э. Ф. Тухбатуллина**[1]

Военная орденов Жукова и Ленина Краснознаменная академия связи
им. Маршала Советского Союза С. М. Буденного

Стиль будущих войн - это в основном локальные войны и региональные конфликты. Этот стиль войны характеризуется непредсказуемостью и нестабильностью, которая может произойти в любое время и в любом месте. Как только это происходит, поле боя становится обширным, краткосрочным и быстро меняющимся. Для того чтобы приспособиться к характеристикам этого вида войны, простая техника и короткое время реакции стали двумя важными факторами при выборе оружия. Коаксиальные винтокрылые машины широко изучаются и применяются в будущих войнах благодаря удобству переноски, хорошей приспособляемости к окружающей среде и большой грузоподъемности. В данной статье проводится обзор коаксиального вертолета. Кроме того, определяется его ключевые технологии, сценарии боевых действий и будущие направления.

беспилотный летательный аппарат, военный конфликт, многофункциональность, управление, передача данных, удобство использования, микрокоаксиальные винтокрылые машины.

Современные технологии изменили методы ведения боя различных служб и видов вооружений. Тенденция развития модернизации, сетевого взаимодействия, информатизации и кластеризации систем вооружения неудержима. Информация на поле боя может быть воспринята командным центром в кратчайшие сроки. Как только на поле боя будет найдена ценная цель, первый удар станет нормой. Это выдвигает повышенные требования к разработке будущих систем оружия. Особенно это касается систем оружия, основанных на применении в условиях хаотичных и непонятных боев, таких как городские уличные бои и бои в джунглях. Как сократить время обнаружения ценной цели, как обработать и оценить эту информацию в первый раз, как повысить точность уничтожения ценной цели и как оценить эффект уничтожения в первый раз, стали фокусом и направлением исследований в разных странах.

Страны, которые занимаются исследованиями микрокоаксиальных винтокрылых машин, в основном включают Чешскую Республику, Соединенные Штаты, Израиль и Китай.

A. Чешская Республика "Pholos". Компания Czech Defense Systems разработала "PHOLOS" (рис. 1) [1], беспилотник с коаксиальным реверсивным винтом, который был описан как «кошмар снайпера». Беспилотный летательный аппарат (БЛА) характеризуется портативностью, ситуационной осведомленностью и мгновенным ударом.

Рис. 1. Коаксиальный винтокрылый аппарат "PHOLOS" производства Чехии

B. Американский "Spirit". Компания Ascent Aero Systems разработала "Spirit" (рис. 2) [2], БЛА с коаксиальным ротором. Благодаря простой конструкции, отличным водо- и пылезащитным характеристикам, он стал самой маленькой, прочной и экологичной моделью БЛА компании. Он предназначен для выполнения задач по обеспечению общественной безопасности, военных и разведывательных миссий.

Рис. 2. Коаксиальный винтокрылый аппарат США " Spirit "

C. Израильский "Firefly". Тактический боеприпас "FireFly" (рис. 3) [3], разработанный совместно компанией Raphael и Министерством обороны, весит всего 3 кг и обеспечивает скрытую и точную атаку пехоты в условиях городской войны. Он может противостоять ветру скоростью 37 км/ч, а максимальная крейсерская скорость составляет 60 км/ч. Самолет может висеть в радиусе 500–1500 метров до 15 минут и может увеличить свою выносливость за счет быстрого извлечения и замены батарей во время тактических разведывательных миссий.

Рис. 3. Израильский Коаксиальный винтокрылый аппарат "FireFly"

D. Китайский "CH-817". Китайская компания China Aerospace Rainbow разработала миниатюрный ударный беспилотник CH-817 (рис. 4) [4]. БЛА может автономно взлетать и садиться в сложных условиях и обладает функцией осознания окружающей обстановки и обхода препятствий. Он может управляться рассредоточенным взводом или небольшими боевыми подразделениями для обнаружения движения целей внутри зданий и нанесения высокоточных смертоносных ударов по противнику.

Рекомендации по тенденциям развития. В качестве мощного оружия на поле боя, миниатюрные коаксиальные винтокрылые машины должны развиваться в направлении миниатюризации, интеллекта и многофункциональности.

Рис. 4. Китайский Коаксиальный вертолет "CH-817"

А. Миниатюризация. Микросамолет дешев и легок по весу, поэтому им можно оснастить каждого солдата без увеличения его нагрузки, что может значительно повысить боевую гибкость солдата. Его можно использовать не только для разведки, но и для укрепления контактов с личным составом и обмена информацией. В отличие от нынешних систем БЛА, требующих работы нескольких человек, он не нуждается в оснащении вспомогательным оборудованием и транспортными средствами. Он полностью управляется самостоятельно солдатами и обладает хорошей маскировкой. Когда он летит в воздухе, его не только трудно обнаружить невооруженным глазом, но и трудно обнаружить радарными детекторами.

В. Интеллектуальный. В будущем эта технология может быть расширена для реализации кластерной сети из нескольких БЛА и роевых атак. Различные летательные аппараты связаны между собой и координируются через канал передачи данных для выполнения задач, которые не может выполнить один самолет, или для повышения эффективности всей системы. Такой кластер имеет более высокую производительность, надежность и низкую стоимость.

С. Многофункциональный. Используя идеи обобщенной и модульной конструкции, и конфигурируя различные модульные задачи, можно реализовать различные оперативные возможности, такие как разведка, наблюдение, постановка помех, оценка ущерба на поле боя и атака, для удовлетворения различных оперативных требований. Для того чтобы адаптироваться к различным требованиям использования, БЛА имеет функции запуска одним человеком и запуска с транспортного средства. В будущем он также сможет осуществлять воздушный запуск и воздушное восстановление. Также возможна разработка серийных изделий различного веса для удовлетворения потребностей различных пользователей.

В последние годы БЛА были замечены в локальных войнах в некоторых частях мира.

Таким образом основными преимуществами коаксиальных винтокрылых аппаратов являются: конструкция прочнее и компактнее; имеют более высокую эффективность полета; имеют лучшую бесшумность; быстрая модульная обработка груза и легкость переноски и транспортировки.

Список используемых источников

1. (2020). G. Times. A Sniper's Nightmare? Pholos Coaxial Attack Drone. Available: https://www.yo uuvs.com/news/detail/202004/6756.html

2.(2021).U.S.Technology. Spirit Coaxial Drone. Available: https://mp.weixin.qq.com/s/FbhgdJkNBU3YXk9nDjuO3g

3. S. J. Frantzman. (2020). Israel Acquires Firefly Loitering Munition for Close Combat.Available:https://www.c4isrnet.com/unmanned/2020/05/05/israel-acquires-fireflyloitering-munition-for-close-combat/

4. (2021). KANZHAJI.COM. Can be Held by a Single Soldier-Ch817 Mini-Attack Drone Real Machine Unveiled. Available: https://mp.weixin.qq.com/s/GBG7bObz402urC_k-5UssQ .

УДК 004.043
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ С ПОМОЩЬЮ МНОГОЗАДАЧНОГО ОБУЧЕНИЯ, ОПТИМИЗИРОВАННОГО С УЧЕТОМ ПОТЕРЬ НА ОСНОВЕ НЕОПРЕДЕЛЕННОСТЕЙ

Х. Донг[1], И. В. Котенко[2]

[1]Национальный исследовательский университет ИТМО

[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Как первая и эффективная линия защиты, система обнаружения вторжений должна обеспечивать высокий показатель количества обнаруженных атак по отношению к общему количеству атак и низкий – близкий к нулевому – показатель ложных срабатываний. В статье предлагается метод многозадачного обучения с жестким разделением параметров для многоклассовой классификации трафика с использованием оптимизации потерь на основе неопределенности. Сравнение с моделями однозадачного обучения показывает, что предлагаемый подход позволяет лучше выявлять редкие вторжения.

обнаружение вторжений, глубокое обучение, многозадачное обучение.

Введение

Системы обнаружения вторжений (СОВ) являются эффективными инструментами защиты от различных сетевых атак, позволяющих анализировать сетевой трафик или поведение защищаемой системы и выявлять вредоносные шаблоны [1, 2, 3]. В последнее время глубокие модели - глубокие нейронные сети (*Deep Neural Network*, DNN), такие как сверточная нейронная сеть (*Convolutional Neural Network*, CNN), рекуррентная нейронная сеть (*Recurrent Neural Network, Long Short-Term Memory*), рекуррентная нейронная сеть с длинной кратковременной памятью (*Long Short-Term Memory*, RNN-LSTM) и автоматический кодировщик (*Auto Encoder*, AE), с успехом используются в качестве детекторов вторжений [4]. Тем не менее, реальные сетевые данные обуславливают множество проблем, связанных, например, с массивными наборами данных, несбалансированной классификацией, ограниченными помеченными данными и противоречивыми отношениями между наиболее важными факторами оценки - частотой обнаружения и ложных тревог.

Хотя исследования в области СОВ на основе глубокого обучения (*Deep Learning*, DL) - популярны, в большинстве из них используется так называемое однозадачное обучение (*Single-task Learning*, STL), основанное на собственной модели обучения для каждой решаемой задачи, как в [5,6], тогда как многозадачное обучение (*Multi-task Learning*, MTL) базируется на одной модели для нескольких связанных задач и одного набора данных [7, 8, 9]. Цель MTL – использовать одну модель для нескольких связанных задач, причем результаты обучения для нескольких задач должны превосходить результаты обучения по отдельной задаче. Это подходит для ситуации, когда имеется много размеченных данных для одной задачи, но очень мало размеченных данных для других связанных задач, а знания, полученные из первой задачи, могут принести пользу процессу обучения для других задач. Таким образом, данные используются продуктивно, а временные затраты на обучение моделей сокращаются. В работе для обнаружения вторжений предлагаются модели MTL, основанные на CNN.

Релевантные работы

Существующие модели обнаружения вторжений на основе MTL базируются на двух подходах: (1) представлении многоклассовой классификации известного трафика как одной задачи и одновременном выполнении других задач [7, 8, 12], или (2) представлении задачи классификации различных типов трафика как отдельной задачи [9, 10, 11]. Использование этих подходов ограничивается проблемами, связанными с отсутствием интерпретированных (помеченных) данных для редких атак [7, 11], несбалансированной классификацией [12] и обнаружением новых атак [8].

Предлагаемый подход

MTL эффективен для использования в нескольких связанных задачах и может использоваться как регуляризатор, чтобы минимизировать риск переобучения и увеличить обобщение для адаптации к новым задачам. Предлагаемый метод включает: (1) многозадачный выбор признаков с эластичной регуляризацией сети, в которой для регуляризации вычисляются запасные коэффициенты с линейной смесью норм l_1, l_2 и l_2 [13]. Он поддерживает как общие, так и специфичные для задачи признаки и подходит для всех задач; (2) использование гибридных методов повторной выборки (*resampling*) с синтетической избыточной выборкой меньшинства (*Synthetic Minority Oversampling Technique*, SMOTE), выполняющие повторную выборку путем вычисления новых выборок на основе правила K ближайших соседей (*K-nearest-Neighbor*, KNN) и отредактированных ближайших соседей (*Edited Nearest Neighbors*, ENN), удаляющих нечеткость из существующих выборок и улучшающих границы между классами; (3) классификацию на основе MTL с тремя функциональными модулями - (а) общие слои, (б) скрытые слои для конкретных задач для бинарных задач классификации различных атак и (в) функциональный слой для оптимизации потерь.

Архитектура модели

Сеть на основе CNN является вертикально глубокой, имеет четыре сверточных слоя, три объединяющих слоя с нормализацией в основной ветви и один сверточный слой с нормализацией в боковой ветви. Боковая ветвь предназначена для обучения низкоуровневых слоев и сохранения этой информации, которая будет связана с глубоко объединенными признаками на промежуточном уровне. Идея использования боковой ветви для извлечения низкоуровневых деталей вдохновлена моделью Hyperface [14]. Затем в специализированном модуле с помощью латентных слоев выполняются разные задачи, а именно бинарная классификация разных типов сетевого трафика. Наконец, функциональный слой для оптимизации потерь принимает все результаты классификации и истинные значения всех задач и вычисляет минимальные общие потери, а также веса задач. Предложенная архитектура представлена в таблице 1 (см. ниже).

Определение потерь

В MTL с T задачами и вектором весов W общие потери равны $L_{total} = \sum_{t\in T}^{T} W_t \cdot L_t$. В работе используется метод оптимизации весов на основе неопределенности, предложенный в [15]. Он использует гомоскедастическую (homoscedastic) неопределенность для нескольких задач, чтобы автоматически вывести относительные веса потерь задач целью минимизации

общих потерь. Используя функцию *softmax* для вычисления вероятностной модели для задач классификации, общие потери можно сформулировать как as $\mathrm{L}(\mathrm{W}, \sigma_1, \ldots, \sigma_t) = \sum_{t=1}^{T} \frac{1}{2\sigma_t^2} L_t(W) + \left(log\sigma_1 + \cdots + log\sigma_t\right)$, тогда как $\{\sigma_1, \ldots, \sigma_t\}$ обозначает соответствующие шумы, наблюдаемые для каждой задачи.

ТАБЛИЦА 1. Архитектура модели MTL

Модуль	Слои	Функция активации	Метод регуляризации
Shared Layers-main branch With 3 cycles	conv1D(256)-MaxPooling1D(3)-BatchNormalization conv1D(512)-MaxPooling1D(1)-BatchNormalization conv1D(256)-MaxPooling1D(1)-BatchNormalization	relu	Dropout=0.1
Shared layers-side branch	Conv1D(256)-BatchNormalization	relu	Dropout=0.1
Shared layers- combine & flatten	Concatenate-BatchNormalization-Conv1D(256)-flatten-Dense(1024)	relu	Dropout=0.1
Task-specific Layers	Dense(32)-Dense(1)	relu, sigmoid	Dropout=0.1

Эксперименты

Базовыми моделями являются четыре модели глубокого обучения STL, представленные в [16]: (1) 5-уровневая DNN, (2) CNN с двумя сверточными слоями и одним объединяющим слоем, (3) трехуровневая RNN и (4) четырехуровневая LSTM. Для активации все бинарные модели используют сигмовидную функцию (*Sigmoid*), а все модели классификации с несколькими метками используют функцию Softmax. Все модели протестированы на наборе данных NSL-KDD [17], содержащего пять типов трафика: normal traffic, DoS, probe, R2L и U2R.

Эффективность оценивается по традиционным показателям обнаружения вторжений - accuracy, precision, recall (также известному как частота обнаружения (*Detection Rate*, DR)) и частоте ложных срабатываний (*false positive rate*, FPR). Как показано в таблице 2, при обнаружении вторжений предлагаемая модель превосходит все базовые модели по показателям accuracy и recall, с хорошим показателем precision и приемлемым уровнем ложных срабатываний (FPR). В классификации трафика с несколькими метками (многоуровневой классификации трафика) MTL превосходит все остальные в U2L и U2R, хотя уступает при обнаружении Probe по сравнению с CNN и RNN. В целом, MTL имеет более сбалансированные показатели на разных типах трафика и лучше работает с редкими классами, тогда как STL имеет тенденцию смещаться к большинству. Таблица 3 доказывает

эффективность функции оптимизации потерь. После подстройки весов задач, соответствующих возможно наименьшим потерям, эффективность на четырех типах трафика улучшается. Кроме того, для модели MTL уровень ложных срабатываний для всех вторжений относительно низок: самый высокий показатель составляет 3,7 %, а самый низкий - 0,2 %. Поскольку для СОВ обычно ожидается контролируемая частота ложных срабатываний, MTL, несомненно, имеет преимущества, особенно при редких атаках.

ТАБЛИЦА 2. Результаты экспериментов

	Бинарное обнаружение вторжений				DR для многоуровневой классификации трафика				
	Accuracy	*Precision*	*Recall*	*FPR*	*Normal*	*DoS*	*Probe*	*R2L*	*U2R*
DNN	0.7934	0.9668	0.6598	0.03	0.97	0.77	0.64	0.15	0.09
CNN	0.7923	0.9688	0.6562	0.0279	0.97	0.8	0.75	0.08	0.12
RNN	0.7653	0.857	0.7054	0.1556	0.97	0.76	0.7	0	0.12
LSTM	0.8078	0.9651	0.6873	0.0328	0.97	0.79	0	0	0
MTL	**0.817**	**0.9523**	**0.7143**	**0.0473**	**0.95**	**0.73**	**0.64**	**0.22**	**0.39**

ТАБЛИЦА 3. Оцениваемые показатели до и после оптимизации

	DoS		R2L		U2R		Normal		Probe	
	До	*После*	*До*	*После*	*До*	*После*	*До*	*После*	*До*	*После*
Accuracy	0.906	0.900	0.877	0.878	0.995	0.997	0.819	0.826	0.925	0.928
Precision	0.962	0.953	0.541	0.556	0.290	0.406	0.717	0.727	0.663	0.676
Recall	0.746	0.734	0.240	0.223	0.403	0.388	0.957	0.954	0.620	0.637
FPR	0.015	0.018	0.030	0.026	0.003	0.002	0.285	0.271	0.038	0.037

Заключение

В статье предложен гибридный подход к обнаружению вторжений на основе MTL, который позволяет определять метки классов трафика как отдельные задачи бинарной классификации. Подход основан на использовании глубокой нейронной сети на основе CNN и многозадачной оптимизации потери весов на основе неопределенности. По результатам эксперимента на наборе данных NSL-KDD предложенная реализация MTL обеспечила сбалансированные показатели эффективности на всех типах трафика, но лучше по сравнению с другими исследованными подходами она работает при ограничении размеченных данных. В последующих исследованиях предполагается протестировать предлагаемый подход на основе актуальных наборов сетевых данных Интернета вещей, оптимизировать гиперпараметры и архитектуру модели.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Росс. академии наук. 2014. Т. 84, N 11. С. 993–1001.

2. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference “Simulation in wider Europe”. ECMS 2005. Riga, Latvia, 1–4 June 2005. PP. 533–543.

3. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. 2018. Vol. 6. PP. 72714–72723. DOI: 10.1109/ACCESS.2018.2881998.

4. Mahdavifar S., Ghorbani A. A. Application of deep learning to cybersecurity: a survey // Neurocomputing. 2019. V. 347. PP. 149–176.

5. Branitskiy A., Kotenko I.V. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. Vol. 23. PP. 145–156.

6. Desnitsky V.A., Kotenko I.V., Nogin S.B. Detection of anomalies in data for monitoring of security components in the Internet of Things // International Conference on Soft Computing and Measurements, St. Petersburg, Russia, 2015. PP. 189–192.

7. Huang W., Stokes J.W. MtNet: a multi-task neural network for dynamic malware classification // Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Donostia-San Sebastián, Spain, 2016. PP. 399–418.

8. Li B., Lin Y., Zhang S. Multi-task learning for intrusion detection on web logs // Journal of Systems Architecture. 2017. Vol. 81. PP. 92–100.

9. Albelwi S. A. An intrusion detection system for identifying simultaneous attacks using multi-task learning and deep learning // 2nd International Conference on Computing and Information Technology. 2022. PP. 349–353.

10. Huang H., Deng H., Chen J., Han L., Wang W. Automatic multi-task learning system for abnormal network traffic detection // International Journal of Emerging Technologies in Learning. 2018. Vol. 13. PP. 4–20.

11. Aljoufi R., Lasebae A. Multi-task learning for intrusion detection and analysis of computer network traffic // E3S Web of Conferences. 2021. Vol. 229. PP. 1–7.

12. Sun L., Zhou Y., Wang Y., Zhu C., Zhang W. The effective methods for intrusion detection with limited network attack data: multi-task learning and oversampling // IEEE Access. 2020. V. 8. PP. 185384-185398.

13. Zou H., Hastie T. Regularization and variable selection via the Elastic Nets // Journal of the Royal Statistical Society. Series B. 2005. V. 67. PP. 301–320.

14. Ranjan, R., Patel, V. M., Chellappa, R. Hyperface: a deep multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019. V. 41. PP. 121–135.

15. Kendall A., Y. Gal, R. Cipolla. Multi-task learning using uncertainty to weigh losses for scene geometry and semantics // IEEE Computer Vision and Pattern Recognition. 2018. PP. 7482–7491.

16. Vinayakumar R., Soman K. P., Poornachandran P. A comparative analysis of deep learning approaches for network intrusion detection systems (N-IDSs): deep learning for N-IDSs // International Journal of Digital Crime and Forensics. 2019. No. 11 (3). PP. 65–89.

17. Tavallaee M., Bagheri E., Lu, W., Ghorbani A. A. A detailed analysis of the KDD CUP 99 data set // IEEE Symposium on Computational Intelligence for Security and Defense Applications. 2009. PP. 1–6.

УДК 004.75
ГРНТИ 81.93.29

АЛГОРИТМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК НА ИНТЕЛЛЕКТУАЛЬНЫЕ ТРАНСПОРТНЫЕ СИСТЕМЫ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА БЛОКЧЕЙН

Е. А. Донсков, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Системы передачи и хранения информации являются неотъемлемой частью жизни человечества. С каждым годом развитие систем, способов хранения и передачи информации развивается с учетом возникающих требований - проводные системы, беспроводные системы, системы движущихся объектов. Помимо необходимости хранения и передачи информации в специфических условиях немаловажную роль играет безопасность хранения и передачи данных. В последнее время наиболее популярной тенденцией при обеспечении безопасности данных в подобных системах является частный случай технологий распределенных реестров – технология блокчейн. В рамках работы авторы рассматривают вопросы безопасности интеграции технологии блокчейн на примере интеллектуальных транспортных систем – одного из видов систем движущихся объектов. Помимо обзора основных атак, наиболее характерных для подобных систем с учетом интеграции технологии блокчейн, авторы рассматривают алгоритмы для обнаружения атак, а также методы их предотвращения.

интеллектуальные транспортные системы, блокчейн.

Системы передачи и хранения информации являются неотъемлемой частью жизни человечества. С каждым годом развитие систем, способов хранения и передачи информации развивается с учетом возникающих требований - проводные системы, беспроводные системы, системы движущихся объектов. Помимо необходимости хранения и передачи информации в специфических условиях немаловажную роль играет безопасность хранения и передачи данных. В последнее время наиболее популярной тенденцией при обеспечении безопасности данных в подобных системах является частный случай технологий распределенных реестров – технология блокчейн.

Блокчейн в рассмотрении концепции ITS является децентрализованной платформой для организации доступности приложений в реальном времени и установлении защищенного соединения между компонентами транспортной инфраструктуры. Несмотря на достоинства, системы ITS с применением технологии блокчейн крайне уязвимы для атак злоумышленниками

ввиду своей самоорганизующейся природы и использовании программных продуктов с открытым исходным кодом. Целью проведенного в данной работе исследования является выделение ряда атак, наиболее свойственных при интеграции блокчейн-решений в интеллектуальные транспортные системы, а также выделение алгоритма обеспечения защиты от приведенных атак.

На данный момент выделяются следующие типы атак: (1) атаки на физическом уровне; (2) атаки на сетевом уровне; (3) атаки, связанные с программным обеспечением.

Атаки на физическом уровне

– **Атака фальсификации** – это тип атаки на систему, в котором злоумышленник пытается подделать компоненты системы для получения несанкционированного доступа или для изменения ее функциональности.

Для предотвращения такой атаки необходимо использовать физический доступ к компонентам системы только для авторизованных лиц или использование устройств с маркировкой подлинности [1].

– **Атака внедрения вредоносного кода** – это тип атаки на систему, в котором злоумышленник пытается внедрить вредоносный код непосредственно в физические компоненты системы.

Для предотвращения такой атаки важно применять комплекс мер безопасности: использование аппаратных модулей безопасности, регулярное обновление программного обеспечение и прошивки компонентов системы, осуществление физического контроля за процессом производства и монтажа компонентов и регулярные проверки на наличие вредоносного кода в системе [2].

– **Атака помех** заключается в создании помех, с целью потери связи между устройствами, участвующими в транспортной системе.

Для защиты от таких атак необходимо использовать средства антенной защиты и алгоритмы, которые могут распознавать и отслеживать помехи в системе. Также необходимо убедиться, что устройства, соответствуют требованиям по электромагнитной совместимости, чтобы минимизировать возможность возникновения помех в системе [1].

– **Атака инъекции поддельного узла** – это тип атаки, когда злоумышленник представляет себя в качестве узла сети.

В блокчейне наиболее эффективный метод – использование механизмов консенсуса. Каждый узел в сети блокчейн должен согласовать любое новое предложение, прежде чем оно может быть принято в целостную версию блокчейна.

– **Атака отказа в обслуживании** – перегрузка системы трафиком или запросами до тех пор, пока система не станет недоступна для легитимного

использования. В случае с ITS на блокчейне, атака может быть направлена на узел сети, который обрабатывает транзакции.

Для защиты стоит использовать алгоритмы мониторинга и обнаружения аномалий, для выявления атаки до того, как она приведет к отказу в работе системы.

– **Атака по побочному каналу** – это метод атаки на систему, который основывается на изучении побочных эффектов, которые происходят во время работы системы и позволяют получить конфиденциальную информацию.

Для защиты от атак по побочному каналу необходимо проводить анализ уязвимостей, внедрять меры по защите от электромагнитных излучений, криптографической защите, физической защите устройств и инфраструктуры системы.

Атаки на сетевом уровне

– **Атака «Сивилла»** (*Sybil attack*) – это тип атаки, при котором злоумышленник создает большое количество ложных идентификационных данных (узлов), с целью захвата контроля над сетью [3].

Один из способов защиты от атаки «Сивилла» – это использование алгоритмов консенсуса и механизма проверки репутации узлов [4]. При таком подходе, узлы считаются надежными, если они успешно завершили несколько проверок или транзакций в прошлом. Это позволяет избежать возможности создания ложных узлов и улучшить целостность данных в сети.

В целом, для защиты интеллектуальных транспортных систем от атак типа "Сивилла" необходимы методы машинного обучения.

– **Атака анализа трафика** является одной из распространенных угроз. Злоумышленник перехватывает трафик между узлами системы, и анализирует чтобы получить конфиденциальную информацию или провести другие виды атак.

Для защиты от атаки анализа трафика системы должны использовать современные методы шифрования и другие механизмы безопасности, такие как идентификация узлов системы и аутентификация пользователей.

– **Атака маршрутизации информации** – изменение информации о маршруте передачи данных между узлами сети. Эта атака может быть использована злоумышленниками для перехвата, модификации или уничтожения передаваемых данных.

Для защиты от атаки маршрутизации должны быть предприняты следующие меры: аутентификация узлов сети, шифрование данных, проверка маршрутов, использование устройств защиты сетевого уровня – специализированных устройств обнаружения и предотвращения атак маршрутизации информации.

– Атака выборочной переадресации – это атака, при которой злоумышленник перехватывает и выборочно пересылает только те сообщения, которые ему нужны, а остальные сообщения блокируются.

Подобная атака направлена на передачу ложной информации о маршрутах движения транспортных средств или передачу ложных данных о состоянии дорожных условий, что может привести к авариям и несчастным случаям. Также атака может быть направлена на увеличение времени ожидания на светофорах и других дорожных знаках, что приводит к пробкам и увеличению времени на дороге.

Для предотвращения следует использовать контроль целостности данных и проверки подлинности сообщений.

– **Атака червоточины** является серьезной угрозой для интеллектуальных транспортных систем. Эта атака позволяет злоумышленнику получить доступ к сообщениям, передаваемым между двумя удаленными узлами, и даже модифицировать или вставить свои сообщения в передаваемый поток [5].

Для защиты необходимо использование криптографических методов для обеспечения безопасности передаваемых сообщений, мониторинг и анализ трафика.

– **Атака «человек посередине»** – это тип атаки, при котором злоумышленник пытается перехватить и изменить коммуникации между двумя узлами в сети. Для защиты от MITM-атак важно использовать защищенные протоколы и шифрование трафика, а также быть осторожным при использовании общественных Wi-Fi-точек доступа и других ненадежных сетей.

– **Атака повтора** – это атака, при которой злоумышленник перехватывает сетевой трафик и повторно отправляет ранее перехваченные пакеты данных. Подобные атаки могут быть использованы для манипулирования транзакциями, а затем привести к потере средств или другим нежелательным последствиям [6].

Для защиты необходимо использовать метки времени или уникальные идентификаторы транзакций, которые позволят отличать повторные транзакции от оригинальных, цифровые подписи и хеширование.

Атаки, связанные с программным обеспечением

– **Атаки с помощью вирусов** представляют серьезную угрозу для интеллектуальных транспортных систем. После инфицирования устройства пользователя, злоумышленники могут получить доступ к личным данным, хранящимся в приложении, или использовать приложение для совершения несанкционированных транзакций на блокчейне [7].

Для защиты следует установить антивирусное программное обеспечение и регулярно обновлять его, не устанавливать программы из ненадежных источников, использовать двухфакторную аутентификацию. Также важно

регулярно проверять устройства на наличие вирусов, чтобы быстро выявлять их и принимать меры к удалению.

На основе проанализированных данных обобщенный класс алгоритмов по защите интеллектуальных транспортных систем выглядит следующим образом:

1. Шифрование данных: выполняется сильное шифрование данных.
2. Аутентификация и авторизация: дают возможность гарантировать, что только авторизованные пользователи могут получать доступ к системе и выполнять операции.
3. Проверка подлинности данных: позволяет использовать механизмы проверки подлинности данных, такие как цифровые подписи.
4. Контроля доступа: дает возможность определять, кто может получить доступ к определенным ресурсам системы и какие операции могут выполняться.
5. Мониторинг системы: необходимо постоянно мониторить систему и обнаруживать любые аномалии в ее работе.
6. Обновление системы и программного обеспечения: необходимо регулярно обновлять ее и устанавливать последние версии программного обеспечения, которые содержат исправления уязвимостей и багов.
7. Обучение пользователей: необходимо обучать пользователей правилам безопасности и требованиям к паролям, а также предупреждать их об опасных действиях, которые могут привести к компрометации системы.

Проведенное исследование позволяет выделить общий подход к обеспечению защиты от приведенного ряда атак на блокчейн-системы в области интеллектуальных транспортных систем. Дальнейшие исследования авторов предполагают уточнение алгоритма, апробацию и выделение частных случаев защиты от приведенного набора атак.

Список используемых источников

1. Ahemd M. M., Shah M. A., Wahid A. IoT security: a layered approach for attacks and defenses // 2017 International Conference on Communication Technologies. 2017. PP. 104–110.

2. Ling Z., Liu K., Xu Y., Jin Y., Fu X. An end-to-end view of iot security and privacy // IEEE Global Communications Conference. 2017. PP. 1–7.

3. John F. Buford, Heather Yu, Eng Keong Lua. P2P Networking and Applications : Morgan Kaufmann, 2009. PP. 319-340.

4. Li G., Wu J., Li J., Guan Z. and Guo L. Fog Computing-Enabled Secure Demand Response for Internet of Energy Against Collusion Attacks Using Consensus and ACE // IEEE Access. 2018. PP. 11278–11288.

5. Parvathy K. Wormhole Attacks in Wireless Sensor Networks (Wsn) & Internet of Things (IoT) // International Journal of Recent Technology and Engineering (IJRTE). 2021.Vol-10 Is-1.

6. Mosenia, A., Jha, N.K. A comprehensive study of security of internet-of-things // IEEE Transactions on Emerging Topics in Computing. 2017. N 5 (4). PP. 586–602.

7. Konigsmark S. T. C., Chen D., Wong M. D. F. Information dispersion for trojan defense through high-level synthesis // 53nd ACM/EDAC/IEEE Design Automation Conference (DAC). 2016. PP. 1–6.

УДК 004.056.53
ГРНТИ 49.33.35

ОЦЕНКА ВРЕМЕНИ ДЛЯ БЛОКИРОВКИ НЕЛЕГИТИМНЫХ ТОЧЕК ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ

В. Е. Дрепа, М. М. Ковцур, Т. В. Петрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время одной из наиболее распространённых атак на корпоративную сеть является подключение нелегитимной точки доступа. С её помощью злоумышленник может получить доступ к защищённой сети предприятия, что даёт ему возможность запускать различные типы сканеров уязвимости, а также возможность совершать атаки на сеть удалённо, не находясь непосредственно в самой организации. Поэтому каждая компания должна уметь бороться с данной атакой эффективно и, что немаловажно, быстро. В докладе представлен один из методов блокировки нелегитимных точек доступа в корпоративной сети. Проведено теоретическое и практическое тестирование оценки времени нахождения нелегитимной точки доступа в проводной сети, а также её отсечение от сети предприятия.

автоматизация, Ansible, безопасность, беспроводные нелегитимные точки доступа.

Корпоративные сети зачастую имеют достаточно сложную архитектуру, в которой могут быть различные устройства, включая беспроводные точки доступа. В некоторых случаях, эти устройства могут быть установлены без разрешения администратора сети и представлять угрозу для безопасности корпоративной сети [1, 2]. Для обнаружения таких устройств можно использовать систему управления конфигурациями Ansible [3, 4].

Модуль Ansible для обнаружения нелегитимных беспроводных точек доступа может работать следующим образом:

1. Сбор информации о сети. Скрипт может собирать информацию о сети, включая список IP-адресов, MAC-адресов и другую информацию об устройствах, подключенных к сети.

2. Проверка легитимности устройств. С помощью модуля можно проверить легитимность каждого из обнаруженных устройств, используя список доверенных устройств или другие методы.

3. Отсечение нелегитимных устройств. После проверки сетевого оборудования, подключенного к корпоративной сети, можно автоматически отсекать нелегитимные устройства.

4. Оповещение администратора сети. Если скрипт обнаружит нелегитимные беспроводные точки доступа, он может оповестить администратора сети о возможной угрозе и предложить дальнейшие действия.

Данный модуль может быть полезен для обеспечения безопасности корпоративной сети и предотвращения возможных утечек данных [5, 6]. Он может работать автоматически и регулярно проверять сеть на наличие нелегитимных беспроводных точек доступа, что позволит своевременно выявлять и устранять угрозы.

Оценка времени для блокировки нелегитимных точек доступа в корпоративной сети зависит от многих факторов, таких как размер и модель сети [7], количество устройств, их тип и назначение, наличие доверенных устройств и т. д.

В целом, время для блокировки нелегитимных точек доступа в корпоративной сети может варьироваться от нескольких часов до нескольких дней, в зависимости от сложности сети и количества обнаруженных устройств. Однако, использование автоматизированных инструментов, таких как Ansible, может существенно ускорить этот процесс.

Время блокировки может быть значительно увеличено, если будет необходимо проверять легитимность каждого обнаруженного устройства вручную или если будут обнаружены множественные нелегитимные беспроводные точки доступа. В случае использования модуля Ansible для обнаружения нелегитимных беспроводных точек доступа, время блокировки может быть значительно сокращено благодаря автоматизации процесса.

Для поиска и блокировки нелегитимных беспроводных точек в корпоративной сети в данной работе используется playbook Ansible.

На рис. 1 представлена блок-схема работы playbook’a. Алгоритм заключается в следующем: сначала происходит обращение к коммутаторам посредством протокола SNMP и извлекаются значения MAC-адресов, индексы портов и название портов, указанные в таблице коммутации на коммутаторах, далее из SQL-таблицы “verification” (табл. 1) извлекаются значения MAC-адресов устройств, которые помечены как нелегитимные устройства (флаг “R”).

Затем происходит сравнение MAC-адресов, полученных с коммутаторов, и MAC-адресов из SQL-таблицы “verification”. Если они идентичны, то блокируется порт коммутатора, к которому подключено устройство с данным MAC-адресом. Данное событие записывается в SQL-таблицу

“alert” (табл. 2), для того чтобы сетевой администратор смог отследить, когда и на каком устройстве произошло отключение порта. После проверки всех коммутаторов скрипт завершает свою работу.

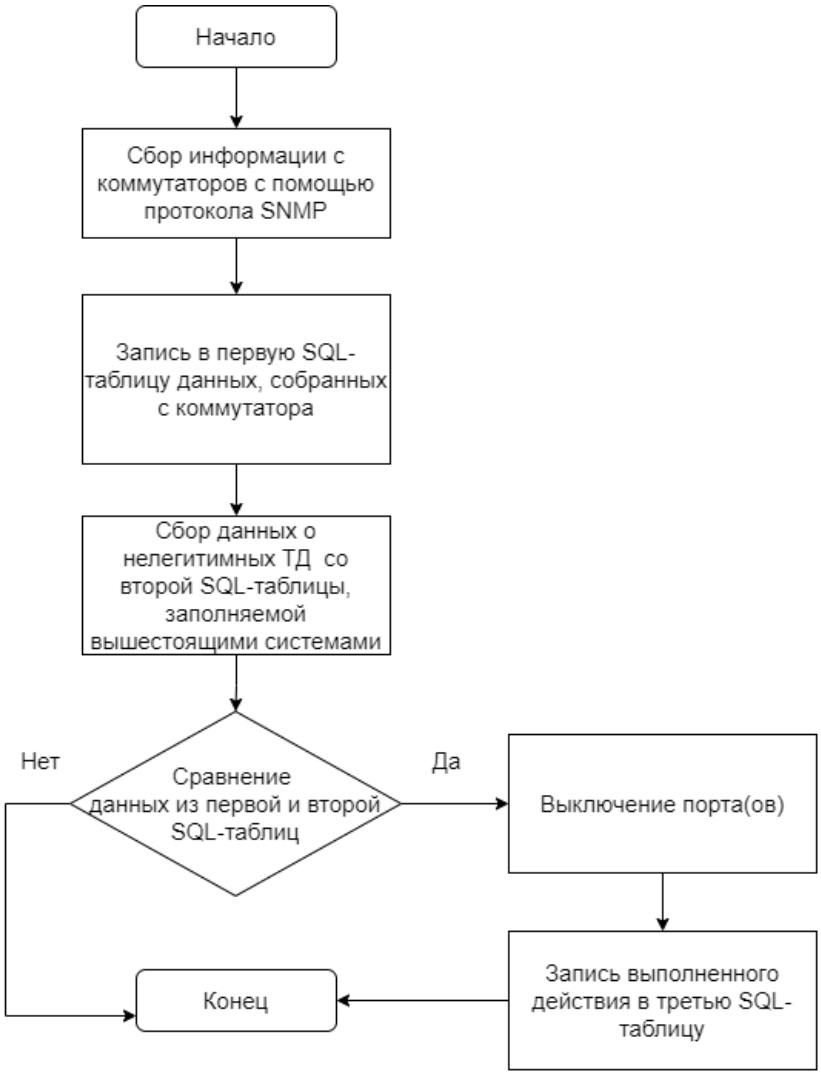


Рис. 1. Блок-схема playbook’a

ТАБЛИЦА 1. Пример заполнения SQL-таблицы “verification”

name	ipadd	macadd	flag
arm	192.168.0.1	00:5c:32:dc:5b:c2	V
unknown	-	00:08:71:4c:68:01	R

ТАБЛИЦА 2. Пример заполнения SQL-таблицы “alert”

ip	port_index	time	action
192.168.10.3	1	2023-01-26 16-37-11	shutdown
192.168.20.7	2	2022-01-26 11-54-03	shutdown

Помимо необходимости отсечения нелегитимного устройства от корпоративной сети, также очень важно учитывать, сколько будет потрачено времени на выполнение данных действий. Каждая компания должна уметь не только бороться с нелегитимными точками доступа, но своевременно и быстро отсекать их от сети.

Оценка времени для блокировки нелегитимных точек доступа [8] в корпоративной сети рассчитывается из следующих составляющих:

1. Времени запуска playbook и проверку каждого коммутатора:

- сбор всех MAC-адресов и соответствующих им индексов портов с коммутаторов;
- скорость обработки запроса коммутатором.

2. Времени на обнаружение нелегитимных MAC-адресов и блокировку портов на коммутаторах:

- обработка скрипта, сравнение SQL-таблиц и поиск нелегитимной беспроводной точки доступа;
- отправка запроса на блокировку порта коммутатора, отработка запроса самим коммутатором.

3. Времени на документирование процесса и результатов:

- сбор информации о выполненных действия в SQL-таблицу и обработка полученных данных администратором сети.

Был произведён эксперимент с тремя, двумя и одним коммутаторами. Результаты эксперимента представлены на рис. 2. При отработке скрипта в трёх разных экспериментах было произведено отключение двух портов на двух разных коммутаторах, за исключением эксперимента с одним коммутатором – на нем был отключен один порт.

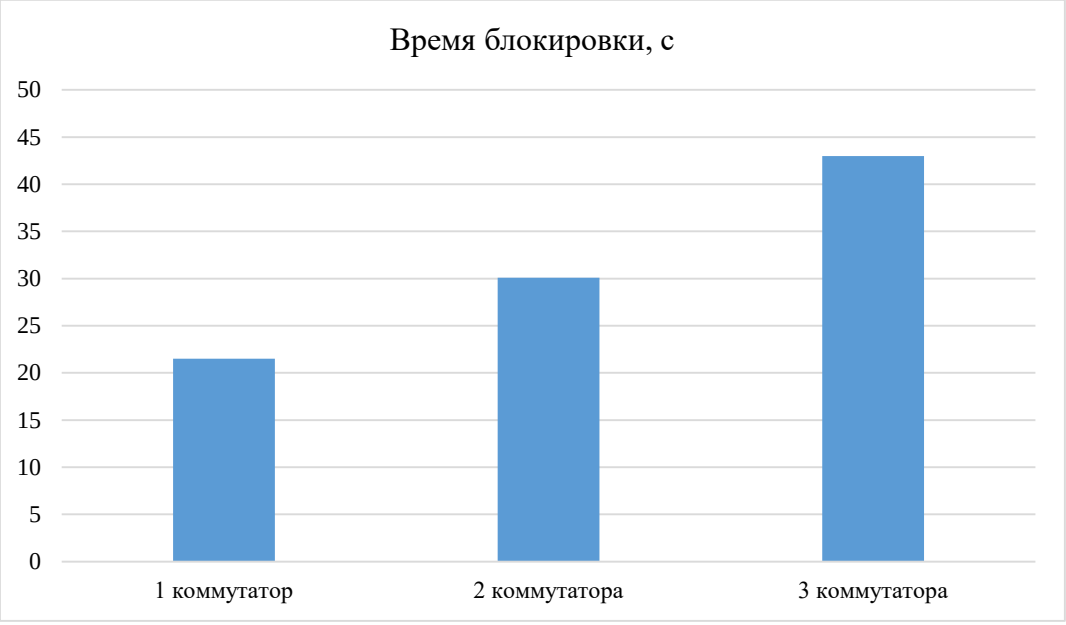


Рис. 2. Время блокировки

Можно сделать вывод о том, что с помощью предложенного метода, время, затраченное на блокировку беспроводных нелегитимных точек доступа, может занимать от нескольких секунд до нескольких минут, в зависимости от размера сети и количества коммутаторов, а также от количества обнаруженных нелегитимных точек доступа. Данный метод значительно сокращает время, которое могло бы быть потрачено на блокировку нелегитимных устройств в корпоративной сети, если бы данную задачу сетевой администратор выполнял вручную.

Список используемых источников

1. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении. 2016. С. 670–675.

2. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных. СПб. : СПбГУТ, 2019. С. 92.

3. Ковцур М. М., Коновалова В. В., Мисливский Б. С., Михайлова А. В., Акилов М. В. Разработка методики удаленного мониторинга трафика в корпоративных сетях // Заметки ученого. 2021. N 6-1. С. 27–31.

4. Красов А. В., Косов Н. А., Холоденко В. Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. N 13-2 (37). С. 243–247.

5. Ушаков И. А., Котенко И. В., Овраменко А. Ю., Преображенский А. И., Пелёвин Д. В. комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 4. С. 66–71.

6. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 734–739.

7. Савинов Н. В., Токарева К. А., Ушаков И. А., Красов А. В., Сахаров Д. В. исследование модели сети ЦОД на основе политик Cisco ACI // Защита информации. Инсайд. 2019. N 4 (88). С. 32-43.

8. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Оценка рисков и угроз безопасности в среде «Умный дом» // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 316–321.

УДК 004.732
ГРНТИ 49.43.29

ТЕХНОЛОГИЯ MU-MIMO В СЕТЯХ СТАНДАРТА IEEE 802.11AC

Р. А. Дунайцев, А. В. Светова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С ратификацией дополнения IEEE 802.11ac в 2013 году появилась возможность, используя технологию MU-MIMO, осуществлять доставку кадров данных нескольким клиентским устройствам одновременно. Для этого и точка доступа или Wi-Fi роутер, и клиентские устройства должны поддерживать функцию формирование луча в многопользовательском режиме. Как много Wi-Fi устройств, выпускаемых сегодня, поддерживают технологию MU-MIMO и как обнаружить ее использование в беспроводной локальной сети стандарта IEEE 802.11ac? Поиску ответов на эти вопросы и посвящено данное исследование.

IEEE 802.11ac, MU-MIMO, Wave 2, Wi-Fi 5.

Стандарт IEEE 802.11, описывающий обмен информацией между устройствами в беспроводных локальных (*Local Area Network*, LAN) и городских (*Metropolitan Area Network*, MAN) сетях, увидел свет в 1997 году [1]. С тех пор стандарт постоянно дополнялся и переиздавался. Так, дополнение IEEE 802.11b (известное как первое поколение Wi-Fi, Wi-Fi 1) позволило повысить скорость передачи кадров от исходных 1 или 2 Мбит/с до 5,5 или 11 Мбит/с за счет использования комплементарного кодирования (*Complementary Code Keying*, CCK) вместо кода Баркера [2]. Дополнение IEEE 802.11a (известное как второе поколение Wi-Fi, Wi-Fi 2) открыло доступ к частотному диапазону 5 ГГц, а с переходом к технологии мультиплексирования с ортогональным частотным разделением каналов (*Orthogonal Frequency Division Multiplexing*, OFDM) максимальная скорость передачи кадров выросла до 54 Мбит/с [3]. С выходом дополнения IEEE 802.11g (известного как третье поколение Wi-Fi, Wi-Fi 3) появилась возможность использовать технологию OFDM и в диапазоне 2,4 ГГц [4]. Дополнение IEEE 802.11n (известное как четвертое поколение Wi-Fi, Wi-Fi 4) принесло еще больше новшеств, что позволило увеличить максимальную скорость передачи кадров до 600 Мбит/с как в диапазоне 2,4 ГГц, так и в диапазоне 5 ГГц [5]. Однако во всех этих дополнениях передача кадров данных могла происходить лишь в однопользовательском (*Single-User*, SU) режиме. Возможность работы в многопользовательском (*Multi-User*, MU)

режиме с доставкой кадров данных нескольким клиентским устройствам одновременно появилась с ратификацией дополнения IEEE 802.11ac (известного как пятое поколение Wi-Fi, Wi-Fi 5) [6]. В основе данной технологии, получившей название многопользовательский множественный вход/множественный выход (*Multi-User Multiple-Input/Multiple-Output,* MU-MIMO), лежит использование технологии формирования луча (*Transmit Beamforming,* TxBF) [7], появившейся в дополнении IEEE 802.11n и получившей дальнейшее развитие в IEEE 802.11ac и IEEE 802.11ax (известном как шестое поколение Wi-Fi, Wi-Fi 6) [8]. Причем в IEEE 802.11ac описаны два варианта этой технологии: однопользовательский (*SU Beamforming*) и многопользовательский (*MU Beamforming*). Однако оба эти варианта являются опциональными, поэтому далеко не все выпускаемые устройства поддерживают TxBF и, соответственно, MU-MIMO.

Устройства IEEE 802.11ac без MU-MIMO принято относить к первой волне (*Wave* 1), а устройства IEEE 802.11ac с поддержкой MU-MIMO – ко второй (*Wave* 2). На рынок такие устройства стали поступать лишь в 2016 году [9]. Как много подобных устройств продается сегодня, по прошествии 10 лет с момента выхода дополнения IEEE 802.11ac? Попробуем это оценить на примере оборудования компании TP-Link, поставляемого в Россию [10]. Согласно таблице 1 (см. ниже), доля точек доступа с поддержкой MU-MIMO составляет 81,8 % от соответствующего модельного ряда, Wi-Fi роутеров – 74,3 %, а Wi-Fi адаптеров – всего лишь 26,0 %. При этом стоит учитывать, что для передачи данных в режиме MU-MIMO требуется поддержка этой технологии как со стороны точки доступа или Wi-Fi роутера, так и со стороны клиентских устройств. Чтобы получить представление, как много мобильных устройств (смартфонов, планшетов и ноутбуков) поддерживают MU-MIMO, воспользуемся данными, представленными на странице инженера компании Google Майка Албано [11]. Из 282 протестированных моделей клиентских устройств, 190 (67,4 %) поддерживают Wi-Fi 5 и 6. Из них 45 поддерживают MU-MIMO, 108 не поддерживают, а функционал 37 в части MU-MIMO остался неизвестным, поскольку перехват кадров Association Request, в которых клиентское устройство сообщает о своих возможностях, был выполнен в диапазоне 2,4 ГГц, где нет Wi-Fi 5. Исключая из рассмотрения такие устройства, получаем, что поддержка MU-MIMO есть у 18,4 % протестированных моделей. Следовательно, можно предположить, что передача кадров данных в многопользовательском режиме представляет собой нечастое явление в современных сетях Wi-Fi.

Как обнаружить использование MU-MIMO в сети стандарта IEEE 802.11ac, если эта технология все же поддерживается взаимодействующими устройствами? Разработчики анализаторов трафика ничего не говорят про перехват кадров данных, передаваемых в многопользовательском режиме (например, см. [12]). Да и сами Wi-Fi адаптеры [13], используемые для

перехвата трафика, MU-MIMO не поддерживают. Однако выход есть! Работу MU-MIMO можно обнаружить по косвенным признакам, а именно по кадрам VHT NDP Announcement с запросом результатов измерений в многопользовательском режиме (*MU feedback requested*). Причем подобные кадры точка доступа или Wi-Fi роутер посылает клиентам с поддержкой MU-MIMO, только когда те одновременно что-либо скачивают (т. е. идет передача данных в нисходящем направлении). В противном случае в кадрах VHT NDP Announcement будут запрашиваться результаты измерений в однопользовательском режиме (*SU feedback requested*).

ТАБЛИЦА 1. Точки доступа, Wi-Fi роутеры и адаптеры TP-Link, поставляемые в РФ

Тип устройства	Название модели	Поколение Wi-Fi	Доля от моделей этого типа, %
Точка доступа	EAP115 EAP110 EAP110-Outdoor EAP115-Wall	Wi-Fi 4	18,2 (4 из 22)
	–	Wi-Fi 5, Wave 1	–
	EAP265 HD EAP245 EAP225 EAP225-Outdoor EAP235-Wall EAP230-Wall	Wi-Fi 5, Wave 2	27,3 (6 из 22)
	EAP670 EAP660 HD EAP653 EAP650 EAP620 HD EAP613 EAP610 EAP650-Outdoor EAP610-Outdoor EAP655-Wall EAP650-Wall EAP615-Wall	Wi-Fi 6, MU-MIMO есть	54,5 (12 из 22)
Wi-Fi роутер	TL-WR940N TL-WR845N TL-WR842N TL-WR841N TL-WR840N TL-WR844N TL-WR820N	Wi-Fi 4	20,0 (7 из 35)
	Archer C24 Archer C20	Wi-Fi 5, Wave 1	5,7 (2 из 35)
	Archer A8 Archer C86 Archer C80 Archer C6 Archer A64 Archer A6 Archer C6U Archer C64 Archer A5	Wi-Fi 5, Wave 2	31,4 (11 из 35)

Тип устройства	Название модели	Поколение Wi-Fi	Доля от моделей этого типа, %
	Archer C50 Archer C54		
	Archer AX80 Archer AX6000 Archer AX73 (RU) Archer AX73 (EU) Archer AX72 (RU) Archer AX55 (RU) Archer AX55 (EU) Archer AX53 (RU) Archer AX53 (EU) Archer AX50 Archer AX23 Archer AX1800 Archer AX20 Archer AX10 Archer AX1500	Wi-Fi 6, MU-MIMO есть	42,9 (15 из 35)
Wi-Fi адаптер	TL-WN823N TL-WN821N TL-WN727N TL-WN725N TL-WN822N TL-WN722N TL-WN881ND TL-WN781ND	Wi-Fi 4	29,6 (8 из 27)
	Archer T2U Archer T2U Nano Archer T2UB Nano Archer T9UH Archer T4U Plus Archer T4U Archer T3U Plus Archer T2U Plus Archer T5E Archer T4E Archer T2E Archer T2UB Nano	Wi-Fi 5, Wave 1	44,4 (12 из 27)
	–	Wi-Fi 5, Wave 2	–
	Archer T3U Nano Archer T3U Archer TX20U Plus Archer TX3000E Archer TX55E Archer TX50E Archer TX20E	Wi-Fi 6, MU-MIMO есть	26,0 (7 из 27)

Исследование выполнено в рамках исполнения ПНИ по государственному заданию СПбГУТ на 2023 год.

Список используемых источников

1. IEEE Std 802.11-1997 – IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks –

Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications // IEEE. November 18, 1997. DOI 10.1109/IEEESTD.1997.85951.

2. IEEE Std 802.11b-1999 – IEEE Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band // IEEE. January 20, 2000. DOI 10.1109/IEEESTD.2000.90914.

3. IEEE Std 802.11a-1999 – IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer in the 5 GHz Band // IEEE. December 30, 1999. DOI 10.1109/IEEESTD.1999.90606.

4. IEEE Std 802.11g-2003 – IEEE Standard for Information Technology – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band // IEEE. June 27, 2003. DOI 10.1109/IEEESTD.2003.94282.

5. IEEE Std 802.11n-2009 – IEEE Standard for Information Technology – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput // IEEE. October 29, 2009. DOI 10.1109/IEEESTD.2009.5307322.

6. IEEE Std 802.11ac-2013 – IEEE Standard for Information technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz // IEEE. December 18, 2013. DOI 10.1109/IEEESTD.2013.6687187.

7. Антоненко А. Д., Герасимова Я. А., Дунайцев Р. А. Исследование эффективности технологии формирования луча в сетях стандарта IEEE 802.11ac // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. Т. 1. С. 100–105.

8. IEEE Std 802.11ax-2021 – EEE Standard for Information Technology –Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN // IEEE. May 19, 2021. DOI 10.1109/IEEESTD.2021.9442429.

9. Стандарт 802.11ac Wave 2: MU-MIMO и другие возможности. Самый полный FAQ по новому стандарту. URL: https://weblance.com.ua/296-standart-80211ac-wave-2-mu-mimo-i-drugie-vozmozhnosti-samyy-polnyy-faq-po-novomu-standartu.html (дата обращения 31.03.2023).

10. TP-Link Россия – Wi-Fi и сетевое оборудование для умного дома и бизнеса. URL: https://www.tp-link.com/ru/ (дата обращения 31.03.2023).

11. The List. URL: https://clients.mikealbano.com/ (дата обращения 31.03.2023).

12. CommView for WiFi – анализ и мониторинг беспроводных сетей. URL: https://www.tamos.ru/htmlhelp/commwifi/ (дата обращения 31.03.2023).

13. Поддерживаемые адаптеры. URL: https://www.tamos.ru/download/main/ca.php (дата обращения 31.03.2023).

УДК 621.39
ГРНТИ 49.01.85

ТЕОРЕМА О ПОЛНОТЕ ФОРМИРОВАНИЯ ПРОФИЛЯ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ СВЯЗИ

И. О. Евтихин[1], О. М. Лепешкин[2], М. А. Остроумов[3], О. А. Остроумов[2], А. Д. Синюк[3]

[1]Российская академия народного хозяйства и государственной службы,
[2]Санкт-Петербургский государственный политехнический университет,
[3]Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Современные системы связи являются критически важными объектами для систем управления. Критичность проявляется в потенциальной возможности нарушения процесса функционирования системы из-за воздействия различных факторов. Предлагается использовать профиль системы связи для контроля и обеспечения устойчивого процесса ее функционирования. Представленная теорема характеризует полноту профиля функционирования, позволяющего описать достижение целевого предназначения системы.

критическая информационная инфраструктура, критически важный объект, система связи, профиль, процесс функционирования системы.

Жизнь современного общества невозможна без новых технологий. Цифровизация, информатизация, использование нейронных сетей и искусственного интеллекта, роботизация производства невозможны без систем связи, которые обеспечивают передачу информации в различных системах, объектах. Системы связи, информационные системы, автоматизированные системы управления становятся критически важными объектами для обеспечения выполнения функций, задач различных систем, объектов, отраслей промышленности, сфер жизни общества [1, 2, 3, 4, 5]. Требуется обеспечение из устойчивого функционирования, одним из элементов которого выступает контроль процесса функционирования системы связи [5, 6, 7].

Современные подходы к описанию моделей системы связи, как правило, учитывают ее структуру [1, 4, 8, 9, 10], а процесс функционирования системы и ее элементов по умолчанию считается устойчивым при устойчивой структуре, что не всегда оправдано, потому что при нарушении структуры и снижении ее устойчивости система может быть функционально устойчива [11, 12, 13, 14, 15, 16]. Требуется учитывать функциональную характеристику системы, направленную на описание возможности достижения целевого предназначения системы.

Под функциональной устойчивостью системы связи понимается способность системы в любой момент времени выполнять свое целевое предназначение, обусловленное выполнением требуемого перечня функций и задач системы, в любых условиях обстановки.

Для описания процесса функционирования системы и выполнения ее целевого предназначения предлагается разрабатывать профиль функционирования системы связи [2, 5, 17]. Разрабатываемый профиль должен в полной степени описывать процесс функционирования системы, для доказательства данного требования сформулирована и доказана теорема о полноте формирования профиля функционирования системы связи.

Теорема

Сформированная на основе синтеза структурно-функциональная модель системы позволяет сформировать профиль функционирования системы и обеспечить ее функциональную устойчивость, обусловленную выполнением своего целевого предназначения, характеризуемого выполнением определенного набора функций и задач, при воздействии на нее и ее элементы дестабилизирующих факторов.

Доказательство

Рассмотрим систему связи, структура которой характеризуется графом, включающем множество вершин графа, характеризующих узлы связи $V = \{v_1, v_2, \ldots, v_i\}$, где i – количество узлов связи в системе, и множество дуг $S = \{s_1, s_2, \ldots, s_k\}$, где i – количество линий связи между узлами в системе, $s_k = (v_i, v_j)$, где i, j – номер узла связи в системе. Предположим, что каждый узел имеет, как минимум одну связь с другим узлом системы. Для каждого узла связи системы обозначим набор задач Z и функций F, использование ресурсов которого позволит их выполнить, и обозначим ее функцией φ, которая сопоставляет каждому узлу связи (вершине графа) v_i из множества V наборы ресурсов, которые она предоставляет, наборы задач и функций, которые этот узел способен выполнить (участвует в выполнении): $\varphi 1$: $V \rightarrow$M, $\varphi 2$: $V \rightarrow$Z, $\varphi 3$: $V \rightarrow F$.

Обозначим функцию γ, которая ставит в соответствие каждой линии связи (дуге графа) непустое множество параметров дуг: γ: $S \rightarrow \Omega$.

1) матрица смежности, характеризует наличие связей между узлами S: $s_{ij} = 1\ if\ \exists s_k = (vi, vj)$, $s_k \in S$, $s_{ij} = 0\ otherwise$ (здесь if представляет собой условный оператор, а $otherwise$ означает «в противном случае»);

2) матрица ресурсов узлов VM: vf_{ij}=1 $if\ f_j \in \varphi 3(v_i)$, vf_{ij}=0 $otherwise$,
матрица задач узлов VZ: vf_{ij}=1 $if\ f_j \in \varphi 2(v_i)$, vf_{ij}=0 $otherwise$,
матрица функций узлов VF: vf_{ij}=1 $if\ f_j \in \varphi 1(v_i)$, vf_{ij}=0 $otherwise$;

3) матрица характеристик для дуг $S\Omega$: $s\omega_{ij} = 1 \ if \ \omega_j \in \gamma(s_k)$, $s\omega_{ij} = 0 \ otherwise$.

В процессе функционирования системы осуществляется воздействие дестабилизирующих факторов на ее элементы, узлы и линии связи. Рассматривая структурно-функциональную модель построения системы связи определяется структура системы, позволяющая для системы предоставить определенный ресурс, и формируется ее функциональная характеристика, показывающая возможности системы по выполнению ее целевого предназначения, определенного набора задач и функций за счет имеющегося ресурса. Объектами воздействия дестабилизирующих факторов могут быть как узлы связи и элементы системы, находящиеся на них, так и линии связи. При этом воздействие может оказываться одними и теми же факторами или разными, одновременно и на линии связи, и на узлы, или отдельно только на линии связи или только узлы, а также на некоторое множество, включающее узлы и линии связи. В каждом из этих случаев результатом воздействия дестабилизирующих факторов могут быть изменения либо числа вершин/дуг, либо их характеристик, либо обоих параметров одновременно, т. е. изменение структуры системы.

Любое изменение структуры системы связи отразится на ее функциональной составляющей, при этом его можно отразить, используя ранее введенные матрицы:

– структурные изменения системы связи отразятся в матрице смежности S, поскольку в этом случае произойдет изменение количества компонентов системы и/или связей между ними;

– изменения в работе узла связи (элемента системы) будут отражаться на функциональной составляющей системы на множестве ресурсов, количественной возможности системой выполнять задач и функций, которые реализует узел связи (либо его элемент), что повлечет за собой изменения в матрицах функций VF, задач VZ, ресурсов VM;

– изменения в линиях связи, характеризующих обмен сообщениями между узлами (его элементами) (например, уменьшение скорости передачи данных, увеличение ошибок в канале, появление помех и т. д.) будут отражены в матрице характеристик $S\Omega$.

Доказательство теоремы сводится к доказательству четырёх утверждений.

Утверждение 1: Изменение, связанное с количеством узлов связи (вершин V графа), приведет к изменению количества связей, ресурса системы и задач и функций которые она выполняет, т. е. матриц S, VM, VZ и VF.

Утверждение 2: Изменение, связанное с параметрами узлов связи (вершин V графа), характеризующих ресурсы из множества M, задачи из множества Z и функции из множества F, в выполнении которых участвует элемент системы, приведет к изменению матриц VM, VZ и VF.

Утверждение 3: Изменение, связанное с количеством линий связи (дуг S графа), приведет к изменению связности системы, т. е. матриц S, $S\Omega$.

Утверждение 4: Изменение, касающееся параметров линий связи (дуг графа), где параметры принадлежат множеству Ω, ведет к изменению матрицы $S\Omega$.

Доказательство утверждений осуществляется от противного. Если для рассматриваемой системы с определенной структурой, набором элементов и связей между ними все утверждения доказаны и соответствуют действительности, то можно сделать вывод о том, что структурно-функциональная модель системы и формируемый на ее основе профиль функционирования системы обладает полнотой наполнения для выполнения требуемого целевого предназначение системы. Профиль функционирования системы связи составляет основу принципа инвариантности, поскольку позволяет отразить корректное функционирование системы, функционирование системы после воздействия на нее различных дестабилизирующих факторов, определить количество выполненных задач, функций системы, т. е. оценить функциональную устойчивость и способность выполнить целевое предназначение системы связи.

Список используемых источников

1. Коцыняк М. А., Карпов М. А., Лаута О. С., Дементьев В. Е. Управление системой обеспечения безопасности информационно-телекоммуникационной сети на основе алгоритмов функционирования искусственной нейронной сети // Известия Тульского государственного университета. Технические науки. 2020. N 4. С. 3–10.

2. Остроумов О. А., Савищенко Н. В., Лепешкин О. М. Выполнение регламента процесса управления – критерий определения критичности системы // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей III Всероссийской научно-технической конференции, Анапа, 21–22 апреля 2021 года. Анапа: ФГАУ «Военный инновационный технополис «ЭРА», 2021. С. 625–634.

3. Лепешкин О. М., Анисимов В. В., Остроумов М. А., Остроумов О. А. К вопросу обеспечения функциональной устойчивости системы связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. 880 с., С. 407–410.

4. Климов С. М., Поликарпов С. В., Рыжов Б. С., Тихонов Р. И., Шпырня И. В. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий // Вопросы кирбербезопасности. 2019. N 6. С. 37–48.

5. Остроумов О. А. Проблема обеспечения функциональной устойчивости систем критически важных объектов // Электросвязь. 2022. N 1. С. 14–18.

6. Ахмадиев И. Р., Мартынюк И. А., Новиков П. А. Мониторинг сетей общего пользования в условиях компьютерных атак // Информационные технологии и системы: управление, экономика, транспорт, право. 2019. N 2 (34). С. 15–18.

7. Груздев Д. А., Закалкин П. В., Кузнецов С. И., Тесля С. П. Мониторинг информационно-телекоммуникационных сетей // Труды учебных заведений связи. 2016. Т. 2. N 4. С. 46–50.

8. Иванов С. А. Устойчивость сетей связи общего пользования в условиях глобализации // Известия Тульского государственного университета. Технические науки. 2021. N 9. С. 86–90.

9. Стародубцев Ю. И., Иванов С. А., Закалкин П. В. Концептуальные направления решения проблем обеспечения устойчивости Единой сети электросвязи Российской Федерации в интересах органов государственной власти и военного управления // Военная мысль. 2021. N 4. С. 39–49.

10. Коцыняк М. А., Лаута О. С., Нечепуренко А. П. Модель системы воздействия на информационно-телекоммуникационную систему специального назначения в условиях информационного противоборства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. N 3-4 (129-130). С. 40–44.

11. Haque M. A., De Teyou G. Shetty K., S., Krishnappa B. Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights // 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 2018. PP. 25–30. doi: 10.1109/ISI.2018.8587398.

12. Шостак Р. К., Лепешкин О. М., Новиков П. А., Худайназаров Ю. К. Активирующая подсистема сетевого мониторинга системы связи специального назначения // Радиолокация, навигация, связь : XXIV Международной научно-технической конференции: сб. тр. в 5-ти т. Воронеж, 17–19 апреля 2018 года. Воронеж: ООО «Вэлборн», 2018. Том 2. С. 39–44.

13. Burlov V., Lepeshkin O., Lepeshkin M. Parameters of the synthesized model of management of technosphere safety in the region // E3S Web of Conferences, Topical Problems of Green Architecture, Civil and Environmental Engineering 2019 (TPACEE 2019). 2020. Vol. 164. 07011 DOI: https://doi.org/10.1051/e3sconf/202016407011.

14. Тарасов А. А. Функциональная реконфигурация отказоустойчивых систем: монография. М. : Логос, 2012. 152 с.

15. Петренко С. А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. 2009. Т. 41. С. 175–193.

16. Дурняк Б. В., Машков О. А., Усаченко Л. М., Сабат В. И. Методология обеспечения функциональной устойчивости иерархических организационных систем управления // Сборник научных статей: Институт проблем моделирования в энергетике, НАН Украины. 2008. Вып. 48. С. 3–21.

17. Лепешкин О. М., Остроумов О. А., Синюк А. Д. Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. N 8. С. 109–114.

УДК 004.492.3
ГРНТИ 81.93.29

ИСПОЛЬЗОВАНИЕ AUTITD ДЛЯ ЛОГИРОВАНИЯ В LINUX СИСТЕМАХ

Е. Д. Едемская, В. В. Пучков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одной из важных составляющих информационной безопасности инфраструктуры компании является SIEM – система управлением событиями и информацией безопасности. Такую систему можно условно поделить на 2 основные части – подсистему сбора событий и подсистему анализа полученных событий. Правильная настройка первой поможет обнаружить вторжение на ранних этапах проникновения, облегчит написание событий тревоги, а если злоумышленник смог проникнуть в инфраструктуру компании, то позволит разобраться, как и почему это произошло. Основным инструментом для сбора системных событий в Linux системах является auditd. На основе этого инструмента созданы и другие, например, auditbeat, go-audit, которые дополняют основной функционал auditd. В работе рассмотрены основные принципы работы базового инструмента логирования, а также представлена настройка auditd, позволяющая журналировать важные события в системе.

логирование, сбор событий, Linux, auditd.

auditd (сокращение от *Linux Audit Daemon*) – нативный инструмент, предназначенный для мониторинга событий операционной системы и записи их в журналы событий. Был создан для тесного взаимодействия с ядром операционной системы – во время своей работы наблюдает за системными вызовами и может записывать события – чтение, запись, выполнение, изменение прав, связанные с файлами ОС. Таким образом, с его помощью можно отслеживать практически любые события, происходящие в операционной системе. В качестве примеров отслеживаемых событий можно привести следующие [1, 2]:

- запуск и завершение работы системы;
- чтение, запись и изменение прав доступа к файлам;
- инициация сетевых соединений;
- попытки неудачной авторизации в системе;
- изменение сетевых настроек;
- изменение информации о пользователях и группах;
- запуск и остановка приложений;
- выполнение системных вызовов.

На рис. 1 представлена схема взаимодействия auditd с ядром и приложением.

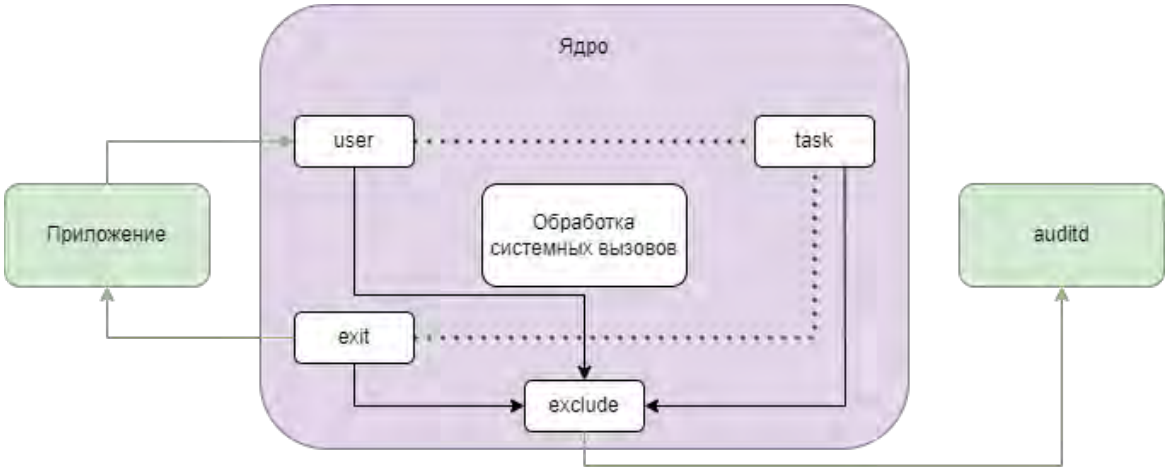


Рис. 1. Схема работы auditd

Получив вызов от приложения в пространстве пользователя, подсистема аудита пропускает его через один из фильтров: user, task или exit. После этого вызов пропускается через фильтр exclude, который исходя из правил аудита передаёт его демону auditd для дальнейшей обработки.

Такая простая схема позволяет вполне эффективно отслеживать любой аспект работы операционной системы, а в случае ее компрометации выявлять подозрительные действия и определять их причину.

При написании правил auditd необходимо учитывать следующее [3, 4]:

- Для каждого события отрабатывает лишь то подходящее правило, которое встретилось первым. Поэтому сначала пишутся фильтры и только потом правила. То же самое касается и выбора между несколькими правилами – выше размещать стоит то правило, которое важнее учитывать.
- Писать правила лучше от частного к общему. Допустим, необходимо журналировать действия в директории /etc/. Чтобы потом в логах не искать прикладными утилитами (*grep, sed* или средствами SIEM) все события, связанные, например, с ssh, sudoers, passwd и т.д., сначала указываются правила для мониторинга конкретных директорий или файлов в /etc/ и только после этого размещается правило для самой директории /etc/.

При создании правил рекомендовано опираться на матрицу MITRE ATT&CK [5], описывающую тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру.

В качестве примера работы auditd рассмотрен сервер, на котором есть http-сервис и ssh. Для взлома сервера на него должны каким-то образом попасть данные от атакующего по сети, в первую очередь необходимо определить пути попадания такой информации. Это любые сервисы, которые устанавливают соединения наружу или принимают входящие соединения.

Этапы проведения атаки:

1. Сканирование сервера. Злоумышленник производит обнаружение открытых портов на сервере извне.

На уровне системных вызовов возможно определить лишь то сканирование, которое использует вызов connect, потому что тогда сервер использует accept во время установления соединения. В большинстве случаев невозможно отличить соединение злоумышленника, поскольку такое соединение ничем не отличается от обычных пользователей. Однако, если такой веб-сервер находится внутри инфраструктуры и есть ограниченное количество сетевых устройств, которые могут к нему подключаться, то такое правило может иметь смысл в случае определения белого списка сетевых устройств, устанавливающих соединение.

Правило будет выглядеть следующим образом:

-a exit,always -S accept -S accept4 -F exe=/usr/sbin/apache2 -k accept

Подразумевается, что всегда на выходе из системных вызовов accept или accept4 для исполняемого файла /usr/sbin/apache2 логировать события и добавлять к ним метку accept.

В широком смысле можно отслеживать все входящие сетевые соединения, а логику для написания правил формирования инцидентов необходимо дополнительно настраивать, например, средствами SIEM.

2. Атака. На данном этапе злоумышленник получил возможность читать файлы ОС или выполнять команды.

Действия атакующего будут затрагивать файлы в директориях /bin/, /usr/bin/, часто пытаются прочитать файл /etc/passwd. Необходимо составить правила для наблюдения за наиболее важными директориями:

-w /bin -k apache_alert
-w /usr/local/sbin -k apache_alert
-w /usr/local/bin -k apache_alert
-w /usr/sbin -k apache_alert
-w /usr/bin -k apache_alert
-w /sbin -k apache_alert

Таким образом при обращении пользователя веб-сервера к исполняемым файлам системы будут созданы соответствующие события.

3. Взаимодействие с сервером. Вслед за взломом злоумышленник может попытаться закрепиться на сервере, найти информацию для продвижения вглубь инфраструктуры (поиск паролей, токенов файлах, базах данных и т. д.).

На данный момент непокрытое поле для злоумышленника остаётся только в директории /var/www/. Он может попытаться записать новый файл с функционалом для веб-приложения или изменить существующий для реализации новой логики. Можно применить следующие правила:

-w /var/www/ -p wa -F uid=www-data -k apache_file_change

Тогда для всех случаев, когда файлы открываются для записи или изменения прав веб-сервером будут записаны события.

SSH изначально предполагает подключение пользователей и предоставление им возможности выполнять команды. Злоумышленника будет интересовать сбор сведений о системе, поиск ценных данных, повышение привилегий в системе.

Начать следует с логирования действий над самим auditd:

-w /etc/audit/ -p wa -k auditconfig
-w /etc/libaudit.conf -p wa -k auditconfig
-w /etc/audisp/ -p wa -k audispconfig
-w /sbin/auditctl -p x -k audittools
-w /sbin/auditd -p x -k audittools
-w /usr/sbin/auditd -p x -k audittools
-w /usr/sbin/augenrules -p x -k audittools

Запись или изменение прав файлов планировщика задач:

-w /etc/cron.allow -p wa -k cron
-w /etc/cron.deny -p wa -k cron
-w /etc/cron.d/ -p wa -k cron
-w /etc/cron.daily/ -p wa -k cron
-w /etc/cron.hourly/ -p wa -k cron
-w /etc/cron.monthly/ -p wa -k cron
-w /etc/cron.weekly/ -p wa -k cron
-w /etc/crontab -p wa -k cron
-w /var/spool/cron/ -p wa -k cron

Также важно логирование выполнения команды sudo всеми пользователями, кроме тех, кому такие права выданы:

-w /usr/bin/sudo -F auid!=<имя пользователя> -k sudo

Настройка наблюдения за работой сетевых утилит:

-w /sbin/iptables -p x -k susp_netutil
-w /sbin/ip6tables -p x -k susp_netutil
-w /sbin/ifconfig -p x -k susp_netutil
-w /usr/sbin/arptables -p x -k susp_netutil
-w /usr/sbin/ebtables -p x -k susp_netutil
-w /sbin/xtables-nft-multi -p x -k susp_netutil
-w /usr/sbin/nft -p x -k susp_netutil

Особый интерес представляют события, связанные с различными нарушениями доступа пользователей (при чтении, записи, изменении файлов):

-a exit,always -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k file_access
-a exit,always -F arch=b32 -S creat -S open -S openat -S open_by_handle_at -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k file_access
-a exit,always -F arch=b32 -S creat,link,mknod,mkdir,symlink,mknodat,linkat,symlinkat -F exit=-EACCES -k file_creation
-a exit,always -F arch=b32 -S link,mkdir,symlink,mkdirat -F exit=-EPERM -k file_creation
-a exit,always -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EACCES -k file_modification
-a exit,always -F arch=b32 -S rename -S renameat -S truncate -S chmod -S setxattr -S lsetxattr -S removexattr -S lremovexattr -F exit=-EPERM -k file_modification
-F auid>=1000 -F auid!=-1 в данном случае используется для исключения ложных срабатываний. Таким образом действия будут логироваться только при их выполнении от имени пользователя.

После применения всех правил в журналах будут отображаться соответствующие записи, отображающие ход действий злоумышленника.

Таким образом, при помощи auditd можно настроить сбор любых событий в Linux системах, для их дальнейшего анализа. Основываясь на определенных последовательностях действий возможно написать правила для SIEM, которые позволят своевременно обнаружить нелегитимную активность в системе и предотвратить атаку.

Список используемых источников

1. Кобзев С. А., Кулешов А. А., Ушаков И. А. Проектирование и реализация прототипа системы централизованного сбора, хранения и обработки системных журналов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017).

VI Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 410–416.

2. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных: учебное пособие. СПб. : СПбГУТ, 2019. 92 с.

3. Defining Audit Rules // Red Hat Customer Portal. URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-defining_audit_rules_and_controls (дата обращения 20.03.2023).

4. Интерактивная система просмотра системных руководств (man-ов) auditctl () // opennet. URL: https://www.opennet.ru/man.shtml?topic=auditctl (дата обращения 20.03.2023).

5. ATT&CK Matrix for Enterprise // MITRE ATT&CK. URL: https://attack.mitre.org/versions/v12/ (дата обращения 20.03.2023).

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук Л. А. Витковой.

УДК 004.891.2
ГРНТИ 49.34.06

АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ РЕЧЕВОЙ АНАЛИТИКИ ДЛЯ ЗАДАЧ CEM

В. С. Елагин, М. П. Заяц

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Данная статья посвящена возможностям применения речевой аналитики для задач Customer Experience Management. В статье рассматривается программное обеспечение, реализующее концепцию управления пользовательским опытом. Чтобы представить задачи, которые должна решить речевая аналитика, рассмотрен жизненный цикл клиента, включающий 9 этапов, на которые необходимо опираться при внедрении вспомогательных технологий. В статье описан принцип работы речевой аналитики для задач CEM и результат внедрения РА.

Customer Experience Management, жизненный цикл клиента, клиентский опыт, лояльность, отток, речевая аналитика.

В условиях современной конкуренции на рынке телекоммуникаций операторы связи уделяют большое внимание решения по управлению опытом и лояльностью клиентов, которые позволили бы выстроить эффективные бизнес-процессы обслуживания клиентов, тем самым снизив отток абонентов и преумножив доходы компании. В связи с этим, все больше

набирает популярность применение концепции Customer Experience Management, в частности внедрение данной концепции в общую инфокоммуникационную специфику оператора связи.

CEM (Customer Experience Management) – это программное обеспечение, реализующее концепцию управления пользовательским опытом [1].

Жизненный цикл клиента (Customer Lifecycle) демонстрирует взаимодействие клиента и оператора, который включает в себя 9 этапов. Каждый этап дает характеристику основным активностям при взаимодействии клиента и оператора. Эти этапы могут быть выполнены как последовательно, так и параллельно. Рассмотрим подробно описание каждого этапа [1, 4].

- Be aware – осведомленность. Этап описывает активности клиента и оператора, присущие маркетинговым аспектам работы с клиентом, а именно, как клиент узнает об услуге, как клиент получает первичные сведения о предложении оператора и как клиент может свою заинтересованность предложением.
- Interact – начало взаимодействия. Данный этап также описывает маркетинговые аспекты работы с клиентом, но при этом носит интерактивный характер, т.е. начинается непосредственное двусторонне взаимодействие клиента и оператора. Этап определяет, как клиент может запросить детали предложения, исследовать тонкости предложения оператора, а также какие имеются возможности для предварительного заказа и бронирования предложения.
- Choose – выбор предложения для покупки. Этап описывает активности, связанные с финальным выбором клиента той или иной конфигурации предложения, его покупку (место совершения сделки покупки и оплата), а также аспекты, связанные с получением сервиса из предложения, в том числе его инсталляцию и первичную настройку.
- Consume – потребление сервиса. На этом этапе рассматриваются аспекты, связанные с тем, насколько клиент удовлетворен использованием сервиса, его качеством и предполагаемой выгодой от него.
- Manage – управление сервисом. На этом этапе рассматриваются возможности управления сервисом, получение помощи при использовании сервиса, а также запросы, связанные с устранением неисправностей при его использовании.
- Pay – платежи. Данный этап характеризует жизненный цикл клиента с точки зрения возможностей и удобства оплаты уже подключенного сервиса, его тарификации, управления тарификацией, получения и управления счетами, в том числе разрешения спорных вопросов.
- Renew – обновление соглашения на использование сервиса. Этот этап описывает аспекты, связанные с возобновлением договорных отношений между клиентом и оператором, например, после истечения срока существующего соглашения.

• Recommend – рекомендации. Этап описывает аспекты, связанные с количеством и эмоциональным окрасом упоминаний сервиса и компании в различных источниках. На данном этапе также рассматриваются вопросы, связанные с наращиванием оператором лояльности клиента.

• Leave – окончание использования. На этом этапе рассматривают вопросы, связанные с окончанием взаимоотношений между клиентом и оператором, включая процедуру отключения сервиса и анализ обратной связи от клиента после ухода.

На каждом этапе взаимодействия клиента с оператором происходят различные ситуации. Все эти этапы влияют на впечатления и опыт клиента – Customer Experience. Каждый разговор с клиентом может оказаться либо положительным, либо отрицательным, что может повлиять на его поведение, склонность к оттоку и лояльность на последующих этапах. Поэтому на каждом этапе необходимо уметь отслеживать и анализировать клиентский опыт и на его основе принимать правильные решения. В результате термин Customer Experience Management означает комплекс процессов, методов и технологий, которые позволяют отслеживать, анализировать и влиять на впечатления и опыт клиента [5].

Цель внедрения концепции управления опытом клиента заключается в создании более удовлетворительного опыта для клиентов, что может привести к повышению лояльности клиентов, увеличению продаж и улучшению репутации бренда.

Конкретные бизнес-цели, которые могут быть достигнуты при внедрении концепции CEM [1, 5], могут варьироваться в зависимости от отрасли и бизнес-модели, но в общем могут включать:

1. Увеличение продаж. Улучшение опыта клиентов может привести к увеличению количества продаж, повторных покупок и увеличению размера покупок.

2. Увеличение лояльности клиентов. Создание более удовлетворительного опыта для клиентов может повысить уровень их лояльности и уменьшить отток клиентов.

3. Улучшение репутации бренда. Компании, которые предоставляют превосходный опыт клиентов, часто имеют более высокую репутацию и лучшую позицию на рынке.

4. Сокращение затрат на обслуживание клиентов. Более удовлетворительный опыт клиентов может снизить затраты на обслуживание клиентов, так как клиенты могут реже обращаться с жалобами или вопросами.

5. Повышение эффективности маркетинга. Улучшенный опыт клиентов может увеличить уровень рекомендаций и положительных отзывов, что может повысить эффективность маркетинга и уменьшить затраты на привлечение новых клиентов.

Однако сегодня каждая компания обрабатывает большое количество звонков и сообщений. От качества их обработки напрямую зависит прибыль компании и количество довольных клиентов. Но оценить полностью работу сотрудников, работающих с клиентами, практически невозможно из-за большого количества данных [2, 4]. Ведь прослушивание всех звонков и сообщений отделом контроля качества – трудоемкий процесс. А частичный анализ неэффективен, поскольку не каждое обращение будет прослушан. Следовательно, некоторые неудачные заявки могут быть упущены, что может привести не только к уменьшению прибыли, но и потере клиента.

Оптимальным решением является автоматизация этих операций с помощью речевой аналитики [5]. Данный автоматический сервис прослушивания и анализа звонков и чатов появился для контроля 100 % своих коммуникаций, в которых обнаруживаются неудачные примеры общения операторов с клиентами.

Речевая аналитика является одной из областей искусственного интеллекта [3], которая занимается анализом и обработкой речевых данных, включая распознавание речи, синтез речи, анализ тональности и настроения, распознавание голосов и др. Если говорить о речевой аналитике в Customer Experience Management, то она используется для анализа обращений клиентов и оценки их удовлетворенности продуктами или услугами компании. Принцип работы речевой аналитики [5, 6] в этом случае может быть описан следующим образом (рис. 1):

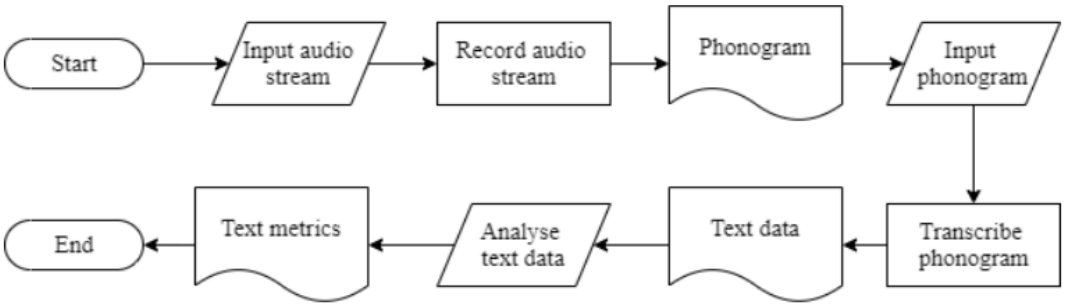


Рис. 1. Схема работы речевой аналитики

1. Сбор данных: для проведения анализа необходимо собрать данные в виде записей звонков, сообщений, отзывов и других форм обратной связи от клиентов.

2. Предобработка данных: на этом этапе происходит очистка данных от шума и преобразование их в единый формат.

3. Транскрибирование: звуковые данные транскрибируются в текстовый формат, чтобы их можно было обработать при помощи методов обработки естественного языка.

4. Анализ тональности: на этом этапе происходит определение тональности высказывания клиента, то есть определяется, является ли высказывание положительным, отрицательным или нейтральным.

5. Анализ тематики: на этом этапе происходит анализ текста обращения клиента, чтобы определить, с какой темой связано обращение, например, с доставкой товара, обслуживанием в магазине и т. д.

6. Анализ ключевых слов и фраз: на этом этапе происходит выделение ключевых слов и фраз из текста обращения клиента, чтобы выявить основные проблемы, которые клиенты испытывают при работе с продуктами или услугами компании.

7. Анализ повторяемости: на этом этапе происходит выявление часто повторяющихся проблем и вопросов, чтобы определить, какие проблемы нуждаются в наиболее срочном решении.

8. Визуализация и интерпретация результатов: результаты анализа представляются в графическом виде, чтобы было удобно воспринимать информацию и принимать решения на основе анализа.

Применение технологий речевой аналитики для задач Customer Experience Management может помочь компаниям более эффективно управлять опытом клиентов, выявлять проблемные области и улучшать процессы обслуживания клиентов.

Один из главных выводов, который можно сделать при использовании технологий речевой аналитики в CEM, - это то, что они помогают компаниям понять, что действительно важно для клиентов и как улучшить опыт обслуживания клиентов на основе этих знаний.

Речевая аналитика может помочь выявить настроение и эмоциональную реакцию клиентов [6] на различные этапы взаимодействия с компанией, что позволяет компаниям быстро отреагировать на проблемы и улучшить процессы обслуживания клиентов. Также технологии речевой аналитики могут использоваться для идентификации ключевых слов и фраз, которые часто употребляются клиентами при обращении в службу поддержки или взаимодействии с компанией, что позволяет определить наиболее часто возникающие проблемы и их причины.

Таким образом, использование технологий речевой аналитики может существенно повысить эффективность CEM, улучшить опыт клиентов и повысить уровень их лояльности, что в свою очередь может привести к увеличению продаж и улучшению репутации бренда.

Список используемых источников

1. Акишин В. А., Кисляков С. В., Феноменов М. А. Функциональная архитектура CEM-комплекса для внедрения в IT-ландшафт крупного оператора связи [Электронный ресурс] // T-Comm: Телекоммуникации и транспорт. 2016. Том 10. N 10. С. 12–16. URL: http://media-publisher.ru/old/pdf/Nom-10-2016-sait.pdf (дата обращения 19.02.2023)

2. Неустроев М. Ю. Оценка эффективности работы центра обслуживания вызовов с использованием аналитики больших данных [Электронный ресурс] // Информационно-технологический вестник: электрон. научн. журн. 2015 С. 127–135. URL: https://ies.unitech-mo.ru/files/upload/publications/15780/e01446b9cf844f1602e_5e001024e8569.pdf (дата обращения 20.02.2023)

3. Заяц М. П. Эффективность внедрения информационных систем с элементами искусственного интеллекта в контакт-центрах и бизнес-процессах компаний // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей: сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2021. Т. 2. С. 458–462.

4. Call Center Guru: Ключевые элементы аналитики пути клиента [Электронный ресурс] // URL: https://callcenterguru.ru/articles/klyuchevyye-elementy-analitiki-puti-kliyenta (дата обращения 20.02.2023)

5. Wang Y., & Wu X. Speech analytics and sentiment analysis for customer experience management: A case study in telecommunications // Journal of Business Research. [Электронный ресурс] // 2020. N 119. PP. 369–377. URL: https://link.springer.com/article/10.1007/s11235-017-0432-0 (дата обращения 22.02.2023)

6. Zhang Y., Wu X., Tao J., & Meng H. A review on speech emotion recognition with deep learning and Attention Mechanism // Electronics. 2021. N 10. P. 1163. [Электронный ресурс] // 2021. URL: https://www.mdpi.com/2079-9292/10/10/1163 (дата обращения: 24.02.2023)

УДК 004.716
ГРНТИ 49.34.39

АНАЛИЗ ТРЕБОВАНИЯ ВКС СИСТЕМ К ШИРИНЕ КАНАЛА ПЕРЕДАЧИ

В. С. Елагин, В. Н. Некрасов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Спрос на видеоконференцсвязь с каждым годом становится все больше и больше. Уже сложно представить корпоративную среду без систем ВКС, они решает множество коммуникативных задач органов государственно власти и крупных корпораций. Любому заказчику очень важно качество групповых и персональных видеоконференций, а оно напрямую зависит от пропускной способности канала связи. Именно об этом пойдет речь в этой статье, мы проанализировали требования различных ВКС систем к ширине канала связи, и на практике посмотрели, как пропуская способность влияет на качество конференции.

видеоконференцсвязь, ширина канала, bitrate, Wireshark.

Введение

Видеоконференцсвязь появилась достаточно давно и постепенно развивалась. Огромный толчок в развития она получила благодаря covid-19. Быстрый переход на удаленную работу привел к быстрому внедрению видеоконференций. Около 82 % компаний используют ВКС в настоящее время, каждая из которых ценит качество видеоконференции, зависит от пропускной способности сети передачи.

Пропускная способность сети – это максимально допустимая скорость обработки трафика, которая определяется стандартами сети. Она показывает, какой максимальный объем может быть передан в единицу времени. Эта величина не зависит от загруженности сети, так как отражает именно максимально возможную скорость. Чаще всего она измеряется в битах в секунду, однако также допустимо характеризовать пропускную способность сети по количеству переданных в единицу времени пакетов [5].

Требования пропускной способности различных ВКС систем

Zoom в настоящее время является одним из самых популярных приложений для проведения конференций и позволяют вам подключаться только с помощью голоса (VoIP) или голоса с видео. На веб-сайте Zoom говорится о требованиях к пропускной способности:

– 600 кбит/с (вверх/вниз) для видео высокого качества;
– 1,2 Мбит/с (вверх/вниз) для HD-видео 720p;
– Для приема HD-видео 1080p требуется 1,8 Мбит/с (вверх/вниз);
– Для отправки HD-видео 1080p требуется 1,8 Мбит/с (вверх/вниз).

Пропускная способность, используемая Zoom, будет оптимизирована для наилучшего взаимодействия в зависимости от сети участников. Он автоматически настраивается для 3G, WiFi или проводной среды [4].

Microsoft Teams – еще один онлайн-инструмент для совместной работы, используемый во многих компаниях и организациях по всему миру.Там, где пропускная способность не ограничена, Teams оптимизирует качество мультимедиа, включая разрешение видео до 1080p, до 30 кадров в секунду для видео и 15 кадров в секунду для контента, а также высококачественный звук [3].

– 500 кбит/с, одноранговые видеозвонки с качеством 360p при 30 кадрах/с;
– 1,2 Мбит/с, одноранговая видеосвязь HD-качества с разрешением HD 720p при 30 кадрах в секунду;
– 1,5 Мбит/с, одноранговая видеосвязь HD-качества с разрешением HD 1080p при 30 кадрах в секунду.

TrueConf – российский разработчик корпоративных и индивидуальных продуктов и оборудования для видеоконференцсвязи (ВКС). На рис. 1 представлена информация о необходимой пропускной способности для совершения видеозвонка [1].

Необходимая пропускная способность, **кбит/с**	Сервер		Клиент	
	Входящий	Исходящий	Входящий	Исходящий
SD	256	256	128	128
HQ	512	512	256	256
ED	1024	1024	512	512
HD	2048	2048	1024	1024
Full HD	4096	4096	2048	2048
WQHD	8192	8192	4096	4096
Ultra HD	16384	16384	8192	8192

Рис. 1. Таблица пропускной способности

В условиях политики импортозамещения в России появилась необходимость создания ВКС-систем отечественной разработки, не уступающих по своим характеристикам зарубежным аналогам. НТЦ ПРОТЕЙ создал российскую систему ВКС, полностью построенную на собственных разработках [2].

В настройках терминала видеоконференцсвязи протей есть таблица соответствия битрейтов и разрешений, она представлена на рис. 2. В двух последних столбцах указаны минимальный и рекомендованный битрейт.

Для приёма и передачи видео в HD (1280×720) требуется минимум 889 кбит/с., а рекомендовано 2,6 мбит/с.

Таблица соответствия битрейтов и разрешений

640x360	☐	222	666
640x480	☐	296	888
704x480	☐	326	978
768x448	☐	332	996
704x576	☐	391	1174
720x576	☐	400	1200
800x600	☐	463	1389
960x540	☐	500	1500
1024x576	☐	569	1707
1024x768	☐	759	2277
1280x720	☐	889	2667
1280x960	☐	1185	3555

Рис. 2. Таблица соответствия битрейтов

Влияние пропускной способности на качество изображения

Рассмотрим, как пропускная способность влияет на качество транслируемого изображения на примере ПРОТЕЙ-ВКС. Для этого достаточно в настройках терминала видеоконференцсвязи поменять максимальный битрейт на передачу.

Для начала поставим ограничение на 6 Мбит/с, на рис. 3 представлен результат. Хорошее качество изображения похожее на Full HD (1920×1080).

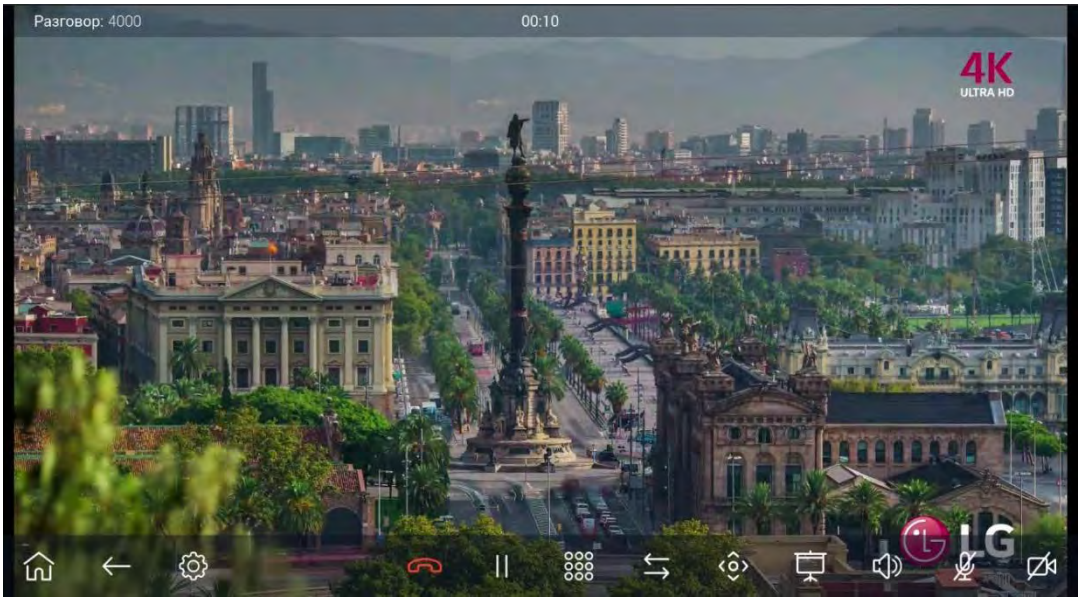


Рис. 3. Качество изображения при ширине канала 6 Мбит/с

Затем, мы ограничили битрейт до 500 Кбит/с. Результат показан на рис. 4. Качество изображения заметно снизилось.

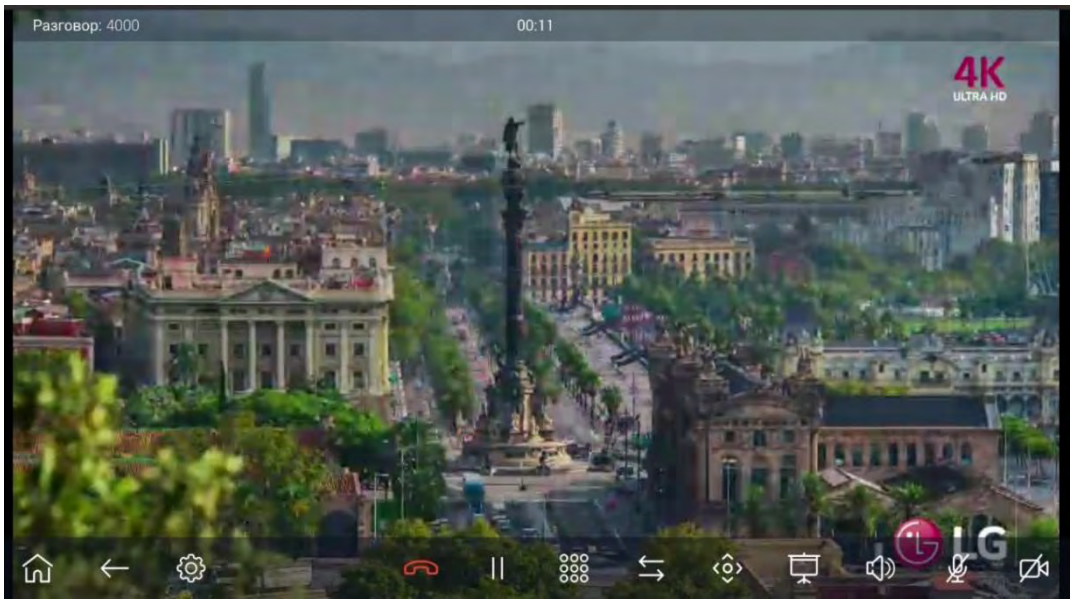


Рис. 4. Качество изображения при ширине канала 500 Кбит/с

Анализ сетевых пакетов

Следует так же сравнить и проанализировать дампы двух вызовов, с полосой пропускания 6 000 Кбит/с и 500 Кбит/с. С помощью программы-анализатора трафика Wireshark мы можем сделать это.

Начнем с первого, и посмотрим на реальный средний битрейт. На рис. 5 видно, что он примерно равен 7 000 000, это около 6 800 Кбит/с = 6,6 Мбит/с.

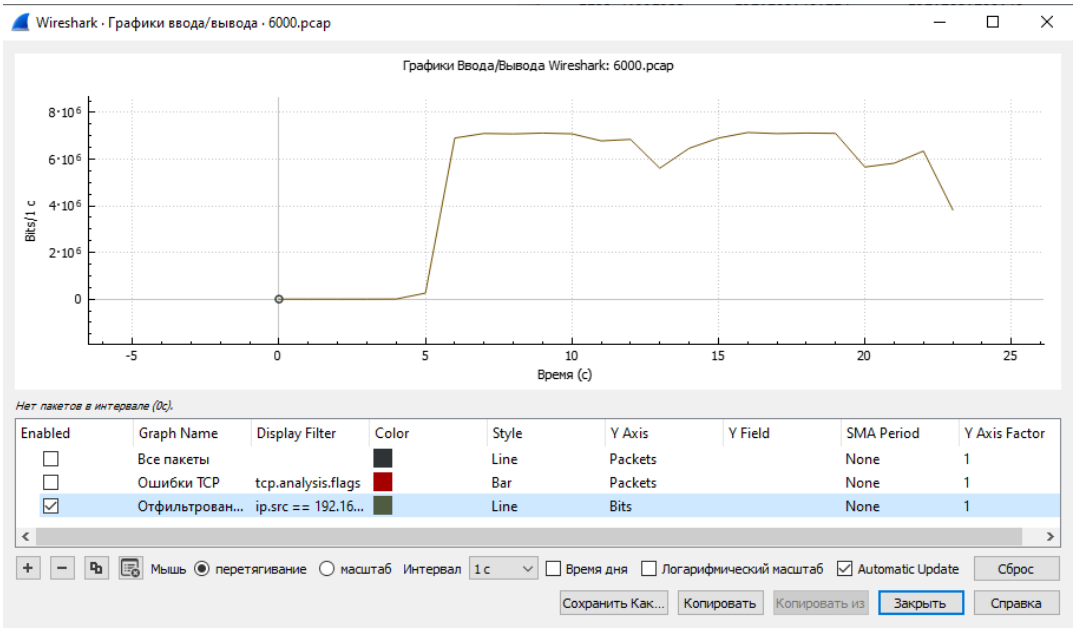


Рис. 5. График ввода/вывода

На рис. 6 более подробно рассмотрены потоки RTP. Обратим внимание на средний джиттер и время между пакетами, оно обозначается параметром «Дельта». Полученные значения считаются нормой.

Полезная Нагрузка	Пакеты	Потеряно	Минимальная Дельта (мс)	Средняя Дельта (мс)	Максимальная Дельта (мс)	Минимальный Джиттер	Средний Джиттер	Максимальный Джиттер
G7221	925	0 (0.0%)	4.231000	20.022166	41.278000	0.001438	3.772792	10.180964
H264	7847	0 (0.0%)	0.012000	2.295195	77.827000	0.000750	3.963063	32.253596
ulpfec	3921	0 (0.0%)	0.082000	4.655274	167.320000	0.526063	53.672640	400.194995
ulpfec	460	0 (0.0%)	4.360000	40.173279	101.089000	15.046625	120.801828	137.603011

Рис. 6. RTP потоки при ширине канала 6000 Кбит/с

Во втором случае, мы ограничили пропускную способность до 500 кбит/с. По графику на рис. 7, видим, битрейт составляет 700 000 бит/с, это примерно 680 Кбит/с.

На рис. 8 представлены RTP потоки, при ширине канала 500 Кбит/с. Средняя дельта при передаче видео (H264) увеличилась примерно в 10 раз. Джиттер возрос примерно в 5 раз, это значит, что пакеты приходят не своевременно, но его численное значение все равно в пределах нормы.

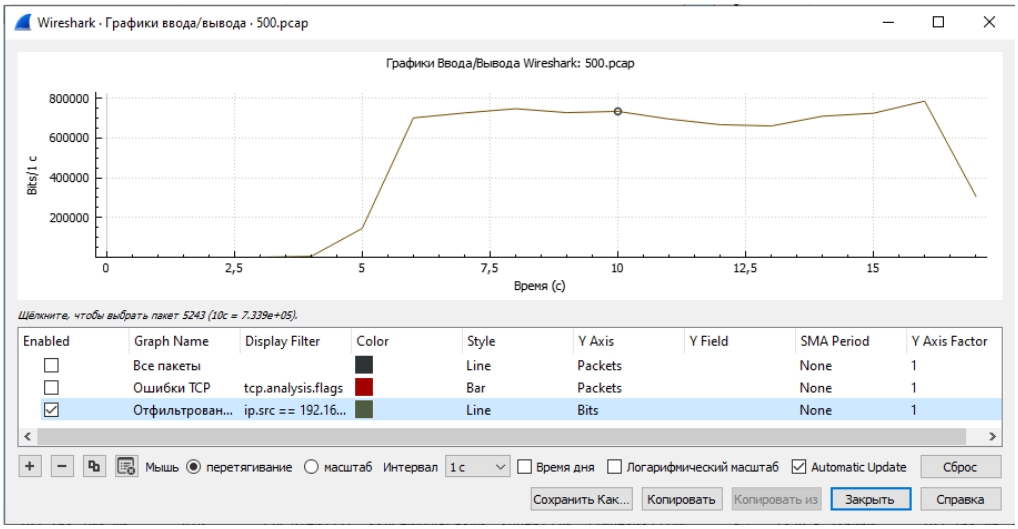


Рис. 7. График ввода/вывода

Полезная Нагрузка	Пакеты	Потеряно	Минимальная Дельта (мс)	Средняя Дельта (мс)	Максимальная Дельта (мс)	Минимальный Джиттер	Средний Джиттер	Максимальный Джиттер
G7221	621	0 (0.0%)	0.003000	20.002998	41.316000	0.088250	3.246563	10.356966
H264	569	0 (0.0%)	0.000000	23.326514	64.956000	0.000000	16.616808	64.437241
ulpfec	308	0 (0.0%)	4.361000	40.197049	102.699000	14.958375	119.204068	138.168505
ulpfec	282	0 (0.0%)	0.857000	42.769139	167.091000	85.849500	432.605918	1012.634201

Рис. 8. RTP потоки при ширине канала 500 Кбит/с

Заключение

В целом все системы видеоконференцсвязи имеют примерно одинаковые минимальные требования к пропускной способности, примерно 1,2 Мбит/с. За исключением более подробно рассмотренного ВКС Протей, требующего до 2 Мбит/с. В будущем я планирую подорбно рассмотреть и сравнить ВКС системы других производителей, а также, в качество параметров сравнения, добавить остальные временные характеристики.

Список используемых источников

1. Труконф. Требования к каналам связи для проведения видеоконференций. URL: https://trueconf.ru/support/communication-channels.html (дата обращения 31.03.2023).

2. Протей. Видеоконференцсвязь. URL: https://protei.ru/solutions/videokonferencsvyaz (дата обращения 31.03.2023).

3. GoBrolly. Data and Bandwidth Requirements for Microsoft Teams. URL: https://gobrolly.com/microsoft-teams-data-and-bandwidth-requirements/ (дата обращения 31.03.2023).

4. GoBrolly. Data and Bandwidth Requirements for Zoom Video Conferencing. URL: https://gobrolly.com/data-and-bandwidth-requirements-for-zoom-video-conferencing/ (дата обращения 31.03.2023).

5. Denstadli J.M., Julsrud T.E., Hjortol R.J. Videoconferencingas a Mode of Communication: A Comparative Study of the Use of Videoconferencing and Face-to-Face Meetings // Journal of Business and Technical Communication, 07.12.2011. PP. 65–90.

УДК 004.896
ГРНТИ 49.33.01

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СЕТЯХ ПОСТ-NGN

В. С. Елагин, С. А. Обухов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Чтобы эффективно использовать все технологии сетей 5G, 6G необходимо оперативно обрабатывать интенсивный сетевой трафик, конфигурировать сети, это реализуется за счет интегрирования вспомогательных систем, таких как машинное обучение, нейронные сети и искусственный интеллект. Методы искусственного интеллекта обладают большим потенциалом для решения проблем интеллектуального распределения ресурсов между базовыми станциями в сетях 5G, способны обрабатывать огромное количество параметров, учиться и адаптироваться к меняющимся условиям, распознавать закономерности. Они способны реализовать потребности в направлениях высокой пропускной способности и низкой задержки. В этой статье описывается основные способы машинного обучения, а также представлены некоторые конкретные примеры применения искусственного интеллекта, которые могут быть использованы в сетях пост-NGN.

сети пост-NGN, 5G, 6G, искусственный интеллект, обучение, глубокое обучение.

Существует множество методов в области искусственного интеллекта (*artificial intelligence*, AI), каждый из которых имеет свои характеристики, область применения, преимущества и недостатки.

Обучение с учителем (*Supervised Learning*, SL) – это способ машинного обучения (*Machine Learning*, ML), работающий за счёт обучающей выборки «стимул-реакция». Модель SL изучает взаимосвязь между заданными (входными) значениями и их метками (выходными значениями). Таким образом, модель может предсказать выход, опираясь на предоставленные входные данные.

При использовании SL, если множество возможных ответов конечно, и желаемый результат определение того, к какой категории принадлежит данное значение, такую модель можно отнести к задачам о классификации и распознавании образов.

Если множество возможных ответов бесконечно, например, ответами являются действительные числа или векторы, говорят о задачах регрессии и аппроксимации. Основная цель регрессии – предсказать числовые значения, не связывая их с каким-либо классом. Она обычно используется для прогнозирования цен, использования ресурсов или показателей производительности.

Хотя методы SL имеют значительный потенциал для решения проблем сетей 5G, у них есть определенные недостатки. SL требует большие объемы данных, что может быть проблематичным при решении конкретных задач управления трафиком [1, 2, 3].

Предполагается, что обучение без учителя (*Unsupervised Learning*, USL) может облегчить этот процесс.

USL (самообучение) – способ ML, при котором система может спонтанно обучаться и выполнять поставленную задачу без явного руководства, вмешательства со стороны экспериментаторов.

После предоставления немаркированных данных USL модели, она может обнаружить некоторые закономерности в зависимости от типа алгоритма, который она использует, или от цели обучения. Некоторые алгоритмы USL способны различать группы, образованные набором данных естественным образом, а количество групп, которые модель должна кластеризовать, в некоторых случаях может быть задано тренером.

Подводя итог, USL имеет потенциал для облегчения оценки перегруженности сети и структуры сетевого трафика в сетях 5G, и оптимизации сетей для большого количества различных сценариев.

Обучение с подкреплением (*Reinforcement Learning*, RL) – это способ ML, в ходе которого система обучается взаимодействую с некоторой средой. RL вычислительная процедура, предназначенная для обучения и принятия решений, ориентированных на достижение цели, чтобы максимизировать вознаграждение агента [2].

RL отличается от других подходов к обучению тем, что оно опирается на агента, который может взаимодействовать с окружающей средой для максимизации своей функции вознаграждения.

RL имеет существенные различия с SL и USL. SL отличается от RL тем, что оно не построено на взаимодействии и системах вознаграждения. USL отличается от RL тем, что оно сосредоточено на выявлении структуры данных, которая не является предопределенной [2].

Агент должен взаимодействовать с окружающей средой и получать вознаграждение в соответствии с полученным результатом, который заключается в уменьшении потери пакетов, задержки и так далее.

Следовательно, агент может принимать правильные решения для максимизации энергоэффективности и минимизации заторов в сетевом потоке.

Глубокое обучение с подкреплением (*Deep reinforcement learning*, DRL) – это подраздел ML, который сочетает в себе RL и *deep learning* (DL).

С точки зрения кибернетики, DRL является одним из видов кибернетического эксперимента. Откликом среды (а не специальной системы управления, как это происходит в SL) на принятые решения являются сигналы подкрепления, поэтому такое обучение является частным случаем USL,

но учителем является среда или её модель. Некоторые правила подкрепления базируются на неявных учителях, например, в случае искусственной нейронной среды, на одновременной активности формальных нейронов, из-за чего их можно отнести к USL [4].

DRL, которые будут развернуты в сетях 5G, обладают большим потенциалом для управления сетевым потоком.

Алгоритм DRL в сетях 5G сможет научиться снижать задержки и потери пакетов, пробуя различные способы, которые вначале будут случайными, но будут развиваться в зависимости от вознаграждения, которое агент получит от этого конкретного способа. DRL имеет преимущества по сравнению с SL, так как для DRL не нужны маркированные данные. Кроме того, обучение модели RL или DRL обычно является непрерывным процессом, это означает, что даже при непрерывном сетевом трафике они могут обучаться и развиваться [4, 5, 6].

RL или DRL не ограничивается данными, которые предоставляются в определенное время или в определенном количестве. В случае аномалии, обнаружении высокой плотности, перегрузки или задержки, которые не наблюдались ранее, система DRL может мгновенно адаптировать существующее состояние и реорганизовать свою модель в соответствии со знаниями, полученными в этом конкретном состоянии.

Таким образом, AI сможет оперативно обрабатывать интенсивный сетевой трафик, конфигурировать сети, распределять ресурсы между базовыми станциями в сетях пост-NGN, учиться и адаптироваться к меняющимся условиям, распознавать закономерности.

Список используемых источников

1. Fu Y., Wang S., Wang C. X., Hong X., McLaughlin S. Artificial intelligence to manage network traffic of 5G wireless networks // IEEE Network. 2018. Vol. 32, N 6. PP. 58–64.

2. Song W., Zeng F., Hu J., Wang Z., Mao X. An unsupervised-learning- based method for multi-hop wireless broadcast relay selection in urban vehicular networks // IEEE 85th Vehicular Technology Conference (VTC Spring). 2017, June. PP. 1–5.

3. Sutton R. S., Barto, A. G. Reinforcement learning: An introduction // MIT press. 2nd edition. 2018.

4. Bojovic B., Meshkova E., Baldo N., Riihijarvi J., Petrova M. Machine learning-based dynamic frequency and bandwidth allocation in self-organized LTE dense small cell deployments // EURASIP Journal on Wireless Communications and Networking. 2016. N 1. PP. 1–16.

5. Yao M., Sohul M., Marojevic V., Reed J. H. Artificial intelligence defined 5G radio access networks // IEEE Communications Magazine. 2019. Vol. 57, N 3. PP. 14–20.

6. Xu Z., Tang J., Meng J., Zhang W., Wang Y., Liu C. H., Yang D. Experience-driven networking: Adeepreinforcement learning based approach // IEEE INFOCOM 2018-IEEE Conference on Computer Communications. 2018. April. PP. 1871–1879.

ГРНТИ 49.33.31
УДК 004.732

АНАЛИЗ ЗАГРУЗКИ СЕТИ ДОСТУПА ПЕРСПЕКТИВНЫМИ СЕРВИСАМИ И ОБЕСПЕЧЕНИЕ QOS

В. С. Елагин, М. А. Петров, Д. А. Чекалов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Активное развитие и внедрение инфокоммуникационных систем, а также задача обеспечения граждан страны широкополосным доступом к сети Интернет, ставит перед сотрудниками сферы инфокоммуникаций большие вызовы. Активное внедрение технологий xPON на сетях доступа позволяет крупным провайдерам связи обеспечивать своих B2C-клиентов высокой скоростью передачи данных. В статье приводится сравнительный анализ загрузки сети доступа трафиком перспективных приложений и прочих Triple-play услуг. На основании анализа сформулированы выводы о целесообразности обеспечения B2C-клиентов тарифами с минимальной шириной канала для передачи данных в 300 Мбит/с и выше.

широкополосный доступ, xPON, B2C-клиент, Triple-play, FTTB, OLT.

Актуальность и принцип построения сети xPON

Расширение зоны покрытия широкополосного доступа (далее ШПД) к сети Интернет (на основании Постановления Правительства РФ от 15 апреля 2014 г. N 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”») привело к появлению и быстрому развитию в районах с высокой плотностью населения сетей доступа, построенных с применением семейства технологий xPON [1]. Большое количество клиентов при больших капитальных вложениях в создание оптической распределительной сети (*Optical Distribution Network*, ODN) и относительная дешевизна ее эксплуатации, позволяют провайдерам связи «подводить» оптоволоконный кабель до многоквартирного дома по технологии FTTB (*Fiber to the Building*) (рис. 1). После чего производится разводка от телекоммуникационного

Рис. 1. Схематическая архитектура сети доступа по технологии FTTB

шкафа до оконечных абонентских терминалов или ONT (*Optical Network Terminal*).

Со стороны провайдера связи, на районных АТС станциях, ставятся OLT (*Optical Line Terminal*) (рис. 2) с необходимым количеством плат и портов на ней. На каждом порту устанавливается гигабитный SFP-модуль, который используется в технологии GPON и соответствует стандарту ITU-T G.984.2. Данный двунаправленный модуль с разъёмом SC работает по симплексному одномодовому оптическому патч-корду. Модуль GPON SFP передаёт и принимает сигналы различной длины волны (к ONT – 2,5 Гбит/с, от ONT – 1,25 Гбит/с) [2, 3]. Модули SFP GPON передают и принимают как восходящие потоки данных, так и нисходящие соответственно, посредством оптического мультиплексирования с разделением по длине волны (WDM) [4]. Важной особенностью использования технологии GPON на ODN-сетях заключается в привязке конкретного ONT-терминала к порту OLT. В случае смены порта привязки необходимо заново регистрировать оборудование абонента. В этом заключается определенная негибкость сети доступа с использованием технологий GPON.

Рис. 2. Оборудование OLT на 8 GPON-портов (ISCOM 6800)

На данный момент все большее количество клиентов получают ШПД к сети Интернет с помощью семейства технологий GPON для использования приложений, подразумевающих Triple-play услуги [5]. Согласно потенциальным запросам клиентов, провайдеры создали линейку тарифов, обеспечивающий высокий Bitrate согласно модели QoS «Differentiated Service» (от 300 Мбит/с и выше), а также низкий ping. Данные тарифы используют для профессионального «гейминга» или подключения сразу нескольких smart-устройств, требующих выход в Интернет.

Проведение анализа загрузки сети доступа

В качестве объектов анализа были взяты два клиента («клиент А» и «клиент Б», рис. 3 и 4), использующие разные тарифные планы. «Стандартный» тариф, широко представленный на рынке и подразумевающий согласно договору ШПД до 100 Мбит/с (стандарт «*FastEthernet*»), и «игровой» тариф, обеспечивающий своего клиента ШПД до 800 Мбит/с.

В течение недели (7 дней) с помощью утилиты NetWorx осуществлялось измерение скорости (*upload*) обоих клиентов. В статистике учитывались данные потребления трафика в ЧНН.

Используя анализатор трафика «Wireshark», было установлено, что «Клиент А» в основном пользовался такими Triple-play приложениями как,

видеохостинг «YouTube», онлайн-кинотеатрами «Ivi» и «Кинопоиск», также веб-браузером «Google» и мессенджерами «WhatsApp» и «Telegram». «Клиент Б» использовал онлайн-платформу «Steam» для «гейминга», стриминговый сервис «Twitch», а также кроссплатформенную систему мгновенного обмена сообщениями с поддержкой VoIP и видеоконференций «Discord» для онлайн-трансляций и мессенджерами «Telegram» и «Vk». Согласно данным, полученным с помощью анализатора трафика, наибольшая интенсивность обмена данными наблюдалась при использовании сервисов «YouTube» и «Twitch» у «клиента А» и «клиента Б» соответственно.

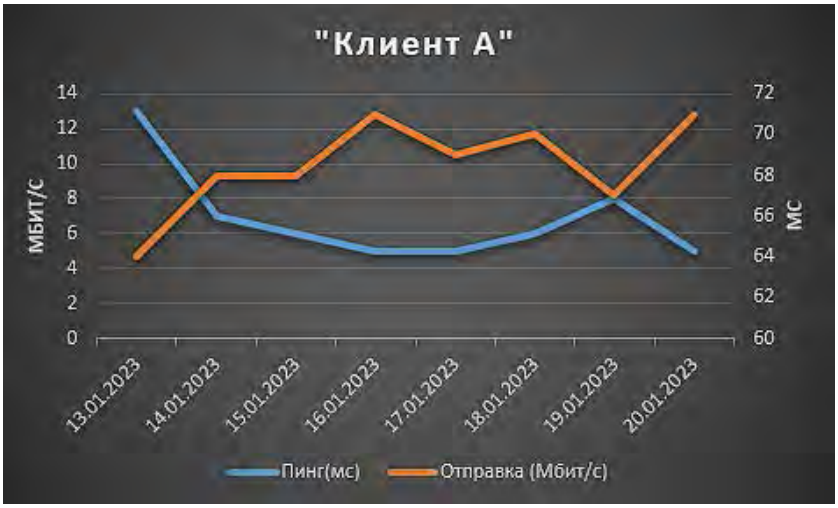


Рис. 3. Анализ трафика «Клиента А»

Рис. 4. Анализ трафика «Клиента Б»

Как можно увидеть согласно собранной статистике, «Клиент А» (рис. 3) в ЧНН потреблял не более 72 Мбит/с, а «Клиент Б» (рис. 4) – не более 180 Мбит/с. При этом за каждым клиентом резервировалась полоса пропускания на порту OLT согласно его тарифу. Из приведенных данных

можно увидеть, что «Клиент Б» использует не более 25 % от своего тарифа и при этом за ним резервируется 64 % мощности SFP-модуля на прием.

Заключение

В результате работы был произведен анализ загрузки 2 сетей доступа с разными тарифными планами и QoS. На основании собранной статистики можно сделать вывод о малой эффективности, предоставляемых B2C-клиентам, «игровых» тарифов с высоким ШПД с технической точки зрения. SFP-модули оказываются де-факто сильно недогруженными (на 2/3) из-за подобных тарифных планов. Что не позволяет подключить большее количество клиентов с более экономичными тарифами. Вместе с тем в текущих условиях удорожания импортного оборудования связи и проблем с его поставками на отечественный рынок, увеличивается необходимость эффективного использования, имеющегося оборудования.

Список используемых источников

1. Постановление Правительства Российской Федерации от 15.04.2014 № 313 "Об утверждении государственной программы Российской Федерации "Информационное общество».

2. Зингеренко Ю. А. Пассивные оптические сети XPON: учебное пособие. СПб. : Университет ИТМО, 2020. С. 63–72.

3. ITU-T G.984.3, Study Group 15. Gigabit-Capable Passive Optical Network (GPON). Transmission Convergence Layer Specification. Geneva, Oct. 2003.

4. Wong E. Next-generation broadband access networks and technologies // Journal of lightwave technology. 2011. V. 30. N. 4. PP. 597–608.

5. Selmanovic F., Skaljo E. GPON in telecommunication network // International Congress on Ultra Modern Telecommunications and Control Systems. IEEE, 2010. PP. 1012–1016.

УДК 004.7
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ГИБРИДНОЙ МОДЕЛИ МОБИЛЬНЫХ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ В СЕТЯХ 5G

В. С. Елагин, Е. В. Чипсанова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием мобильных и инфокоммуникационных сетей является актуальным развитие систем периферийных вычислений. Гибридная модель мобильных граничных

вычислений позволяет правильно распределять ресурсы, однако, чтобы иметь дело с гибридной моделью, нужно изучить стандартные варианты расположения граничных серверов. В данной статье будет проведен анализ расположения граничных серверов, а также будут рассмотрены факторы, которые влияют на их расположение.

5G, MEC, расположение серверов, гибридная модель.

Введение

Новые способы использования беспроводной технологии создают спрос на новые подходы к подключению, полосе пропускания и сетевой архитектуре.

Огромный рост трафика обусловлен главным образом пятью основными факторами [1]:

- эволюция в сторону более интеллектуальных мобильных устройств;
- эволюция 4G и грядущее внедрение 5G;
- массовое внедрение мобильного Интернета всего (IoE);
- универсальность Wi-Fi и расширение его использования;
- определение новых мобильных приложений и требований.

Однако из-за ограничений ресурсов (вычислительная мощность, срок службы батареи и возможности хранения) мобильные устройства не могут эффективно работать и обслуживать множество приложений, интенсивно использующих полосу пропускания, со строгими требованиями, что требует участия облачных вычислений. Таким образом, традиционная централизованная модель облачных вычислений не соответствует требованиям 5G и может привести к некоторым ограничениям, таким как высокая задержка, ограниченная пропускная способность и проблемы с масштабируемостью.

MEC был разработан в ответ на потребность операторов мобильной связи свести обработку и хранение некоторых услуг и приложений на грань, а также повысить производительность мобильной сети и использование ресурсов в режиме реального времени.

Аббревиатура MEC больше не относится к мобильным граничным вычислениям, а скорее относится к граничным вычислениям с множественным доступом (Multi-Access Edge Computing), так как оно расширяет охват и потенциал MEC в современных развивающихся беспроводных сетях, которые состоят из различного набора технологий доступа и структур регулирования спектра.

Сценарии приложений

Варианты использования MEC, которые на сегодняшний день привлекли внимание можно разделить на три основные категории [2]:

– услуги оператора и третьих лиц,

– услуги, ориентированные на пользователя,

– улучшение производительности сети и QoE.

Варианты использования [3]:

- Интеллектуальное ускорение видео

Видеосерверу предоставляется информация о предполагаемой пропускной способности, доступной на интерфейсе нисходящей радиосвязи.

Эта информация может использоваться для помощи в принятии решений по управлению перегрузкой TCP, а также для обеспечения того, чтобы кодирование на уровне приложения соответствовало расчетной пропускной способности на нисходящем радиоканале, а затем позволяло улучшить качество видео и пропускную способность. Используются данные о состоянии сети, особенно о состоянии RAN и нагрузке RAN, для выработки рекомендаций для поставщиков контента и приложений о том, как управлять трафиком, которым обмениваются с подписчиком. Когда сеть имеет достаточную пропускную способность, провайдеры могут обмениваться контентом с максимально доступным качеством. Когда пропускная способность сети ограничена или она перегружена, контент и TCP-передача могут быть адаптированы для предоставления подписчикам наилучших возможностей с учетом доступности сетевых ресурсов в режиме реального времени.

- Кэширование локального контента

MEC не может снизить задержку в сети RAN, но может сократить сквозную задержку за счет локального хранения наиболее популярного контента, потребляемого в определенной географической области. После запроса контент предоставляется из локального кеша. В этом случае нет необходимости передавать контент всегда через опорную сеть.

- Дополненная реальность

Мобильный граничный хост может выполнять ресурсоемкие функции с высокой производительностью вместо мобильных устройств, улучшая взаимодействие с пользователем, и потребитель может использовать устройства с низкой сложностью, разгружая вычислительные мощности на мобильный граничный хост.

- Видеоаналитика

Аналитика распределенных видеопотоков в реальном времени, в котором события запускаются автоматически (например, движение, отсутствие объектов, толпа) позволяет быстро обнаруживать и инициировать действия; что полезно и применимо к общественной безопасности, умным городам.

- Подключенные автомобили

Существующие облачные сервисы распространяются на высокораспределенную среду мобильных базовых станций, используя существующую связь LTE. Приложение MEC может работать как придорожное устройство для связи транспортного средства с инфраструктурой (V2I), может распознавать дорожные опасности и отправлять предупреждения ближайшим ав-

томобилям с чрезвычайно малой задержкой, что позволяет соседнему автомобилю получать данные в режиме реального времени за считанные миллисекунды, а водителю реагировать моментально.

Расположение сервера MEC

Перемещение обработки и хранения данных на дальний край значительно улучшит качество обслуживания и производительность. Однако существует множество ограничивающих параметров, таких как стоимость, сложность, пространство и задержка, на которых основывается выбор местоположения MEC. Чтобы выбрать наилучшее место, выбор должен основываться на компромиссе между указанными выше критериями.

В таблице 1 показано, как расположение MEC влияет на ключевые параметры сети по мере приближения к UE и наоборот по мере приближения к централизованному облаку [4]:

ТАБЛИЦА 1. Влияние расположения MEC на производительность сети.

Ограничивающие параметры сети	Расположение MEC	Ближе к пользователю	Ближе к централизованному облаку
Задержка		Низкая	Высокая
Емкость хранилища		Ограниченная	Высокая
Вычислительная мощность		Ограниченная	Высокая
Сложность сквозной связи		Высокая	Низкая
Оптимизация ресурсов		Низкая	Высокая
Размер покрытой площади		Малый	Большой

По мере того, как расположение MEC приближается к UE, задержка уменьшается, что повышает производительность и QOE, особенно для приложений, чувствительных ко времени.

Аппаратное обеспечение имеет меньшую емкость хранилища, что ограничивает объем контента, который можно хранить на периферии.

Вычислительная мощность становится ограниченной, поэтому запуск некоторых приложений с периферии может оказаться неподходящим.

Сложность сквозной сети возрастает, поскольку сетевым операторам приходится развертывать, интегрировать и управлять большим количеством оборудования в большем количестве местоположений.

Если бы приложения можно было беспрепятственно запускать из централизованного местоположения, распределение ресурсов на периферии может быть бессмысленным.

Еще одним важным фактором является площадь покрытия. По мере того, как граничный хост удаляется от централизованного облака, где обрабатываются управление мобильностью и оптимизация RAN, зона покрытия

становится меньше. Оптимизация пограничного трафика адаптирована для этой области.

Таким образом, географически распределенные серверы MEC могут оптимизировать свои соответствующие области покрытия, но по отдельности.

Но если только один сервер MEC покрывает всю область, оптимизацию можно координировать по всей области. Такая координация делает оптимизацию более эффективной, но в то же время увеличивает расстояние до RAN, что может свести на нет возможности оптимизации. Доступ к граничным приложениям и службам сохраняется при перемещении абонентов из одной области в другую в пределах одной сети.

Если пограничный хост охватывает несколько сетей, доступ приложений может быть сохранен в разных сетях. По мере того, как абонент перемещается в область, которая не имеет таких же возможностей MEC или вообще не поддерживает MEC, абонент может столкнуться с ухудшением качества доступа к пограничному приложению или потерей связи при выходе из зоны обслуживания. Во многих случаях этот последний аспект желателен, особенно для участников, которые хотят, чтобы их услуги были доступны только в пределах определенной области. Когда выбранное местоположение MEC перемещается в сторону централизованного облака, сохраняется обратное, что дает большую задержку, большую емкость хранилища, большую вычислительную мощность, меньшую сложность, более эффективное использование ресурсов.

В таблице 2 представлены факторы, которые играют важную роль при выборе места расположения MEC [5].

ТАБЛИЦА 2. Ключевые факторы, определяющие выбор местоположения MEC

Факторы	Как MEC удовлетворяет потребности сети
Ресурсы RAN	Возможности MEC должны соответствовать возможностям RAN для обслуживания зоны обслуживания.
Транспортные ресурсы	MEC может устранить ограничения пропускной способности и задержки в транзите и не допустить, чтобы транзитное соединение стало узким местом в производительности.
Приложения	Требования к задержке, обработке и хранению, влияющие на расположение MEC, различаются в зависимости от приложения.
Ожидания подписчиков и клиентов	Ожидания в отношении QoE могут быть разными для сотрудников предприятий и посетителей торговых центров.
Настройки оператора	Операторы могут захотеть предоставлять на рынке более качественные услуги конкретному корпоративному клиенту.

Таким образом, были рассмотрены вопросы расположения серверов MEC, а именно: как расположение MEC влияет на производительность сети и факторы, которые определяют выбор местоположения MEC.

Проведя анализ, можно сказать, что на положение MEC влияет множество факторов, поэтому для каждой конкретной ситуации выбирается индивидуальное местоположение.

Однако не освещен вопрос выбора гибридной модели, где могут сочетаться в себе несколько мест обработки данных, это может усовершенствовать использование систем MEC, а именно: улучшить распределение ресурсов, уменьшить задержку, повысить мобильность, повысить разгрузку задач.

Заключение

MEC позволяет ускорять контент, сервисы и приложения за счет повышения скорости отклика на периферии. Выбор граничного местоположения является важным вопросом в сетях 5G.

Список использованных источников

1. Chen M., Zhang Y., Hu L., Taleb T., and Sheng Z. Cloud-based wireless network: Virtualized, reconfigurable, smart wireless network to enable 5g technologies // Mobile Networks and Applications. 2015. Vol. 20, No. 6. PP. 704–712.

2. Sabella D., Sprecher N., Patel M., Young V., Chao Hu Y. Mobile Edge Computing a key technology towards 5G [Электронный ресурс] // Whitepaper. 2015. URL: http://www.etsi.org (дата обращения 10.03.2023).

3. Jiang X., Yu F. R., Song T., & Leung V. C. M. A Survey on Multi-Access Edge Computing Applied to Video Streaming: Some Research Issues and Challenges // IEEE Communications Surveys & Tutorials. 2021. N 23 (2), PP. 871–903.

4. Spinelli F., & Mancuso, V. Towards enabled industrial verticals in 5G: a survey on MEC-based approaches to provisioning and flexibility // IEEE Communications Surveys & Tutorials. 2020. 1–1.

5. Klas G. ETSI MEC Use Cases and Requirements [Электронный ресурс] // ETSI. 2016. URL: http://www.etsi.org (дата обращения 10.03.2023)

УДК 654.197.6
ГРНТИ 19.61.31

МОДЕЛИ ПРОГНОЗИРОВАНИЯ НАСТУПЛЕНИЯ ОТКАЗОВ В РАБОТЕ ВЕЩАТЕЛЬНОГО ОБОРУДОВАНИЯ

В. С. Елагин, И. С. Шалимов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Эксплуатация вещательного оборудования характеризуется сравнительно невысокими расходами на поддержание функционирования в случае своевременного обнаружения неисправностей и их устранения за счёт применения ЗИП – запасных частей, инструментов и принадлежностей. Однако при несоблюдении периодичности технического обслуживания или при экстраординарных событиях в сети ремонт или замена оборудования оказываются высокозатратными. Возникает необходимость оптимизировать расходы.

моделирование отказов, цифровое телевидение, вероятность, прогнозирование.

С целью обеспечения населения России многоканальным вещанием к 2019 году завершилось создание сети станций ЦНТВ – цифрового наземного телевизионного вещания. Они осуществляют передачу 20 программ, разделенных на 2 мультиплекса, по 10 каналов в каждом. Сеть РТПС – радиотелевизионных передающих станций работает в круглосуточном режиме с запланированными кратковременными перерывами во время проведения ТО – технического обслуживания.

Объективно, исходя из того, что ТВ применяется не только для доставки зрителям развлекательного контента, но и для передачи правительственных сообщений, выпусков новостей, роликов по ГО и ЧС – гражданской обороне и чрезвычайным ситуациям крайне нежелательны прерывания вещания, связанные с поломками оборудования. Соответственно, требуется минимизировать наступление отказов и нарушений работы сети РТПС.

Для достижения указанной задачи главным образом необходимо предупреждение поломок. То есть их выявление на ранней стадии, прежде чем это приведёт к критическим нарушениям. В качестве средства предупреждения возможно использование системы прогнозирования наступления отказов на основе моделей, построенных с применением машинного обучения, или на основе математических моделей, задействующих методы математической статистики и теории вероятности [2].

В работе рассматривается возможность построения модели последнего типа, которая функционирует на основе статистической информации, прогнозируя вероятность наступления отказа конкретного блока или системы на определенном отрезке времени [1]. Необходимо принимать во внимание, что увеличение интервала времени предсказания снижает точность этого предположения. После разработки модели должна проводиться её проверка с целью валидации получаемых данных.

Как было сказано ранее, рассматриваемая модель работает на основе методов математической статистики. Следовательно, необходимо обеспечить её массивом данных, который подвергается статистической обработке.

Для сбора и накопления телеметрии используется система дистанционного контроля версии 5.3 – СДК 5.3. Она включает в себя сам модуль и транспортную сеть. Общение системы с оборудованием осуществляется на основе протокола SNMP – simple network management protocol, который работает на прикладном уровне TCP/IP. Он включает в себя набор стандартов сетевого управления, в том числе протокол прикладного уровня, схему баз данных и набор объектов данных.

Архитектура SNMP строится на базе трех основных компонентов:

– Элементы сети (network elements). Это сами управляемые устройства, содержащие SNMP-агент, то есть запущенное на них ПО. Оно обрабатывает локальную управляющую информацию и переводит её в форму, с которой работает протокол, или обратно в понятную устройству;

– Система сетевого управления (network management system). Это блок СДК, который содержит SNMP-менеджер, то есть ПО, установленное на промышленный компьютер в составе блока. Оно обрабатывает данные о конфигурации и функционировании систем, которыми управляет, переводя их во внутренний формат для работы протокола.

– База управляющей информации (management information base). Это сервер, обеспечивающий структурирование данных, которыми обмениваются агенты и менеджеры. Все переменные организуются в иерархии, которые и описываются с помощью базы.

SNMP похож на протокол HTTP – он использует методы GET/SET. Соответственно, для отправки запросов на устройства применяется метод SET, а для получения ответов – метод GET. Чтобы минимизировать число опросов оборудования, используется режим SNMP trap. Он предполагает, что контроллер устройства самостоятельно обрабатывает все параметры и уведомления, получаемые от внутренних блоков, и в случае нарушения отправляет уведомление на СДК. А тот обрабатывает поступившие данные и сохраняет на сервере.

Следующий вопрос, требующий внимания, это выбор элементов, на анализе работы которых основывается прогнозирование отказов. Цифровой вещательный тракт может быть представлен в виде следующих ключевых блоков:

– цифровой передатчик. Он в свою очередь подразделяется на 4 модуля:

- формирователь, который синтезирует полный DVB-T2 сигнал на радиочастоте;
- усилитель мощности, который повышает мощность сформированного сигнала до номинальной с учётом запаса по мощности на потери в следующих трактах;
- фильтр гармоник, который снижает уровень побочного излучения;
- полосовой фильтр, который снижает уровень внеполосного и побочного излучения;

– ЦРРС – цифровая радиорелейная станция, включающая:

- IDU – indoor unit, то есть размещаемое в контейнере оборудование;
- ODU – outdoor unit, то есть антенны и приемо-передатчики;

– ЗССС – земная станция спутниковой связи, состоящая из:

- приемной спутниковой станции;
- приёмной антенны;

– АМС – антенно-мачтовая система, включающая вышку и волноводные фидеры;

– система мониторинга и контроля, в которой выделяются 2 основных модуля:

- блок СДК;
- VSAT – very small aperture terminal, то есть спутниковый приемо-передатчик и спутниковая тарелка малого диаметра;

– инженерные системы и оборудование, главным образом система электропитания:

- основной ввод – трехфазная линия, питающая объект от ближайшей трансформаторной подстанции;
- резервный ввод – либо трехфазная линия, запитанная от другой подстанции, либо ДГУ – дизель-генераторная установка;
- устройство АВР – автоматического ввода резерва для коммутации между вводами.

Определившись с выбором элементов для анализа, следует рассмотреть принципы построения искомой модели.

Оценка надёжности разных элементов возможна на основе двух основных типов моделей: нагрузка-прочность, то есть прочностная надёжность, и параметр-поле допуска, то есть параметрическая надёжность [3].

Прочностная надёжность подразумевает сохранение работоспособности элемента под воздействием внешних нагрузок, характерных для него. Основные показатели надёжности по прочности – средняя наработка до отказа или вероятность безотказной работы. Эти параметры могут быть определены на основе данных об эксплуатации оборудования за предыдущий период, выбранный для оценки.

Применительно к элементам радиоэлектронной аппаратуры, к которой относится вещательное оборудование, распространенной причиной потери работоспособности служит перегрузка. Она может быть вызвана коротким замыканием, разрывом цепи или резким изменением параметров элемента.

1) Вероятность безотказной работы – есть вероятность того, что на рассматриваемом интервале времени отказы не происходят.

Для её приближенного расчёта возможно использование формулы:

$$P(t) \approx \frac{N(t)}{N_0} = \frac{N_0 - n(t)}{N_0}, \quad (1)$$

где N_0 –общее количество изделий; $N_{(t)}$ – число сохранивших работоспособность за время t изделий; $n(t)$ – число отказавших за время t изделий.

При этом $n(t)$ определяется согласно формуле:

$$n(t) = \sum_{i=1}^{\Delta t} n_i, \quad (2)$$

где n_i – число отказавших в интервале Δt изделий.

Δt определяется по данным эксплуатации.

2) Наработка на отказ – есть среднее время работы без отказов для восстанавливаемого изделия между двумя соседними отказали.

Данный параметр определяется согласно формуле:

$$T_0 \approx \frac{t}{n} = \frac{\sum_{i=1}^{n} t_i}{n}, \quad (3)$$

где t – общее время исправной работы изделия;

n – число отказов за время эксплуатации;

t_i – время исправной работы изделия между $(i-1)$-м и i-м отказами.

Параметрическая надежность предусматривает, что каждый элемент может быть характеризован каким-либо параметров X, определяющим его. Применительно к вещательному оборудованию, например, усилителю мощности, таким параметром могут быть токи на MOSFET-транзисторах. Для них существует указываемое изготовителем номинальное значение. Несоответствие токов номиналу свидетельствует о нарушении работоспособности усилителя мощности.

Отличие этого типа надёжности от прочностной заключается в постепенном выходе параметров за указанные интервалы. В рассмотренном примере, токи транзисторов со временем могут либо расти, в конечном счёте приведя к перегрузке, либо падать, в итоге приведя к неработоспособности усилителя из-за неспособности выдавать требуемую мощность.

Скорость изменения параметра определяется формулой:

$$\gamma = \frac{dX}{dt}, \tag{4}$$

где $dX -$ приращение значения параметра за время dt.

В этом случае средняя наработка до отказа *T* отвечает выражению:

$$T = \frac{X_{\text{пр}} - X_0}{\gamma}, \tag{5}$$

где $X_{\text{пр}}$ – предельное значение параметра, X_0 – начальное значение параметра.

Для расчётов используется допущение, что аргументы X_0 и γ имеют нормальное распределение с МОЖ $M(X_0) = \overline{X_0}$ и $M(\gamma) = \bar{\gamma}$; СКО, соответственно, σ_{X_0} и σ_γ.

Тогда параметр X в момент *t* также распределяется нормально:

$$M(X) = \bar{X} = M(X_0) + M(\gamma)t = \overline{X_0} + \bar{\gamma}t, \tag{6}$$

$$\sigma_X = \sqrt{{\sigma_{X_0}}^2 + (\sigma_\gamma t)^2}, \tag{7}$$

Отсюда следует, что вероятность безотказной работы элемента равна:

$$P(t) = p\left(X \le X_{\text{пр}}\right) = \frac{1}{2} + \Phi\left[\frac{X_{\text{пр}} - (\overline{X_0} + \bar{\gamma}t)}{\sqrt{{\sigma_{X_0}}^2 + (\sigma_\gamma t)^2}}\right].$$

Таким образом, возможно построение модели прогнозирования наступления отказов путем сочетания двух рассмотренных выше видов надёжности. Выбор обуславливается типом элементов, работоспособность которых оценивается.

В частности, для ЗССС рационально применение прочностной надежности. Так как изменение состояния атмосферы периодически приводит к неустойчивости приема или его отсутствию в течение конкретного интервала времени.

В то же время, для формирователя передатчика больше подойдет параметрическая надёжность. Так как входящие в его состав радиоэлектронные компоненты склонны к деградации характеристик. Расположенные на плате конденсаторы со временем высыхают, из-за чего изменяется их ёмкость.

Модель, которая может быть получена в результате, задействует данные об отказах и изменении параметров, собираемые блоками СДК объектов. На основании этой информации рассчитываются вероятности безотказной работы отдельных элементов. После чего определяются вероятности отказа систем, в которые входят элементы. По полученным зависимостям можно получить предположения об отказе конкретных элементов в указанный момент времени.

Список используемых источников

1. ГОСТ Р 27.004-2009. Надёжность в технике. Модели отказов : Приказ Федерального агентства по техническому регулированию и метрологии № 1244-ст. 15.12.2009 г.

2. Шаханов Н. И., Варфоломеев И. А., Виноградова Л. Н., Юдина О. В., Ершов Е. В. Обобщенный алгоритм функционирования системы прогнозирования отказов промышленного оборудования в условиях малого количества поломок // Теплотехника и информатика в образовании, науке и производстве. Сб. докладов IX Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных (ТИМ'2021) с международным участием (Екатеринбург, 13–14 мая 2021 г.). Екатеринбург: УрФУ, 2021. С. 318–322.

3. Труханов В. М., Султанов М. М., Кухтик М. П., Горбань Ю. А. Математическая модель прогнозирования отказов статистическим методом при испытаниях головных образцов энергетического оборудования ТЭС // Надежность и безопасность энергетики. 2018. Т. 11, N 3. С. 235–240

УДК 004.85
ГРНТИ 28.23.24

ОБЗОР МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЗАДАЧ АНАЛИЗА ТРАФИКА

В. С. Елагин, Ю. Е. Щегольский

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Машинное обучение – это направление искусственного интеллекта, сосредоточенное на создании систем, которые обучаются и развиваются на основе получаемых ими данных.

Технология машинного обучения позволила выполнять некоторые операции быстрее чем человек. С годами эта технология усовершенствовалась, были придуманы новые алгоритмы работы. Сейчас же, машинное обучение применяется во многих областях человеческой деятельности, в том числе, в области анализа трафика.

В статье рассмотрены задачи, решаемые методами машинного обучения. Рассмотрены алгоритмы, применяемые для анализа трафика. Проведено сравнение приведенных алгоритмов, и выделен один, наиболее подходящий для выполнения задач анализа трафика.

машинное обучение, анализ трафика, классификация трафика, кластеризация.

Введение

Компьютеры давно применяются для решения задач, с которыми человек и сам справляется. С увеличением объемов данных, стало понятно, что скорость выполнения у машин выше. Задав условие на входе, компьютер достаточно быстро выдает результат.

Машинное обучение изучает методы построения алгоритмов, способных обучаться. Компьютеры учатся на основе входных данных и совершенствовании при помощи опыта. В процессе машинного обучения алгоритмы учатся поиску закономерностей и корреляций в больших наборах данных [1]. Рост объема данных способствует увеличению точности и улучшению машинного обучения.

Задачи, решаемые методами машинного обучения, можно разделить следующим образом.

- Идентификация. Задаются параметры, по которым должны быть определены и отделены нужные данные.
- Прогнозирование. Определение следующего значения на основе анализа данных за конкретный промежуток времени.
- Кластеризация. Объединение в группы (кластеры) объектов по сходным признакам.
- Классификация. По имеющимся параметрам выделяется принадлежность объекта одному из классов.

Задача кластеризации

Рассмотрим задачи, решаемые с помощью машинного обучения в области анализа трафика.

Одной из таких задач является кластеризация трафика. Основа данной задачи – выявление естественных групп (кластеров) в данных, на основе эвристики. Кластеризация относится к типу машинного обучения без учителя, т. е. алгоритм сам определяет зависимости, на основе которых впоследствии машина может работать с данными.

Популярным методом для решения задачи кластеризации является алгоритм *k*-средних. Работа алгоритма выражается следующими этапами:

- Берем данные и определяем желаемое количество кластеров *k*;
- Расположим кластеры и рассчитаем расстояния до каждого из них;
- Каждая точка теперь относится к кластеру.

Эти шаги повторяются до тех пор, пока алгоритм не стабилизируется, т. е. пока наблюдения не перестанут переходить от одного кластера к другому [2]. Цель алгоритма – минимизировать сумму квадратов внутрикластерных расстояний до центра кластера.

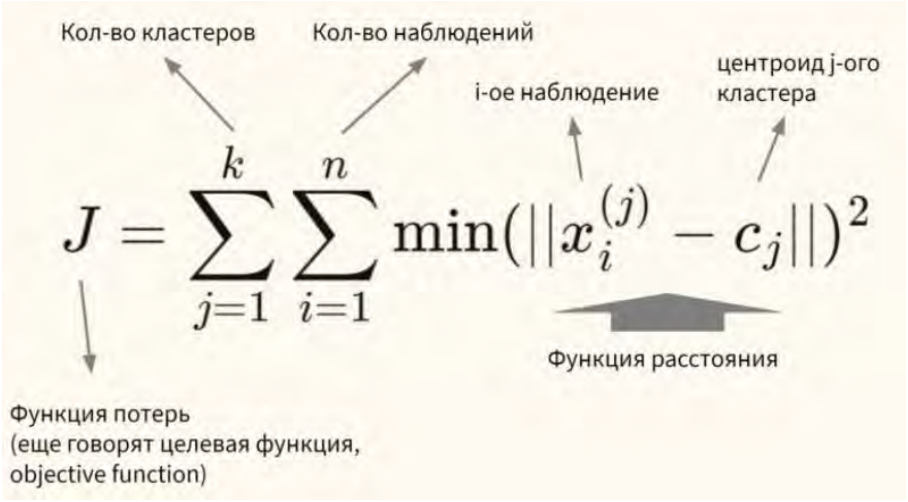


Рис. 1. Формула целевой функции

Метод *k*-средних работает хорошо, в том случае, если данные компактные и образуют примерно сферические группы. Для этого метода следует указать количество кластеров, на которые будет разделено исследуемое множество. Также при большом числе входных признаков, данный алгоритм показывает плохой процент ошибочно классифицированных пакетов.

Задача классификации

Еще одной немаловажной задачей является классификация трафика. Задача классификации трафика, как и другие задачи классификации, обычно рассматривается как задача обучения с учителем. Обучение с учителем – тип машинного обучения, при котором имеется специальный набор данных, в которых присутствует правильный ответ. Результатом является – выдача ответа по описанию на входе.

Для классификации трафика используются различные методы, выделим два из них – метод опорных векторов и дерево принятия решений.

В методе опорных векторов каждый элемент данных – это точка в *p*-мерном пространстве, где *p* – количество признаков. Алгоритм должен построить плоскость (*p* – 1), которая будет разделять точки, относящиеся к разным классам. Задача – разделять этой плоскостью как можно лучше, чтобы разделенные классы находились, как можно дальше о плоскости [3]. Для разделения на N классов, используется два способа:

– попарного сравнения: строится $N*(N-1)/2$ классификаторов, каждый из которых учится различать между собой два класса

– один против всех: строится *N* классификаторов, каждый из которых учится различать один класс от всех остальных

Следующий метод классификации – это дерево решений. Двумя его составляющими являются узлы и листья. В узлах находятся решающие правила и производится проверка соответствия примеров этому правилу по какому-либо атрибуту обучающего множества. В результате проверки, множества разбиваются на подмножества, в одно из которых попадают примеры, удовлетворяющие правилу, а в другое – неудовлетворяющие [4]. Алгоритм продолжает работать до тех пор, пока не будет достигнуто условие остановки. Последний узел называется листом. Лист определяет решение для каждого попавшего в него примера. В листе содержится подмножество, которое удовлетворяет всем правилам ветви, по которой прошло множество примеров. Основными этапами построения дерева являются:

1. Выбор атрибута для разбиения подмножества в узле.
2. Выбор критерия остановки обучения.
3. Выбор метода отсечения ветвей (упрощения).
4. Оценка точности построенного дерева.

Преимущества дерева принятия решений:

– быстрый процесс обучения;

– понятная классификационная модель;

– высокая точность предсказания, по сравнению с другими методами.

Сравнение методов

Помимо алгоритмов, приведенных в статье, существуют и другие. Они так же подходят для решения задач анализа трафика. У всех алгоритмов есть преимущества и недостатки. Поэтому проведем сравнение, приведенных методов.

Метод *k*-средних в отличие от методов опорных векторов и дерева решений обучается на неразмеченных данных. Алгоритм сам ищет похожие объекты и объединяет их в кластеры. Размечаются только признаки, по которым и будет проходить объединение в кластеры.

Метод опорных векторов эффективен в многомерных пространствах признаков, но требует много памяти и вычислительных ресурсов. Может легко переобучаться, то есть подстраиваться только под параметры множества примеров, на которых алгоритм обучался.

Преимущества алгоритма дерева решений были описаны выше, но конечно же, у него имеются и недостатки, к ним можно отнести:

– проблема получения оптимального дерева решений (оптимальное решение выбирается локально в каждом узле);

– необходимость регулировать длину дерева из-за риска переобучения;

– неустойчивость дерева при небольших изменениях входных данных.

Заключение

Машинное обучение применяется во многих сферах жизнедеятельности человека, и анализ трафика не исключение. Существует множество методов, которые справляются с задачами анализа трафика. У каждого метода есть свои преимущества и недостатки, и каждый метод может справляться с определенной задачей лучше.

Из приведенных в статье методов, больше всего для анализа трафика подойдет дерево решений. Это наиболее оптимальный метод, у него больше преимуществ наравне с другими приведенными. Алгоритм дерева решений имеет интуитивно понятную классификационную модель, способен быстро обучаться, может работать с большим объемом данных, обладает высокой точностью предсказаний на уровне статистики и нейронных сетей, а также не требует специальной подготовки данных.

Список используемых источников

1. Информационно-аналитический ресурс по машинному обучению. URL: http://www.machinelearning.ru/wiki/

2. Halkidi M., Batistakis Y. and Vazirgiannis M. Cluster validity methods: part I // SIGMOD Rec. 2002. Vol. 31, No. 2. PP. 40–45.

3. Гетьман А. И., Иконникова М. К. Обзор методов классификации сетевого трафика с использованием машинного обучения // Труды ИСП РАН. 2020. Т. 32, вып. 6. С. 137–154.

4. Breiman Leo, Friedman J., Olshen R., and Stone C. Classification and Regression Trees. Wadsworth, Belmont, CA, 1984.

УДК 004.056
ГРНТИ 81.93.29

СТАТИСТИЧЕСКИЙ АНАЛИЗ ПУБЛИКАЦИОННОЙ АКТИВНОСТИ УЧЕНЫХ ПО РАЗЛИЧНЫМ ОБЛАСТЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л. Р. Елизарова[1], К. Е. Израилов[1,2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Работа посвящена анализу статистики научных публикаций по исследованиям, направленным на решение задач в различных областях информационной безопасности. Данные области были получены авторами ранее с помощью аппарата категориального

деления. Метод анализа заключается в поиске научных статей и их отнесению к соответствующим областям. Делаются выводы относительно текущей и будущей актуальности задач информационной безопасности.

информационная безопасность, публикационная активность, прогнозирование.

Введение

Для обеспечения полноценной информационной безопасности (далее – ИБ) важно определить ее область, чтобы применять в ней соответствующие меры. Поэтому первой задачей являлась разработка классификации областей ИБ, что было уже осуществлено авторами в предыдущих исследованиях.

Исходя из этого, текущая задача ставится, как сбор статистики научных исследований и публикаций по подобластям ИБ для проверки корректности полученной ранее классификации.

Аппарат категориального деления

Авторская классификация областей ИБ, обладающая безусловной новизной, была получена с помощью категориального деления.

Суть категориального деления состоит в том, что выделяются пары категорий взаимно противоположных объектов, комбинируя которые можно получить классы (количество которых равно значению числа 2 в степени числа категориальных пар) и, как результат, разделить по ним области ИБ [1].

Авторская классификация

Для области ИБ были выделены такие категориальные пары как «Статика ***vs*** Динамика», «Аппаратный ***vs*** Программный», «Внешний ***vs*** Внутренний».

Комбинация 3-х категориальных пар дает $2x2 = 8$ следующих классов областей ИБ:

1) K_{SHE} – пересечение статических данных, аппаратного обеспечения и внешнего доступа; например, защита портативных устройств хранения информации, таких, как USB-Flash или аппаратная система распознавания отпечатка пальца на мобильном телефоне.

2) K_{SHI} – пересечение статических данных, аппаратного обеспечения и внутреннего доступа; например, защита внутренних устройств хранения данных, таких как жесткий диск.

3) K_{SSE} – пересечение статических данных, программного обеспечения и внешнего доступа; например, защита Интернет-ресурсов.

4) K_{SSI} – пересечение статических данных, программного обеспечения и внутреннего доступа; например, защита базы данных.

5) K_{DHE} – пересечение динамических данных, аппаратного обеспечения и внешнего доступа; например, использование аппаратной системы обнаружения вторжений.

6) K_{DHI} – пересечение динамических данных, аппаратного обеспечения и внутреннего доступа; например, аппаратные средства обеспечения резервного хранения и обработки данных, такие, как, дополнительные RAID-массивы.

7) K_{DSE} – пересечение динамических данных, программного обеспечения и внешнего доступа; например, обеспечение конфиденциальности обмена информацией между абонентами в процессе телефонного разговора.

8) K_{DSI} – пересечение динамических данных, программного обеспечения и внутреннего доступа; например, технология электронно-цифровой подписи.

Наглядная система деления классов по категориальным парам представлена в таблице 1.

ТАБЛИЦА 1. Деление классов ИБ по категориальным парам

Статика				Динамика			
Аппаратный		Программный		Аппаратный		Программный	
Внеш.	Внутр.	Внеш.	Внутр.	Внеш.	Внутр.	Внеш.	Внутр.
K_{SHE}	K_{SHI}	K_{SSE}	K_{SSI}	K_{DHE}	K_{DHI}	K_{DSE}	K_{DSI}

Корреляция с существующими областями

Полученную ранее классификацию можно применить к классическим и наиболее распространенным областям ИБ:

1) Компьютерная безопасность заключается в защите компьютерных систем и сетей – одновременно относится к классам K_{SHE} и K_{DHE}.

2) Безопасность инфраструктуры обеспечивает защиту внутренних сетей, лабораторий, центров обработки данных, серверов, настольных компьютеров и мобильных устройств [2] – относится к классу K_{SHE}.

3) Безопасность баз данных с помощью средств ИБ обеспечивает защиту баз данных от нарушения их конфиденциальности, целостности и доступности – относится к классу K_{SSI}.

4) Операционная безопасность обеспечивает идентификацию и защиту критически важной информации [3] – относится к классам K_{SSI} и K_{DSI}.

5) Безопасность приложений заключается в разработке и улучшении методов обеспечения ИБ приложений – относится к классу K_{DSE}.

6) Физическая безопасность серверов обеспечивает защиту серверных помещений, по авторской классификации относится к классу K_{SHE}.

7) Сетевая безопасность занимается обеспечением ИБ компьютерной сети и ее ресурсов [4] – относится к классу K_{DSI}.

8) Криптография заключается в разработке методов шифрования информации [5] – относится к классу K_{DSI}.

Проверка модели категориального деления

Для проверки новой классификации были собраны научные исследования и публикации по теме ИБ, которые затем были отнесены к одной из подобластей ИБ; шаги метода состояли из следующих:

1) На электронном ресурсе научной библиотеки elibrary.ru в поисковую строку вводится ключевое слово «информационная безопасность».

2) Получается список релевантных научных статей.

3) Анализируются 100 наиболее релевантных (т. е. первых в списке) публикаций путем изучения для каждой статьи названия, ключевых слов и аннотации.

4) Каждая статья экспертно относится к одной из областей.

Статистика публикаций

Полученная статистика научных исследований и публикаций по подобластям ИБ представлена на рис. 1. Площадь подобластей на рисунке тождественна количеству публикаций.

Рис. 8. Статистика публикаций по подобластям информационной безопасности

Анализ полученного распределения публикаций по авторским подобластям позволяет сделать два важнейших вывода. Во-первых, отсутствуют пустые подобласти, то есть для каждой из них существует по крайней мере

одна публикация – выполнено требования *необходимости деления* (отсутствуют лишние подобласти). Во-вторых, каждую публикацию удалось отнести к одной и только одной подобласти – выполнено требования *достаточно деления* (отсутствуют пересекающиеся подобласти). Все это подтверждает «удачность» предложенной классификации.

Выводы

В работе собраны научные исследования и публикации по новой классификации областей ИБ. Полученная статистика публикационной активности показала, что отсутствуют как пустые, так и пересекающиеся подобласти. Все это говорит о корректности авторской классификации.

В дальнейших исследованиях планируется разработка метода автоматического сбора и анализа статистики научных исследований и публикаций для каждого из классов с целью выявления наиболее актуальных и/или малоизученных из них, что, в том числе позволит строить прогнозы касательно будущих угроз ИБ [6, 7, 8].

Список используемых источников

1. Буйневич М. В., Израилов К. Е. Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. 2016. Т. 4. N 3. С. 95–106.

2. Красов А. В., Гельфанд А. М., Коржик В. И., Котенко И. В., Петрив Р. Б., Сахаров Д. В., Ушаков И. А., Шариков П. И., Юркин Д. В. Построение доверенной вычислительной среды: учебное пособие. СПб. : Индивидуальный предприниматель Петрив Роман Богданович, 2019. 108 с.

3. Никулин В. В. Безопасность Windows и Windows defender // Вестник образовательного консорциума Среднерусский университет. Информационные технологии. 2021. N 2 (18). С. 7–13.

4. Лаврова Д. С., Попова Е. А., Штыркина А. А., Штеренберг С. И. Предупреждение dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика // Проблемы информационной безопасности. Компьютерные системы. 2018. N 3. С. 70–77.

5. Кушнир Д. В., Шемякин С. Н, Исследование возможных методов аутентификации согласования данных в классическом канале в протоколах квантовой криптографии // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. N 4. С. 63–67.

6. Last D. Using historical software vulnerability data to forecast future vulnerabilities // Resilience Week (RWS). 2015. PP. 1–7.

7. Домкин К.И., Тростянский А.Г. Применение диверсионного подхода для прогнозирования уязвимостей сетей связи // Труды международного симпозиума "Надежность и качество". 2020. Т. 2. С. 349–352.

8. Buinevich M., Izrailov K., Stolyarova E., Vladyko A. Combine method of forecasting VANET cybersecurity for application of high priority way // The proceedings of 20th International Conference on Advanced Communication Technology (Chuncheon, South Korea, 2018). IEEE, 2018. PP. 266–271.

УДК 004.056
ГРНТИ 81.93.29

ВЫБОР МЕТОДА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т. В. Ершова, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Со стремительным развитием информационных технологий растут и угрозы безопасности информации. Крайне актуальной становится тема проведения аудита безопасности, являющегося одним из важнейших способов своевременного нахождения уязвимостей и предотвращения возможных несанкционированных действий в дальнейшем. В статье рассматриваются методы проведения аудита информационной безопасности.

аудит информационной безопасности, активный аудит, CRAMM, OCTAVE, RiskWatch.

С развитием технологий растёт и потребность в обеспечении информационной безопасности. В последние годы резко возросло число возможных способов влияния на конфиденциальность, целостность и доступность информации, обрабатываемой в частных и корпоративных сетях. Крайне актуальной становится тема проведения аудита безопасности, являющегося одним из важнейших способов своевременного нахождения уязвимостей и предотвращения возможных несанкционированных действий в дальнейшем.

Процедура аудита информационной безопасности подразумевает под собой исследование и оценку текущего состояния безопасности и защищенности информационной системы на соответствие действующим стандартам и требованиям. Она позволяет получить объективную оценку текущего состояния защищенности информационных ресурсов, также предоставляет подробный отчет по выявленным возможностям угроз для информационной системы. Кроме того, можно получить развернутый план дальнейших действий по работе с этими угрозами [1].

Целями проведения аудита безопасности являются [2]:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов;
- оценка текущего уровня защищенности;
- локализация узких мест в системе защиты;
- оценка соответствия существующим стандартам и нормативным документам в области ИБ;

- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов.

Среди основных видов аудита информационной безопасности выделяют следующие [3, 4]:

1. Активный аудит. Также его часто называют инструментальным анализом защищённости. Он включает в себя исследование состояния защищенности информационной системы с позиции злоумышленника: при помощи специального программного обеспечения собирается информация о состоянии системы (параметры и настройки, на основании использования которых злоумышленник может получить доступ к сети и произвести атаку).

2. Экспертный аудит. На основании требований заказчика и опыта компании-аудитора формируется некоторая идеальная модель системы обеспечения ИБ, с которой сравнивается текущая реализация комплекса средств обеспечения ИБ в исследуемой ИС. При экспертном аудите производится детальное обследование ИС со сбором информации об источниках и способах обработки её исходных данных, а также имеющейся организационно-распорядительной документации. Полученная информация анализируется аудитором для выявления недостатков системы безопасности.

3. Аудит на соответствие стандартам. При проведении данного вида аудита основное внимание уделяется тому, соблюдает ли организация государственные стандарты, нормативные акты и связанные с ними правила обеспечения ИБ. Аудит на соответствие стандартам также проверяет, соблюдает ли организация внутренние правила, предписания, политики, решения, направленные на повышение уровня ИБ.

Одним из вариантов проведения аудита ИБ являются инструментальные средства оценки рисков информационной безопасности. Рассмотрим некоторые из них и их методы анализа [5].

Метод CRAMM. Самый распространенный метод анализа рисков и управления ими, подходит как для коммерческого, так и для государственного сектора. В основе него лежит системный подход к оценке рисков ИБ, учитывается как денежный эквивалент ущерба, так и ранжирование по шкалам. В первую очередь анализируется все, что касается идентификации и определения ценности ресурсов системы. Проводится идентификация ресурсов: физических, программных и информационных, содержащихся внутри границ системы. В программном обеспечении CRAMM ценность физических и не физических ресурсов определяется по-разному. В случае физических ресурсов это стоимость восстановления после успешной реализации атаки, а в не физических ценность зависит от ситуации последующей после удачной атаки на ресурсы системы (полное или частичное уничтожение информации, атаки на доступность ресурса и т. д.). Программа CRAMM

генерирует список вопросов и в зависимости от ответов оценивается уровень угроз (очень высокий, высокий, средний, низкий и очень низкий).

Методика OCTAVE. Особенность данной методики заключается в том, что анализ рисков производится без привлечения сторонних аудиторов. При оценке рисков методом OCTAVE требуется сформировать основную аналитическую группу из числа сотрудников организации. Данная группа производит сбор информации с разных уровней организации для выявления критических активов. OCTAVE включает три основных этапа:

– создание профиля угроз активов;
– определение уязвимостей;
– выработка стратегии безопасности.

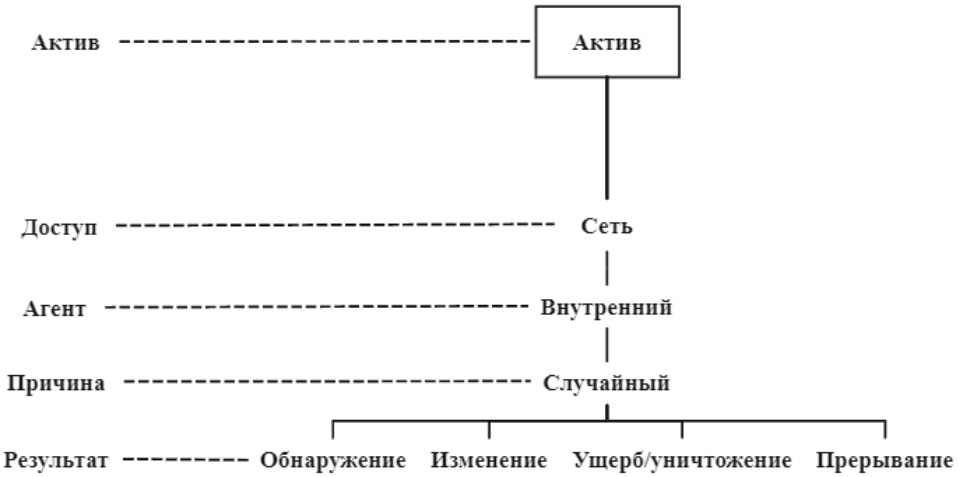


Рис. 1. Пример ветви дерева угроз,
которое используется при описании профиля в методике OCTAVE

На первом этапе создается профиль угроз, прорабатывается взаимосвязь угрозы ИБ и ресурса. В результате получается сводное представление обо всех угрозах, которое затем отображается в виде дерева угроз (рис. 1), структурированного таким образом, чтобы дать углубленное представление об источнике и последствиях угроз по категориям «актив», «доступ», «агент», «причина» и «результат».

Методика компании RiskWatch. Данный метод оценки рисков использует ожидаемые годовые потери и возврат инвестиций в качестве критериев для оценки рисков и управления ими. RiskWatch ориентирован на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. На первом этапе определяются базовые параметры: тип организации, состав информационной системы, основные требования безопасности. На втором этапе вносятся данные, которые характеризуют определенные параметры системы. На третьем этапе происходит количественная оценка риска. Этот инструмент позволяет оценить, как

риски, которые в настоящее время существуют на предприятии, так и выгоды, которые может принести внедрение физических, технических, программных и других средств и механизмов защиты. На четвертом этапе формируется отчетность.

В данной статье были рассмотрены виды аудита ИБ и один из способов его проведения с помощью инструментальных средств оценки рисков. В основном рассмотренные методики оценки рисков предлагают активный вид аудита, но некоторые программные обеспечения также проводят аудит на соответствие стандартам.

Список используемых источников

1. Комарова А. В., Толокольникова К. В. Основные угрозы безопасности и устранение их методом аудита информационной безопасности // Взаимодействие науки и общества: проблемы и перспективы : сб. ст. Международной научно-практической конференции: в 4 ч., Казань, 08 июня 2017 г. Часть 3. Казань: ООО «ОМЕГА САЙНС», 2017. С. 63-66.

2. Кураленко А. И. Методика аудита информационной безопасности информационно-телекоммуникационной системы : дис. ... канд. техн. наук : 05.13.19 / Кураленко Алексей Игоревич. Томск, 2015. 147 с.

3. Виды аудита информационной безопасности // Искусство управления информационной безопасностью ISO27000 [Электронный ресурс]. URL: http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/vidy-audita-informacionnoi-bezopasnosti (дата обращения 29.03.2023).

4. Сагитова В. В. Модели и алгоритмы анализа информационных рисков при проведении аудита безопасности информационной системы персональных данных : дис. ... канд. техн. наук : 05.13.19 / Сагитова Валентина Владимировна. Уфа, 2019. 229 с.

5. Губарева О. Ю. Разработка методики оценки рисков информационной безопасности корпоративных телекоммуникационных сетей : дис. ... канд. техн. наук : 05.12.13 / Губарева Ольга Юрьевна. Самара, 2018. 175 с.

6. Гельфанд А. М., Казанцев А. А., Красов А. В., Орлов Г. А. Оценка рисков и угроз безопасности в среде "умный дом" // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 316–321.

Статья представлена научным руководителем, заведующем кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004
ГРНТИ 28.23.25

АНАЛИЗ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРЕДСКАЗАНИЯ ВРЕМЕННЫХ РЯДОВ

К. Э. Есалов, М. С. Кузнецов, К. А. Романенко

Санкт–Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматриваются принципы анализа и методы предварительной обработки данных для прогнозирования временных рядов, а именно: преобразование Бокса-Кокса, нормализация и дифференцирование. Для предсказания будущих значений временных рядов при помощи моделей машинного обучения были рассмотрены такие регрессионные модели, как Линейная регрессия, Случайный лес и Градиентный бустинг. В результате экспериментов, опираясь на данные прошлых периодов, удалось построить прогноз временного ряда на несколько значений вперед и оценить эффективность рассматриваемых моделей машинного обучения.

машинное обучение, предсказание, временные ряды, предобработка данных.

В настоящее время создание высококачественных прогнозов – непростая задача ни для машин, ни для большинства аналитиков. Однако сама задача предсказания временных рядов не теряет своей актуальности.

В задачу предсказания временных рядов входит не только построение моделей машинного обучения, но и предобработка данных в целях приведения временного ряда к стационарному виду, без которой модели не смогут давать наилучшие результаты.

Модели, построенные по данным, характеризующим один объект за ряд определенных последовательных периодов, называется моделями временных рядов. Существует множество моделей для предсказания временных рядов, были рассмотрены линейная регрессия, случайный лес и градиентный бустинг [1, 2].

Линейная регрессия (LinearRegression) [1] – это математическая модель, которая описывает связь нескольких переменных. Модели линейной регрессии представляют собой статистическую процедуру, помогающую прогнозировать будущее. Она применяется в научных сферах и в бизнесе, а в последние десятилетия используется в машинном обучении. Формула линейной регрессии:

$$y = ax + b,$$

где a и b – параметры, подбираемые при обучении, x – набор параметров, характеризующий наблюдение, y – предсказываемый параметр.

Случайный лес (*Random forest*) [1] – это множество решающих деревьев, каждое из которых обучается на случайном участке данных. В задаче регрессии их ответы усредняются.

CatBoostRegressor [2] – алгоритм градиентного бустинга, тоже представляет собой множество решающих деревьев, каждое из которых пытается исправить ошибку предыдущего дерева.

Для повышения точности прогнозов целесообразно изменять начальные данные с помощью дифференцирования, нормализации и преобразования Бокса-Кокса [3].

Дифференцированием временного ряда называют вычисление разницы следующего члена временного ряда от предыдущего.

Для деревьев и бустингов крайне важно, чтобы анализируемый ряд не имел «тренда», то есть был стационарным. Дифференцирование прекрасно справляется с подобной задачей, преобразуя данные между соседними промежутками времени в разницу между ними (рис. 1).

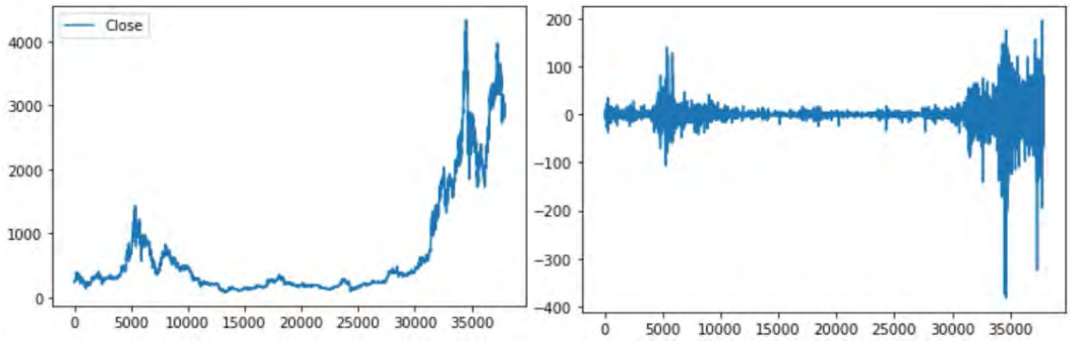


Рис. 1. Результаты до и после дифференцирования данных

Ключевая цель нормализации – приведение различных данных в самых разных единицах измерения и диапазонах значений к единому виду, который позволит сравнивать их между собой или использовать для расчёта схожести объектов. На практике это необходимо, например, для кластеризации и в некоторых алгоритмах машинного обучения.

$$x_{norm} = \frac{x - x_{min}}{x_{max} - x_{min}},$$

где x – значение последовательности, x_{min} – минимальное значение последовательности, x_{max} – максимальное значение последовательности

Одной из задач Бокс-Кокс преобразования является приведение закона распределения входной последовательности к «нормальному» виду (рис. 2), что особенно полезно в моделях линейной регрессии.

Для исходной последовательности $x = \{x_1, \dots, x_n\},\ x_i > 0, \mathrm{i} = 1, \dots, n$ однопараметрическое преобразование Бокса-Кокса с параметром определяется следующим образом:

$$x_i(\lambda) = \begin{cases} \frac{x_i^{\lambda}-1}{\lambda}, \lambda \neq 0 \\ ln(x_i), \lambda = 0 \end{cases},$$

где λ – подбираемый параметр, x_i – член исходной последовательности.

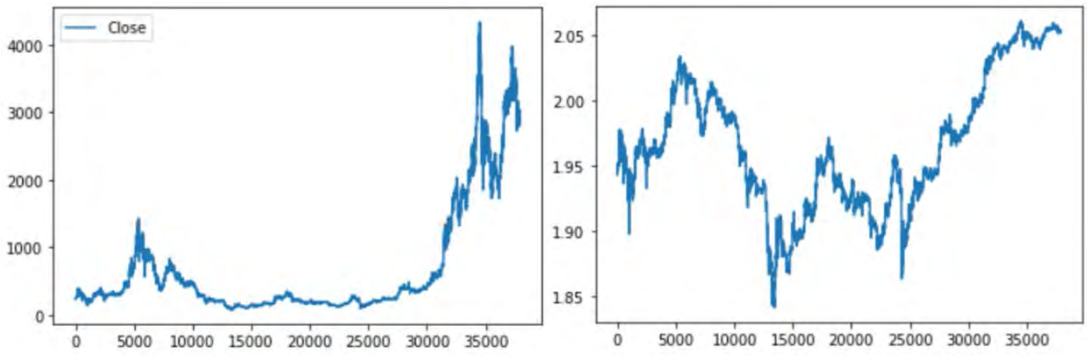


Рис. 2. Результаты до и после преобразования данных методом Бокса–Кокса

Для подсчета точности моделей были использованы следующие метрики: MSE, R^2, MAE, MAPE [4].

MSE – среднеквадратическая ошибка. Измеряет среднее квадратов ошибок, то есть среднеквадратичную разницу между оценочным и фактическим значением. Чем эта разница меньше, тем лучше модель предсказывает значения.

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2,$$

где N – количество предсказанных данных, y_i – реальные данные (фактические значения), $\hat{y}_i$ – предсказанные данные (оценочные значения).

R^2 – это коэффициент линейной детерминации. Показывает, во сколько предсказанные нашей моделью данные лучше, чем среднее значение. Чем ближе к 1, тем лучше работает модель.

$$R^2 = 1 - \frac{MSE(model)}{MSE(baseline)},$$

где MSE (*model*) – среднеквадратичное отклонение между фактическими и предсказанными данными, MSE (*baseline*) – среднеквадратичное отклонение между фактическими данными и средним значением.

Характеризует степень сходства исходных данных и предсказанных. В отличии от *MSE* не зависит от единиц измерения данных, поэтому поддается сравнению. Когда R^2 отрицательно, это означает, что модель хуже, чем предсказание среднего значения.

MAE – средняя абсолютная ошибка. Измеряет средне абсолютную разницу между оценочным и фактическим значением. Чем эта разница меньше, тем лучше модель предсказывает значения.

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|y_i - \hat{y}_i|,$$

где N – количество предсказанных данных, y_i – реальные данные (фактические значения), $\hat{y}_i$ – предсказанные данные (оценочные значения).

MAPE – средняя абсолютная процентная ошибка. Измеряет среднее абсолютное процентное отклонение между оценочными и фактическими значением, является мерой точности прогноза. Чем меньше, тем лучше модель предсказывает значения.

$$MAPE = \frac{1}{N}\sum_{i=1}^{N}\left|\frac{y_i - \hat{y}_i}{y_i}\right|,$$

где N – количество предсказанных данных, y_i – реальные данные (фактические значения), $\hat{y}_i$ – предсказанные данные (оценочные значения).

Результаты работы моделей по метрикам *MSE*, *MAE*, *MAPE* и R^2 представлены в таблице 1.

ТАБЛИЦА 1. Результаты работы моделей

Без преобразований			
	LinearRegression	**RandomForestRegressor**	**CatBoostRegressor**
MSE	2,44E–07	1,14E–05	2,16E–06
MAE	0,000341439	0,003032631	0,001116104
MAPE	0,00561768	0,047441466	0,018375411
R^2	0,886587309	–2,045632	–2,119898
Дифференцирование			
MSE	2,46E–07	2,49E–07	2,60E–07
MAE	0,00034473	0,000347381	0,000354213
MAPE	0,00567991	0,005728233	0,005831853
R^2	0,89239508	0,889871705	0,877883247
Дифференцирование + BTC			
MSE	7,39E–07	9,07E–08	8,04E–08
MAE	0,000689551	0,000201506	0,000206301
MAPE	0,01155619	0,003332528	0,003406357
R^2	0,78427254	0,961175389	0,965539517
Дифференцирование + Бокс–Кокс + BTC			
MSE	5,36E–07	9,36E–08	9,34E–08
MAE	0,000632356	0,000207116	0,000218858
MAPE	0,010467014	0,003418947	0,003610056
R^2	0,803756025	0,958533815	0,959471415

За исходные данные были взяты данные открытия, закрытия, максимальная и минимальная цены криптовалюты VeChain к доллару США или «VET-USD» в период с 1 мая 2021 года по 1 мая 2022 года с разницей во времени в 1 час.

Как видно из таблицы 1, на данных без преобразований лучше всего себя показывает линейная регрессия, так как для ее работы достаточно небольшого количества непреобразованных данных. В свою очередь из-за этого случайный лес и градиентный бустинг показывают плохой результат. Благодаря дифференцированию случайный лес и градиентный бустинг приближаются к значениям линейной регрессии. При увеличении количества данных линейная регрессия уже не справляется с предсказанием так же хорошо, как нелинейные модели. Дополнительно добавив преобразование Бокса-Кокса, данные только стали хуже, так как из-за большого количества преобразований, моделям стало сложнее предсказывать временной ряд.

На основе полученных результатов был сделан вывод о том, что CatBoost работает лучше остальных моделей на большом объеме стационарны данных. Поэтому было решено использовать данную модель для прогнозирования временного ряда на несколько значений вперёд.

На рис. 3 представлены предсказанные значения наивысшей и наинизшей цен криптовалюты VeChain на 24 вперёд, которые показывают примерное движение цены в будущем и позволяет сделать выводы о дальнейшей торговле.

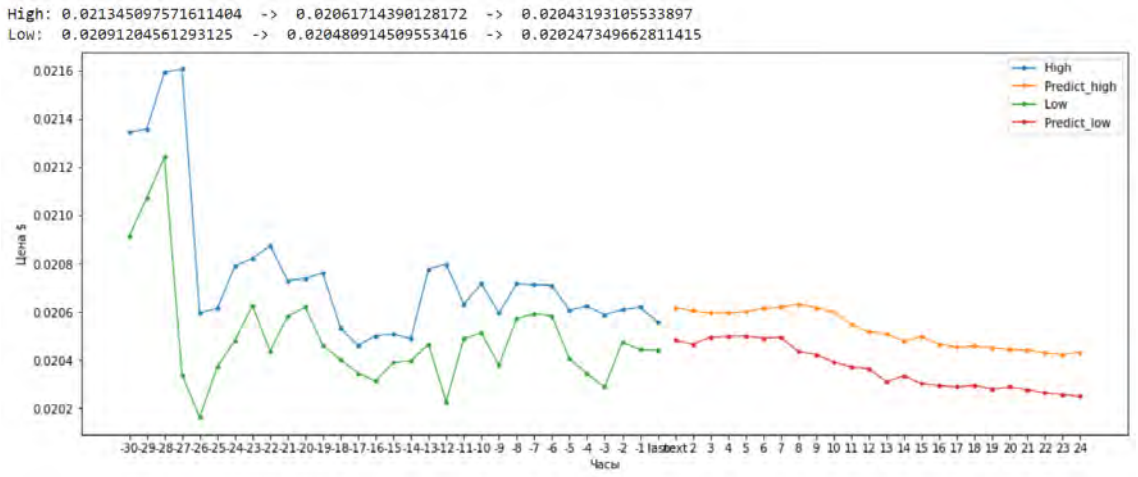


Рис. 3. График зависимости цены криптовалюты от времени (часы).
Предсказание на 24 часа вперед

Список используемых источников

1. Sklearn Ensemble Documentation. URL: https://scikit–learn.org/stable/modules/classes.html#module–sklearn.ensemble (дата обращения 10.01.2023).

2. CatBoost Documentation. URL: https://catboost.ai/docs/ (дата обращения 9.01.2023).

3. Sklearn Preprocessing Documentation. URL: https://scikit–learn.org/stable/modules/classes.html#module–sklearn.preprocessing (дата обращения 9.01.2023).

4. Sklearn Metrics Documentation. URL: https://scikit–learn.org/stable/modules/classes.html#module–sklearn.metrics (дата обращения 11.01.2023).

Статья представлена доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004
ГРНТИ 28.23.37, 28.23.29

СЕРВИС ИДЕНТИФИКАЦИИ, ОПРЕДЕЛЕНИЯ АКТИВНОСТИ И ВОВЛЕЧЕННОСТИ ПОЛЬЗОВАТЕЛЯ В ПРОЦЕССЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

К. Э. Есалов, М. С. Кузнецов, К. А. Романенко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье рассматривается проблема оценки участия в видеоконференции, которая становится все более актуальной в связи с современными дистанционными и смешанными формами образования, а также распространением технологий видеоконференций. Чтобы решить данную проблему, был разработан программный продукт, созданный на языке программирования Python. В основе разработки лежит технология компьютерного зрения для анализа видео и определения времени присутствия участников на видеоконференции. При решении задачи компьютерного зрения были использованы две нейросети, а именно MTCNN – для детектирования лиц и InceptionResnetV1 – для распознавания лиц. Результаты исследования показывают высокую точность работы программы и её применимость для автоматизации процесса подсчёта времени присутствия людей на видеоконференциях.

нейронные сети, распознавание лиц, детектирование лиц, видеоконференция.

Отслеживание присутствия пользователей на видеоконференции задача актуальная, сложная и ресурсозатратная. Для решения этой задачи необходимо использование нескольких нейронных сетей, одну для детектирования лиц и другую для их распознавания.

В качестве нейронной сети для детектирования лиц на кадре видеоконференции была выбрана MTCNN [1]. Модель представляет собой каскад нескольких последовательно работающих нейросетей, благодаря чему достигает средней точности в 97 % [2]. Модель анализирует изображение, находит на нем все присутствующие лица, после чего возвращает либо координаты самого лица, а также координаты носа, глаз и левого и правого уголков рта, либо вырезанное изображение лица в виде массива.

В качестве нейронной сети для распознавания лиц была выбрана InceptionResnetV1 [3]. Это одна из наиболее эффективных архитектур свёрточной нейронной сети, разработанных для классификации изображений. После анализа изображения вырезанного лица формируется вектор, содержащий его отличительные черты. Таким образом, после работы InceptionResnetV1, каждое лицо будет иметь свои собственные векторные признаки, благодаря чему их можно сравнивать друг с другом.

Считается, что человек присутствует на видеоконференции, если у него включена камера, на изображении с камеры хорошо видно его лицо, а также это изображение не статично в течение некоторого периода времени. Программа считает, что неподвижное изображение участника видеоконференции свидетельствует о плохом интернет соединении у этого человека, попытке подмены изображения или других факторах, являющихся основой для исключения времени присутствия статичного лица в финальном отчете.

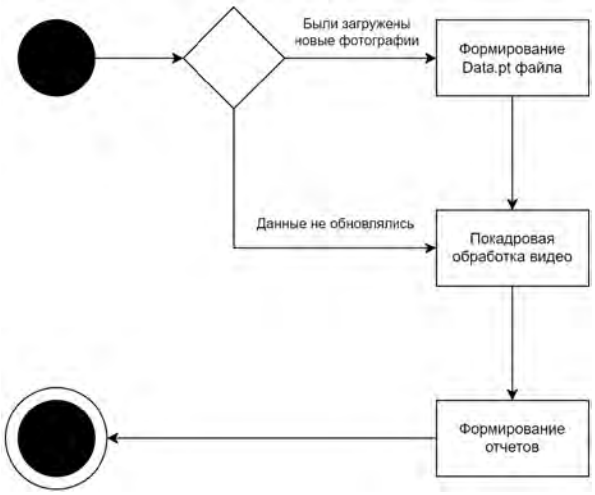


Рис. 1. Диаграмма работы программы

Из рис. 1 видно, что первым шагом для работы программы является формирование Data.pt файла, содержащего признаки лиц каждого из присутствовавших на видеоконференции. Data.pt файл необходим для того, чтобы программа могла распознавать нужных нам людей на видеоконференции и отличать их друг от друга. Схема формирования Data.pt файла подробно описана на рис. 2. Сначала вручную сортируются изображения сотрудников по их собственным папкам внутри директории photos. Затем, после вызова программы, MTCNN ищет и вырезает все лица с изображений, а InceptionResnetV1 анализирует их и формирует вектора признаков, которые в последствие запишет в Data.pt файл.

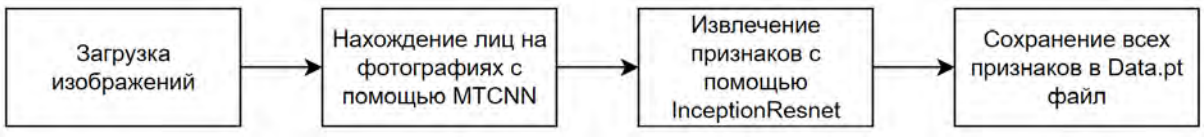


Рис. 2. Диаграмма формирования Data.pt файла

После того как файл Data.pt был сформирован, запускается цикл, в котором извлекается первый кадр от каждой секунды записи видеоконференции. Такой подход помогает снизить нагрузку на систему и обеспечить более эффективную обработку видео, поскольку извлечение кадров слишком

часто может привести к избыточной обработке и потере производительности и усложняет процесс определения статичных лиц. Полученный кадр передается в функцию для распознавания лиц, диаграмма которой представлена на рис. 3.

Рис. 3. Диаграмма функции распознавания лиц

Внутри данной функции MTCNN ищет все лица на переданном кадре. Затем для каждого найденного лица InceptionResnetV1 извлекает вектор признаков. Далее измеряются расстояния между векторами признаков найденных лиц и лиц, находящихся в файле Data.pt. Если расстояние между двумя векторами признаков меньше заданного порога, то это значит, что лица принадлежат одному и тому же человеку [4]. В этом случае имя человека и его координаты на изображении сохраняются в словарь. Если расстояние между всеми векторами оказалось больше заданного порога, то найденное лицо вместе сохраняется как неизвестное. В конце функция возвращает словарь, где ключами являются имена распознанных лиц, а значениями – кортежи с минимальным расстоянием между векторами признаков найденного лица и лиц из файла Data.pt и координатами распознанного лица на изображении. Если на изображении не было найдено ни одного лица, то возвращается словарь с ключом 'no face' и значением None.

После выполнения описанной функции, программа проходится по всем именам из полученного словаря, проверяя, присутствовал ли человек с таким именем на предыдущей секунде записи видеоконференции. Если такой человек присутствовал и его лицо не было статично, то человеку прибавляется 1 секунда к его времени присутствия. В противном случае, время присутствия не изменяется.

При завершении анализа видеоконференции строится отчет. Основную часть отчёта составляет CSV-файл [5]. В первой колонке данного файла записываются имена всех людей, которые находились на видеоконференции. Во второй – подсчитанное время присутствия в формате часы:минуты:секуды. В третьей – время присутствия в процентах. В дополнение к CSV-файлу, для большей наглядности, строятся две диаграммы: столбчатая и круговая. На рис. 4 показан пример отчёта в виде CSV-файла и круговой диаграммы.

Также, если при запуске программы значение параметра --do_video было выбрано как True, то в конце работы программы мы получим видео, где на каждое найденное лицо наложится прямоугольник, подписанный

именем человека. Если человек достаточно долго находится неподвижно, к его имени припишется «Sleeping». Благодаря этому можно будет наглядно понять какие именно моменты видеоконференции люди упустили.

Names	Time	Time %
Gigachad	0:01:32	97
ruslan	0:00:16	17
evgeniy	0:00:12	12
bradley_cooper	0:00:12	12
paul_rudd	0:00:11	11
shea_whigham	0:00:11	11
dvorec	0:00:11	11
kate_siegel	0:00:11	11
roman	0:00:03	3
unknown	0:00:01	1

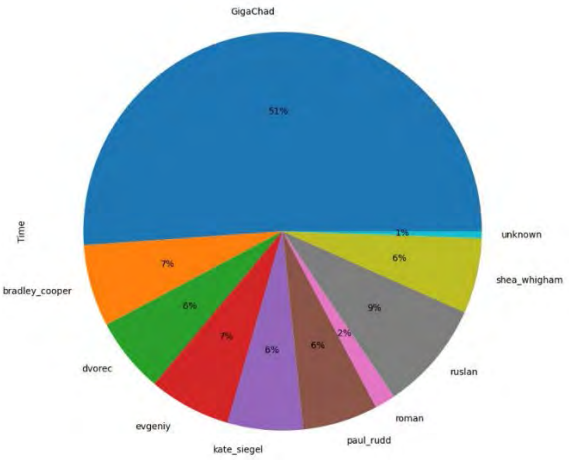


Рис. 4. Пример отчета

В бизнесе, такая программа поможет руководству и менеджерам понять, насколько эффективно проводятся видеовстречи в компании, и как распределены временные ресурсы сотрудников, что может помочь улучшить продуктивность и оптимизировать рабочие процессы.

В образовании программа поможет в анализе эффективности онлайн-уроков и семинаров, позволяя учителям и преподавателям понять, какие материалы вызывают наибольший интерес учеников, а какие наоборот, вводят их в скуку.

Список используемых источников

1. MTCNN documentation. URL: https://github.com/ipazc/mtcnn (дата обращения 01.01.2023)

2. Каляшов Е. В. Сравнительный анализ систем распознавания лиц, построенных с использованием блоков стандартных архитектур // Информационные технологии и телекоммуникации. 2020. Том 8. № 3. С. 94–101. DOI 10.31854/2307-1303-2020-8-3-94-101. URL: https://www.sut.ru/doci/nauka/1aea/itt/2020_3/94-101.pdf (дата обращения 03.01.2023)

3. InceptionResnetV1 documentation. URL: https://iq.opengenus.org/inception-resnet-v1/Sdfs (дата обращения 04.01.2023)

4. TORCH.DIST documentation. URL: https://pytorch.org/docs/stable/generated/torch.dist.html (дата обращения: 05.01.2023)

5. Read a comma-separated values (csv) file documentation. URL: https://pandas.pydata.org/docs/reference/api/pandas.read_csv.html (дата обращения 02.01.2023)

Статья представлена доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 004.75
ГРНТИ 20.53.23

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ КРОССЧЕЙН НА ПРИМЕРЕ ЭКОСИСТЕМЫ POLKADOT

В. В. Жаворонкова, И. Ф. Тарабанов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире все большую популярность приобретают блокчейн-сети в различных сферах инфокоммуникационных технологий. В данной статье обзорно рассмотрена экосистема Polkadot с применением кроссчейн-мостов, что позволяет решить проблему масштабируемости, взаимодействия и передачи информации между различными блокчейн сетями. Сделан анализ, в котором выявлены сетевые критерии оценки кроссчейн технологий, меняющиеся в зависимости от их функций, уровня доверия, направления передачи активов, механизмов и уровней централизации.

блокчейн, кроссчейн, Polkadot, смарт-контракт, токен.

Кроссчейн

Индустрия блокчейн-технологий остается фрагментированной, где каждый проект – это самостоятельная и независимая экосистема, практически не взаимодействующая с другими подобными сетями. Данный подход ставит перед разработчиками серьезную проблему: на этапах планирования проекта команда вынуждена выбрать лишь одну блокчейн-платформу, оставляя неизменными такие серьезные показатели, как масштабируемость, скорость и производительность. Малое и среднее предпринимательство сильно рискует, так как из-за отсутствия практического опыта они не имеют представления, какой именно блокчейн в их нише будет самым удачным [1].

Каждая цепочка блоков разных блокчейнов соответствуют разным независимым реестрам, и между ними нет связи. Решить данную проблему невозможно без сторонних методов, так как параметры задаются при создании платформы и в дальнейшем не подлежат изменениям [2]. Такой технологией стал кроссчейн (*Cross Chain*) – приложения, позволяющие передавать не только токены разных стандартов между блокчейнами-сетями, но и в целом любой тип данных [3]. Благодаря его использованию, разработчики в своих проектах смогут объединять несколько блокчейн-платформ, применяя каждую в соответствии с ее преимуществами в сравнении с другими.

Для того чтобы полноценно сравнить Кроссчейн-решения в отношении конкретных требований к использованию, а также для того, чтобы обеспе-

чить понимание самой технологии, необходим анализ их типов. Проведя тщательный обзор, были выявлены критерии оценки Кроссчейн-технологий в таблице 1 [4].

ТАБЛИЦА 1. Свойства Кроссчейн-технологий

Свойства Кроссчейн-технологий	Описание
Администрирование	Управлением и распределением обязанностей по эксплуатации и обслуживанию
Гибкость	Возможности разработчиков в настройке технологии, подключенных к распределенным реестрам
Производительность	Эффективность обмена данными – их точность, полнота, стоимость и скорость
Сетевые параметры/ работа в сети	Структура и процессы, обеспечивающие обмен данными между распределенными реестрами

Экосистема Polkadot

Структура *Polkadot* изображена на рис. 1. Она включает следующие компоненты:

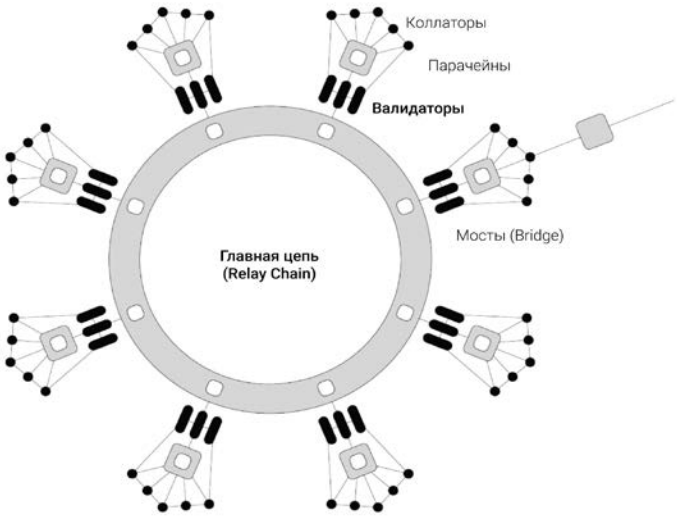


Рис. 1. Структура экосистемы Polkadot

– *Relay Chain* (главная цепь или связующая цепь). Это основная сеть, к которой подключаются все блокчейны, способные поддерживать протоколы Polkadot, соединяющая все блокчейны в сети;

– *Parachain* (парачейн, параллельная цепь) – любая блокчейн-сеть, подключенная к Polkadot . Парачейны содержат в себе коллаторов и валидаторов – участников сети, которые отвечают за обслуживание, проверку и объединение транзакций в блоки парачейна;

– *Bridge* (мост). Мосты предназначены для соединения блокчейнов, не использующих протоколы управления Polkadot.

Для того чтобы совершить транзакцию, узлы валидаторов делятся закрытым ключом, либо используют кошелек с мультиподписями [5]. Событие (например, разблокировка активов в блокчейне Б) выполняется только в том

случае, если определенное количество валидаторов подтверждает событие (например, блокировка активов в блокчейне А). На рис. 2 показан поток данных между двумя блокчейн-системами через Сеть Валидаторов. То есть, группа узлов участвует в качестве доверенной независимой роли, которая проверяет транзакции обеих сторон. Только транзакции, проверенные узлами валидаторов, будут переданы в блокчейн назначения через шлюз [6].

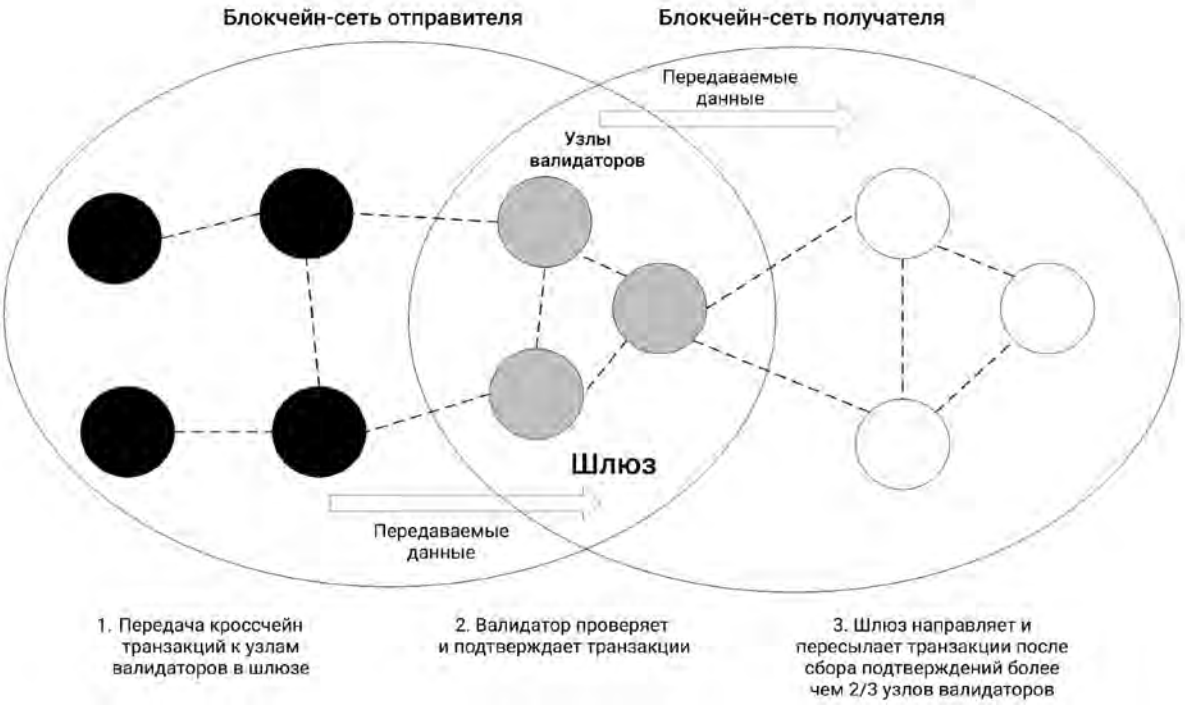


Рис. 2. Путь транзакции в экосистеме *Polkadot*

Рассмотрим свойства кроссчейн-технологии, применяемые к Polkadot:

– *Администрирование* – благодаря тому, что доверительное управление распределено между несколькими валидаторами, соответствующими транзакциями легче управлять, чем в других платформах.

– *Гибкость* – Платформу легче расширять за счет новых распределенных реестров. В сеть можно легко добавлять или исключать из нее распределенные реестры, устанавливая соответствующие узлы-коннекторы [2, 7].

– *Производительность* – Сети валидаторов ускоряют транзакции между разными блокчейнами благодаря привлечению доверенной третьей стороны, которая управляет согласованием и проверкой транзакций. Таким образом, валидаторы часто несут ответственность за потенциальные ошибки в обмене [4].

– *Сетевые параметры/работа в сети* – рассмотрены в таблице 2.

ТАБЛИЦА 2. Раскрытие сетевых параметров

Сетевые параметры	Принцип работы в Polkadot
Процедура	Консорциум валидаторов подтверждает события
Связь	Косвенная Двунаправленная В цепи или вне цепи
Соединительный Механизм (выдержка)	Распределенный закрытый ключ с мультиподписью кошелька
Маршрутизация	Коннектор Узел(ы) Консорциум валидаторов
Топология^{A}	N ←→C←→N
Механизм Верификации (подтверждения)	Верификация группой валидаторов (например, ППП^{B})

A: Топология использует следующую нотацию:
C – коннектор (например, валидатор или шлюз),
N – произвольное количество распределенных реестров,
B: простая проверка платежей.

Заключение

Широкое разнообразие кроссчейн решений делает необходимым дальнейшие исследования в области классификации и их применения. В данной статье был произведен анализ технологии на примере экосистемы *Polkadot*. Были выявлены сетевые критерии оценки кроссчейн технологий, а именно – принципы работы, связь, тип маршрутизации, топология сети, механизмы соединения и верификации (подтверждения).

Использование кроссчейн-платформ в разработке новых проектов является одним из немногих решений проблем масштабируемости, взаимодействия и передачи информации между различными блокчейн сетями. Главная мотивация использования Polkadot содержится в лояльности для многих существующих блокчейн-сетей, вне зависимости от поддержки протоколов платформы. Данное решение является прорывом в сфере блокчейна, что позволило взглянуть по-новому на саму технологию и расширить потенциал реализуемых проектов.

Список используемых источников

1. Кожина В. О., Григорьева М. В. Технология блокчейн как инструмент формирования экосистемы бизнеса // Журнал «Инновационная экономика: Информация, аналитика, прогнозы». 2022. N 2. С. 12–19.

2. Niclas Kannengießer, Sebastian Lins, Tobias Dehling, Ali Sunyaev. Trade-offs between Distributed Ledger Technology Characteristics // ACM Computing Surveys. 2020. Vol. 53. PP. 1–37.

3. Liping Deng, Huan Chen, Jing Zeng & Liang-Jie Zhang .Research on Cross-Chain Technology Based on Sidechain and Hash-Locking // EDGE 2018: Edge Computing – EDGE. 2018. PP. 144–151. URL: https://link.springer.com/book/10.1007/978-3-319-94340-4

4. Niclas Kannengießer, Michelle Pfister, Malte Greulich, Sebastian Lins , Ali Sunyaev. Bridges Between Islands: Cross-Chain Technology for Distributed Ledger Technology // Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020. PP. 5298–5307. URI: https://hdl.handle.net/10125/64394

5. Loïc Lesavre, Priam Varin, Dylan Yaga. Blockchain Networks: Token Design and Management Overview // National Institute of Standards and Technology. 8301. 2021. URL: https://doi.org/10.6028/NIST.IR.8301

6. Yiming Jiang,Chenxu Wang ,Yawei Wang and Lang Gao. A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management // Sensors Journal. May 2019. N 19 (9). P. 2042. URL: https://doi.org/10.3390/s19092042

7. Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, Miguel Correia. A Survey on Blockchain Interoperability: Past, Present, and Future Trends // 2021 Association for Computing Machinery. URL: https://arxiv.org/pdf/2005.14282.pdf

Статья предоставлена заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.51
ГРНТИ 81.93.29

ПРОЕКТИРОВАНИЕ ГЛОБАЛЬНО-ОПТИМАЛЬНОГО ЧЕЛОВЕКО-КОМПЬЮТЕРНОГО ИНТЕРФЕЙСА

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук»

Существуют различные методы оценивания человеко-компьютерных интерфейсов, которые могут применяться для оценки интерфейса после принятия мер по защите данных во время взаимодействия оператора с интерфейсом. Чаще всего эффективность человеко-компьютерного интерфейса измеряется с помощью формальных показателей, таких как скорость и точность, которые сравниваются с показателями других интерфейсов. Также можно оценивать удобство использования интерфейса с помощью опросов пользователей, анализа видеозаписей испытаний интерфейса и т. д. Третьим возможным способом оценить человеко-компьютерный интерфейс является измерение расстояния показателей эффективности и удобства использования интерфейса до показателей некоторого глобально-оптимального интерфейса, то есть, та-

кого интерфейса, который был бы полностью защищён и при этом достаточно эффективен. В докладе рассматривается возможность проектирования такого глобально-оптимального интерфейса.

человеко-компьютерное взаимодействие, информационная безопасность, пользовательские интерфейсы, оценка защищённости.

Введение

Существуют различные способы оценки человеко-компьютерных интерфейсов. Чаще всего оценивают эффективность и удобство использования. Можно также оценивать защищённость интерфейса [1]. Способы оценки делятся на сильные (объективные), слабые (субъективные) и относительно сильные (включающие в себя черты объективных и субъективных способов) [2]. Сильные способы представляют собой количественную оценку формальных показателей качества, слабые способы включают в себя субъективную оценку пользователями эффективности и удобства использования интерфейсов, относительно сильные комбинируют черты сильных и слабых способов [3]. Однако для выполнения данных оценок требуется сравнивать один интерфейс с другим существующим или с некоторыми допустимыми пороговыми значениями интересующих показателей.

В целях повышения качества оценки интерфейса и во избежание необходимости сравнения разрабатываемого интерфейса с каким-либо существующим интерфейсом, предполагается разработать модель глобально-оптимального интерфейса, который позволит измерять расстояние от оцениваемого интерфейса до глобально-оптимального.

Модель глобально-оптимального интерфейса

Глобально-оптимальный интерфейс – это такой человеко-компьютерный интерфейс, который является одновременно защищённым, и в то же время эффективным. Однако построение такого интерфейса сопряжено с рядом трудностей, поскольку интерфейсы постоянно развиваются и появляются новые, то есть, человеко-компьютерные интерфейсы не являются статической системой. Тогда модель глобально-оптимального интерфейса должна быть достаточно общей, чтобы учитывать динамичность развития интерфейсов, и при этом задавать ряд необходимых требований и ограничений. Приближенная модель глобально-оптимального интерфейса приведена на рис. 1.

На рис. 1 представлена концептуальная модель глобально-оптимального человеко-компьютерного интерфейса, суть которой состоит в следующем. Глобально-оптимальный интерфейс не содержит в себе никаких рисков для конфиденциальности, целостности или доступности, а также отвечает требованиям к эффективности, выраженным в виде формальных показателей точности принятия решений оператором интерфейса, а также

скорости принимаемых им решений. Таким образом, для того, чтобы интерфейс соответствовал глобально-оптимальному интерфейсу, к нему предъявляются требования по части защищённости и эффективности.

Рис. 1. Концептуальная модель глобально-оптимального интерфейса

(1) Требования к защищённости состоят в том, что в архитектуре интерфейса не должно быть рисков для конфиденциальности, доступности и целостности. Таким образом, риски принимают следующие значения:

– риск конфиденциальности – 0;

– риск целостности – 0;

– риск доступности – 0.

(2) Требования к эффективности представлены ниже:

– скорость принятия решений оператором должна составлять 1–3 минуты, поскольку взаимодействие с интерфейсами систем информационной безопасности должно быть приближено к реальному времени;

– точность принятия решений оператором в различных работах обычно задаётся не менее 95 %.

Для оценки рисков нарушения конфиденциальности, целостности и доступности предполагается использовать методы наподобие общей системы оценки уязвимостей (CVSS) [4].

Скорость и точность принятия решений оператором предполагается измерять экспериментально. При этом за скорость принимается среднее время, которое оператор затрачивает на выполнение задания. Точность измеряется как средняя доля ошибок при выполнении заданий оператором.

Выводы

В данной работе рассмотрена приближенная концептуальная модель глобально-оптимального интерфейса. Данная модель разработана в целях повышения качества оценки защищённости человеко-компьютерных интерфейсов. Предложенная модель в будущем может позволить избавиться от необходимости сравнения разрабатываемого интерфейса с уже существующими для его оценки. В дальнейших исследованиях планируется расширить и усовершенствовать предложенную модель, а также разработать алгоритмы расчёта расстояния от оцениваемого интерфейса до глобально-оптимального интерфейса.

Работа выполнена при финансовой поддержке РФФИ (проект 20-37-90130 Аспиранты).

Список используемых источников

1. Жернова К. Н., Чечулин А. А. Алгоритмы оценивания защищённости человеко-компьютерного интерфейса // Информатизация и связь. 2022. N 4. С. 56–66. DOI: 10.34219/2078-8320-2022-13-4-56-66. EDN UCYMNF.

2. Travis D., Hodgson P. Think Like a UX Researcher: How to Observe Users, Influence Design, and Shape Business Strategy. CRC Press, 2019.

3. Котенко И. В. и др. Визуальная аналитика для информационной безопасности: оценка эффективности и анализ методов визуализации // Вопросы кибербезопасности. 2021. N 6 (46). С. 36–46.

4. First.org [Электронный ресурс] // Common Vulnerability Scoring System: [сайт]. [2023]. URL: http://www.first.org/cvss (дата обращения 14.03.2023).

УДК 004.51
ГРНТИ 81.93.29

МЕТОДЫ ПОИСКА УЯЗВИМОСТЕЙ БЕСПИЛОТНОЙ ТРАНСПОРТНОЙ СРЕДЫ «УМНОГО ГОРОДА»

К. Н. Жернова, А. А. Чечулин

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Важную часть «умного города» составляет беспилотная транспортная среда. Защита обмена данных между беспилотными транспортными средствами и инфраструктурой «умного города» представляется значимой задачей. Беспилотная транспортная среда может обладать уязвимостями, которые позволяют злоумышленнику атаковать беспилотные транспортные средства и пассажиров, что может наносить

физический ущерб участникам дорожного движения, а также повлечь за собой финансовые потери. По этой причине актуальна проблема поиска и устранения уязвимостей беспилотной транспортной среды «умного города». В данном докладе рассматриваются различные классы методов поиска уязвимостей беспилотной транспортной среды «умного города».

человеко-компьютерное взаимодействие, беспилотная транспортная среда, «умный город», информационная безопасность, пользовательские интерфейсы.

Введение

Между устройствами инфраструктуры беспилотной транспортной среды передаются большие объёмы данных, которые могут быть уязвимы к действиям злоумышленников. Результатом атак могут быть не только финансовые потери, но и физический ущерб участникам дорожного движения. По этой причине следует искать и устранять возможные уязвимости беспилотной транспортной среды. Существуют различные методы поиска данной категории уязвимостей. В научных работах предлагаются разные подходы к классификации поиска и оценки уязвимостей, присущих киберфизическим системам [1]. В данной работе предлагается классификация на основе парных признаков, которая позволит выделить наиболее релевантный подход при разработке системы поиска уязвимостей в беспилотной транспортной среде «умного города».

Классификация подходов к поиску уязвимостей в беспилотной транспортной среде

Предлагается следующая классификация методов поиска уязвимостей, основанная на парах признаков, приведённых ниже:

– *участие человека:* поиск проводится без участия человека или с участием человека;

– *интеллектуальность метода:* при поиске используется искусственный интеллект или набор правил.

На основе данных пар можно выделить следующие типы методов:

1) без участия человека, с использованием искусственного интеллекта – интеллектуальные методы;

2) без участия человека, с использованием правил – методы, основанные на правилах;

3) с участием человека – экспертные методы. При этом следует учитывать, что экспертные методы предполагают оценку защищённости на основании правил и эвристик, однако не предполагают использование искусственного интеллекта. По этой причине для признака «с участием человека» в этой группе возможен только один тип методов.

ТАБЛИЦА 1. Классификация методов поиска уязвимостей беспилотной транспортной среды

Тип подхода	Участие человека	Интеллектуальность
Основанные на правилах	–	–
Интеллектуальные	–	+
Экспертные	+	–
–	+	+

Таким образом, в данном докладе рассматриваются три основных типа подходов к поиску уязвимостей беспилотной транспортной среды: (1) основанные на правилах, (2) интеллектуальные подходы и (3) экспертные подходы к поиску. Краткое описание данных подходов представлено ниже.

Подходы, основанные на правилах

В системах обнаружения вторжений и поиска аномалий часто применяются подходы, основанные на правилах. Примерами таких подходов могут служить сигнатурный и статистический анализ. Суть сигнатурного анализа состоит в сравнении поступающих данных с сохранёнными образцами данных, свидетельствующих об атаке [2]. Например, сигнатурный анализ может проводиться с помощью набора правил, выраженных формулировкой «если А, то В». Статистический анализ позволяет выявлять аномалии в трафике беспилотной транспортной среды на основе его поведения [3]. Также часто производится на основе определённых правил обработки поведения сетевого трафика. Достоинства таких подходов состоят в том, что они достаточно простые в реализации и позволяют обработать большое количество данных, однако недостатком могут быть ошибки при анализе трафика.

Интеллектуальные подходы

Часто основываются на методах машинного обучения и методах вычислительного интеллекта, например, на технологиях нейронных сетей [3].

И основанные на правилах, и интеллектуальные подходы также могут быть адаптивными [3, 4]. Адаптивные методы и подходы предполагают, что алгоритмы поиска уязвимостей будут постоянно отслеживать и подстраиваться под изменения в поведении трафика инфраструктуры умного города и беспилотной транспортной среды [5]. С помощью методов, обладающих свойством адаптивности, можно вести проактивный поиск уязвимостей, то есть, обнаруживать уязвимости до момента их эксплуатации и возникновения критической ситуации [6].

Достоинство интеллектуальных подходов заключается в возможности обработать большое количество трафика, а также в возможности по поведению трафика предсказывать появление уязвимостей. Однако, в таких системах всё ещё возможны ложные срабатывания.

Экспертные подходы

Последним из рассматриваемых типов поиска уязвимостей являются экспертные подходы. Данный тип может быть реализован в виде вопросно-ответной формы, при которой оператор взаимодействует с системой, отвечая на заранее заготовленные вопросы о признаках атак.

На основе модели, представленной в работе [7], был создан прототип подобной системы, требующий участия эксперта. В качестве входных данных выступают интерфейсы, присущие интерфейсам признаки, характерные для них уязвимости, а также связанные с интерфейсами и их уязвимостями вопросы и варианты ответов. В процессе взаимодействия с экспертом, на основе алгоритма, предложенного в работе [7], система вычисляет, какие уязвимости имеются на данный момент. Достоинством подобных систем является простота реализации, а также лёгкость использования при небольшом количестве оцениваемых признаков, однако с возрастанием их количества сложность будет повышаться.

Выводы

В данной работе представлена классификация подходов к поиску уязвимостей в беспилотной транспортной среде, основанная на двух парах признаков: участие человека и интеллектуальность метода. Такая классификация является достаточно простой, однако позволит выделить наиболее релевантные подходы в зависимости от сложности реализации, точности, объёма обрабатываемых данных и некоторых других условий, что может быть важно при проектировании системы поиска уязвимостей беспилотной транспортной среды.

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Левшун Д. С., Гайфулина Д.А., Чечулин А. А., Котенко И. В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. 2020. Т. 19. N 5. С. 1050–1088.

2. Скатков А. В., Брюховецкий А. А., Моисеев Д. В., Воронин Д. Ю. Обеспечение безопасности интеллектуальных транспортных средств в инфраструктуре умного города // International Journal of Open Information Technologies. 2020. Т. 8. N 11. С. 122–127.

3. Гайфулина Д. А. Аналитический обзор методов обнаружения аномалий сетевого уровня киберфизических систем // Альманах научных работ молодых ученых Университета ИТМО. 2018. Т. 1. С. 4–5.

4. Моисеев Д. В., Брюховецкий А. А., Скатков А. В. Адаптивное обнаружение уязвимостей интерфейсов БТС // Modern Science. 2020. N 8-1. С. 375–378.

5. Скатков А. В., Брюховецкий А. А., Моисеев Д. В. Обнаружения уязвимостей интерфейсов БТС на основе адаптивной нечеткой модели оценки информационных состояний ресурсов //Экологическая, промышленная и энергетическая безопасность-2020. 2020. С. 521–526.

6. Паращук И. Б., Чечулин А. А. Обеспечение безопасности беспилотных транспортных средств «умного города» с использованием проактивного поиска уязвимостей в человеко-машинных интерфейсах взаимодействия на основе методов теории катастроф // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская. 2022. С. 116.

7. Израилов К. Е., Левшун Д. С., Чечулин А. А. Модель классификации уязвимостей интерфейсов транспортной инфраструктуры «умного города» // Системы управления, связи и безопасности. 2021. N 5. С. 199–223.

УДК 621.396.4
ГРНТИ 50.37.03

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ МЕТОДОВ И СРЕДСТВ ОБРАБОТКИ РАЗНОРОДНЫХ ДАННЫХ О ПАРАМЕТРАХ СТРУКТУРНОЙ НАДЕЖНОСТИ МОДУЛЬНЫХ И ПЕРЕДВИЖНЫХ ДАТА-ЦЕНТРОВ

С. А. Шинкарев[1], М. И. Носов[2], В. Э. Жигадло[3]

[1]Военная орденов Жукова и Ленина Краснознамённая академия связи им. Маршала Советского Союза С. М. Буденного
[2]Михайловская военная артиллерийская академия
[3]ЗАО «Институт телекоммуникаций»

Исследована современная проблематика и предложен новый подход к развитию методов и средств обработки больших объемов разнородных – гетерогенных – данных о значениях параметров структурной надежности модульных и передвижных дата-центров. Этот подход включает шесть этапов создания соответствующих методов, обеспечивающих ключевые целевые функции: сбор и предварительную обработку данных, оперативное обнаружение аварий и отказов, оценку уровня структурной надежности, а также анализ и управление рисками нарушения структурной надежности объектов такого класса. Предложены современные, включая интеллектуальные, аналитические методы и механизмы, с помощью которых эти целевые функции могут быть практически реализованы.

обработка разнородных данных, структурная надежность, модульный дата-центр, передвижной дата-центр, методы, средства, большие объемы данных.

Стремительное внедрение современных автоматизированных информационно-поисковых и вычислительных систем в государственную, социально-культурную, промышленно-экономическую и военную сферы жизнедеятельности страны является важным стимулом их дальнейшего развития и предопределяет максимальное приближение оказываемых этими системами услуг, к местам обитания пользователей. Это тем более справедливо для модульных и передвижных (подвижных, мобильных, транспортируемых) дата-центров, предназначенных для предоставления услуг по хранению и обработке данных в удаленных, труднодоступных районах, где строительство стационарных дата-центров для создания информационной инфраструктуры нерентабельно или существенно затруднено [1, 2, 3].

Вместе с тем, с учетом того факта, что модульные и передвижные дата-центры (МПДЦ) предназначены для работы в сложных климатических условиях, при разработке, построении и проведении проверочных (контрольных) испытаний систем такого класса, наряду с решением задач по повышению эффективности функционирования МПДЦ, безусловно может и должна решаться задача по текущему и прогностическому контролю их структурной надежности [4, 5].

При этом под структурной надежностью МПДЦ будем понимать их суммарную, итоговую надежность при установленной структуре и определенных значениях частных параметров надежности всех входящих в них компонентов. Для получения результирующих оценок структурной надежности исследуют процесс функционирования модульных и передвижных дата-центров, анализируют функциональные связи между их компонентами, изучают типы аварий, отказов и причины их появления. При получении результирующих оценок структурной надежности МПДЦ количественно оценивают влияние степени работоспособности каждого компонента дата-центра на его работоспособность в целом [5].

Ключевая проблема состоит в том, что для того, чтобы получать суммарную, итоговую оценку структурной надежности МПДЦ необходимо собирать и оперативно аналитически обрабатывать большие объемы разнородных (гетерогенных) данных о значениях частных параметров безотказности, ремонтопригодности и восстанавливаемости всех отдельных компонентов модульных и передвижных дата-центров.

Иными словами, многообразие, разнородность и большие объемы собираемых (наблюдаемых, измеряемых) статистических данных о значениях частных параметров, характеризующих различные аспекты надежности для множества компонентов дата-центров, влияющих на итоговую структурную надежность МПДЦ в целом, остро ставят проблему разработки методов и построения на их основе современных систем аналитической обработки

больших объемов разнородных данных о параметрах структурной надежности модульных и передвижных дата-центров в интересах оценки их технического состояния и поддержки принятия решений по поддержанию требуемого уровня надежности объектов такого класса.

Эти методы и построенные на их основе системы призваны обеспечить оперативную обработку больших объемов разнородных данных о параметрах структурной надежности модульных и передвижных дата-центров, их точный анализ для оптимального управления поддержанием требуемого уровня надежности, а также высокую полноту и достоверность оценки технического состояния МПДЦ, используя при этом современные методы искусственного интеллекта, методы и средства обработки больших данных, платформы параллельных вычислений и методы онтологического представления данных, а также, в случае необходимости, методы и средства оперативной визуализации отказов и сбоев в работе компонентов МПДЦ.

Исходя из целей создания методов и средств обработки больших объемов разнородных данных о параметрах структурной надежности МПДЦ, перспективным подходом, на наш взгляд, является декомпозиция общей задачи на ряд подзадач, ориентированных на решение отдельных этапов и создание соответствующих этим этапам частных средств обработки данных, таких как, например, этап сбора, предварительной обработки и хранения больших объемов разнородных данных о параметрах структурной надежности (организация хранилища разнородных данных о параметрах структурной надежности).

К перспективам развития методов и средств обработки больших объемов разнородных данных о параметрах структурной надежности МПДЦ, следует отнести:

- создание методов оперативного, надежного и устойчивого к воздействиям внешних, зачастую, мешающих, факторов, сбора и предварительной обработки больших объемов разнородных данных о параметрах структурной надежности МПДЦ, а также построение и испытание реализующих эти методы распределенных интеллектуальных сканеров гетерогенных данных об аварийных событиях (например, каскадных аварий) и других событиях отказа работоспособности и отказа функционирования компонентов модульных и передвижных дата-центров;
- разработка методов оперативного обнаружения аварий (типовых либо каскадных) и иных событий отказа работоспособности и отказа функционирования компонентов МПДЦ, а также построение и испытание реализующих эти методы аппаратно-программных средств для выявления в реальном масштабе времени типа и места аварий и других событий «обрушения» надежности, например, с использованием приемов и алгоритмов параллельных вычислений, адаптированных к обработке больших дан-

ных, методов моделирования сложных каскадных аварий и лавинных отказов компонентов модульных и передвижных дата-центров, основанных на графах, сетях Петри и имитационных многоагентных моделях;

- формулировка методов оперативного обнаружения мест (аномальных точек) возможных (потенциальных и предаварийных) групповых, массовых отказов работоспособности и отказов функционирования компонентов МПДЦ, а также построение и испытание реализующих эти методы средств оперативного выявления типа, времени и мест возможного проявления массовых аварий и отказов, например, с использованием методов распределенного машинного обучения на больших данных, методов эволюционных вычислений, приемов и методов параллельных вычислений;
- создание методов оперативной оценки количественных либо качественных значений уровня структурной надежности МПДЦ, а также разработка и применение реализующих эти методы средств, обеспечивающих расчет метрик структурной надежности (с задаваемой пользователем точностью и полнотой), использующих многоуровневые системы метрик безотказности, ремонтопригодности и восстанавливаемости компонентов модульных и передвижных дата-центров надежности, связанные с результатами моделирования сложных лавинных аварий и массовых отказов работоспособности и отказов функционирования компонентов МПДЦ;
- разработка методов анализа и управления рисками нарушения структурной надежности МПДЦ, а также создание реализующих эти методы аппаратно-программных средств, предназначенных для оперативного расчета показателей (метрик) структурной надежности, характеризующих риски возникновения одиночных либо лавинных аварий, одиночных либо групповых, массовых отказов работоспособности и отказов функционирования компонентов модульных и передвижных дата-центров, построенных на основе использования моделей и методов нечеткой классификации и кластеризации;
- создание методов визуализации больших объемов разнородных данных об авариях, отказах и сбоях в работе компонентов МПДЦ, а также построение реализующих эти методы средств реализации сценариев визуализации, обеспечивающих последовательное графическое представление данных об авариях, отказах и сбоях и комбинированное представление результатов обработки разнородных данных с использованием диаграммных, древовидных и графовых структур, построенных на основе использования современных моделей и методов визуализации данных, в том числе, средств виртуальной и дополненной реальности.

Таким образом, исследована современная проблематика и предложен новый подход к развитию методов и средств обработки больших объемов разнородных (гетерогенных) данных о значениях параметров структурной

надежности модульных и передвижных дата-центров. Этот подход включает шесть этапов создания соответствующих методов, обеспечивающих ключевые целевые функции: сбор и предварительную обработку данных, оперативное обнаружение аварий и отказов, оценку уровня структурной надежности, а также анализ и управление рисками нарушения структурной надежности объектов такого класса. Предложены современные (включая интеллектуальные) аналитические методы и механизмы, с помощью которых эти целевые функции могут быть практически реализованы.

Список используемых источников

1. ГОСТ Р 58812-2020 Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация. М. : Стандартимформ, 2020. 36 с.

2. Крюкова Е. С., Ткаченко В. В., Михайличенко А. В., Паращук И. Б. Вопросы оценки надежности современных систем хранения данных для мобильных дата-центров // Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. N 5. С. 86–95.

3. Hwaiyu G. Data Center Handbook: Plan, Design, Build, and Operations of a Smart Data Center, 2nd Edition. NY: Wiley, 2021. 55 p.

4. Ditlevsen O., Madsen H.O. Structural Reliability Methods. Copenhagen: Technical University of Denmark, 2007. 373 p.

5. Melchers R. E. Structural Reliability Analysis and Prediction. NJ: John Wiley & Sons Limited, 2018. 497 p.

УДК 004.89
ГРНТИ 82.01.85

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ RPA ДЛЯ ОПТИМИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ УПРАВЛЕНИЯ КАЧЕСТВОМ УСЛУГ

Д. В. Жих[1], С. В. Кисляков[1,2], М. Ю. Скоринов[1,3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]НТЦ Аргус
[3]АО «Нэксайн»

Появление новых технологий за последние несколько лет привело к преобразованиям в области обеспечения качества услуг.

Поскольку оптимизация бизнес-процессов становится неотъемлемой частью цифровой трансформации, для повышения качества услуг компании внедряют роботи-

зированную автоматизацию процессов. Применение данной технологии позволяет использовать программных ботов для решения простых в исполнении задач, при этом повышая эффективность и снижая операционные затраты.

В статье рассматриваются бизнес-процессы, касающиеся качества услуг, а также подходы к автоматизации этих бизнес-процессов с применением роботизации.

бизнес-процесс, управление качеством услуг, robotic process automation.

В условиях быстро меняющейся бизнес-среде компании стремятся найти пути увеличения эффективности, снижения затрат и повышения лояльности клиентов. Одной из областей, которая имеет решающее значение для поддержания конкурентоспособности компании является управление качеством услуг.

Процесс управления качеством услуг, предоставляемых клиенту в соответствии с его ожиданиями, называется управлением качеством услуг. Он в основном оценивает, насколько хорошо была оказана услуга, чтобы улучшить ее качество в будущем, выявить проблемы и устранить их. Качество услуги может относиться либо к потенциалу услуги (квалификация лиц, предлагающих услугу), либо к процессу обслуживания (быстрота, надежность и т. д.), либо к результату обслуживания (соответствие ожиданиям клиента).

Бизнес-процессы оператора связи строятся на основе модели ETOM [1]. Группировка бизнес-функций управления качеством услуг предназначена для управления, контроля, мониторинга, анализа, информирования и восстановления значений параметров качества отдельных услуг (рис. 1). Эти бизнес-функции необходимы для поддержания постоянных стандартов качества обслуживания и обеспечения соответствия ожиданиям клиентов.

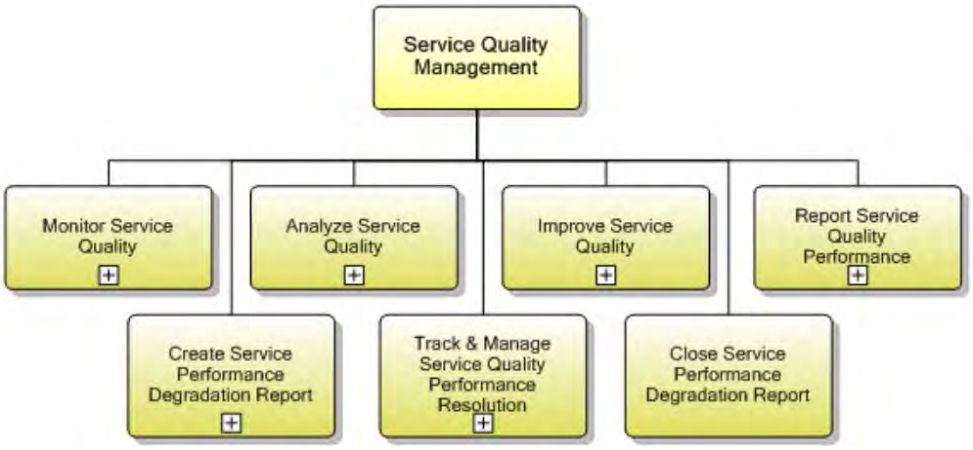


Рис. 1. Группировка бизнес-функций управления качеством услуг

Группировка бизнес-функций управления качеством услуг включает в себя следующие элементы:

1. Monitor Service Quality – «Мониторинг качества услуг» должен осуществлять мониторинг поступающей информации о качестве услуг и выполнять первичное обнаружение данных о качестве;

2. Analyze Service Quality – «Анализ качества услуг» должен выполнять анализ и производить вычисление значений параметров качества отдельных услуг;

3. Improve Service Quality – «Улучшение качества услуг» должен обеспечивать наиболее рациональным образом восстановление качества услуг до нормального рабочего состояния;

4. Report Service Quality Performance – Процесс «Информирование о параметрах качества услуг» должен обеспечивать мониторинг статуса отчетов об ухудшении параметров услуг, выпускать уведомления о любых изменениях статуса и создавать отчеты об управлении параметрами услуг;

5. Create Service Performance Degradation Report – «Создание отчета об ухудшении параметров услуг» должен обеспечивать создание нового отчета об ухудшении параметров услуг, а также выполнять модификацию или аннулирование существующих отчетов;

6. Track & Manage Service Quality Performance Resolution – «Контроль и управление восстановлением параметров качества услуг» должен назначать, координировать и контролировать деятельность по анализу, восстановлению и улучшению параметров качества отдельных услуг;

7. Close Service Performance Degradation Report – «Закрытие отчета об ухудшении параметров услуг» должен закрывать отчет после того, как проблемы со значениями параметров качества услуг будут устранены.

Одним из подходов к оптимизации процессов управления качеством услуг является использование технологии RPA – Robotic Process Automation. Технология RPA отображает человеческий процесс или задачу на языке программного обеспечения RPA для последующего программного сценария, обычно известного как «робот» или «бот», с выделенной средой выполнения для выполнения сценария с помощью панели управления. Она тесно взаимодействует с новыми технологиями, такими как искусственный интеллект, машинное обучение и интеллектуальная автоматизация [2].

RPA может включать автоматизацию процессов центра обработки вызовов, развертывание чат-ботов для помощи клиентам, внедрение голосовых помощников. Программные роботы ускоряют обслуживание клиентов, собирая данные из нескольких систем, выполняя запросы на обслуживание и обновляя записи клиентов, а также способствуют созданию новых моделей обслуживания клиентов и улучшению работы других подразделений компании [3]. Кроме того, благодаря использованию RPA для сбора данных, риск человеческой ошибки значительно снижается, что приводит к повышению удовлетворенности клиентов.

Рассмотрим возможности RPA для поставщика цифровых услуг.

1. Помощь представителям службы поддержки клиентов

Бот RPA может собрать данные о клиенте, включающие в себя данные о продажах, предыдущие жалобы, и отправить ее представителю службы поддержки клиентов. Данная информация поможет понять требования и ожидания клиента.

2. Анализ часто задаваемых вопросов

RPA-боты для обслуживания клиентов или чат-боты на основе ИИ могут собирать информацию о частых запросах пользователя в тикет-систему. Получив в нее доступ, чат-боты могут решить простые проблемы клиентов, включающие в себяобновление пароля или информации для входа в систему, обновление заказов, внесение изменений в платежную информацию.

3. Общение с жалобами клиентов

Боты RPA могут использовать технологии обработки естественного языка (NLP) и оптического распознавания символов (OCR) для понимания жалоб клиентов в электронных письмах или текстовых сообщениях для их последующего ввода в электронные таблицы и текстовые документы, а также длясоздания отчетов [4].

Полученные отчеты могут распространяться среди соответствующего персонала службы поддержки клиентов, использоваться для выявления моделей проблем.

4. Автоматизация процесса возврата средств

Автоматизация данного процесса позволяет клиентам сразу же получить возврат денег за продукцию без длительного взаимодействия со службой поддержки.

Вернувшись к упомянутой ранее группировке бизнес-функций управления качеством услуг и возможностям применения технологии RPA, определяются следующие группировки, в которых возможно использование ботов RPA. К таким бизнес-функциям относятся мониторинг качества услуг анализ качества услуг, создание отчета об ухудшении параметров услуг.

Список используемых источников:

1. Process Framework (eTOM) [Электронный ресурс]. URL: https://www.tmforum.org/oda/business/process-framework-etom/ (дата обращения 02.03.2023).

2. 5 benefits of a quality management system (QMS) in 2023 [Электронный ресурс]. URL: https://www.qualio.com/blog/the-5-noticeable-benefits-of-implementing-a-quality-management-system (дата обращения 02.03.2023).

3. Service Quality Management: How to Measure and Manage It [Электронный ресурс]. URL: https://blog.udemy.com/service-quality-management/#:~:text=The%20process%20of%20managing%20the,them%20to%20increase%20customer%20satisfaction. (дата обращения 02.03.2023).

4. Ensuring Quality with Robotic Process Automation (RPA) [Электронный ресурс]. URL: https://amzur.com/blog/ensuring-quality-with-robotic-process-automation-rpa/ (дата обращения 02.03.2023).

УДК 004.7
ГРНТИ 81.93.29

СПОСОБ ОПРЕДЕЛЕНИЯ В СЕТИ ПЕРЕДАЧИ ДАННЫХ ЦЕПОЧКИ МАРШРУТОВ ДО ГЕОГРАФИЧЕСКОГО МЕСТОПОЛОЖЕНИЯ ЗЛОУМЫШЛЕННИКА

В. А. Задбоев, В. А. Липатников, К. В. Мелехов

Военная орденов Жукова и Ленина Краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Любая сетевая инфраструктура нуждается в защите от внешних угроз, однако этого все равно недостаточно, потому необходимо пресекать любые попытки входа во внутреннюю сеть, например, путем обратной атаки на злоумышленника, для вычисления его местонахождения. Цель статьи повысить безопасность внутреннего сетевого трафика сети передачи данных критически важного объекта путем определения злоумышленников на основе их IP-адресов. Задача – разработать систему определения географического местоположения злоумышленника и алгоритм её действий.

местоположение злоумышленника, IP-адрес, модель угроз, внешние угрозы, сеть передачи данных, критически важный объект, сканирование сети.

В связи с быстрым развитием информационных технологий, в том числе сети Интернет, объединяющей разнородные сети, и переходом к информационному обществу, проблема обеспечения информационной безопасности (ИБ) и построения сетей передачи данных (СПД) стала одной из наиболее актуальных [1]. К средствам защиты в настоящее время предъявляются более жесткие требования [2, 3]. Известны методы обеспечения необходимого уровня защищенности различных систем, например, способ управления ИБ информационно-вычислительной сети (ИВС) путем реализации ложной сети на основе выделенного сервера с контейнерной виртуализацией [4, 5]. Однако в этом случае при управлении ИБ не используются данные анализа динамики действий нарушителя Основным требованием, предъявляемым системам обеспечения безопасности сейчас, является способность находить аномалии и соответственно, вторжения в реальном времени, а также определения географического местоположения злоумышленника. Возникает противоречие между новыми эффективными средствами кибернетического вторжения и существующими способами защиты СПД от кибернетического вторжения. **Цель**: повысить безопасность внутреннего

сетевого трафика СПД критически важного объекта путем определения злоумышленников. **Задача** – разработать систему определения географического местоположения злоумышленника и алгоритм её действий.

Для определения в СПД цепочки маршрутов предлагается использовать утилиту Tracert в Windows или Traceroute в Unix. Данная утилита формирует UDP-запрос и упаковывает его в IP-пакет и передает транзитным узлам. В заголовке такого IP-пакета есть поле TTL *(Time to Live)* – время жизни пакета. Оно определяет количество переходов между узлами до конечного IP-адреса, так же утилита показывает список всех *IP*-адресов по которым совершены переходы.

Рассмотрен процесс использования утилитой определения цепочки маршрута в Windows и Unix системах:

1. Для использования утилиты необходимо открыть терминал или консоль в Unix или Windows системах соответственно;

2. Ввести команду Tracert или Traceroute в зависимости от операционной системы дополнительно прописав необходимый IP-адрес, пример представлен на рис. 1 и 2;

3. Получить данные и занести во временную базу данных;

4. Сравнить полученные данные;

5. Сформировать отчет по результатам работы.

Получение цепочки маршрутов до IP-адреса злоумышленника или до ближайшего к нему проводится параллельно или с минимальной задержкой.

```
root@194-67-116-72:~# traceroute 172.217.16.110
traceroute to 172.217.16.110 (172.217.16.110), 30 hops max, 60 byte packets
 1  node82-msk1.cloudvps.reg.ru (89.108.69.216)  0.122 ms  0.091 ms  0.074 ms
 2  kiae-r1.hosting.reg.ru (31.31.194.4)  0.249 ms  0.483 ms  0.484 ms
 3  * * *
 4  150-192-212-88.host.exepto.ru (88.212.192.150)  0.445 ms  0.461 ms  0.446 ms
 5  msk-m9-b1-ae30-vlan342.fiord.net (62.140.239.222)  0.848 ms  0.678 ms  0.666 ms
 6  * * msk-m9-b3-ae7-vlan712.fiord.net (62.140.243.141)  0.780 ms
 7  * * *
 8  72.14.222.198 (72.14.222.198)  1.554 ms  1.541 ms  1.527 ms
 9  108.170.250.34 (108.170.250.34)  2.133 ms 108.170.250.66 (108.170.250.66)  1.981 ms 108.170.250.130 (108.1
70.250.130)  1.899 ms
10  172.253.66.116 (172.253.66.116)  19.098 ms 216.239.51.32 (216.239.51.32)  16.914 ms *
11  142.250.227.131 (142.250.227.131)  34.112 ms 142.250.227.7 (142.250.227.7)  31.685 ms  34.253 ms
12  72.14.237.108 (72.14.237.108)  46.935 ms 66.249.94.20 (66.249.94.20)  47.887 ms 64.233.175.142 (64.233.175
.142)  45.672 ms
13  74.125.242.225 (74.125.242.225)  47.746 ms 74.125.242.241 (74.125.242.241)  45.421 ms 74.125.242.225 (74.1
25.242.225)  47.698 ms
14  72.14.239.201 (72.14.239.201)  46.715 ms  45.131 ms 72.14.239.195 (72.14.239.195)  48.336 ms
15  prg02s12-in-f14.1e100.net (172.217.16.110)  45.997 ms  48.276 ms  45.973 ms
root@194-67-116-72:~#
```

Рис. 1. Пример использования команды traceroute

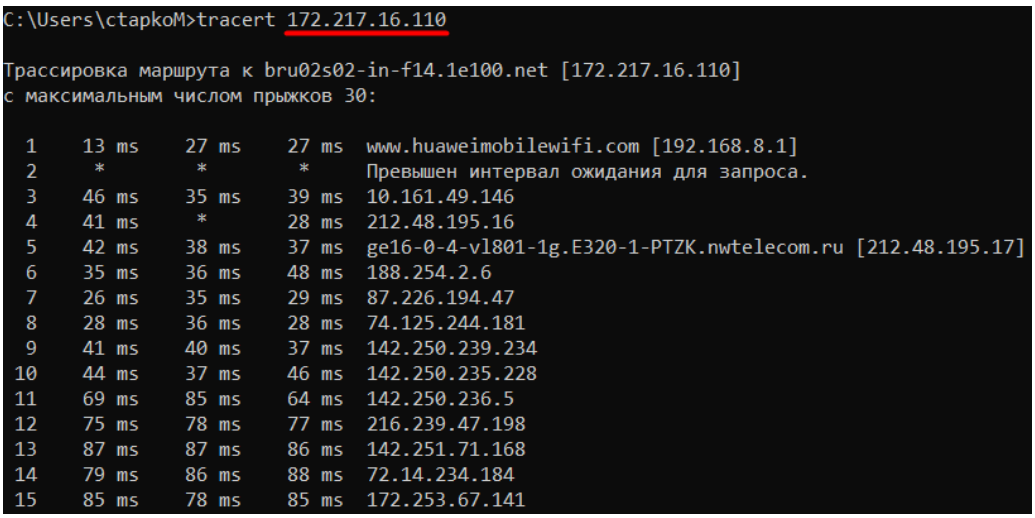


Рис. 2. Пример использования команды tracert

Использование данных утилит для определения реального графического местоположения злоумышленника с кибернетического вторжения, возможно в разработанном ниже алгоритме, определяющий политику ИБ серверов, то есть представить комплекс мер, правил и принципов, используемых при организации сети передачи данных. В алгоритме представлены процессы сканирования СПД и действия, применяемые при обнаружении подозрительных IP-адресов или действий со стороны доверенных пользователей. На рис. 3 представлен алгоритм сканирования трафика, обрабатываемого в сети передачи данных.

Во время сканирования сетевого трафика, происходит регистрация и внесение IP-адреса кибернетического вторжения в список поступивших адресов, далее после получения списка достоверных IP-адресов, полученный ранее IP-адрес, сравнивается с данным списком на наличие совпадения, при положительном ответе предоставляется доступ к системе, при несоответствии проводятся следующие мероприятия:

1. Мониторинга сетевого трафика и обнаружения в нем аномальной активности, а также идентификации и классификации кибератак, необходимо учитывать большое число факторов и параметров, включая возможные сетевые маршруты, времена задержки данных, потери пакетов и новые свойства трафика, отличающиеся от нормальных. Регистрация инцидента;
2. Анализ информации о не совпадающем IP-адресе из списка;
3. Выявляется предполагаемое местоположение данного IP-адреса злоумышленника на основе полученной ранее информации;
4. Формируется и выводится отчет о НСД.

По окончанию всех выполненных мероприятий выводится общий отчет о проделанной работе.

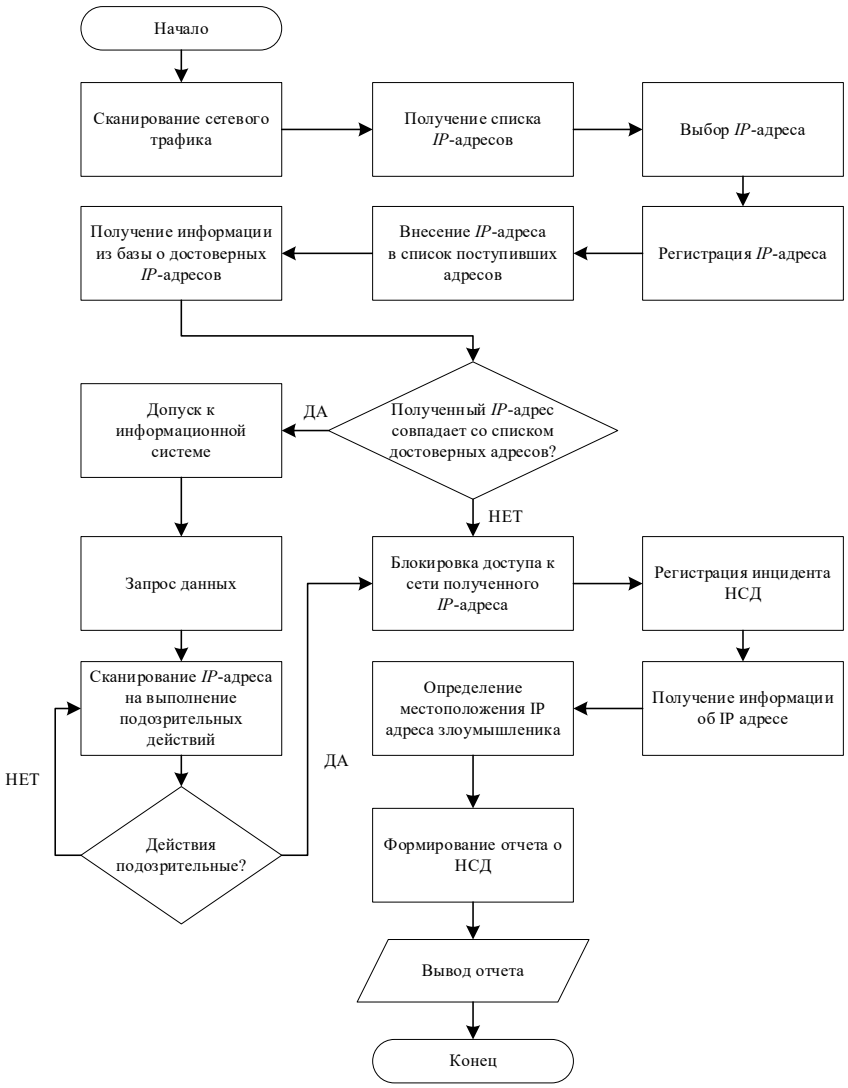


Рис. 3. Алгоритм сканирования сети передачи данных

При условии, что полученный IP-адрес находится в списке доверенных, ему предоставляется доступ к СПД, однако продолжается постоянное наблюдение за ним на выявление подозрительных действ. При обнаружении таких действий ему так же блокируется доступ к СПД, регистрируется инцидент и определяется географическое местоположение по данному IP-адресу. По окончанию данных мероприятий выводится сформированный отчет представляется администратору сети.

Первым шагом к правильной технической реализации процесса выявления злоумышленника является представление результатов сканирования, с которыми придется работать. Если используется несколько разнородных сканеров, предложено ввести процессы мониторинга сетевого трафика и обнаружения в нем аномальной активности, а также идентификации и классификации Способ обнаружения и классификации многоэтапных атак и объединять информацию по узлам в одном месте. Для этого целесообразно

использовать аналитические системы, где также будет храниться вся информация о трафике.

Предложена система обнаружения IP-геолокации злоумышленника, интернет-хостов, использующих IP-адреса с кодами стран, отличными от того, где они фактически находятся.

Новая система определения местоположения:

1. Обязана не полагаться на информацию, предоставляемую злоумышленниками;
2. Должна быть способна принимать автоматизированные решения, когда это возможно;
3. Должна собирать дополнительную информацию, чтобы помочь человеку решить, использует ли IP правильную геолокацию или нет;
4. Должна иметь возможность обрабатывать множество IP-адресов одновременно без контроля.

Источниками измерений являются:

1. Монитор – это сервер, способный выполнять измерения, такие как, пинг и трассировка;
2. Алгоритмы пассивной геолокации выполняют геолокацию без использования каких-либо активных измерений до цели;
3. Алгоритмы активной геолокации используют такие измерения, как ping и traceroute, чтобы ограничить местоположение цели.

Выводы

Рассмотрен метод обнаружения аномалий и кибератак, предназначенный для использования в современных СПД, который основывается на интеграции методов анализа и машинного обучения.

Предложен алгоритм сканирования сетевого трафика и определения местонахождения злоумышленника.

Определены особенности работы сетевых мониторов, используемых при определении географического местонахождения на основе полученного IP-адреса.

Разработаны принципы построения системы определения местоположения на основе сетевых адресов.

Список используемых источников

1. Williams J. Identification of IP address using fraudulent geolocation data // Imperial College London. 15 June 2020. PP. 60–65.

2. Wang, Zhihao, et al. Towards IP Geolocation with Intermediate Routers Based on Topology Discovery // Cybersecurity. Apr. 2019. Vol. 2, No. 1. PP. 13–16.

3. Hufaker B., Fomenkov M., and kc claffy. Geocompare: a comparison of public and commercial geolocation databases // In Proceedings of the Network Mapping and Measurement Conference (NMC). 2011. PP. 34–37.

4. Липатников В. А., Шевченко А. А., Яцкин А. Д., Семенова Е. Г. Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. N 4. С. 67–76.

5. Липатников В. А., Тихонов В. А., Шевченко А. А. Метод управления кибернетической безопасностью в системах критических инфраструктур, основывающийся на интеллектуальных сервисах защиты информации // Технологии построения когнитивных транспортных систем : материалы всероссийской научно-практической конференции с международным участием, Санкт-Петербург, 28–29 мая 2019 года. СПб. : Институт проблем транспорта им. Н. С. Соломенко РАН, 2019. С. 207–214.

6. Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя // Информационно-управляющие системы. 2022. N 1 (116). С. 54–67.

7. Липатников В. А., Шевченко А. А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий // Информационные системы и технологии. 2022. N 2 (130). С. 107–115.

8. Липатников, В. А., Коршунов Г. И., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. N 4 (95). С. 61–72. DOI 10.31799/1684-8853-2018-4-61-72.

9. Липатников В. А., Парфиров В. А. Модель процесса наблюдения за множеством источников информации в стохастических условиях. Информация и космос. 2022. N 1. С. 35–44.

10. Липатников В. А., Ломанов А. А. Способ обнаружения и классификации многоэтапной атаки на основе долгой краткосрочной памяти // Технологии. Инновации. Связь. Сб. материалов научно-практической конференции. Санкт-Петербург, 19 апреля 2021 года. СПб. : ВАС, 2022. С. 104–108.

УДК 004.716
ГРНТИ 49.33.29

БЕСПИЛОТНЫЙ АВТОТРАНСПОРТ КАК СОСТАВЛЯЮЩАЯ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ

А. А. Задорожняя

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье описаны источники, которые описывают современный беспилотный автотранспорт, преимущества его внедрения и развитие Промышленного Интернета вещей. Промышленный Интернет вещей играет важную роль в разработке концепции беспилотных транспортных средств будущего. Также предлагается способ

уменьшения сетевой задержки в беспилотном автотранспорте как системы Промышленного Интернета вещей. Данное решение позволяет уменьшить нагрузку на сеть передачи данных, оптимизировать использование сети и уменьшить сетевую задержку, что способствует снижению к минимуму риск аварийных ситуаций.

IIoT, Промышленный Интернет, Промышленный Интернет вещей, беспилотный автотранспорт, беспилотное транспортное средство, автоматизированное транспортное средство.

Беспилотные транспортные средства в первую очередь должны обеспечивать ключевые преимущества по сравнению с традиционными транспортными средствами, управляемыми людьми. Такими преимуществами являются:

– высокий уровень безопасности и, как следствие, сокращение количества дорожно-транспортных происшествий;

– комфортное функционирование транспортных средств, условленное отсутствием пробок и, как следствие, сокращение времени, затраченного на перемещение из пункта А в пункт Б;

– сохранение природных ресурсов, способствующее снижению степени антропогенного воздействия на экологию и частичное устранение последствий загрязнения окружающей среды.

Перечисленные преимущества способствуют повышению качества жизни человека. Внедрение подобного транспортного средства в жизнь современного человека может освободить его от «транспортных забот» [1, 2].

Под беспилотным автотранспортом здесь имеется ввиду транспортное средство, работающее за счет сетевой системы содействия при вождении (NDA) и электродвигателя. NDA (*Network-based driving assistance*) – набор возможностей, помогающий транспортным средствам принимать решения для обеспечения безопасного и эффективного вождения, используя данные, собранные сетями от транспортных средств и объектов придорожной инфраструктуры [3]. Такое определение возникает из рекомендаций Международного союза электросвязи (МСЭ), стандартов Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК). Рекомендация МСЭ описывает функциональную архитектуру сетевой системы содействия при вождении для автономных транспортных средств. Стандарт ИСО устанавливает требования безопасности к аккумуляторным системам хранения энергии (СХЭА), находящихся на борту транспортных средств на электрической тяге, в том числе к аккумуляторным батареям электромобилей (ЭМА), СХЭА электромобилей на топливных элементах (ЭМТ) и гибридных электромобилей (ЭМГ), для обеспечения защиты людей внутри и вне автомобиля и окружающей среды [4]. Стандарты МЭК распространяются на литий-ионные аккумуляторы, ис-

пользуемые для приведения в движение аккумуляторных (ЭМА) и гибридных (ЭМГ) электромобилей, и устанавливает методы испытаний по определению рабочих характеристик [5].

Несмотря на большое количество исследований по теме внедрения беспилотного автотранспорта и существующих примеров эксплуатации беспилотных транспортных средств, функционирующих без участия человека, описанные выше БТС представляют собой альтернативу передвижения в будущем. Так как многие путешественники совершают поездки с помощью существующих, привычных способов, таких как традиционные автомобили, и общественный транспорт, велосипеды и др. [6]. Эти способы сменятся за счет использования автоматизированных транспортных средств, что обусловлено переходным процессом. В России существует уже немало стандартов, описывающих системы автоматизации управления, из них можно выделить ГОСТ Р 58837-2020 и ГОСТ Р 58823-2020, так как в них подробно представлена классификация, описывающая все уровни автоматизации управления движением автомобильных транспортных средств, а также функциональные определения для систем с высокой степенью автоматизации управления движением и связанных с ними терминов и понятий [7, 8]. В рекомендации МСЭ карта высокого разрешения является необходимой технологией автоматического вождения на уровнях от 3 до 5 (уровни автоматизации вождения определены Обществом инженеров-автомобилестроителей (SAE)) [9]. Принцип автоматизации беспилотного автотранспорта схож с автоматизацией в Промышленном Интернете вещей.

Привычное понимание системы промышленной автоматизации и управления (IACS) заключалось в том, что производственные процессы в значительной степени изолированы от обычных цифровых сетей, то есть представлены в виде корпоративных ИКТ-сред. Там, где необходимо было подключение, применялась зональная архитектура с брандмауэрами и/или демилитаризованными зонами, используемыми для защиты основных компонентов системы управления. Внедрение технологий Интернета вещей (IoT) в промышленность привела к архитектурным изменениям в IACS и увеличению возможностей подключения к промышленным системам. Концепция систем промышленной автоматизации и управления (IACS) хорошо зарекомендовала себя. Эти системы, часто называемые операционными технологиями (OT), используются в различных отраслях, включая производство, транспорт и коммунальные услуги, и иногда их называют киберфизическими системами (CPS). [10] Сейчас в основе киберфизических систем лежит много ключевых технологических тенденций, в том числе искусственный интеллект (AI), автономный транспорт (AV) и многие другие.

Промышленный Интернет или Промышленный Интернет вещей (*Industrial IoT*, IIoT) направлен на подключение промышленных активов, та-

ких как двигатели, электрические сети и датчики, к облаку по сети [11]. Промышленный Интернет вещей состоит из множества устройств, соединенных коммуникационным программным обеспечением. Полученные системы и даже отдельные устройства, входящие в их состав, могут отслеживать, собирать, обмениваться, анализировать и мгновенно воздействовать на информацию, чтобы разумно изменить свое поведение или окружающую среду – и все это без вмешательства человека [12]. Основное преимущество этого все еще, по общему признанию, расплывчатого определения заключается в том, что оно проясняет, какова функция устройств IIoT: отслеживать, собирать, обмениваться и анализировать информацию, чтобы позволить им изменить свое собственное поведение или дать указания другим устройствам делать это. Из рис. 1 видно, что одной из областей применения Промышленного Интернета вещей является транспорт.

Рис. 1. Сферы применения Промышленного Интернета вещей

Таким образом, беспилотный автотранспорт можно представить как Промышленный Интернет вещей. Важным вопросом является существующая сетевая задержка при передачи данных, от которой зависит скорость реакции беспилотного автомобиля на ту или иную экстренную ситуацию, например, на пешехода, внезапно сменившего траекторию. Из примера понятно, что эта задержка является критически важной.

Необходимую задержку достичь не так легко, поэтому предлагается способ уменьшить задержку за счет внедрения программно-аппаратного

комплекса, состоящего из двух модулей – модуля инжекции принятых данных и контроллера, изначально предлагаемого для решения задач IIoT. Модуль инжекции принятых данных отвечает за прием, дешифрацию, гарантированную доставку и инжекцию на стороне клиента. Алгоритм работы модуля инжекции принятых данных: входящая агрегированная команда проходит процесс дешифрации (сверка с графом команд на стороне модуля), проверяется на целостность и интегрируется в шаблон пакета данных в виде исходного (до процесса архивирования) набора пакетов трафика. Контроллер отвечает за предиктивную аналитику на базе рекуррентной нейронной сети, основанной на узлах LSTM, взаимодействие с сервером и передачу агрегированной команды. Алгоритм работы: взаимодействие с сервером происходит в момент передачи данных от сервера на любое клиентское устройство, модуль перехватывает поток данных, производит предварительную обработку трафика, после чего обработанный трафик поступает на вход нейронной сети, которая, проведя анализ входных данных, предоставляет результат предиктивной аналитики в виде графа спрогнозированных пакетов данных алгоритму отправки архивированной команды. Данный модуль позволяет отправлять по сети одну архивированную команду, которая будет дешифрована на устройстве получателя в набор спрогнозированных нейронной сетью пакетов данных, вместо множества единичных пакетов.

Таким образом, предложенный способ позволяет уменьшить нагрузку на сеть передачи данных, оптимизировать использование сети и уменьшить сетевую задержку, что способствует снижению риска аварийных ситуаций на дорогах. Надо отметить, что внедрение данного способа требует большого количества тренировок для нахождения оптимального решения и продуманных сценариев вопроса защищенности системы.

Список используемых источников

1. Olaverri-Monreal C. Promoting trust in self-driving vehicles // Nature Electronics. 2020. N 3 (6). PP. 292–294.

2. Runzhuo Xiao Economic benefit, challenges, and perspectives for the application of Autonomous technology in self-driving vehicles // Highlights in Science, Engineering and Technology TPCEE. 2022. URL: https://www.researchgate.net/publication/369465506_Economic_benefit_challenges_and_perspectives_for_the_application_of_Autonomous_technology_in_self-driving_vehicles (дата обращения 16.03.2023).

3. Рекомендация МСЭ-Т Y.4471 Функциональная архитектура сетевой системы содействия при вождении для автономных транспортных средств (05/2021).

4. ГОСТ Р ИСО 6469-1-2016 Транспорт дорожный на электрической тяге. М. : Стандартинформ, 2016.

5. ГОСТ Р МЭК 62660-1-2020. Аккумуляторы литий-ионные для электрических дорожных дорожных транспортных средств. Часть 1. Испытания по определению рабочих характеристик. М. : Стандартинформ, 2020.

6. Azam S., Munir F., Rafique A., Ko Y., Sheri A. M., & Jeon M. Object modeling from 3d point cloud data for self-driving vehicles // IEEE Intelligent Vehicles Symposium (IV) IEEE. (2018). PP. 409–414.

7. ГОСТ Р 58837-2020 Национальный стандарт Российской Федерации. Автомобильные транспортные средства. Системы автоматизированного управления. Общие принципы проектирования. М. : Стандартинформ, 2020.

8. ГОСТ Р 58823-2020 Автомобильные транспортные средства. Системы автоматизации управления движением. Классификация и определения. М. : Стандартинформ, 2020.

9. Стандарт SAE J 316 -2021 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. URL: https://doi.org/10.4271/J3016_202104 (дата обращения 16.03.2023).

10. Hugh Boyes, Bil Hallaq, Joe Conningham, Tim Watson The industrial internet of things (IIoT): An analysis framework // Computers in Industry. 2018-10-01. Vol. 101. PP. 1–12. URL: https://www.researchgate.net/publication/327991572_The_industrial_internet_of_things _ IIoT_An_analysis_framework (дата обращения 15.03.2023).

11. Helmiö P. Open Source in Industrial Internet of Things: A Systematic Literature Review // Master's Thesis, School of Business and Management Lappeenranta University of Technology. 2018. P. 21.

12. Real Time Innovations Inc Industrial Internet of Things RTI FAQ. 2015. P. 1. URL: https://info.rti.com/hubfs/docs/Industrial_IoT_FAQ.pdf (дата обращения 15.03.2023).

Статья представлена научным руководителем, ректором СПбГУТ, доктором технических наук, доцентом, Р. В. Киричком.

УДК 681.7.068
ГРНТИ 49.13.13

ТЕХНИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ СОЕДИНИТЕЛЯ ПО ТЕХНОЛОГИИ РАСШИРЕННОГО ПУЧКА

Н. А. Захаренков, К. А. Захаренков, К. И. Лукин, И. Г. Стахеев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Волоконно-оптический соединитель по технологии расширенного пучка представляет собой коллиматор, предназначенный для преобразования расходящегося светового пучка с выхода оптического кабеля в расширенный пучок параллельных лучей. На основе теоретического моделирования перечня важнейших параметров соединителя по технологии расширенного пучка были проанализированы технические аспекты реализации конструкции, представляющие значительную трудность при разработке изделия.

оптические соединители, технология расширенного пучка, оптические и геометрические параметры.

В волоконно-оптических системах передач преимущественно распространены два типа соединителей: физический контакт или оптический контакт по технологии расширенного пучка (ТРП).

К преимуществам оптического контакта по сравнению с физическим, следует отнести: устойчивость к загрязнениям из-за расширенного выходного диаметра модового поля; увеличенное количество циклов соединения (разъединения) из-за наличия воздушного зазора между линзами, что обеспечивает стойкость к изнашиванию контактов; упрощенный процесс очистки контактов от загрязнений в полевых условиях с минимальным риском их повреждения и выхода из строя [1].

Но при этом они обладают недостатками, ограничивающими их область применения: вносимые потери в одномодовом режиме составляют 1,5 дБ по сравнению с 0,3 дБ в физическом контакте; возвратные потери даже с просветляющими покрытиями на линзах оказываются значительнее; устойчивость к влиянию воды значительно ниже вследствие изменения коэффициента преломления на поверхности линзы [1].

Несмотря на указанные недостатки, ТРП имеет широкое значение в системах передач, где потери в оптическом бюджете компенсируется малой протяженностью линии или регенерационными модулями.

Основные сферы применения ТРП: военная, для построения линий связи оперативного развертывания; решение геофизических задач (добыча полезных ископаемых, разведка нефти и т. д.); развертывание и функционирование внутрибортового оборудования (судостроение, авиационная и аэрокосмическая промышленности).

Конструктивно соединитель состоит из трех частей: внешний защитный корпус оптической полумуфты; вставка оптического узла (ВОУз), вмонтированная в корпус; отрезок оптического кабеля, вмонтированный в вставку.

Анализ реализации ВОУз для одномодового кабеля с 4-я каналами, изображенного на рис. 1, показывает, что его стоимость может достигать от 300 до 400$, что во много раз дороже изделий по технологии физического контакта. Такая стоимость обусловлена не только дорогостоящими линзами с просветляющим покрытием, но и необходимостью реализации прецизионных допусков, включая допуски по диаметру отверстия, позиционные, посадочные и перпендикулярности, что представляют собой значительную трудность при его производстве на токарно-фрезерном станке.

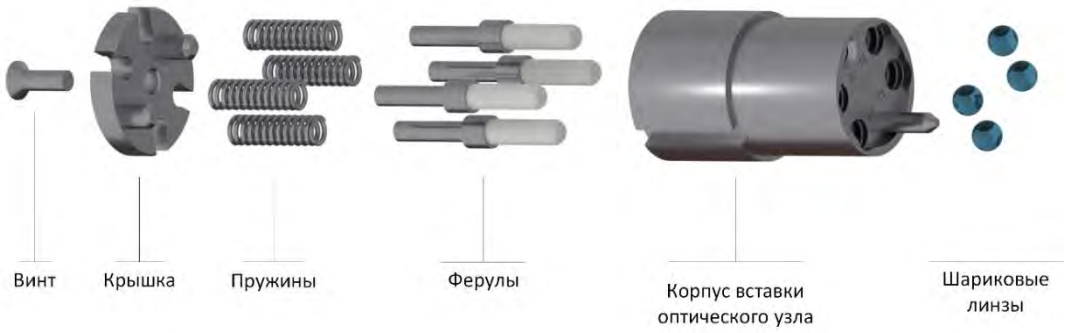


Рис. 1. Вставка оптического узла с комплектом монтажных частей

Важнейшими параметрами ВОУз являются: показатель преломления; фокусное расстояние; боковое и угловое выравнивание оптических осей ферулы и шариковой линзы. Необходимо знать их предположительные допуска [1, 2].

Фокусное расстояние и показатель преломления. Конструктивно корпус ВОУз можно реализовать двумя способами: при наличии или отсутствии непосредственного контакта между торцевой поверхностью ферулы и шариковой линзой. Так как первый подход сопряжен с дополнительными технологическими трудностями, которые могут привести к нарушению прецизионной соосности между шариковой линзой и ферулой, практически всегда выбирают последний.

В связи с этим воспользуемся формулой (1) для расчёта требуемого показателя преломления линзы, полагая, что её заднее фокусное расстояние равно $BFL = 0$.

$$BFL = \frac{nD}{4(n-1)} - \frac{D}{2}, \quad (1)$$

где D – диаметр шариковой линзы, n – показатель преломления материала, BFL – заднее фокусное расстояние, представленные на рис. 2.

Независимо от выбранного диаметра линзы D при расчётах с $BFL = 0$, её показатель преломления всегда будет равен $n = 2$.

Наиболее подходящими оптическими материалами под соответствующие рабочие длины волн – 1310 и 1550 нм – оказываются марки стекла LASF35, TAFD65 и H-ZLaF95.

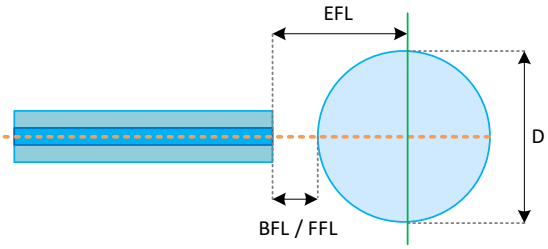


Рис. 2. Основные параметры шариковой линзы

Немаловажным становится нанесение просветляющего покрытия на обе поверхности, так как по формулам Френеля при $n = 2$ коэффициент отражения может составлять $R = 0{,}11$, что приводит к большим потерям мощности сигнала.

Боковое выравнивание. Существует несколько конструкций ВОУз, предназначенных для выравнивания осей шариковой линзы и ферулы, в которой с высокоточным позиционным допуском располагается сердцевина волокна.

Данные, приведенные на рис. 3, были получены методом моделирования в ПО COMSOL Multiphysics и MATLAB при следующих условиях: одномодовое волокно – 9/125 нм, гауссов луч – 1310 нм, диаметр шариковой линзы – 3 мм, показатель преломления – 2. Следует учитывать, что суммарные вносимые потери от всех ранее перечисленных параметров не должны превышать 1.5 дБ.

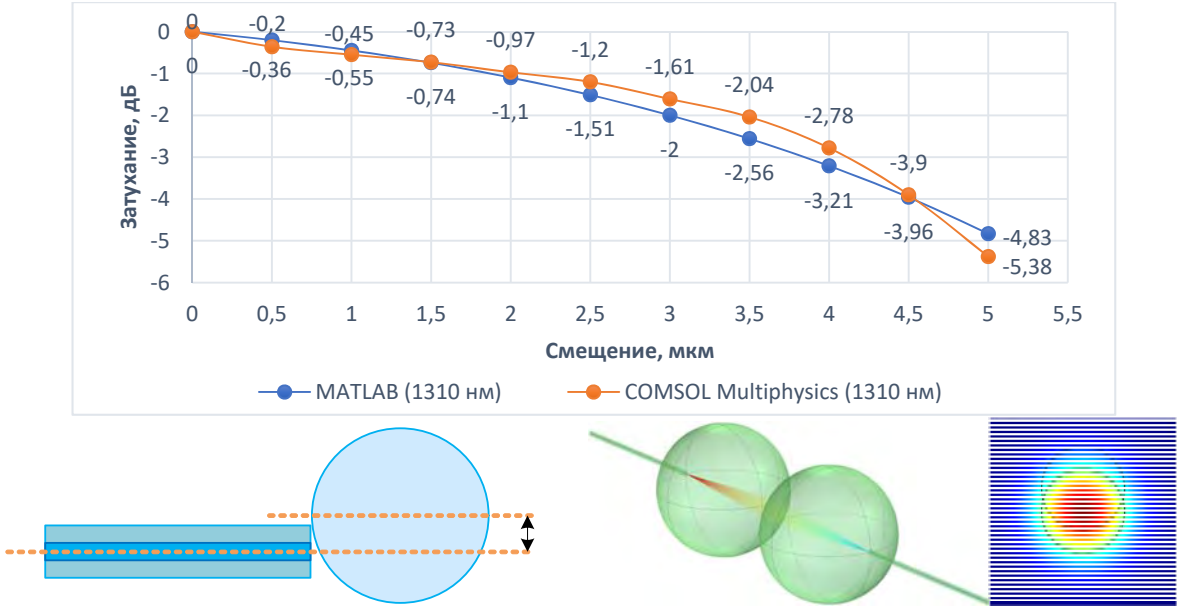


Рис. 3. Моделирование вносимых потерь от бокового смещения

Результаты моделирования показали, что допуск на радиус отверстия под ферулу не должен превышать 2 мкм с учётом вносимых потерь от возможных погрешностей ранее перечисленных параметров.

Необходимо отметить, что боковое выравнивание оптических осей сопрягаемых шариковых линз, расположенных в разных корпусах ВОУз, не нуждается в высокоточных допусках [2].

Угловое выравнивание. При сопряжении двух вставок оптического узла, потери на угловом выравнивании могут возникнуть из-за нарушения перпендикулярности сопрягаемых торцевых поверхностей к осям отверстий при изготовлении или попадании загрязняющих частиц на них.

При сопряжении ферулы и линзы, потери на угловом выравнивании могут возникать из-за бокового смещения ферулы, неправильной полировки торцевой поверхности или загрязнения частицами.

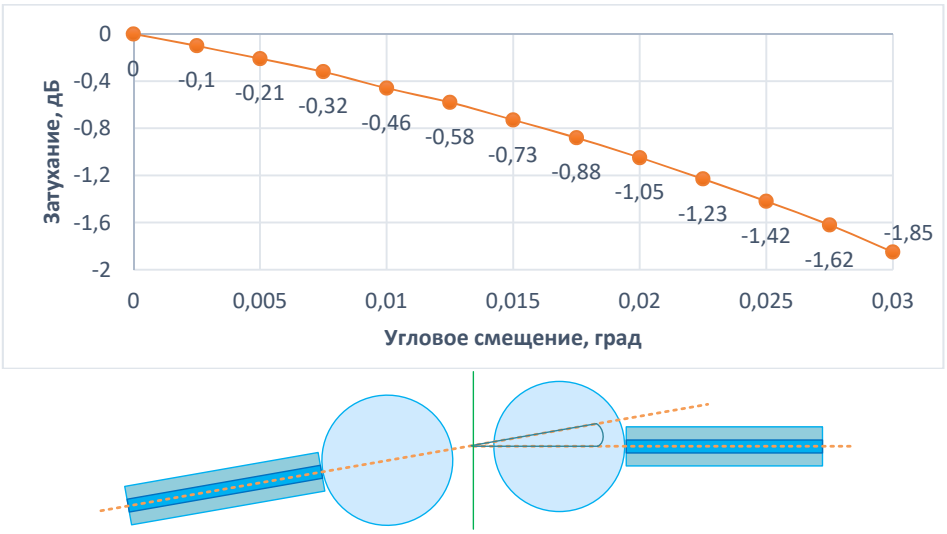


Рис. 4. Вносимые потери от углового смещения вставки оптического узла

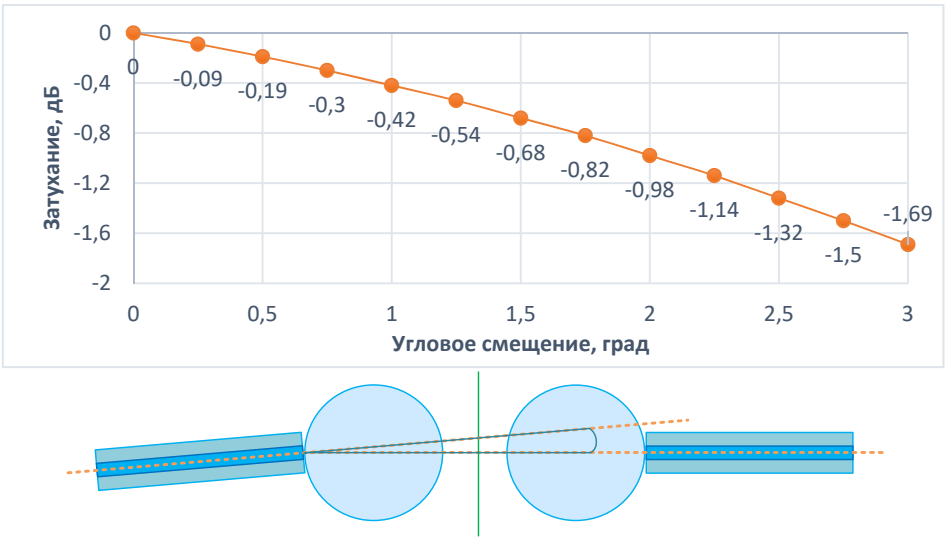


Рис. 5. Вносимые потери от углового смещения ферулы

Из графиков, приведенных на рис. 4 и 5, можно сделать следующий вывод: допуск по перпендикулярности на сопрягаемую поверхность корпуса ВОУз должен разрабатываться с учётом углового отклонения менее 0,005 градусов. В том числе для обеспечения корректного углового выравнивания ферулы и линзы, необходимо проводить тщательную очистку отверстий перед сборкой ВОУз.

Список используемых источников

1. Simonini Edward, Douthit James. Expanded Beam & Physical Contact Fiber Optic Connectors. [Электронный ресурс]. URL: https://amphenol-ns.com/Blog/post/expanded-beam-physical-contact-fiber-optic-connectors (дата обращения 22.10.2022).

2. Lee Y.G.; Park C.H.; Back, S.W.; Kim, H.J.; Lee, S.S. Alignment tolerant expanded beam connector based on a gapless fiber-lens interface. Appl. Opt. 2016, 55, PP. 341–344.

УДК 681.785.64
ГРНТИ 59.45.37; 59.14.23

ПРОБЛЕМАТИКА ИЗМЕРЕНИЯ ПАРАМЕТРОВ ЛИНЗ МИКРООПТИКИ, ИСПОЛЬЗУЕМОЙ В ОПТИЧЕСКИХ СИСТЕМАХ ПЕРЕДАЧ

К. А. Захаренков, Н. А. Захаренков, К. И. Лукин, О. В. Титова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Существует множество приборов для измерения оптических или геометрических параметров линз. В оптических системах передач часто используется микрооптические линзы и их сборки, отклонения параметров которых может сильно повлиять на затухании в узловой системе. В работе рассмотрены типы линз, используемые в оптических системах передач, и проведен анализ пригодности данных приборов для измерения фокусного расстояния таких линз. Сделан вывод о недостатках приборов, и представлены предложения по разработке или модернизировать имеющееся оборудование.

оптические и геометрические параметры линз, effective focal length, back focal length, front focal length, фокусное расстояние, микрооптика, линзы, шариковые линзы, оптоволокно.

Существующие оптические системы передачи (ОСП) не рассматриваются без компонентов микрооптики с довольно небольшими короткофокусными коллимирующими и фокусирующими линзами или системами линз. Данные системы подразделяются:

- Линзы в лазерных модулях TOSA и ROSA трансиверов, ресиверов и трансмиттеров. Для коллимирования или фокусирования пучков обычно применяются линзы (сферические или асферические) или системы линз с Back focal length (BFL) не более 10 мм, не считая цилиндрические линзы или анаморфные призмы, используемые для исправления эллиптичности выходящего пучка [1].
- Линзы в лазерных диодах с волоконным выводом [2] (*Fiber-Coupled Laser Diode*). Используются в различных отраслях, в том числе в оптических системах передачи, как лазеры накачки в усилителях оптический линии.

• Технология *Expanded Beam*. Обычно для этой технологии применяются шариковые линзы и реже стержневые линзы с градиентным показателем преломления.

В таких системах целесообразно использовать качественные линзы с необходимыми допусками по сферичности линз и менее критичными допусками по диаметру для достижения наилучшего коэффициента полезного действия (КПД), в которых необходимо сфокусировать луч в сердцевину оптоволокна с довольно малым диаметром: 9 мкм для одномодового (*SM*) и 50/62,5 для многомодового (*MM*). Боковое смещение главной оптической оси линзы относительно оптоволокна всего на 4 мкм может привести к потерям более чем на 50 %, как видно на рис. 1. Сферичность линзы или угол наклона главной оптической оси линзы так же сильно сказываются на затухании [3]. Поэтому для достижения наилучшего КПД планируемой узловой системы необходимы качественные линзы с малыми погрешностями.

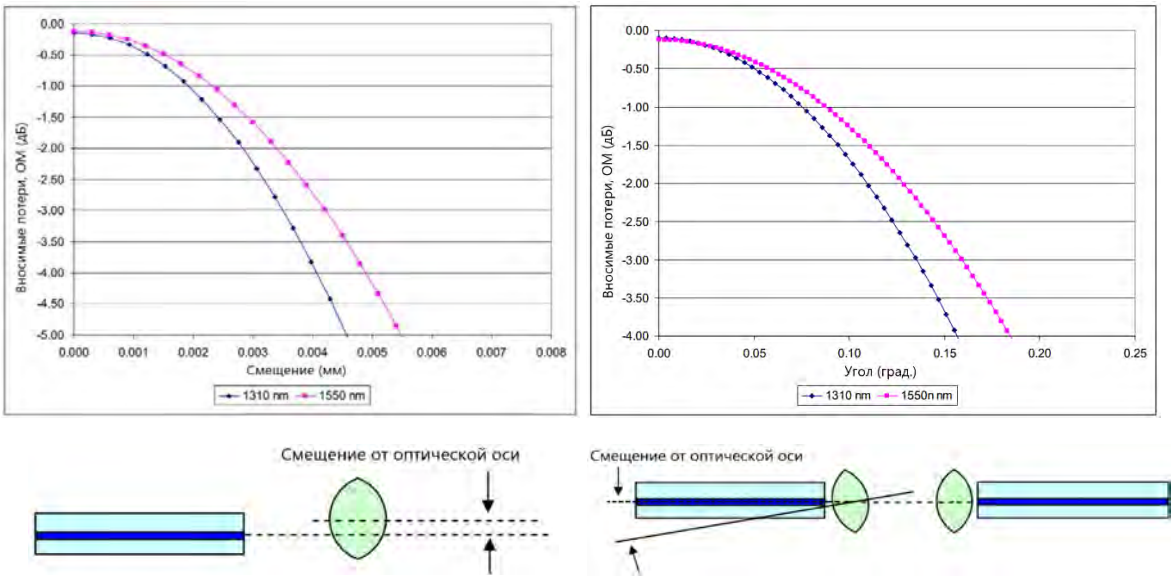


Рис. 1. Вносимые потери от бокового смещения
и наклона линзы относительно оптоволокна диаметром приблизительно 3 мм

Для таких систем существует рассчитываемые минимально необходимые диапазоны измерительные параметры линз.

Первым и основным параметром является расчет диапазона минимальных и максимальных необходимых параметров измерения BFL, front focal length (FFL) и effective focal length (EFL).

Из рассмотренных сфер ОСП для рассмотрения и расчета минимального BFL и FFL прибора за основу возьмем технологию Expanded Beam, в которой зачастую применяются шариковые линзы с BFL (FFL) = 0–1 мм для коллимирования и фокусировки пучка. В Expanded Beam обычно используются линзы диаметром 3 мм.

В TOSA и ROSA могут применяться различные сферические и асферические линзы: шариковые, плоско-выпуклые, купольного типа и т. д. В данных системах применяются линзы размером 0,5, 1,25, 2,5 мм [4, 5, 6].

На практике эффективное фокусное расстояние (EFL) линзы, если в конструкции применяется одна линза для коллимации, как правило не будет превышать 10 мм. Отдельные производители применяют систему из двух линз для уменьшения сферических аберраций. В таком случае по формуле (1) для расчета фокусного расстояния системы двух линз можно оценить, что фокусное расстояние отдельной линзы обычно не будет превышать 20 мм.

$$BFL = \frac{f_2(d - f_1)}{d - (f_1 + f_2)}, \quad (1)$$

где d – расстояние между вершинами линз; f_1 и f_2 – фокусное расстояние линз.

Пример конструкции TOSA изображен на рис. 2.

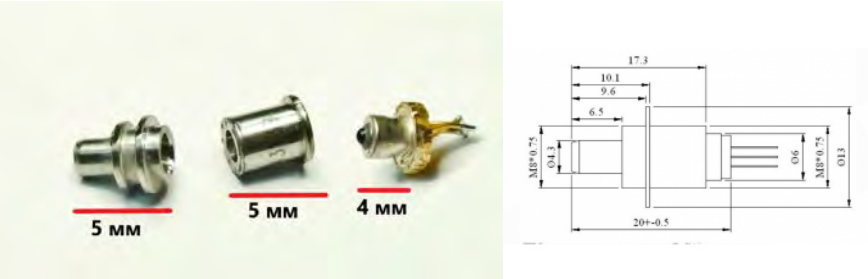


Рис. 2. Конструкция TOSA

Лазерные диоды с волоконным выводом устроены не так, как TOSA. Поскольку волокно сразу заводится в лазер, то в некоторых конструкциях оптоволокно подводится довольно близко к лазеру и между ними устанавливают линзы для коллимации быстрой оси (FAC) с малым BFL/FFL, которые имеют асферическую цилиндрическую форму.

В наиболее сложных конструкциях используются: зеркала; линзы для коллимации FAC; линзы для коллимации медленной оси (SAC); рассеивающие; цилиндрические линзы для исправления формы пучка и призмы для отвода части сигнала на встроенный рядом фотодиод для мониторинга параметров лазерного диода.

Конструкция лазерного диода с волоконным выводом, представлена на рис. 3 (см. ниже). Оценивая EFL по формуле (1) для системы из 2 линз, имеет значение не превышающие 40 мм.

Следует отметить в целом, что в оптических приборах, где сигнал заводится или выводится из оптоволокна, нет смысла использовать коллимирующие и фокусирующие сигнал линзы с большим фокусным расстоянием,

поскольку обычно системы сами по себе устроены так, что эти линзы довольно близко расположены к фотодиоду, светодиоду и ко входу/выходу оптоволокна, где и требуются линзы с малым фокусным расстоянием для коллимации или фокусировки луча из светодиода или оптического волокна или фокусировки луча в оптическое волокно. А призмы и зеркала уже направляют луч.

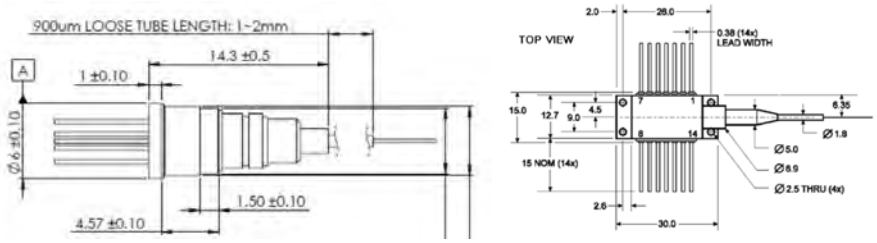


Рис. 3. Конструкция лазерного диода с волоконным выводом

Таким образом, можно сказать, что в сфере ОСП в основном используются сферические и асферические линзы: с радиусом кривизны 0,5–3 мм; EFL, BFL, FFL равными 0–40 мм; шариковые линзы, линзы для коллимации FAC; линзы для коллимации SAC; плоско-выпуклы; цилиндрические. Также имеет место применения призм и зеркал.

Вторым параметром является коэффициент преломления.

При анализе литературы оптических материалов на рынке для производства линз [7] крайне мало материалов имеют коэффициент преломления выше 2. Это связано с тем, что прозрачные материалы с таким показателем преломления дороже производить, и есть альтернатива в виде сборок линз или шариковых линз.

Шариковая форма линз позволяет максимально уменьшить BFL, FFL и EFL для выбранного материала. Такие линзы тривиальны в технологии изготовления, что делает процесс массового производства гораздо дешевле и позволяет добиваться довольно высокого качества с малыми погрешностями, в основном по этой причине шариковые линзы активно используются в технологии Expanded Beam.

Эффективное фокусное расстояние шариковой линзы (EFL):

$$EFL = \frac{n * 2R}{4(n-1)}, \quad (2)$$

Заднее фокусное расстояние шарового объектива (BFL):

$$BFL = EFL - R, \quad (3)$$

где R – радиус шариковой линзы; n – показатель преломления.

Чтобы $BFL = 0$, необходимо, чтобы $EFL = R$. Это происходит только в том случае, когда показатель преломления материала $n = 2$, независимо

от радиуса самой линзы. На рис. 4 представлена зависимость показателя преломления *n* от заднего фокусного расстояния *BFL*.

Третьим параметром является погрешность измерения *BFL*, *FFL*, *EFL*.

Поскольку в устройствах для ОСП используются линзы с довольно малым фокусным расстоянием, а то и с *BFL* ≈ 0 мм, то рассчитаем допустимую погрешность для такого показателя.

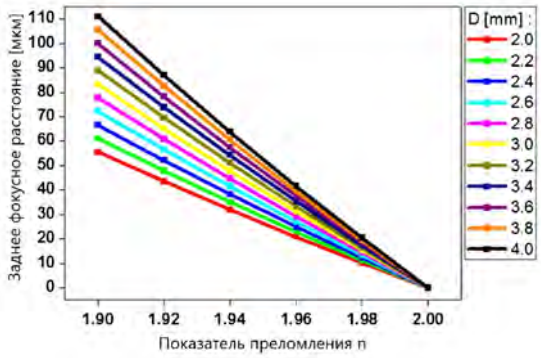


Рис. 4. Зависимость BFL шариковой линзы от показателя преломления

В ходе моделирования в программе COMSOL Multiphysics 6.0 было выяснено, что при коллимировании пучка в оптоволокно шариковой линзой с *BFL* = 0, *n* = 2, *R* = 1,5 с допустимым затуханием в 1,5 дБ для технологии Expanded Beam, допустимая погрешность показателя преломления линзы равна Δn = ±0,025. Пересчитаем эти данные в допустимую погрешность BFL по формуле 2 и получим значения равные от +0,0192 мм до −0,0182 мм. Как видно, приборы могут обладать довольно высокой погрешность по позиционированию оси *z* для нашего случая.

Если требуются более низкие потери при фокусировке пучка в оптоволокно, нежели 1,5 дБ, то погрешность можно пересчитать.

Приборы для измерения параметров линз делятся на разные типы: сферометры, гониометры призм и зеркал, приборы для центрирования и склейки линз, приборы, измеряющие оптические или геометрические характеристики линз. Рассмотрим наиболее подходящие приборы различных компаний с акцентом на измерение оптических характеристик линз и сравним их с рассмотренными требованиями. Приборы для измерения параметров линз в микрооптике представлены в таблице 1 [8, 9, 10, 11, 12]. Представленные на рынке приборы имеют высокоточные осевые двигатели, поэтому погрешность по позиционированию вноситься в сводную таблицу не будет. Все значения берутся с учетом предлагаемой опциональной возможности модернизировать оборудование.

Данные приборы предназначены для измерения параметров линз, но они лишь частично удовлетворяют требованиям измерения микрооптики, применяемой в ОСП, в том числе не в полной мере отвечают требованиям технологии Expanded Beam из-за трудностей с измерением BFL линз, которые обычно равны менее 1 мм. Прибор LensCheck конструктивно подходит для измерения параметров объективов, чем для микрооптики, из-за горизонтального способа размещения.

ТАБЛИЦА 1. Приборы для измерения параметров линз в микрооптике

Приборы / Требования	OTS 200	LensCheck	MELOS 530	OptiSpheric	IAM-BT
Измерение *BFL*, *FFL* и *EFL* от 0 до 40 мм соответственно	+ (?) ...+530мм - (?) ...-530мм ± (?) ... ±530мм	от 0 мм	+2 ...+530мм - ±1 ... ±115мм	+3 ...+250мм -3 ...-250мм ±3 ... ±250мм	+5 ...+50мм -5 ...-15мм ±5 ...+50/-15мм
Измерение линз диаметром от 0.5 … 3 мм	от 1 мм	от 1,5 мм	от 1 мм	от 0,5 мм	от 0,5 мм

Таким образом, возникает необходимость разработать новое или модернизировать имеющееся оборудование с решением следующих вопросов: измерения линз диаметром от 0,5 мм или от меньшего диаметра; измерение *BFL* (*FFL*) от 0 мм; *EFL* от 0,5 мм или от меньшего значения.

Список используемых источников

1. Выбор оптики для коллимации и коррекции эллиптичности пучка излучения лазерного диода [Электронный ресурс]. URL: https://azimp.ru/articles/tech/ 82179/ ?ysclid=lcl97qfog8104448736 (дата обращения 20.03.2023).

2. Лазерные диоды с волоконным выводом [Электронный ресурс]. URL: https://in-science.ru/library/article_post/lazernye-diody-s-volokonnym-vyvodom?ysclid=lcqux08sck 381905997 (дата обращения 20.03.2023).

3. Edward Simonini, James Douthit. Expanded Beam & Physical Contact Fiber Optic Connectors. URL: https://amphenol-ns.com/Blog/post/expanded-beam-physical-contact-fiber-optic-connectors (дата обращения 24.03.2023).

4. Optical design of 4-channel TOSA/ROSA for CWDM applications – art. no. 68990I [Электронный ресурс]. URL: https://www.researchgate.net/publication/242244230_ Optical_ design_of_4-channel_TOSAROSA_for_CWDM_applications_-_art_no_68990I (дата обращения 21.03.2023).

5. Contamination Effects on Lens-Based Optics Modeling and Experimental Analysis [Электронный ресурс]. URL: https://thor.inemi.org/webdownload/newsroom/ Presentations/ OFC_ NFOEC_09/OFC09_poster.pdf (дата обращения 21.03.2023).

6. High Assembly Tolerance and Cost-Effective 100-Gb/s TOSA With Silica-PLC AWG Multiplexer [Электронный ресурс]. URL: https://ieeexplore.ieee.org/stamp/ stamp.jsp? arnumber=8742533 (дата обращения 21.03.2023).

7. nd-vd Diagramm [Электронный ресурс]. URL: https://www.ohara-gmbh.com/ en/shop/nd-vd-diagram.html

8. Optics Test Stations for single lenses and optical systems [Электронный ресурс]. URL: https://www.oeggmbh.com/?p=12&k=14&kj=&z=&l=1 (дата обращения 23.03.2023).

9. Optikos Corporation [Электронный ресурс]. URL: https://www.optikos.com/lens-testing-equipment/ (дата обращения 23.03.2023).

10. Measuring Equipment for Optical Systems: MELOS 530 [Электронный ресурс]. URL: https://www.haag-streit.com/moeller-wedel-optical/products/optical-testing-instruments/ measuring-equipment-for-optical-systems-melos/ (дата обращения 23.03.2023).

11. OptiSpheric [Электронный ресурс]. URL: https://trioptics.com.sg/optispheric/

12. IAM-BT image Analysis Measurement [Электронный ресурс]. URL: https://www.optoalignment.com/iam-bt (дата обращения 23.03.2023).

УДК 004.056.57
ГРНТИ 81.93.29

МОДЕРНИЗАЦИЯ СИСТЕМЫ ЗАКРЫТОГО КОНТУРА ЛВС ОТЕЧЕСТВЕННЫМИ КОМПЛЕКСАМИ РАЗГРАНИЧЕНИЯ ДОСТУПА

А. М. Зверев, О. И. Шелухин

Московский технический университет связи и информатики

Внедрение аппаратно-программного комплекса шифрования в локальные сети является универсальным средством для обеспечения защиты корпоративной сети и конфиденциальной информации. Но немаловажным фактором является подготовка специалистов. Когда речь идёт об обучении пользоваться данным АПКШ, возникает необходимость в создании виртуальной среды, в которой можно практиковаться, не нарушая закон и целостность компьютерных сетей и систем. Для этого существует возможность разворачивать виртуальную инфраструктуру Континента, где можно научиться настраивать сетевые устройства комплекса и их защитные механизмы.

АКПШ Континент, индустрия 4.0, криптошлюз, лабораторный стенд.

Информация – это сведения об окружающем нас мире. О происходящих в нем действий и явлениях, воспринимаемые живыми существами и техническими устройствами. **Передача информации** – физический процесс, с помощью которого осуществляется перемещение информации в сетевом пространстве. Наиболее распространенным и древним способом передачи информации между людьми является устная речь, с появлением письменности – книги. Для передачи информации на большое расстояние используется электронная почта, телефонные линии, телевидение. На сегодняшний момент для передачи информации, используются сетевые информационные технологии [4].

1. Обосновать актуальность разрабатываемой методики.

2. Собрать необходимый материал по выбранной теме магистерской диссертации: «Модернизация системы закрытого контура ЛВС отечественными программными комплексами разграничения доступа».

3. Изучить принципы и способы резервирования сетевых устройств.

4. Рассмотреть основные нововведения в Четвертой промышленной революции.

5. Подготовить лабораторный стенд.

В текущее время, когда сети и Интернет все больше внедряются в Нашу жизнь, как комфортное средство коммуникаций, наряду с ними появляется потребность в организации защиты локальных сетей и конфиденциальной

информации. Такой подход позволяет осуществлять криптографическую защиту информации при её передаче между локальными вычислительными сетями и их сегментами. Также для защиты от проникновения несанкционированного доступа со стороны сетей общего пользования используются известные защитные механизмы такие как: фильтрация пакетов, трансляция адресов, VPN и т. п. При работе с комплексом могут возникать проблемы и непредвиденные сбои, поэтому в системе рекомендуется организовывать резервный канал связи. В таком случае, локальные сети должны незамедлительно переключаться на него и таким образом передаваемые данные не будут утеряны [4].

Исходя из этого, можно сказать, что внедрение аппаратно-программного комплекса шифрования в локальные сети является универсальным средством для обеспечения защиты корпоративной сети и конфиденциальной информации. Но немаловажным фактором является подготовка специалистов. Когда речь идёт об обучении пользоваться данным АПКШ, возникает необходимость в создании виртуальной среды, в которой можно практиковаться, не нарушая закон и целостность компьютерных сетей и систем. Для этого существует возможность разворачивать виртуальную инфраструктуру Континента, где можно научиться настраивать сетевые устройства комплекса и их защитные механизмы [5].

Создание резервного криптошлюза

При создании резервного криптошлюза, параметры сети остаются такими же, как и для основного. Все пакеты проходят по тем же ip-адресам. Различие только в том, что создаётся подсеть для резервирования между основным и резервным КШ, и при сбое основного весь трафик будет проходить через резервный [2]. На рис. 1 представлена схема для резервирования криптошлюза.

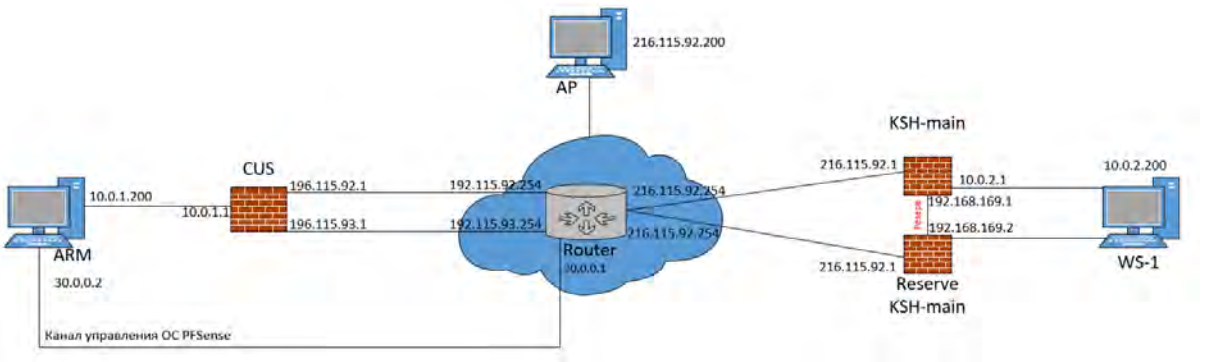


Рис. 1. Схема для создания резервного криптошлюза

Создание резервного центра управления сетью

При создании резервного ЦУС параметры для него не будут совпадать с основным, как это происходит при резервировании криптошлюза. Но внешние и внутренние интерфейсы резервного будут находиться в одной сети с интерфейсами основного ЦУС. Ниже на рис. 2 представлена схема для резервирования ЦУС.

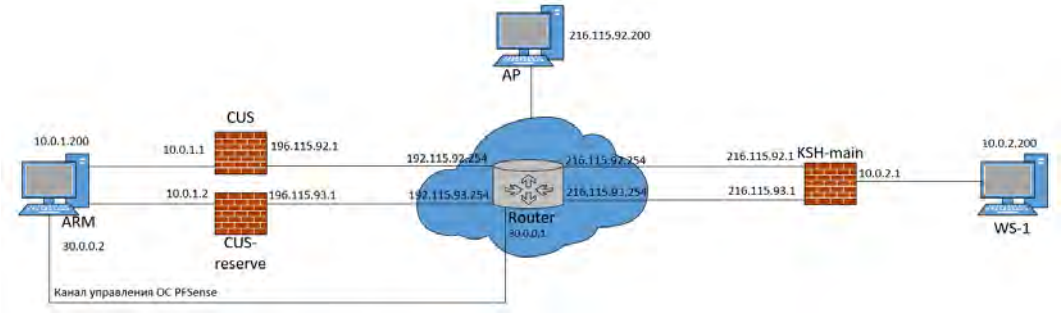


Рис. 2. Схема для создания резервного центра управления сетью.

Четвертая промышленная индустрия

Четвертая промышленная революция (Индустрия 4.0) предполагает новый подход к производству, основанный на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и распространение искусственного интеллекта [1].

Преимущества Четвертой промышленной революции очевидны:

- повышение производительности, большая безопасность работников за счет сокращения рабочих мест в опасных условиях труда;
- повышение конкурентоспособности, принципиально новые продукты и много другое [3].

На рис. 3 представлено содержание Индустрии 4.0 и её развитие.

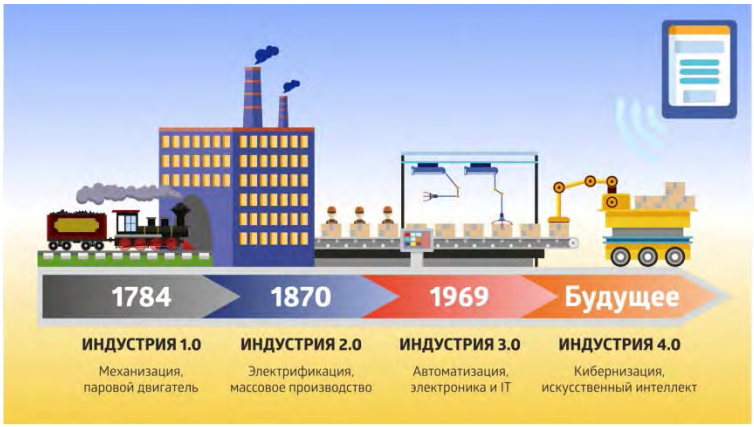


Рис. 3. Содержание и развитие индустрии 4.0

Лабораторный стенд «Инициализация криптошюза»

Создание криптошлюза представлено на рис. 4. Настройка внешнего IP-адреса показана на рис. 5.

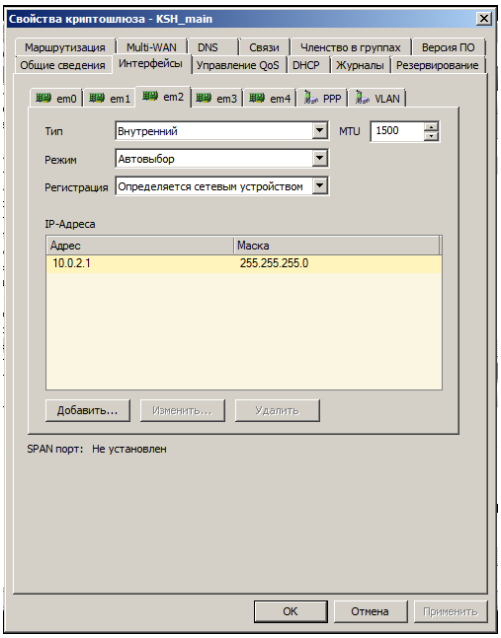


Рис. 4. Окно создания криптошюза

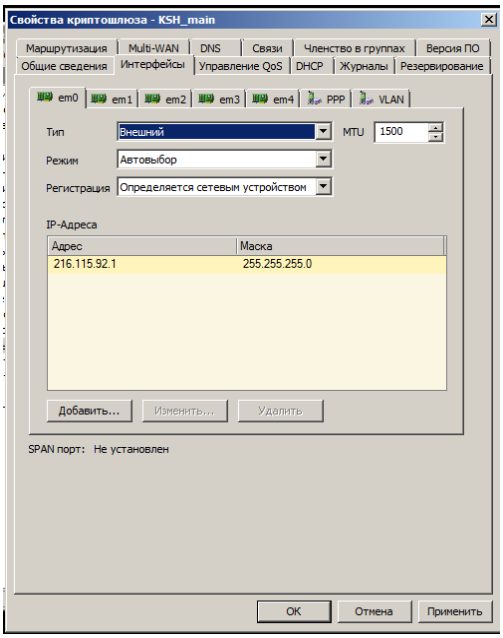


Рис. 5. Окно настройки интерфейса em0

Настройка внутреннего IP-адреса представлена на рис. 6. Результат стенда показан на рис. 7.

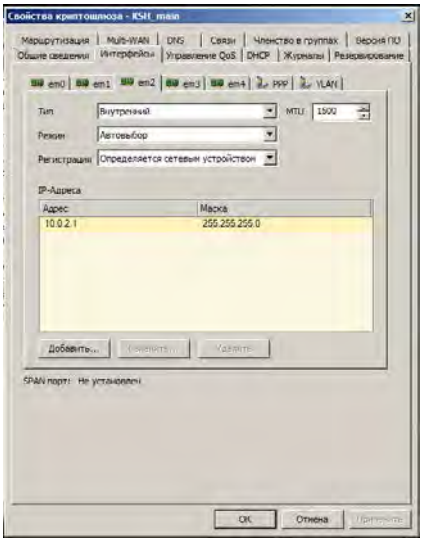


Рис. 6. Окно настройки интерфейса em2

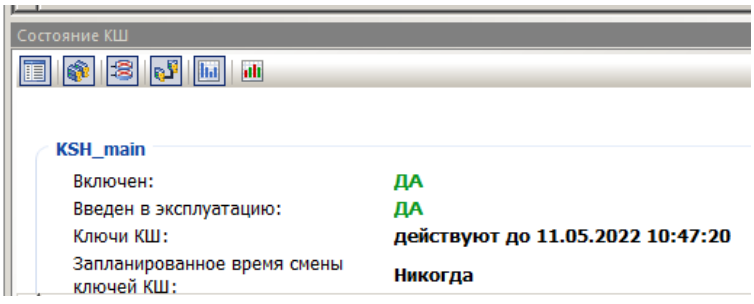


Рис. 7. Результат стенда №1

Список используемых источников

1. Петренко С. А., Киберустойчивость Индустрии 4.0: научная монография. СПб. : «Издательский Дом «Афина», 2020. 256 с.

2. Основы применения АКПШ «Континент» для организации сетевой защиты: учебно-методическое пособие // Код Безопасности. 2017. 146 с.

3. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. 2018. N 3 (15). С. 47–54.

4. Штеренберг С. И., Данилова Ю. С. Разработка методики внедрения скрытой подписи кода в GITLAB // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. N 3. 2022. С. 44–49.

5. Штеренберг С. И., Пестов И. Е., Казаков Д. Б., Ильин М. В. Основные рекомендации для организаций перед переносом своих данных в облачную среду. Анализ эффективности на примере ЗКУ РВС // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 1. С. 26–36.

УДК 004.056
ГРНТИ 81.96

АРХИТЕКТУРА И РЕАЛИЗАЦИЯ ПРОТОТИПА МОДУЛЯ ВЫЯВЛЕНИЯ МНОГОШАГОВЫХ АТАК ПРИ ПОМОЩИ КРАТКОСРОЧНОГО И ДОЛГОСРОЧНОГО АНАЛИЗА

И. Ю. Зеличенок, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В условиях стремительно вырастающего потока данных, выявление малозаметных угроз информационной безопасности, реализуемых на нескольких этапах, становится все более сложным. При автоматизации процесса многошаговых атак при большом потоке данных важное значение имеет использование технологий машинного обучения и обработки больших данных. В работе предлагается архитектура модуля обнаружения многошаговых атак, которая базируется на этих технологиях и состоит из двух компонентов: подсистемы краткосрочного анализа данных, выявляющей атаки в реальном времени, однако ограниченной коротким временным окном, и подсистемы долгосрочного анализа, реконструирующей сценарии на основе данных, предоставленных модулем краткосрочного информирования. Модель машинного обучения делает окончательный вывод о проведенной многошаговой атаке. Представляется также первоначальная реализация данного модуля.

информационная безопасность, кибер-атаки, многошаговые атаки, выявление атак.

Современные средства обнаружения многошаговых атак имеют большое разнообразие реализаций, основанных на разных алгоритмах и используемых технологиях [1, 2, 3, 4]. При стремительно растущем информационном потоке на всех уровнях, с каждым годом становится все труднее обнаружить взаимосвязи, релевантные атакам, при помощи оператора, статистики или при помощи правил. Машинное обучение позволяет обнаруживать неочевидные признаки [5], актуальные для текущей или потенциальной атаки, а технологии обработки больших данных позволяют получать и обрабатывать такой поток данных в реальном времени.

В работе представлена архитектура модуля обнаружения многошаговых атак, которая базируется на этих технологиях и состоит из двух компонентов: подсистемы краткосрочного анализа данных и подсистемы долгосрочного анализа, реконструирующей сценарии на основе данных, предоставленных модулем краткосрочного информирования. Модель машинного обучения делает окончательный вывод о проведенной многошаговой атаке.

На рис. 1. представлена архитектура прототипа модуля обнаружения многошаговых атак, состоящая из нескольких элементов:

- агенты (*Agent* 1 … *n*);
- потоковый обработчик событий. (*Processing stream* 1 … *n*);
- модуль краткосрочного анализа (*e1, STIM*);
- модуль долгосрочного анализа (*e2*, *LTIM*);
- база данных (*DB*).

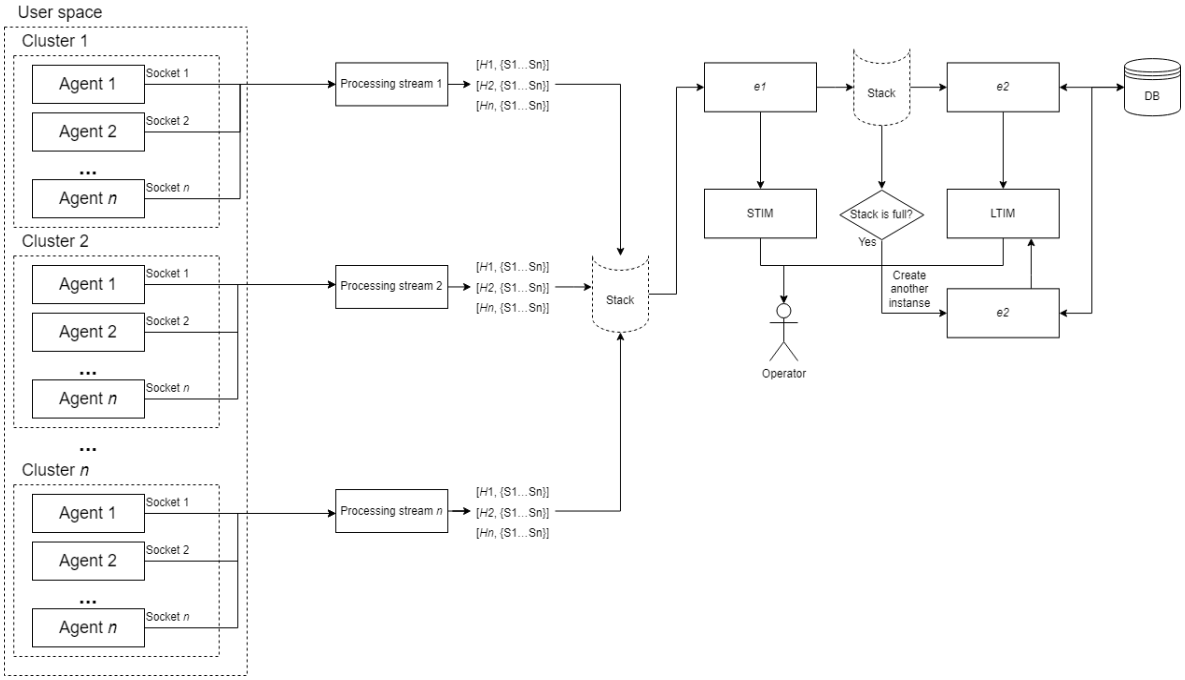


Рис. 1. Архитектура представленного модуля выявления многошаговых атак

Агентская система [6, 7] собирает данные о состоянии виртуальной машины на сетевом уровне [8] и делает ее первичную предобработку, например, отсечение лишних данных, перевод текстовых значений в числовые.

Далее, поток событий по HTTP [9] перенаправляется в модуль *Processing stream* (PS), в котором делается более ресурсозатратная обработка - приведение данных к единому виду (унификация событий, собранных на других уровнях).

Затем получаемая информация за период t из одиночных событий информационной безопасности формирует цепочки, что позволяет делать выводы именно на последовательностях (1, 2):

$$s = [H_1, H_2, \dots, H_n] \quad (1)$$

$$H_n = [S_1, S_2, \dots, S_n] \quad (2)$$

где S_{1-n} – одиночные события из одного источника, H_{1-n} – цепочки одиночных событий, агрегированные по узлам сети, s – конечный поток событий.

При перегрузке PS повышенным потоком данных от агентов, создается дополнительный экземпляр обработчика потока, а часть агентов переходит в дополнительный кластер, тем самым снижая нагрузку на отдельный поток CPU.

Сформированный поток событий s поступает на модуль краткосрочного анализа (e_1), состоящий из нейросети с LSTM (*Long short-term memory*) [10], позволяющей делать оценку о проводимой атаке (или ее отсутствии) на основе анализа блока данных. Она собирает данные за короткие промежутки времени ($t_{\text{кор}}$) и дает оценку ситуации в реальном времени. На данный момент анализируется 13 наиболее важных сетевых параметров и делается оценка об одном типе проведенной атаки (13 входных и 2 выходных параметра).

Модуль долгосрочного анализа (e_1) позволяет реконструировать потенциальную

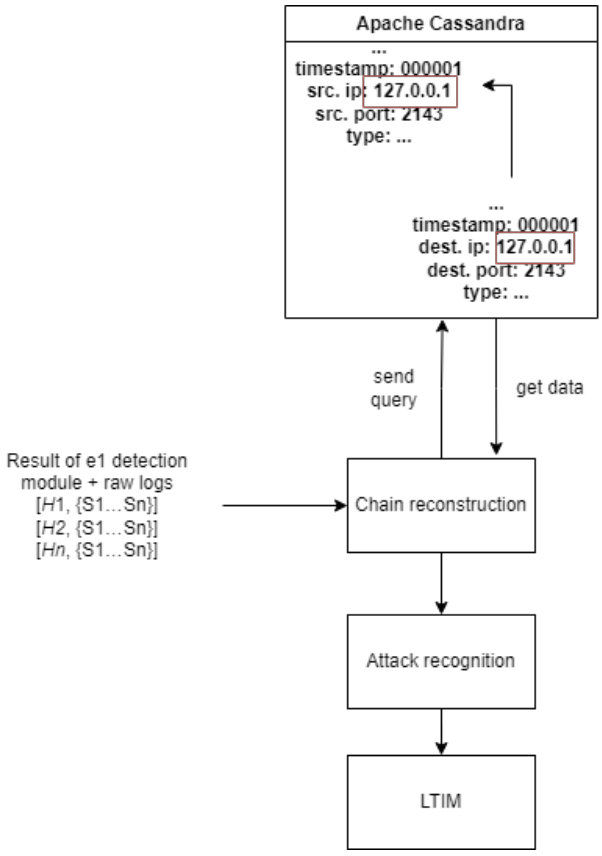


Рис. 2. Процесс реконструкции сценария

атаку (рис. 2, см. выше) на основе анализа исторических данных, хранящихся в базе данных. На основе этих данных составляется последовательность событий с длительным периодом ($t_{\text{длин}}$), а затем модель машинного обучения на основе этих данных выдвигает предположение о совершенной или потенциальной атаке.

Как и в случае с PS, при перегрузке модуля долгосрочного анализа, создаются дополнительные экземпляры процесса, что позволяет своевременно реагировать на выявление потенциальных угроз.

В качестве вспомогательных модулей используются STIM (*Short-term information module*) и LTIM (Long-*term information module*). Эти модули занимаются агрегацией результатов обнаружения модулями e_1, e_2 и доведением их до оператора.

По результатам экспериментов (табл. 1), лучший показанный результат по целевой метрике был $f_1 \sim 0.85$ на модели краткосрочного анализа.

ТАБЛИЦА 1. Выборка из результатов тестирования

Precision	Recall	F1	Accuracy
0.8354	0.8751	0.8561	0.8500
0.8232	0.7662	0.8123	0.8265
0.7976	0.8587	0.8352	0.8318

Результат модели долгосрочного анализа содержал в себе большое количество ложноположительных срабатываний в конечном предупреждении.

Полнота информации, поставляемой оператору, а также точность, с которой будет обнаруживаться атака, является наиболее важным аспектом в текущей архитектуре. Предложенный подход позволит не только отследить прошлые шаги и предупредить о текущей атаке, но и предотвратить будущие пути распространения угрозы.

Количество ложноположительных срабатываний и F-меру планируется корректировать путем усовершенствования моделей машинного обучения, а также путем более тщательного отбора характерных признаков.

В дальнейшем планируется расширить функционал и скорость работы путем добавления новых уровней сбора данных, введения стриминговых протоколов.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список использованных источников

1. Ramaki A. A., Rasoolzadegan A., Bafghi A. G. A systematic mapping study on intrusion alert analysis in intrusion detection systems // ACM Computing Surveys (CSUR), 2018, Vol. 51, N 3. PP. 1–41.

2. Husák M. et al. Survey of attack projection, prediction, and forecasting in cyber security // IEEE Communications Surveys & Tutorials. 2018. Vol. 21, N 1. PP. 640–660.

3. Kovačević I., Groš S., Slovenec K. Systematic Review and Quantitative Comparison of Cyberattack Scenario Detection and Projection // Electronics, 2020, T. 9, N 10. PP. 17–22.

4. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol. 8407. PP. 462–471.

5. Kotenko I., Chechulin A. Computer Attack Modeling and Security Evaluation based on Attack Graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013. 2013. PP. 614–619.

6. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. N 11. С. 993–1001.

7. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. N 2. С. 7–24.

8. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. 2018. Vol. 6. PP. 72714–72723.

9. Manganiello F., Marchetti M., Colajanni M. Multistep attack detection and alert correlation in intrusion detection systems // International Conference on Information Security and Assurance. Springer, Berlin, Heidelberg, 2011. PP. 101–110.

10. Jia B. et al. Bidirectional RNN-Based Few-Shot Training for Detecting Multi-stage Attack // International Conference on Information Security and Cryptology. Springer, Cham, 2020. PP. 37–52.

УДК 004.056
ГРНТИ 50.41.25

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ПО ОГРАНИЧЕНИЮ ЗАПУСКАЕМЫХ ПОЛЬЗОВАТЕЛЯМИ ПРИЛОЖЕНИЙ

Д. С. Золотова, А. И. Катасонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В наши дни с увеличением объемов передаваемой информации растут и требования к обеспечению безопасности этих данных. Злоумышленники разрабатывают все но-

вые методы получения несанкционированного доступа к операционным системам с целью получения доступа, нанесения ущерба секретной информации. Одним из наиболее уязвимых узлов, которыми пользуются злоумышленники, является персонал компании, которые могут открыть зараженное приложение или перейти по фишинговой ссылке. Для обеспечения безопасности от такого рода атак предлагается использовать технологии для ограничения пользователям запускаемых приложений. В данной работе проведён сбор, определены характерные особенности и составлена сравнительная таблица средств по ограничению запускаемых пользователями приложений.

ограничение доступа; приложения; Deskman; Security Administrator. WinLock.

Вопрос ограничения доступа к компьютеру и хранящимся на нем данным в той или иной мере актуален для всех компьютерных пользователей. Рассмотрим 2 случая, из-за которых было бы желательно использовать средства ограничения доступа. Первый случай: если компьютером пользуется человек, который не разбирается в компьютерах. При неосторожном и невнимательном использовании компьютера могут возникнуть проблемы в работе отдельных приложений либо операционной системы. Например, если случайно удалить принтер, то тогда печать документов окажется невозможной, изменить сетевые настройки – и компьютер перестанет работать в локальной сети. Второй случай: сотрудники компаний. Необходимость блокирования доступа к включенному компьютеру в отсутствие законного пользователя в офисе, ведь даже при наличии собственного компьютера пользователь не может находиться рядом с ним постоянно и нередки ситуации, когда включенный компьютер оказывается без присмотра, чем могут воспользоваться находящиеся рядом люди.

Средства ограничения доступа – это технологии, которые могут препятствовать вредоносному ПО. Существуют коммерческие готовые системы ограничения доступа к приложениям на ПК, которые пользователи могут установить и использовать. Рассмотрим 3 программы по ограничению доступа, этого количества будет достаточно для дальнейшего вывода о функциональных возможностях подобных программ.

Начнём с Deskman. Это программа, которая помогает ограничить доступ к Windows, защищая ПК от несанкционированного доступа. Раздел Restrictions разделен на подразделы: рабочий стол, система, меню «Пуск», приложения, Веб и папки.

В подразделе Desktop, например, можно отключить возможность редактировать или удалять файлы рабочего стола, блокировать компьютер, когда пользователь простаивает в течение X минут, отключить разные комбинации клавиш (рис. 1, см. ниже).

В подразделе System можно отключить доступ к настройкам Windows и панели управления, заблокировать доступ к проводнику файлов и анало-

гичным ему устройствам, таким как Панель управления и другие окна конфигурации системы, отключить доступ к параметрам папки в проводнике (рис. 2).

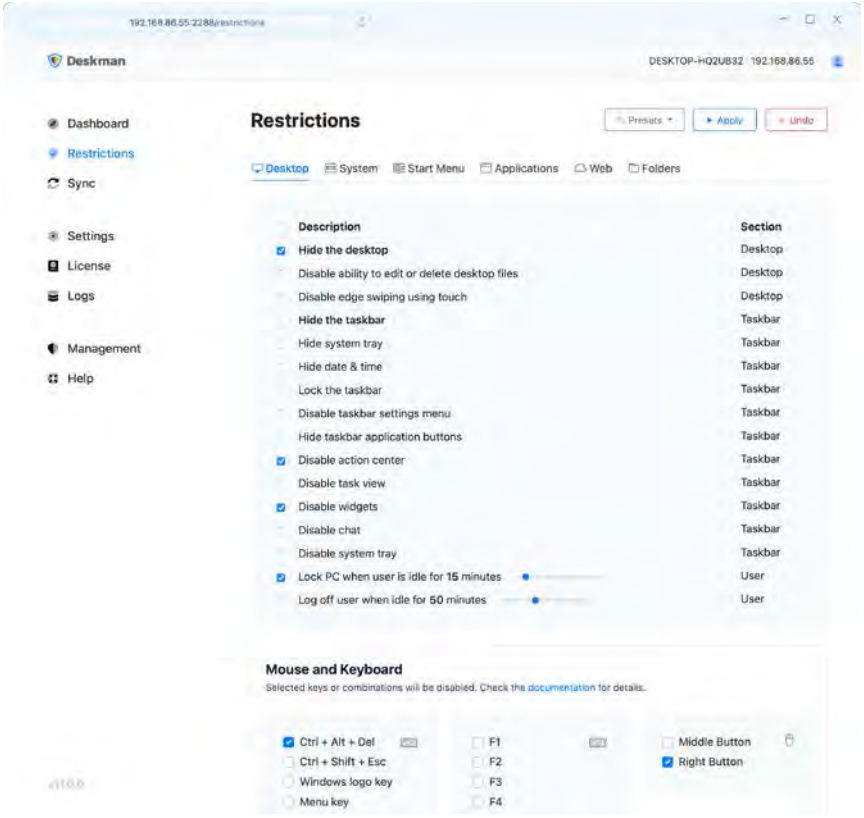


Рис. 1. Подраздел Desktop

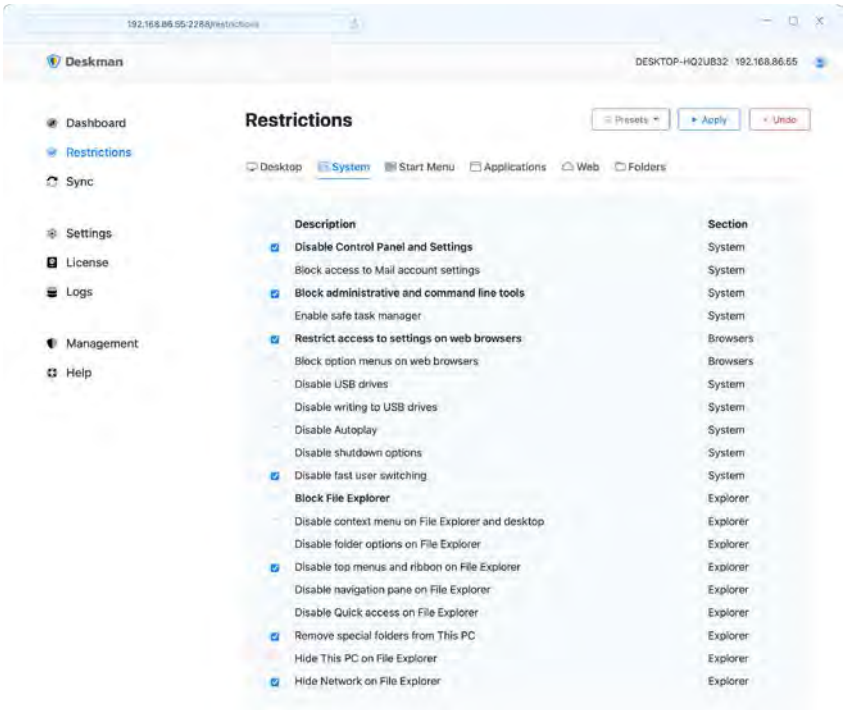


Рис. 2. Подраздел System

В подразделе Start Menu можно блокировать возможность изменения приложений, завершения работы или выхода из системы, отключить доступ к списку приложений в меню «Пуск» [1].

Пользовательское меню «Пуск». Этот раздел позволяет создать свое собственное меню «Пуск». Как только пользовательское меню «Пуск» установлено, исходное меню «Пуск» остается скрытым, сохраняется и возвращается в нормальное состояние после отключения этой опции [1].

Подраздел Web представляет собой программный фильтр, который позволяет остановить нежелательные приложения и заблокировать приложения, добавляя разрешенные исполняемые файлы или папки [1].

Также есть раздел Журнал событий (*Logs*), который содержит заблокированные приложения, отфильтрованные веб-сайты, активность пользователей, изменения конфигурации и предупреждения об использовании [1].

Это далеко не все функции, которые есть в Deskman, поэтому более подробно с возможностями этой программы можно ознакомиться на официальном сайте. Но даже исходя из того, что было рассмотрено, можно сделать вывод, что Deskman – это инструмент безопасности, который позволяет администраторам комбинировать ограничения для достижения желаемого уровня безопасности [2].

Теперь рассмотрим программу Security Administrator, предназначенную для ограничения доступа и настройки параметров безопасности ОС.

Программа содержит 2 раздела: общие (*Common Restrictions*) и пользовательские ограничения (*User Restrictions*).

В разделе Common Restrictions – параметры и подразделы, которые касаются всех пользователей системы. К ним относятся загрузка и вход в систему, сеть, Проводник, Интернет, система, Панель управления и другие.

У каждого подраздела можно настроить свои ограничения. Например, в подразделе System можно настроить автоматическую перезагрузку Windows после сбоя, отключить контроль доступа к учетной записи пользователя и так далее.

В разделе User Restrictions можно настроить индивидуальный уровень доступа каждому пользователю Windows. В список ограничений входят разделы Панели управления, элементы интерфейса, кнопки, горячие клавиши, съемные носители и др.

Если рассматривать эту программу как средство для ограничения доступа, то она позволяет настроить запрет на использование к элементам панели управления, отключить пункты меню "Пуск", скрыть диски и настольные значки, можно также скрыть системную панель и заблокировать компьютер паролем, установить ограничений на запуск определенных приложений [3].

Последняя обозреваемая программа WinLock, представленная на рис. 4, состоит из 5 разделов: Общее (*General*), Система (*System*), Интернет (*Internet*), Доступ (*Access*), Таймер (*Timer*).

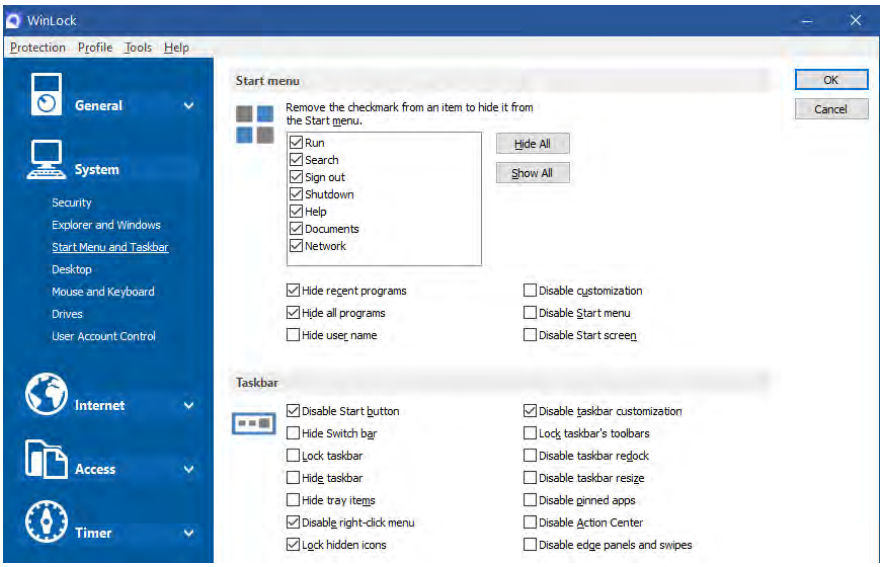


Рис. 3. Интерфейс программы WinLock

В разделе System можно настроить проводник, скрыв меню параметров папки или отключив контекстное меню, вызываемое правой кнопкой мыши. В подразделе «Drives» можно запретить отображение указанных дисков в компьютере или проводнике и полностью блокировать доступ к съемным дискам [4].

В разделе «Access» доступно управление приложениями, например, можно внести необходимое приложение в черный список по названию либо ручным добавлением, можно заблокировать как всё приложение, так и его часть: окно, всплывающее сообщение, диалоговое окно. Также можно запретить пользователям устанавливать какое-либо программное обеспечение. В подразделах «Файлы» и «Папки» можно поместить данные, которые необходимо скрыть от других пользователей [4].

WinLock поддерживает настраиваемый журнал событий, а значит любые изменения в системе будут зафиксированы и при желании отправлены на почту.

В ходе проведённого сравнительного анализа, была составлена таблица 1, из которой видно, что, все рассмотренные программы подходят для использования в качестве ограничения доступа к приложениям на ПК, так как содержат основные и необходимые функции, при правильном использовании которых можно построить хорошую защиту от несанкционированного доступа. Но следует обратить внимание на версию ОС, так как не все программы поддерживают Windows 10, 11.

ТАБЛИЦА 1. Сравнение функциональных возможностей программ

	Deskman	Security Administrator	WinLock
Ограничение доступа к папкам и приложениям	+	+	+
Блокировка доступа к определенным сайтам	+	+	+
Блокировка/скрытие диска	+	+	+
Журнал событий	+	+	+
Версия ОС	Windows 10, 11	Windows 7, Vista, XP	Windows 2000 Windows Server Windows XP, Vista Windows 7, 8, 10, 11
Стоимость	163 евро в год	69 долларов – лицензия	31,95 долларов – лицензия

Список используемых источников

1. Документы Deskman. URL: http://www.anfibia-soft.com/docs/11/ (дата обращения 15.03.2023).

2. Deskman | Менеджер безопасности рабочего стола для Windows. URL: http://www.anfibia-soft.com/ (дата обращения 15.03.2023).

3. Администратор безопасности – Интерактивная справка. URL: https://www.softheap.com/secagent.html (дата обращения 20.03.2023).

4. WinLock | Офисные системы Crystal. URL: https://www.crystaloffice.com/winlock/?utm_source=ixbtcom (дата обращения 21.03.2023).

Статья представлена заведующим кафедрой ЗСС СПБГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056
ГРНТИ 81.93.29

СРАВНЕНИЕ СИСТЕМ ВИРТУАЛИЗАЦИИ ПК СВ «БРЕСТ» И VMWARE

П. С. Зылева, И. Е. Пестов, И. С. Тремель, У. С. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Все большее применение в IT сфере находит виртуализация. Она обеспечивает снижение стоимости обслуживания, позволяет проводить тестирование новых си-

стем, повышает уровень безопасности, помогает повысить адаптивность, производительность, доступность, гибкость и масштабируемость ИТ-среды. При виртуализации возможности оборудования реализуются с помощью программного обеспечения и создается виртуальная компьютерная система. Благодаря этому ИТ-отделы могут использовать несколько виртуальных систем (несколько операционных систем и приложений) на одном сервере. В связи с уходом из страны зарубежных поставщиков систем виртуализации, актуально сравнительное исследование российской системы аппаратной виртуализации с ушедшими иностранными решениями, чтобы предоставить подробную информацию о сходствах и различиях для устранения проблем.

виртуализация, аппаратная виртуализация, ПК СВ «Брест», VMware, VMware vSphere, Astra Linux, импортозамещение, информационная безопасность.

Виртуализация серверов стала важной частью каждой современной информационной системы, имея несомненные преимущества в сравнении с классической инфраструктурой. Виртуализация дает возможность уменьшить количество серверов, уменьшить энергопотребление и понизить стоимость инфраструктуры и ее обслуживания, что оптимизирует адаптивность и рабочие нагрузки системы [1]. Этот подход позволяет экономить при масштабировании и повышение эффективности.

Аппаратная виртуализация

Виртуальная компьютерная система или виртуальная машина (ВМ), – это строго изолированный контейнер программного обеспечения (ПО), который содержит операционную систему (ОС) и приложения. При размещении нескольких ВМ на одном компьютере обеспечивается работа нескольких ОС и приложений на одном физическом сервере, так же называемом узле или хосте. ВМ на одной физической платформе может быть несколько, при этом каждая ВМ функционирует под управлением собственной ОС и обеспечена собственными виртуальными аппаратными компонентами: памятью, процессором, жестким диском, сетевыми адаптерами. Данные ресурсы резервируются ВМ за счет физических ресурсов аппаратного обеспечения компьютера [2, 3]. Гипервизор – ПО, создающее ВМ и управляющее ими. На практике на ВМ могут применяться разные операционные системы для разных целей – к примеру, Windows Server под контроллер домена Active Directory и Debian под веб-сервер NGINX.

При аппаратной виртуализации на сервере устанавливаются гипервизор или операционная система со встроенным гипервизором с последующим предоставлением ВМ вычислительных ресурсов (виртуальные процессоры), ресурсов памяти, ресурсов дисковой и сетевой подсистем.

Аппаратная виртуализация решает задачи быстрого предоставления сервисов бизнесу, возможности использования разного окружения ОС (на одном хосте системы Linux и Windows), снижения затрат на получение новых серверов за счет утилизации существующих [4].

Программный комплекс средства виртуализации «Брест» (ПК СВ «Брест»)

ПК СВ «Брест» – инструмент, с помощью которого можно создать защищённую виртуальную среду, обеспечивающую функционирование ВМ и управление ими в ОС Astra Linux Special Edition в условиях мандатного и дискреционного разграничения доступа.

Astra Linux Special Edition – отечественная операционная система специального назначения (ОССН) на базе ядра Linux. ОССН дает возможность обеспечения защиты конфиденциальных данных и гос.тайны до уровня «особой важности» [5].

Компоненты, которые входят в состав комплекса (система управления базами данных, средства электронной почты, виртуализация, офисные средства, веб-технологии и др.) дают возможность применять его как в составе автономных ЭВМ, так и территориально-распределенных автоматизированных систем любой сложности [6].

Базовый функционал виртуализации реализован в составе ОС с помощью KVM (модуль ядра Linux), QEMU (эмуляция аппаратного обеспечения), libvirt (демон и набор инструментов для управления виртуализацией) и virt-manager (приложение для управления ВМ).

ПК СВ «Брест» обеспечивает функционирование системы виртуализации Astra Linux и позволяет централизованно управление кластером виртуализации, масштабирование IT-системы, создание защищенных сред виртуализации серверов и рабочих столов, обеспечение миграции работающих виртуальных машин между узлами кластера.

ПК СВ «Брест» решает задачи:

– Консолидации серверов или ресурсов;

– Одновременного размещения нескольких серверных ресурсов;

– Разработки и проверки информационных систем;

– Масштабирования и оптимизации сервиса или системы при увеличении нагрузки;

– Объединения локальных серверных мощностей и «облачных» вычислительных ресурсов;

– Обеспечения отказоустойчивости сервисов;

– Перераспределения нагрузки на оставшиеся ресурсы при сбое на хосте, который обеспечивает работоспособность и доступность ВМ.

В состав средств управления средой виртуализации и мониторинга ПК СВ «Брест» входит программное обеспечение OpenNebula и Virtmanager, решающие задачу создания, установки, резервного копирования, настройки, запуска и миграции виртуальных машин между узлами кластера, включая создание конфигураций, необходимых для эффективного решения задачи управления доступом встроенными в операционную систему средствами защиты информации.

VMware vSphere

VMware – вендор с несколькими продуктами, среди которых существует VMware vSphere – платформа для виртуализации. Платформа создана для оптимизации работы серверов: использование их ресурсов эффективнее, получения дополнительной гибкости управления ВМ, быстрой выдачи ресурсов под новые проекты и легкого масштабирования их под существующие. vSphere предлагает широкий набор функций, которые варьируются от организации к организации в зависимости от используемых компонентов набора. Некоторые особенности vSphere:

– Миграция рабочих нагрузок и техническое обслуживание центра обработки данных в режиме реального времени и предотвращение простоев;

– Управляет офисами удаленно с небольшим количеством местных ИТ-администраторов или без них;

– Создает гибкую среду, адаптированную к конкретным потребностям и требованиям вашей организации.

В состав платформы входят несколько основных компонентов и механизмов:

– Гипервизор VMware ESXi, отвечающий за саму виртуализацию, позволяющий использование ресурсов физического сервера для создания ВМ;

– Файловая система vSphere VMFS, предоставляющая ВМ доступ к общим устройствам хранения;

– VMware vSphere vMotion для миграции запущенных ВМ между серверами без простоев;

– VMware vCenter Server для управления виртуальной инфраструктурой и доступа к другим инструментам.

В зависимости от версии можно добавить инструменты такие, как vRealize Operations, использующийся для мониторинга ВМ и инфраструктуры, программно-определяемое хранилище VMware vSAN и виртуализацию сетевых функций VMware NSX [7].

Каждая ВМ включает конфигурационный файл, в котором осуществляется хранение параметров виртуальной машины, файла виртуального диска, представляющего программную версию жесткого диска, и файла журнала, в котором ведется мониторинг деятельности ВМ, включая системные сбои, изменения аппаратного обеспечения, миграции с одного хоста на другой, а также состояние ВМ.

VMware располагает большим выбором инструментов и функций для защиты хостов ESXi от несанкционированного доступа и неправильного использования. Имеется возможность шифровать ВМ, их файлы, файлы виртуальных дисков и файлы дампа памяти. Имея гибкий механизм управления доступом на основе ролей, можно определять политики доступа для каж-

дого пользователя виртуальной инфраструктуры. Более эффективный мониторинг обеспечивается ведением журнала аудита, который охватывает трафик сети, активность брандмауэра и изменения в ОС.

Сравнение ПК СВ «Брест» и VMware vSphere

Сравнение решений виртуализации по основным терминам представлено в таблице 1 (см. на сл. стр.).

Bare metal – это серверная платформа без ОС, позволяющая ПО получать прямой доступ к аппаратной части.

Central processing unit (CPU) – основной элемент аппаратного обеспечения вычислительного устройства, с его помощью происходит обработка информации.

High-availability – минимальное время восстановления работоспособности системы или сервиса в случае выхода из строя хоста.

Fault Tolerance – это технология, которая разработана для защиты критически важных ВМ с реальной непрерывной доступностью. Для защищенных машин постоянное копирование всего состояния памяти и процессорных инструкций в реальном времени [8].

vMotion – технология переноса работающей виртуальной машины с одного физического узла на другой, не прерывая ее работу и не останавливая сервисы.

Dynamic Resource Scheduler (DRS) – технология, позволяющая в автоматическом режиме обеспечивать балансировку нагрузки на ЦПУ и ОЗУ.

Виртуальные рабочие места (VDI) – технология виртуализации рабочего места, при которой образ рабочего стола запускается на виртуальной машине и доставляется клиенту по сети.

Каждая система виртуализации обладает широким списком функционала, разными возможностями. Функционал частично пересекается, но есть и ряд отличий. Конвергентная и гиперконвергентная инфраструктуры двух решений виртуализации упрощают поддержку инфраструктуры виртуальных рабочих столов и виртуализации настольных систем, так как они разработаны с ориентацией на простую установку и выполнение сложных задач. Гибкость гиперконвергентной инфраструктуры делает ее более масштабируемой и рентабельной, по сравнению с конвергентной [9].

Многие критерии функционала VMware vSphere поддерживаются в ПК СВ «Брест» с помощью ряда Open Source-решений, обеспечивающих функционирование сред виртуализации, кластеров и распределённых файловых хранилищ.

Преимуществом использования vSphere является его стабильность и надежность. Недостатками использования vSphere являются его цена и сложность.

ТАБЛИЦА 1. Сравнение решений виртуализации

Критерий сравнения	VMware vSphere	ПК СВ «Брест»
Российское ПО	Нет	Да + open source
Установка bare-metal	Да	Нет
Тип архитектуры	Классическая и гипер-конвергентная (vSAN)	Классическая или гипер-конвергентная
Платформа	ESXi	OpenNebula
Поддержка CPU	x86_64	x86_64
Отказоустойчивость		
Поддержка High-availability	Да	С помощью RAFT (open source)
Поддержка Fault Tolerant	Да	Нет
Функционал		
Централизованное управление	Да	Да
Централизованный мониторинг производительности и сбоев	Да	С помощью Zabbix (open source)
Управление операциями (performance management, capacity management, alerting and configuration/compliance)	Да	С помощью Foreman+Puppet (open source)
Портал самообслуживания	Да	Да
Автоматизация инфраструктуры (профили узлов, автоматическое развертывание узлов)	Да	Нет
Поддержка vMotion	Да	Да
Поддержка DRS	Да	Нет
VDI	Да (Horizon) VDI – по числу пользователей	Да (БРЕСТ.VDI) VDI – по кол-ву параллельных соединений
Максимальный размер кластера	до 96 узлов, до 10000 ВМ на кластер	Рекомендуемый максимум на систему управления 500 узлов
Макс. количество VM	До 1024 ВМ на хост	Нет ограничений
Поддерживаемые гостевые ОС	Windows, Linux	Windows, Linux
Поддерживаемые хост операционные системы	ESXi	Astra Linux SE
Схема лицензирования	Серверная виртуализация – по сокетам	Серверная виртуализация – 1 лицензия на 2 CPU конкретного сервера

В заключение

Средства виртуализации все шире используются для построения ИТ-инфраструктуры предприятий. В то же время нормативные требования подталкивают госкомпании и компании с госучастием к переходу на отечественное ПО. Раньше системы виртуализации разворачивались по большей части в рамках зарубежных решений, сегодня российские разработчики решений виртуализации уже хорошо зарекомендовали себя на рынке. Наши российские системы аппаратной виртуализации достаточно зрелые по сравнению с ушедшими иностранными решениями.

Список используемых источников

1. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 262–266.

2. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. N 3 (88). С. 38–46.

3. Багомедова А. Р., Ушаков И. А., Цветков А. Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С. 58–63.

4. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. N 1. С. 47–58.

5. Девянин П. Н Модели безопасности компьютерных систем. Управление доступом и информационными потоками. 3-е изд. М. : Горячая Линия - Телеком, 2020. 352 с.

6. Девянин П. Н Основы безопасности операционной системы Astra Linux Special Edition. Управление доступом. 3-е изд. М. : Горячая Линия - Телеком, 2023. 404 с.

7. Альшаев В. А., Цветков А. Ю. Разработка модуля разграничения сетевого трафика для повышения уровня защиты в платформе виртуализации vmware vsphere // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 53–57.

8. Зимин А. Е., Косов Н. А Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 343–348.

9. Гельфанд А. М., Ложкина А. А. Краткий анализ российских и зарубежных банков уязвимостей // Технологии информационного общества. 2021. С. 153–155.

Статья представлена заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ASTRA LINUX SPECIAL EDITION

П. С. Зылева, И. Е. Пестов, И. С. Тремель, У. С. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Устойчивость, безопасность, удобность в использовании, защита данных от несанкционированного доступа важны для каждого пользователя информационной системы. Следовательно, особую важность для всех пользователей имеет выполнение основных задач информационной безопасности – защита конфиденциальности, целостности и доступности данных. Выполнение этих задач необходимо, начиная с обеспечения безопасности личных данных, далее к коммерческой тайне и вплоть до государственной тайны. Astra Linux Special Edition – операционная система специального назначения предназначена для создания на ее основе автоматизированных систем в защищенном исполнении.

Astra Linux Special Edition, средства защиты информации (СЗИ), мандатный контроль целостности (МКЦ), замкнутая программная среда (ЗПС), изоляция приложений, Astra Linux Directory (ALD), мандатное управление доступом (МАС), единое пространство пользователей (ЕПП).

Каждый пользователь информационной системы придает особую важность ее безопасности, к тому, чтобы, данные, которые обрабатываются системой были защищены от несанкционированного доступа и были доступны только тем, кому они предназначены. То есть всем владельцам ИС важно выполнение основных задач информационной безопасности – защита конфиденциальности, целостности и доступности данных.

В связи со всем вышеперечисленным, в данной статье будут рассмотрены методы обеспечения безопасности в операционной системе (ОС) Astra Linux Special Edition.

Операционная система специального назначения (ОССН) Astra Linux Special Edition

Astra Linux Special Edition – операционная система специального назначения (ОССН), архитектурной основой которой является проект Debian GNU/ Linux. ОССН дает возможность обеспечения защиты конфиденциальных данных и гос. тайны до уровня «особой важности». Вводится в РФ как

отечественная альтернатива Microsoft Windows. ОССН соответствует требованиям, установленным системами сертификации средств защиты информации Министерства обороны, ФСТЭК и ФСБ РФ.

Одной из главных особенностей данного дистрибутива является то, что в его состав входят средства защиты информации, которые обеспечивают реализацию таких функций как [1]:

- использование модульного окружения NSS (*Name Service Switch*) в идентификации пользователей локально и в рамках единого пространства пользователей;
- аутентификация пользователей с использованием инфраструктуры PAM (*Pluggable Authentication Modules*) локально и в рамках единого пространства пользователей (ЕПП), двухфакторная аутентификация на основе цифровой подписи и инфраструктуры открытых ключей, которые поддерживаются внешним носителем аутентификационной информации «Рутокен»;
- дискреционное управление доступом с поддержкой стандартов Minimal ACL и Extended ACL [2].

Обеспечения безопасности ОССН с использованием мандатного управления доступом. Проблемы в реализации

В настоящее время в защищенных системах все чаще используется комбинация дискреционного разграничения доступа (*Discretionary Access Control*, DAC), и мандатного разграничения доступа (*Mandatory Access Control*, MAC). По общему правилу, их реализация проходит следующим образом: следующий «поверх» предыдущего.

Astra Linux получил от общепринятого для ОС семейства Linux механизм дискреционного управления доступом [3], который позволяет явно запрещать или явно разрешать различные доступы субъектов к сущностям (например к файлам), но не позволяет управление информационными потоками, которые содержат данные разных уровней конфиденциальности. К примеру, после того как данные из одной сущности были прочитаны процессом, они потенциально могут быть помещены в какую-то другую сущность, которая доступна ему для записи, и механизм дискреционного управления доступом не будет иметь возможности каким-либо способом противостоять этому. Таким образом, отсутствие понятных и корректно сформулированных правил обработки конфиденциальной информации может стать причиной для её утечки. Поэтому основой при реализации защиты в операционной системе специального назначения является механизм мандатного управления доступом (*Mandatory Access Control*, MAC), который построен на основе мандатной сущностно-ролевой модели управления доступом и информационными потоками (МРОСЛ ДП-модели).

Реализация МАС в ОССН

Основной задачей, которую решает механизм МАС, есть не полная блокировка каналов утечки защищаемых данных, а существенное затруднение их получения злоумышленником. Даже с учетом того, что ОССН имеет какие-либо уязвимости, которые позволяют в некоторых условиях обходить правила МАС, факт существования данных правил дает возможность в большей мере повысить безопасность ОССН.

В ОССН систему принудительного контроля доступа SELinux замещает МРОСЛ ДП-модель, запатентованная разработчиками ОССН.

В основании реализации МАС в ОССН лежит подсистема безопасности PARSEC, самостоятельно разработанная ОАО «НПО «РусБИТех» и включающая программный интерфейс и модуль расширения ядра ОССН, который, в свою очередь, поддерживает виртуальную файловую систему /parsecfs, и набор системных вызовов, которые позволяют пользователям, имеющим необходимые полномочия брать на себя управление политикой безопасности ОССН. Кроме мандатного управления доступом, PARSEC также отвечает за реализацию МКЦ и дополнительные функции аудита.

Средства защиты информации(СЗИ) ОС Astra Linux special edition

Режимы функционирования СЗИ

Как известно, в наиболее распространённом релизе с 2021 г., в ОС Astra Linux Special Edition в зависимости от приобретенной лицензии СЗИ, существует три режима функционирования ОССН: «Орел» («Базовый»), «Воронеж» («Усиленный») и «Смоленск» («Максимальный»). Режим «Воронеж» содержит и дополняет СЗИ, которые реализованы в режиме «Орел». Аналогично режим «Смоленск» содержит и дополняет СЗИ режима «Воронеж».

1. «Орел» («Базовый»). В ОССН владельцы имеют доступ к таким функциям безопасности: защита памяти, изоляция процессов, регистрация событий безопасности и пр.

2. «Воронеж» («Усиленный»). С этого режима начинают функционирование СЗИ собственной разработки, которые входят в подсистему безопасности PARSEC. Прежде всего это механизмы МКЦ и замкнутая программная среда (ЗПС). Самое важное, что обеспечивают эти СЗИ – значительно повышают безопасность ОС следующих угроз: взламывание, поражение вирусами, вложение закладок, атака повышения привилегий и пр. [4].

3. «Смоленск» («Максимальный»). Полная совокупность СЗИ в ОС Astra Linux Special Edition доступна в данном режиме. В него входит возможность использования МАС.

Следовательно, режим «Воронеж» самостоятельно или как входящий в режим «Смоленск», необходим для использования большинством пользователей ОССН.

Astra Linux Directory

Служба Astra Linux Directory (ALD) представляет из себя систему управления единым пространством пользователей (ЕПП)[5].

Релиз «Смоленск» ОССН поддерживает доменную сетевую инфраструктуру, которая основана на технологии Active Directory (AD). Эта сетевая инфраструктура совместима с технологией Microsoft Directory Service и основана на реализации ниже представленных протоколов:

- OpenLDAP – реализация протокола прикладного уровня LDAP (*Lightweight Directory Access Protocol*) с открытым исходным кодом, обеспечивающего механизм «I&A» (*Identification and Authentication*), а также поиск, добавление, изменение и удаление записей в единый каталог сетевых объектов;
- Samba – реализация протокола прикладного уровня SMB/CIFS (*Server Message Block/Common Internet File System*) с открытым исходным кодом. Реализация этого протокола обеспечивает удалённый доступ к ресурсам сети, а также реализацию механизма IPC (*Inter-Process Communication*) для удалённой работы приложений;
- Kerberos – это протокол аутентификации для доверенных хостов перед установлением соединения между ними, реализующий механизм единого входа.

Следовательно, ALD является надстройкой над технологиями LDAP, Kerberos 5, CIFS и автоматически настраивает все необходимые файлы конфигураций служб, которые реализуют перечисленные технологии и предоставляет интерфейс управления и администрирования.

Благодаря поддержке данных протоколов в пределах корпоративного уровня сетевой инфраструктуры ОССН зарегистрированным пользователям представляется возможным:

- централизованное хранение данных личных учётных записей и информации о их пользовательском окружении;
- монтирование домашних каталогов, расположенных на PDC, пользователей в их учётные записи, в состав локальной файловой системы хоста;
- сквозная аутентификация на хостах, входящих в состав доменной сетевой инфраструктуры.

Представленные выше возможности обеспечивают формирование для пользователя хоста на основе ОССН, который включен в доменную сетевую инфраструктуру, его ЕПП.

Мандатный контроль целостности (МКЦ)

В настоящем большая часть успешных взломов операционных систем осуществляется с помощью программных закладок [6]. Программная закладка – это программа, состоящая из небольшого по объему кода, которую

внедряют в атакуемую систему и предоставляют злоумышленнику несанкционированный доступ к ресурсам подвергающейся атаке ОС, тем самым, внося уязвимость в её систему безопасности.

МКЦ предназначен для того, чтобы затруднить внедрение программных закладок в ОС и дальнейшее существование в ней. Недоверенным процессам, имеющим низкий уровень целостности запрещается совершать любые модификации сущностей с более высоким уровнем целостности. Обращения процессов ОССН к сущностям, которые могут потенциально нарушить их целостность (операции записи, перемещения или удаления и пр.), допускаются только тогда, когда уровень целостности процесса не уступает уровню целостности сущности, к которой он обращается.

Замкнутая программная среда (ЗПС)

ЗПС представляет собой одну из важных систем зашиты информации. При активированной ЗПС запуск исполняемых файлов и загрузка исполняемых библиотек возможна только в том случае, если они имеют электронную цифровую подпись (ЭЦП) на доверительном ключе [8]. Таким образом, ЗПС предоставляет защиту от загрузки произвольного исполняемого файла или библиотеки, которые не обладают подходящей ЭЦП [8].

Изоляция приложений

МКЦ, присутствующий в ОС Astra Linux SE, обеспечивает разработку и внедрения новых уникальных методов обеспечения защиты информации. К примеру, адаптированную контейнерную виртуализацию, которая в совокупности с мандатным контролем целостности предоставляет возможность создания для недоверенного ПО своеобразных «песочниц», которые работают на пониженном уровне целостности, на котором процессы данных недоверенных ПО изолируются от прочих доверенных приложений [9].

Кроме этого, в ОССН существуют дополнительные СЗИ – запрет запуска интерпретаторов и ограничение прав непривилегированных пользователей – режим Киоск-2. В том числе Киоск-2 предусматривает возможность присваивания для каждого пользователя ОССН личных профилей безопасности. Каждый из таких профилей включает перечень имен каталогов или файлов, права доступа к которым надо дополнительно ограничить.

Заключение

Безопасность ОССН основана на использовании отечественных надежных технологий разработки, входящих в ее состав СЗИ, в основе которых лежат не представляющие особой сложности в реализации правила управления доступом. Использование режима «Воронеж» непосредственно или

как входящего в режим «Смоленск», необходимы для использования большинством пользователей ОССН, так как в них сосредоточена максимальная совокупность СЗИ. Грамотное использование совокупности данных СЗИ, предоставляет реальную защищенность от основных современных угроз информационной безопасности.

Список используемых источников

1. Девянин П. Н Модели безопасности компьютерных систем. Управление доступом и информационными потоками. 3-е изд. М. : Горячая Линия – Телеком, 2020. 352 с.

2. Девянин П. Н Основы безопасности операционной системы Astra Linux Special Edition. Управление доступом. 3-е изд. М. : Горячая Линия – Телеком, 2023. 404 с.

3. Кирилова К. С., Красов А. В., Цветков А. Ю Разработка метода обнаружения руткитов уровня ядра в работающих linux-системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 457–460.

4. Катасонов А. И., Цветков А. Ю Анализ механизмов разграничения доступа в системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 563–568.

5. Цветков А. Ю. Исследование существующих механизмов защиты операционных симстем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 657-662.

6. Темченко В. И., Цветков А. Ю Проектирование модели информационной безопасности в операционной системе // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 740–745.

7. Штеренберг С. И., Цветков А. Ю., Красов А. В. Компьютерные вирусы. СПб. : СПбГУТ, 2015. 63 с.

8. Гельфанд А. М., Ложкина А. А. Краткий анализ российских и зарубежных банков уязвимостей // Технологии информационного общества : сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества», Москва, 03–04 марта 2021 года. М. : ООО "Издательский дом Медиа паблишер", 2021. С. 153–155.

9. Зимин А. Е., Косов Н. А Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 2. С. 343–348.

Статья представлена заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.057
ГРНТИ 81.93.29

ИНТЕГРАЦИЯ КЛИЕНТСКОЙ МАШИНЫ НА ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX В ДОМЕН ACTIVE DIRECTORY

П. С. Зылева, И. Е. Пестов, И. С. Тремель, У. С. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Большинство средних и крупных предприятий используют Microsoft Active Directory для централизованного управления доступом к ресурсам, принадлежащим организации. Так было на протяжении десятилетий, и компании вложили значительные средства в создание инструментов и рабочих процессов автоматизации, направленных на повышение безопасности и эффективности своих групп IT-администраторов. Согласно последним данным, из-за ухода с российского рынка ключевых зарубежных IT-вендоров спрос на использование отечественных ОС резко вырос. Сейчас это связано с вопросами безопасности и позицией Microsoft по работе в стране, хотя сам процесс начался еще в 2020 году. Самой популярной системой остается Astra Linux – это UNIX-подобная ОС, основанная на дистрибутиве Debian, разработку которой с 2008 г. ведет компания «Русбитех». Перевод IT-систем предприятия потребует настройки корректного взаимодействия обновленных систем с теми решениями, что уже есть, со всеми ресурсами, которые используют пользователи, поэтому перед администраторами встают задачи по интеграции серверов и рабочих станций Linux в среду домена Active Directory.

Active Directory, Samba, Winbind, Kerberos, домен, LDAP-протокол, идентификатор пользователя UID, идентификатор группы GID, идентификатор безопасности SID, SMB (Server Message Block), CIFS (Common Internet File System), NSS (Name Service Switch).

В данной работе представлен процесс интеграции операционной системы Astra Linux в домен Active Directory. Предполагается, что все файлы конфигурации находятся в неизмененном состоянии после установки [1]. На протяжении всей статьи пример домена Active Directory будет использовать следующую конфигурацию:

Имя домена NetBIOS: MAIN

DNS-имя домена: main.domain.ru

Область Kerberos: MAIN.DOMAIN.RU

IP контроллеров домена – 192.168.1.1, 192.168.1.2

Для осуществления взаимодействия пользователей Windows (имеющих идентификатор безопасности SID) и локальных пользователей Astra Linux (с их идентификаторами UID и GID) в данной работе будет использоваться демон Winbind. При использовании данного метода Name Service Switch (NSS)

работает совместно с Winbind, который в свою очередь осуществляет «разрешение» пользовательских имен (т. е. идентификаторов SID) в UID и GID с помощью LDAP и Kerberos – вызовов. После чего создается пользовательская запись в файлах демона winbindd: winbindd_cache.tdb и winbindd_idmap.tdb.

В случаях, когда для получения данных об учётных записях пользователей не применяется сервер LDAP Active Directory, каждый из серверов, являющийся членом домена AD, поддерживает свою уникальную базу данных присоединенных пользователей. Это значит, что пользователь, который имеет доступ к двум серверам, входящим в домен, имеет разные UID/GID на обоих серверах. В то же время, для пользователя сети Windows, это прозрачно, потому что разграничение доступа к ресурсам осуществляется на основании имен пользователей и групп, а не на основании идентификаторов [2].

Подготовка системы

Samba – это стандартный набор программ взаимодействия Windows для Linux и Unix, который состоит из трёх служб: smbd, nmbd и winbindd. Демон smbd – отвечает за совместное использование и доступ к файлам и принтерам, nmbd – регистрирует компьютер в сети и занимается разрешением имен по протоколам SMB/CIFS, winbindd обеспечивает аутентификацию пользователей домена Active Directory и взаимодействие с контроллером. В Debian, smbd и nmbd демоны находятся в пакете samba, а в пакете winbind содержатся демон winbind и утилита net, позволяющая решать задачи администрирования, в том числе присоединение машины к домену AD.

Active Directory зависит от DNS. Для начала устанавливаем статические настройки сети для сервера в файле /etc/network/interfaces. Далее, крайне важно, чтобы в /etc/resolv.conf файле были указаны правильные DNS-серверы и суффикс поиска домена. Для примера конфигурации домена подходит следующее содержимое:

```
# Generated by NetworkManager
search main.domain.ru
nameserver 192.168.1.1
nameserver 192.168.1.2
```

Для установки пакетов samba, winbind и Kerberos, выполните команду: *$sudo apt-get install ntp krb5-user samba cifs-utils \ smbclient winbind libnss-winbind libpam-winbind*

На этапе установки Kerberos нужно ответить на несколько вопросов. При получении запроса для указания области, вписываем в верхнем регистре имя домена с его доменной зоной. Далее указываем сервер Kerberos, то есть полное имя контроллера домена. После вводим имя управляющего

хоста области. Если контроллер домена всего один, используем его имя еще раз [3]. Установка необходимых пакетов завершена.

Для успешной настройки обязательным условием является одинаковое время на подключаемом компьютере и контроллере. Для автоматической синхронизации времени устанавливаем еще один пакет: *$sudo apt install ntp*

Теперь в файле /etc/ntp.conf, открытом с правами суперпользователя, находим строку *#Specify one or more ntp servers*, после которой комментируем все имеющиеся серверы и вписываем имя контроллера с его доменной зоной.

Протокол Kerberos в среде AD работает в группе совместно со службами DNS, LDAP и протоколом SMB. Каждый из данных компонентов выполняет свою роль, и если хотя бы один из них функционирует неверно, то ввод клиента в домен будет невозможен.

Вносим правки в файл настройки Kerberos /etc/krb5.conf, в секции [domain_realm] вписываем данные о своей области:

[domain_realm]

.main.rissianpost.ru = MAIN.DOMAIN.RU

main.russianpost.ru = MAIN.DOMAIN.RU

Проверяем возможность получения билета TGT от KDC-сервера с помощью команды: *$sudo kinit Administrator*

Вводим пароль и проверяем полученный TGT: *$sudo klist*

Чтобы Samba могла сопоставлять имена пользователей с UID и GID, нужно модифицировать строки в файле /etc/nsswitch.conf, согласно рис. 1, для указания порядка, в котором NSS будет осуществлять поиск имен пользователей, хостов, паролей, сетей и т. д.:

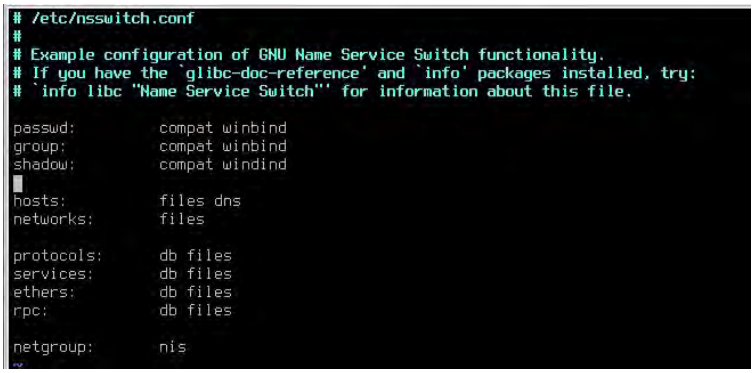


Рис. 1. Конфигурация файла nsswitch.conf

Согласно приведенной настройке, Linux при запросе имен пользователей, групп или паролей будет сначала обращаться к своей встроенной базе данных (файлы */etc/passwd, /etc/group, /etc/shadow*), а только потом – к демону winbind. При разрешении имени хоста в первую очередь будет использоваться файл /etc/hosts, потом DNS и только затем служба имен NetBIOS.

Это нужно в том случае, если в вашей сети имеются хосты, не зарегистрированные в DNS, но при этом имеющие имена NetBIOS, например, компьютеры под управлением ОС Windows в составе рабочей группы [4].

Настройка SAMBA.

Создаем копию конфигурационного файла Samba с помощью команды: $cp /etc/samba/smb.conf /etc/samba/smb.conf.orig

После чего редактируем файл/etc/samba/smb.conf, приводя его к следующему виду (рис. 2 и 3):

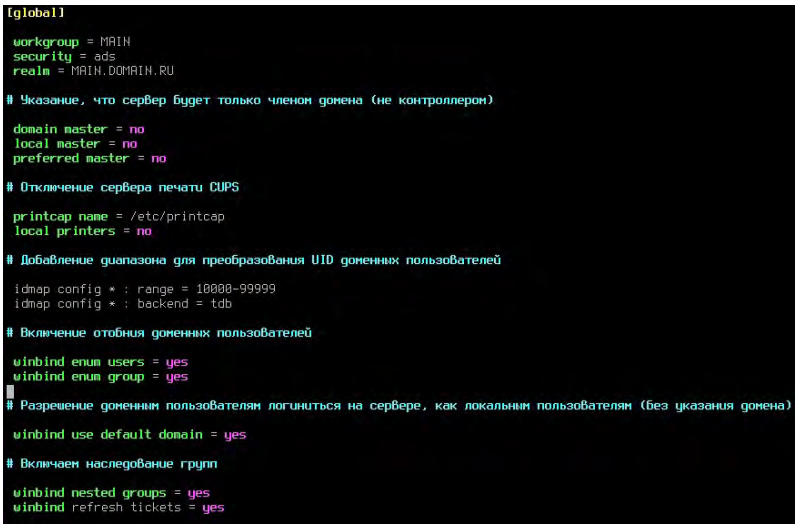


Рис. 2. Пример конфигурации файла smb.conf

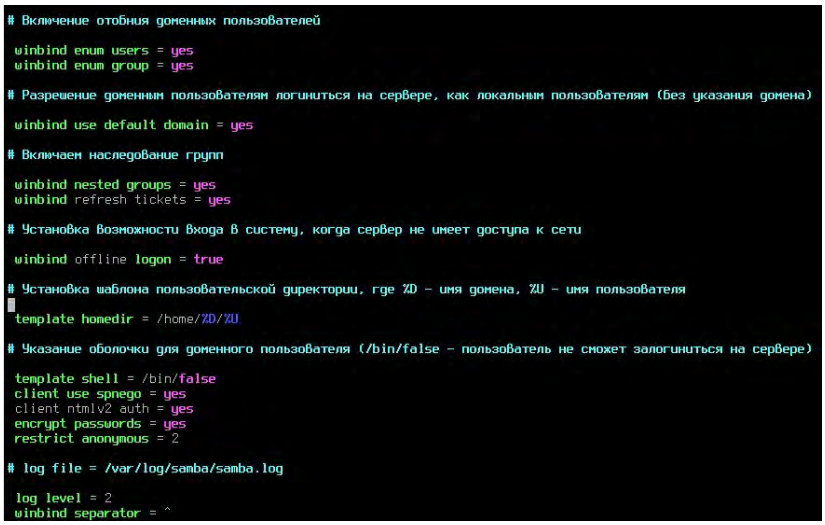


Рис. 3. Пример конфигурации файла smb.conf

Ввод SAMBA в домен Active Directory

Перед добавлением не забываем проверить, что у нас получен TGT или билет, удостоверяющий личность пользователя, и синхронизировано время между сервером и контролером домена [5].

Выполняем команду и после вводим пароль: *$net ads join -U domain_admin*

При этом вместо учетной записи «domain_admin» необходимо использовать имя пользователя с правом присоединения компьютера к домену. Стоит учитывать, что если в конфигурационном файле “samba” параметр “winbind use default domain” не указан, то имя пользователя вводится в формате domain_admin@AD.LOCAL. Сообщение: Using short domain name -- AD и Joined 'FILES' to realm 'ad.local', выводимое после выполнения команд указывает, что ввод в домен был успешно осуществлён. А сообщение: “Join to domain is not valid”, говорит об ошибке.

Далее, для корректной работы SAMBA с доменной аутентификацией Active Directory, необходимо перезапустить демонов samba и winbind и поставить их на автозагрузку [6].

Настраиваем центральную политику аутентификации, выполнив команду:

$pam-auth-update

Теперь можно увидеть список доменных учетных записей пользователей AD и список групп AD:

$wbinfo -u

$wbinfo -g

Заключение

В наше время возможность безопасной и не трудоёмкой эксплуатации ПК на базе Windows ставиться под вопрос. Если в сети организации имеются множество Windows-клиентов или уже работают службы AD, то стоит подумать об интеграции Linux-серверов в доменное окружение Active Directory. Одной из самых привлекательных и конкурентных систем является Astra Linux. Несмотря на существование различных методов интеграции серверов на базе ОС Astra Linux в домен AD, Samba позволяют упростить управление и настройку, не требуя внесения изменений в службу каталогов. Таким образом, Samba является важным компонентом для беспрепятственной интеграции серверов и рабочих столов Linux/Unix в среды Active Directory.

Список используемых источников

1. Анзина А. В. Исследование способов установки операционной системы Astra Linux // Научно-практические исследования. 2020. N 1-3. С. 14–16.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. Организация единого пространства пользователей в автоматизированных системах специального назначения // Информационная безопасность регионов России (ИБРР-2021) : Материалы XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27–29 ноября 2021 года. СПб. : Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2021. С. 156–158.

3. Binduf A. et al. Active directory and related aspects of security // 2018 21st Saudi Computer Society National Computer Conference (NCC). IEEE, 2018. PP. 4474–4479.

4. Булатов А. С. Автоматизация управления доступом в операционной среде специального назначения astra linux // Матрица научного познания. 2021. N 2-2. С. 34–43.

5. Цветков А. Ю. Исследование существующих механизмов защиты операционных симстем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 657–662.

6. Голуб С. А., Коркин И. Ю. Анализ безопасности подсистем локальной аутентификации ос семейств windows и linux // Безопасность информационных технологий. 2022. Т. 29. N 1. С. 57–69.

7. Долгопятов А. Ю., Долгопятов О. А. Уязвимости программного обеспечения // Межотраслевые исследования как основа развития научной мысли : сборник статей Международной научно-практической конференции в 2 ч., Оренбург, 27 декабря 2022 года. Часть 1. Уфа : ООО «ОМЕГА САЙНС», 2022. С. 60–67.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.396.2
ГРНТИ 49.03.05

ПОМЕХОУСТОЙЧИВОСТЬ КОГЕРЕНТНЫХ СИСТЕМ СВЯЗИ В ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ

Р. З. Ибрагимов

Сибирский государственный университет телекоммуникаций и информатики

В виду развития техники когерентного приема оптического сигнала одним из важных критериев работы является помехоустойчивость. Важность данного критерия обусловлена использованием многоуровневых форматов модуляции, которые в большей степени подвержены искажению из-за близко расположенных сигнальных состояний. Для улучшения передаточных характеристик систем связи сегодня является использование каскадных схем кодирования. Гибридные схемы, реализующие совместную работу SD-FEC и HD-FEC, позволяют снизить количество ошибок в принимаемом сигнале.

магистральные сети, отношение сигнал-шум, помехоустойчивость, FEC.

Совершенствование технологических процессов по улучшению передаточных характеристик лазеров, снижению шумов оптических усилителей, волокна с низким уровнем потерь является хорошим драйвером роста для развития техники передачи данных. Кроме улучшения волоконно-оптической базы когерентных систем связи повышается эффективность алгоритмов помехоустойчивости. Так, основная тенденция, направленная на увеличение пропускной способности, приводит к усложнению методов формирование сигнальных комбинаций (PAM4, DP-32QAM и др.), что в конечном счете влечет за собой высокие требования к отношению сигнал-шум в оптическом диапазоне (OSNR).

Для борьбы с ошибками в оптических системах связи, в процессе формирования оптического сигнала в структуре фрейма OTN, организуется специальное поле для передачи избыточной информации для обнаружения ошибок с помощью специальных кодов FEC. На приемной стороне в оптических транспондерах помехоустойчивость реализуется в два этапа: обнаружение ошибок (обычно это проверка на четность) и последующее исправление ошибок.

На сегодняшний день наиболее популярным решением для помехоустойчивости когерентных систем связи является использование SD-FEC в качестве внешнего кода, а HD-FEC в качестве внутренних кодов как показано на рис. 1. Каскадные схемы кодирования использует более сложные варианты размещения данных (маппинг), а также турбо-коды, сверточные коды и др. Начиная со второго поколения помехоустойчивых кодов ведущие вендоры телекоммуникационного оборудования начинают использовать проприетарное кодирование, а также более сложные алгоритмы маппинга данных.

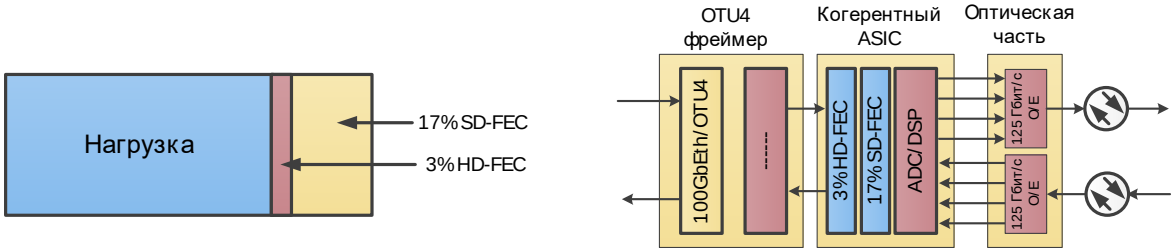


Рис. 1. Вариант использование SD-FEC внутри фрейма OTN

Помехоустойчивость магистральных систем связи обеспечивается проприетарными алгоритмами, используемыми такими производителями как Huawei, NEC, ClaryPhy, Lumentun и др. [1, 2].

Для повышения помехоустойчивости системы и упрощения технологических процессов при проектировании блоков цифровой обработки сигнала

применяются гибридные системы, комбинирующие более производительные коды с малой проверкой на четность (LDPC) и коды с «жестким» алгоритмом принятия решения (коды Рида-Соломона и др.) [3, 4]. В этом случае, структурная схема будет выглядеть следующим образом.

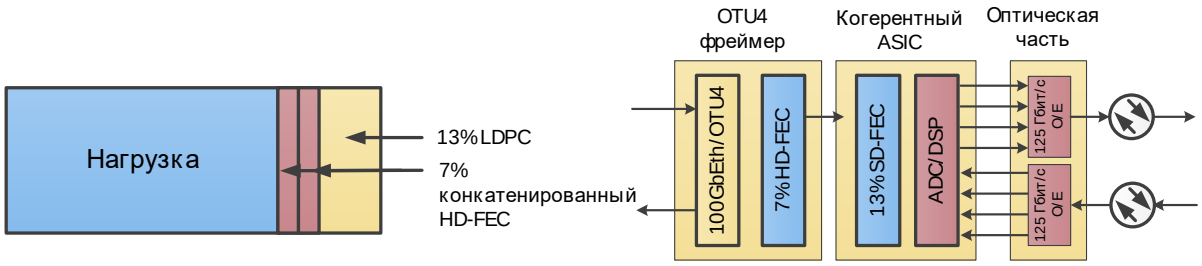


Рис. 2. Гибридное использование SD-FEC с HD-FEC

Анализ крупных производителей DSP-процессоров показывает общую тенденцию на использование LDPC-кодов, а также их модифицированных версий, где заявляемая избыточность может достигаться 20 %.

Наиболее привлекательным для производителей транспондеров является семейство лестничных кодов. Основной идеей данных кодов является объединение блочного кодирования с рекурсивным сверточным (конволюционным) кодированием. Лестничные коды построены для итерационного декодирования, при котором процесс декодирование осуществляется поочередно для горизонтальной и вертикальной составляющей. Каждый бит данного кода перекрестно проверяется двумя компонентными кодами. Поэтому значения бит могут обновляться в процессе итеративного декодирование компонентного кода.

При этом, наблюдается совершенно противоположная ситуация в сегменте оптических систем для центров обработок данных (ЦОД), а также для городских и региональных систем связи. Большую часть данного рынка занимают съемные приемо-передающие модули использующие унифицированные коды (cFEC и oFEC) в качестве основного алгоритма для поддержания требуемого отношение сигнал-шум в оптическом диапазоне [5]. Алгоритм коррекции ошибок для таких интерфейсов могут использовать лестничные коды совместно с HD-FEC (255, 239).

Использование унифицированных кодов обеспечивает избыточность до 15 % и позволяет перекрывать расстояния вплоть до 480 км (интерфейс OpenZR+), что говорит о хорошей перспективе перехода с традиционных DWDM-систем, поддерживающих до 96 спектральных каналов, к системам передач, использующим пару волокон для организации систем связи вплоть до 400 Гбит/с без дополнительного слоя OTN, где обеспечивается упаковка разнородного трафика в структуру OTUCn [6].

Взгляд на сегмент межсоединения ЦОД показывает, что все производители модулей придерживаются стандартов OpenROADM и OIF [5, 6], стремясь к упрощению алгоритмов FEC, таким образом, удешевляя себестоимость приемо-передающих модулей различного форм-фактора, и повышая гибкость в выборе построения городских сетей и межсоединений ЦОД.

Список используемых источников

1. Chang D. et al. LDPC convolutional codes using layered decoding algorithm for high speed coherent optical transmission // OFC/NFOEC 2012: IEEE. PP. 1–3.

2. Smith B. P. et al. Staircase codes: FEC for 100 Gb/s OTN // Journal of Lightwave Technology. 2011. Vol. 30. N 1. PP. 110–117.

3. Scholten M., Coe T., Dillard J., Chang F. Enhanced FEC for 40G/100G // Proc. ECOC 2009. PP. 1–12.

4. Yu F. et al. Application aspects of enhanced FEC for 40/100G systems // Proc. European Conference on Optical Communication 2010.

5. OIF Implementation Agreement 400ZR. URL: https://www.oiforum.com/wp-content/uploads/OIF-400ZR-01.0_reduced2.pdf (дата обращения 12.02.2023).

6. Reis J. 400G White Paper // Technology Options for 400G Implementation (OIF-Tech-Options-400G-01.0).

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ БОЛЬШИХ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. А. Игнатьева, И. Е. Пестов, Е. С. Федорова, А. Д. Федотовская

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

XXI век является эпохой информационного потока. Данные, которые человечество накопило за последнее десятилетие, намного превышают данные, которые были доступны человечеству в течение предыдущего столетия. Общество находится «на пороге огромной волны инноваций, производительности и роста, а также новых способов конкуренции и создания ценности — и все это благодаря большим данным». Анализ больших данных зарекомендовал себя как эффективный инструмент во многих областях современной обработки информации, в том числе информационной безопасности. Путем предоставления большего количества данных и применяя различные аналитические методы, все реальные и потенциальные риски могут быть проанализированы очень быстро, можно оценить множество альтернатив для защиты и противодействия, сделать более точные прогнозы будущего развития, а также, могут быть проведены более подробные экспертные заключения.

большие данные, информационная безопасность, аналитика больших данных.

В литературе термин «большие данные» относится к тем данным, в которых объем, требуемая скорость обработки или представления данных ограничивает возможности эффективного анализа традиционными реляционными подходами или требуется значительное горизонтальное масштабирование для обеспечения эффективной обработки [1, 2]. Это создалонеобходимостьдляновогопоколенияпрограммныхприложенийиинструментов.

Большие данные отличаются от традиционных баз данных четырьмя основными характеристиками, связанными с:

– объемом набора данных;

– скоростью генерации и передачи данных;

– разнообразием данные в виде различных типов структурированных и неструктурированных данных;

– сложностью структуры, поведения и перестановки наборов данных, когда различные критические факторы находятся в работе.

Важным фактором для платформ больших данных является защита, которая должна быть реализована на каждом этапе жизненного цикла платформы и использовать комбинацию традиционных инструментов безопасности, новые инструменты и технологии, а также интеллектуальную безопасность мониторинга процессов. На рис. 1 показаны несколько этапов обработки больших данных.

Рис. 1. Этапы обработки больших данных

Источники больших данных разнообразны. Например, каждый щелчок мышью в интернет-магазине может быть зафиксирован в файлах веб-журналов и проанализирован, чтобы лучше понять поведение покупателей и влиять на их покупки, автоматически рекомендуя продукты. Источники социальных сетей, такие как Одноклассники и Вконтакте, генерируют огромное количество комментариев и постов.

Согласно источникам, большие данные бывают трех типов:

– Данные генерируемые людьми – текст, фотографии, видео;

– Данные генерируемые машинами – компьютерами, управляющими документами, базами данных, мультимедиа, GRS, RFID, так называемые умные «дома»;

– Транзакционные данные– покупки, перевод денег, операции с банкоматами.

К примеру, пользовательские данные включают данные CRM(CustomerRelationshipManagement), такие данные, как электронная

почта, телефоны, SMS или сообщения в социальных сетях, и многое другое. Существует множество данных о транзакциях, которые хранятся в разных базах данных. Существует также огромное количество данных, генерируемых пользовательским программным обеспечением и датчиками. Все данные, передаваемые из источников на платформу, должны быть защищены.

Хранимые данные имеют большое значение для бизнеса. Они относятся к традиционным базам данных и новым технологиям, таким как Hadoop. В случае если данные будут надлежащим образом сохранены, их можно будет проанализировать и обработать с большой скоростью, что впоследствии может иметь еще большую ценность. Появилось множество аналитических технологий, подходов и продуктов, которые особенно применимы к большим данным, таким как аналитика в памяти, аналитика в базе данных и устройства.

Аналитическая обработка (анализ и результаты) различных типов данных – это суть Больших данных. Результаты, полученные в результате этой обработки, направляются в приложения, отчеты и информационные панели являются целью атак. Поэтому шифрование результатов, контроль доступа и трафика чрезвычайно важно.

Классическими технологиями, используемыми для защиты больших данных, являются:

– Шифрование;
– Контроль доступа пользователей;
– Обнаружение вторжений и противодействие им;
– Физическая защита.

Шифрование защищает данные как при хранении, так и при их передаче. Следует отметить, что шифрование должно работать с различными типами данных и с различными аналитическими инструментами, реляционными и нереляционными базами данных, специальными файловыми системами и т. д.

Контроль доступа пользователей является ключевым инструментом защиты на сетевом уровне. Это важно для платформы больших данных. Он должен быть очень точным и основываться на четко определенной политике.

Системы обнаружения вторжений и реагирования на них также важны для платформы больших данных, поскольку они способствуют своевременному обнаружению попыток вторжения.

Физическая защита связана с защитой здания и помещений центра обработки данных организации или поставщика облачных услуг.

Анализ больших данных значительно сложнее, чем тот, который используется в традиционных базах данных. Большие данные имеют большие неагрегированные объемы, в разных форматах, и их обработку трудно выполнить в памяти только одного компьютера. Обработка больших данных

включает в себя механические процессы и алгоритмы. Методы, используемые для анализа больших данных, бывают двух основных типов: адаптивный и прогностический анализ.

Адаптивный анализ направлен на получение статистических данных по текущим и историческим данным и предоставление информации о том, что произошло и почему это произошло. Он включает в себя такие методы, как статистическое моделирование, отчетность о тенденциях, визуализация, ассоциативный и корреляционный анализ [3].

Прогностический анализ же, фокусируется на использовании известных данных (обучающих данных), которые включают входные свойства данных (атрибуты) и значения отклика (целевые модели) для построения предсказуемой модели (решения) для прогнозирования невидимых данных (тестовых данных). В нем используются такие методы, как векторные машины, дерево решений, теория Байеса, нейронные сети и другие.

Технологии больших данных, используемые в системах безопасности, способны заранее обнаруживать угрозы. Например, они могут обнаруживать нетипичное поведение в сети, действия компьютерных вирусов прогнозировать атаку и анализировать источники атаки [4].

Большие данные создают условия для эффективного применения методов обнаружения мошенничества. В специализированной литературе они делятся на две основные группы: статистические методы и приемы с использованием искусственного интеллекта. В таблице 1 представлены примеры этих методов.

ТАБЛИЦА 1. Примеры методов анализа больших данных

Статические методы
1. Обработка профилей пользователей. 2. Анализ рядов данных, зависящих от времени. 3. Кластеризация и классификация для выявления возможных моделей/схем и зависимостей/ассоциаций в группах данных. 4. Объединение алгоритмов для обнаружения аномалий в поведении транзакции или пользователи.
Методы, использующие искусственный интеллект
1. Интеллектуальный анализ данных. 2. Экспертные системы. 3. Автоматическое распознавание образов. 4. Методы машинного обучения. 5. Нейронные сети.

Анализ больших данных используется во многих областях, в частности, в маркетинге, розничной торговле, онлайн-рекламе, поисковых системах, социальных сетях и телекоммуникациях. Во всех этих случаях основной целью анализа BD (*BigData*) является анализ поведения потребителей

или покупателей с целью предложения им наиболее подходящей рекламы, то есть конечной целью является получение финансов или программных продуктов [5].

Еще одной довольно известной областью применения BD (*BigData*) является их анализ специальными службами. Специальные службы, включая правительственные ведомства и правоохранительные органы, используют анализ больших данных для выявления угроз национальной безопасности, борьбы с терроризмом, поддержания правопорядка и борьбы с киберпреступностью [6].

Наряду со многими возможностями, которые Большие данные предоставляют потребителям (бизнес пользователям и частным лицам), они несут с собой множество угроз для общества, бизнеса и отдельных лиц. Стремительный рост внедрения технологий в различные аспекты жизни значительно обострил проблемы защиты информационных систем. С прогнозируемым ростом интернет-трафика до 161,3 Эксабайт в месяц в 2022 году, вероятность атаки быстро растет и, вероятно, выходит из-под контроля. Устаревшие технологии обнаружения угроз не успевают за динамичным характером атак, которые используются каждый день [7].

Использование преимуществ больших данных при создании надежных, адаптивных и быстрых систем информационной безопасности становится скорее необходимостью, чем выбором. При больших потоках данных классические методы обнаружения отстают с точки зрения точности и способности обнаруживать угрозы. Большинство современных систем информационной безопасности в значительной степени полагаются на журналы, генерируемые сетевыми устройствами, хостами, идентификаторами и IP-адресами (как сетевыми, так и хостинговыми) и т. д. Эти журналы могут легко составлять несколько гигабайт в день для сетей среднего размера. Без использования больших данных и аналитики больших объемов данных, машинного обучения и облачных вычислений системы обнаружения угроз могут легко и быстро отстать. Следовательно, будущее информационной безопасности тесно связано с большими данными.

Список используемых источников

1. Петренко А. С. Технологии больших данных (Big Data) в области информационной безопасности // Вторая международная научно-техническая конференция, Innopolis, 01–03 октября 2018 года. Innopolis: ООО «ИД «Афина», 2018. С. 248–255.

2. Назаренко Ю. Л. Обзор технологии «большие данные» (Big Data) и программно-аппаратных средств, применяемых для их анализа и обработки // European science. 2017. N 9 (31). С. 25–30.

3. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. N 11. С. 39–47.

4. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы: учеб. пособие. Ч. 1. СПб. : СПбГУТ, 2014. 63 с.

5. Цветков А. Ю. Эллауи Ю. Б. Поиск уязвимостей в программном обеспечении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 684–688.

6. Штеренберг С. И. Методика управления системами обработки и сбора Больших данных с поддержкой мониторинга встроенными программными агентами // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 4. С. 26–35.

7. Карев А. С., Бирих Э. В., Сахаров Д. В., Виткова Л. А. Проблемы информационной безопасности в Интернете вещей // Интернет вещей и 5G, Санкт-Петербург, 07 декабря 2016 года. СПб. : СПбГУТ, 2016. С. 66–70.

Статья представлена научным руководителем, заведующий кафедрой ЗСС, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056
ГРНТИ 81.96

АНАЛИЗ МОДЕЛЕЙ ПРОГНОЗИРОВАНИЯ ВРЕМЕННЫХ РЯДОВ ДЛЯ ПРЕДСКАЗАНИЯ ТРЕНДОВ РАЗВИТИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. Е. Израилов[1,2], Н. А. Пономарев[1], Е. В. Таров[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Работа посвящена задаче предсказания угроз информационной безопасности. Для этого производится анализ существующих моделей прогнозирования временных рядов для выявления трендов развития угроз. В результате критериального сравнения приведенных моделей определены наиболее подходящие из них. Предлагается методологическая схема выбора моделей прогнозирования. Указаны теоретическая и практическая значимость результатов исследования, а также пути его продолжения.

информационная безопасность, временные ряды, прогнозирование, модели прогнозирования.

Развитие информационных технологий и все более широкое использование сети интернет приводят к росту угроз информационной безопасности. Исследования, проведенные «Лабораторией Касперского», показали, что таргетированные кибератаки обходятся крупному российскому бизнесу в $695 000, а малому и среднему – в $32 000; при этом 60 % малых компаний

прекращают свою деятельность в течении шести месяцев после кибератак (остальные 40% терпят огромные убытки). В связи с этим, все большую актуальность приобретает прогнозирование трендов развития угроз информационной безопасности, которое позволяет оперативно реагировать на возможные киберугрозы и принимать меры по их предотвращению. Потому необходимо эффективно использовать существующие методы прогнозирования, что позволит своевременно разрабатывать проактивные (т. е. принимаемые заранее) меры по защите от угроз и минимизировать потенциальный риск [1, 2, 3].

В данной работе производится анализ современных моделей прогнозирования временных рядов с точки зрения их применимости для задач информационной безопасности. Цель исследования – разработка обоснованной и эффективной методологической схемы выбора конкретной модели в зависимости от определенного сценария.

На сегодняшний день наиболее часто для предсказания временных рядов применяются следующие модели [4]:

M1. Регрессионные модели прогнозирования;
M2. Авторегрессионные модели прогнозирования;
M3. Модели экспоненциального сглаживания (ES);
M4. Модель по выборке максимального подобия (MMSP);
M5. Модель на нейронных сетях (ANN);
M6. Модель на цепях Маркова (Markov chains);
M7. Модель на классификационно-регрессионных деревьях (CART);
M8. Модель на основе генетического алгоритма (GA);
M9. Модель на опорных векторах (SVM);
M10. Модель на основе передаточных функций (TF);
M11. Модель на нечеткой логике (FL);
M12. Модель сингулярного спектрального анализа (SSA).

Для того чтобы иметь возможность оценить пригодность каждой из модели для предсказания трендов развития угроз информационной безопасности введем следующие критерии:

– точность прогнозирования (К1), показывающая, насколько хорошо модель предсказывает будущие значения; чем выше показатель, тем меньше ошибок в прогнозах и тем лучше модель;

– скорость работы (К2), показывающая, насколько быстро модель может выполнять расчеты; чем выше показатель, тем быстрее модель может произвести прогнозы, что особенно важно в случаях, когда требуется быстрый ответ;

– ресурсоемкость (К3), показывающая, насколько много ресурсов требуется для работы модели, таких как память, вычислительная мощность и т. д.; чем ниже показатель, тем меньше требуется ресурсов, что может быть важно в случаях, когда ресурсы ограничены;

– робастность (К4), показывающая, насколько хорошо модель работает на различных данных и в различных условиях; чем выше показатель, тем более универсальной является модель и тем меньше вероятность, что она даст неправильные прогнозы на новых данных;

– интерпретируемость (К5), показывающая, насколько легко понять, как работает модель и какие факторы она учитывает при прогнозировании; чем выше показатель, тем легче объяснить результаты модели и использовать ее для принятия решений;

– автоматизированность (К6), показывающая способность автоматизировать процесс построения модели и дальнейшего прогнозирования временных рядов; чем выше показатель, тем меньшее участие человека требуется в процессе.

Важно отметить, что каждый из этих критериев может иметь различную важность в зависимости от конкретной задачи, поэтому при выборе модели необходимо учитывать их все вместе, а не рассматривать по отдельности.

Для большего удобства проведения сравнительного анализа «разобьем» рассматриваемые модели на группы в соответствии с особенностями каждой из них. В результате этого можно получить следующие группы:

– Группа № 1: М1, М2, М4 (эти модели основываются на статистических методах и используют исторические данные для прогнозирования будущих значений);

– Группа № 2: М5, М6, М7, М8 и М9 (эти модели используют алгоритмы машинного обучения для построения прогнозных моделей и не требуют знания теории временных рядов);

– Группа № 3: М10, М11 (эти модели представляют собой комбинацию различных методов и могут использоваться для моделирования сложных систем с нелинейными зависимостями между переменными);

– Группа № 4: М12 (эта модель использует матричные методы для анализа временных рядов и может использоваться для выявления трендов и циклов в данных).

Проанализируем рассматриваемые модели (М1–М12) в соответствии с предложенными критериями (К1–К6), используя следующие оценки: 0 – модель показывает плохие результаты относительно данного критерия; 0,5 – модель может показывать, как плохие, так и хорошие результаты; 1 – модель показывает исключительно хорошие результаты; 1,5 – модель идеально подходит под данный критерий.

Результаты экспертного анализ представлены в таблице 1.

Теперь обратимся к группам, на которые были разбиты рассматриваемые модели прогнозирования и найдем среднее арифметическое значений критерий для каждой из группы в соответствии с оценками, полученными из таблицы 1.

В результате чего можно сформировать таблицу 2.

Анализ таблицы 2 позволяет сделать следующие выводы касательно каждой из групп. Группа №1 обладает высокой точностью (К1), скоростью работы (К2), а также ресурсоемкостью (К3). Для Группы № 2 характерен ощутимый потенциал с точки зрения автоматизации процесса предсказания (К6). Группа № 3 отличается высокой точностью, робастностью (К4) и возможностью автоматизации (К6). Группа № 4 имеет самый высокий показатель интерпретируемости (К5).

ТАБЛИЦА 1. Критериальное сравнение моделей

	К1	К2	К3	К4	К5	К6
М1	1.5	1	1	0.5	1	1
М2	1.5	1	0.5	0.5	0.5	1
М3	1.5	1.5	1.5	0.5	0.5	1
М4	0.5	1.5	1.5	0.5	1	1
М5	1.5	0.5	0	1	0	1.5
М6	0.5	1.5	1.5	0.5	1	1.5
М7	1	0.5	0.5	0.5	0.5	1.5
М8	1	0.5	0	1.5	0.5	1.5
М9	1	0.5	0.5	1	0	1.5
М10	1	0.5	0.5	1	1	1
М11	1.5	0.5	0.5	1	1	1.5
М12	1	1	1	0.5	1.5	1

ТАБЛИЦА 2. Критериальное сравнение групп моделей

	К1	К2	К3	К4	К5	К6
Группа № 1	1.25	1.25	1.125	0.5	0.75	1
Группа № 2	1	0.7	0.5	0.9	0.4	1.5
Группа № 3	1.25	0.5	0.5	1	1	1.25
Группа № 4	1	1	1	0.5	1.5	1

В результате проведенного анализа была разработана методологическая схема выбора моделей прогнозирования, представленная на рис. 1.

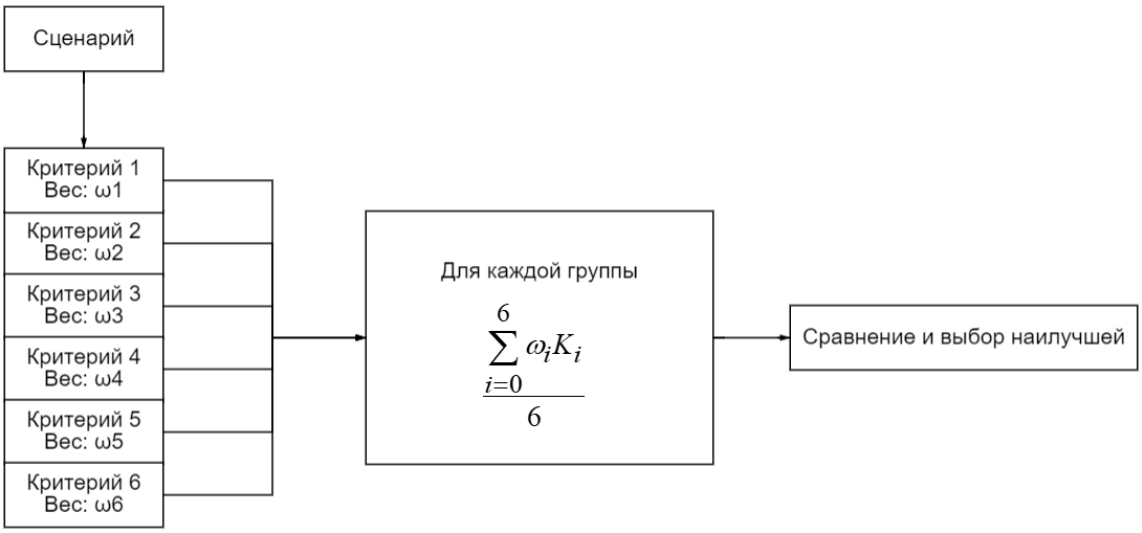


Рис. 1. Методологическая схема выбора моделей прогнозирования

На рис. 1. K_i соответствует значению *i*-го критерия на основании данных, представленных в таблице 2 (или табл. 1), а параметр ω_i определяет вес критерия, определяемого вручную в зависимости от конкретного сценария.

После того, как были определены веса, для каждой из группы возможно вычислить следующее значение, названное *оценкой группы относительно данного сценария*:

$$\frac{\sum_{i=0}^{6} \omega_i K_i}{6}.$$

После всех вычислений производится сравнение этих значений и выбор наилучшей группы на основании максимального значения из четырех оценок. Далее данная методологическая схема применяется уже к моделям из выбранной группы, а для значений K_i рассматривается уже таблица 1. Таким образом осуществляется эффективный выбор модели для предсказания трендов развития угроз информационной безопасности.

В рамках проведенного исследования были рассмотрены 12 наиболее популярных моделей прогнозирования, которые были поделены на 4 группы. Для оценки каждой модели были использованы 6 критериев, учитывающих особенности угроз информационной безопасности. Также был произведен сравнительный анализ групп и моделей, результаты которого обладают теоретической значимостью. На основе полученных результатов была разработана методологическая схема выбора моделей прогнозирования, которая обладает практической значимостью и может быть использована для повышения уровня безопасности информационных систем. Продолжением исследования должна стать детализация методологической схемы и ее применение в «боевых условиях» [5, 6, 7].

Список используемых источников

1. Израилов К. Е. Модель прогнозирования угроз телекоммуникационной системы на базе искусственной нейронной сети // Вестник ИНЖЭКОНа. Серия: Технические науки. 2012. N 8 (59). С. 150–153.

2. Мещеряков С. В., Кучерова К. Н., Щемелинин Д. А., Буйневич М. В., Израилов К. Е. Программа прогнозирования больших данных облачных систем на основе моделей временных рядов // Свидетельство о государственной регистрации программы для ЭВМ № 2020617736 от 10.07.2020.

3. Гудаков А. П., Израилов К. Е., Котенко И. В. Дискуссионная статья: прогнозирование возможностей применения неевклидовой геометрии в информационной безопасности // Информатизация и связь. 2022. N 3. С. 15–21. DOI 10.34219/2078-8320-2022-13-3-15-21.

4. Чучуева И. А. Модель прогнозирования временных рядов по выборке максимального подобия : дис. ... канд. техн. наук: 05.13.18 / Чучуева Ирина Александровна. Москва, 2012. 154 с.

5. Тоноян С. А., Черненький М. В., Тоноян А. С. Адаптивная модель прогнозирования временны́х рядов // Информационно-измерительные и управляющие системы. 2017. Т. 15. N 7. С. 46–53.

6. Политов М. С. Экспериментально-аналитический метод оценки и прогнозирования уровня защищенности информационных систем на основе модели временных рядов : дис. ... канд. техн. наук: 05.13.19 / Политов Михаил Сергеевич. Уфа, 2010. 145 с.

7. Блохин А. В. Исследование методов прогнозирования моделей временных рядов, используемых в области информационных технологий // Прикладная математика и фундаментальная информатика: материалы XII Международной молодежной научно-практической конференции с элементами научной школы (Омск, 16–21 мая 2022 года). Омск, 2022. С. 71–72.

УДК 004.056
ГРНТИ 81.93.29

ГИПОТЕТИЧЕСКИЙ МЕТОД ВОССТАНОВЛЕНИЯ МОДУЛЕЙ АРХИТЕКТУРЫ МАШИННОГО КОДА С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ВЫСОКОУРОВНЕВЫХ УЯЗВИМОСТЕЙ

К. Е. Израилов[1,2], И. В. Умаралиев[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Данная работа посвящена исследованию авторского метода восстановления архитектуры программы из машинного кода с целью поиска высокоуровневых уязвимостей. Описан метод по выделению логических модулей программы, что позволит восстановить и саму архитектуру. Работа метода основана на кластеризации метаинформации, полученной из машинного кода. Приводится графическая иллюстрация примера кластерного деления взаимных вызовов функций программы в 2D-пространстве, производится анализ результатов.

информационная безопасность, машинный код, реверс-инжиниринг, безопасность программного обеспечения, восстановление архитектуры.

Введение

Актуальность данного исследования обусловлена необходимостью выявления высокоуровневых уязвимостей программного обеспечения, определения потенциальных архитектурных проблем, определения системных

проблем, связанных с базовой архитектурой [1]. Обнаружение такого типа уязвимостей достигается путём применения к восстановленной метаинформации метода кластеризации для определения взаимодействий между компонентами.

Теоретически ожидается, что реализация идеи приведёт к открытию потенциально-успешных возможностей структурирования сложных, постоянно обновляющихся программных систем, в которых функции и логически/физически связанные файлы масштабируются со стечением времени [2]. В таких ситуациях повышение сложности программного обеспечения обратно пропорционально ремонтопригодности системы, где обновления могут не соответствовать требованиям и ограничениям к основополагающим модулям [3].

Также для проведения оценки эффективности предлагаемого метода на реальных примерах, необходима визуализация выделенных модулей программного обеспечения в 2D-пространстве.

Гипотеза

Гипотезой, лежащей в основе метода является предположение, что кластеризация метаинформации о взаимодействии функций программы (точек расположения в памяти, вызовов и пр.) позволить частично восстановить ее архитектуру. Как результат, можно будет выделить модули программы, интерфейсы их взаимодействия, безопасность процесса обмена информацией через интерфейсы, общие архитектурные проблемы и т. п. [4].

Метод выделения архитектуры

Опишем более детально шаги метода выявления высокоуровневых уязвимостей, основанного на модульном восстановлении архитектуры и показанного на рис. 1.

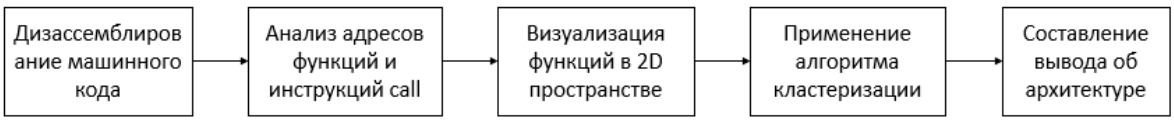


Рис. 1. Структурная схема метода восстановления
и анализа модулей архитектуры программного обеспечения

Дизассемблирование машинного кода будет осуществляться с помощью программного инструмента IDA Pro, который позволяет выделить такую метаинформацию из кода, как адрес начала функций программы и точки вызова других функций [5].

В интересах проведения дополнительного анализа IDA Pro позволяет автоматизировать действия над исследуемым машинным кодом с помощью

программных скрипов в IDC-нотации. Полученные результаты необходимы для определения положения функций в системе координат, где ось абсцисс соответствует точке вызова функции, а ось ординаты – расположению самой функции в памяти. Назовем множество точек, определяемых этими осями – пространством взятия функций.

Для модульного разбиения функций в двухмерном пространстве применяется алгоритм кластеризации k-mean. Алгоритм создаст группы из наборов объектов, чтобы предать членам группы однородность для изучения набора данных. Выбор данного метода кластерного анализа обосновывается его простотой, высокой скоростью выполнения и эффективностью по сравнению с другими алгоритмами [6].

Предполагается, что по выделенным кластерам можно будет делать выводы о безопасности архитектуры программного обеспечения, возможных трудностях в конструировании безопасного дизайна программы, интерфейсах подсистем и т. п. [7]

Эксперимент

Работоспособность метода была протестирована на примере межмодульного взаимодействия функций программы, содержащей 5 вызовов из текущего и другого модуля.

После запуска исполняемого файла и подключения разработанного IDC-скрипта в дизассемблере IDA Pro, были получены адреса расположения функций в памяти и информация о том, откуда они были вызваны.

Далее точки вызовов отображались в пространстве взятия функций с последующим выделением кластеров, отображая полученные области в 2D-пространстве (рис. 2).

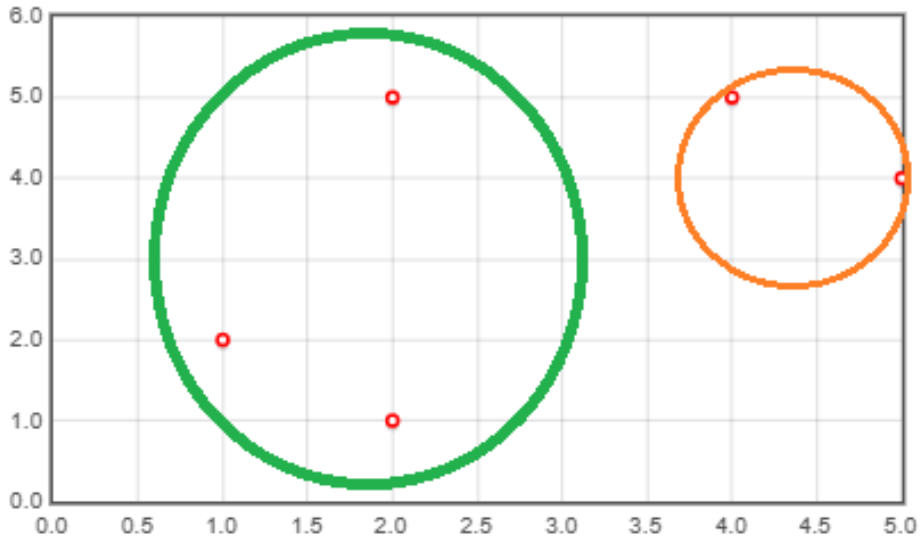


Рис. 2. Визуализация кластеризации модулей функции

Интерпретация кластеризации (рис. 2) с позиции восстановления архитектуры заключается в том, что было выделено два кластера, показывающих, что программа содержит вызовы, выполняющиеся из двух логических разделенных модулей.

Результаты эксперимента позволяют сделать вывод о правильности работы метода кластерного выделения модулей в задачах восстановления архитектуры программы из машинного кода, обосновывая описанную ранее гипотезу. В данном примере была частично восстановлена архитектура, что позволит эксперту произвести дельнейший анализ о потенциальных высокоуровневых уязвимостях.

Заключение

Проведенное исследование ставило своей целью попытку обоснования гипотезы, согласно которой учет точек расположения в памяти и вызовов функции дает возможность восстановления архитектуры программы, что может быть применено в интересах обеспечения информационной безопасности; проведенный эксперимент частично обосновал это.

Необходимо отметить, что анализ как полной архитектуры, так и подмножества компонентов и взаимосвязей между ними, с проведением реверс-инжиниринга гипотетически позволит разработчику продукта сфокусироваться на проблемах в тестировании и обслуживании программных продуктов [8].

Продолжением исследования должно стать улучшение и расширение методов и инструментов для анализа архитектуры программ с целью обеспечения ее безопасности. В частности, следует изучить возможность использования автоматизированных инструментов для анализа архитектуры и выявления уязвимостей, а также разработку методологий для проведения такого анализа.

Список используемых источников

1. Santos J. C. S., Tarrit K. and Mirakhorli M. "A Catalog of Security Architecture Weakes" // 2017 IEEE International Conference on Software Architecture Workshops (ICSAW), Gothenburg, Sweden, 2017. PP. 220–223. doi: 10.1109/ICSAW.2017.25.

2. Stringfellow, Catherine & Amory, C. D. & Potnuri, D. & Andrews, A. & Georg, Manfred. Comparison of software architecture reverse engineering methods // Information and Software Technology. 2006. N 48. PP. 484–497. doi: 10.1016/j.infsof.2005.05.007.

3. Harris D. R., Reubenstein H. B. and Yeh A. S. "Reverse Engineering to the Architectural Level" // 1995 17th International Conference on Software Engineering, Seattle, WA, USA, 1995. PP. 186–186. doi: 10.1145/225014.225032.

4. Буйневич М. В., Израилов К. Е. Идентификация архитектуры процессора выполняемого кода на базе машинного обучения. Часть 2. Способ идентификации // Труды учебных заведений связи. 2020. Т. 6. No 2. С. 104–112. DOI:10.31854/1813-324X-2020-6-2-104-112.

5. Израилов К. Е. Метод и программное средство восстановления алгоритмов машинного кода телекоммуникационных устройств для поиска уязвимостей // Региональная информатика «РИ-2014»: материалы XIV Санкт-Петербургской международной конференции (Санкт-Петербург, 29–31 октября 2014 г.). 2014. С. 140–141.

6. Израилов К. Е., Кузнецов С. А. Применение искусственного интеллекта и методов машинного обучения для поиска уязвимостей исходного кода // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020). IX Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 361–366.

7. Израилов К. Е. Визуализация многопризнаковых уязвимостей программного кода с помощью метода главных компонент // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 1. С. 3–8.

8. Acher M., Cleve A., Collet P., Merle P., Duchien L., Lahire P. Reverse Engineering Architectural Feature Models / In: Crnkovic, I., Gruhn, V., Book, M. (eds) Software Architecture. ECSA 2011 // Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2011. Vol. 6903. https://doi.org/10.1007/978-3-642-23798-0_25

УДК 004.056.52
ГРНТИ 50.41.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕШЕНИЙ ПО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО РАСПРОСТРАНЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

К. Е. Израилов[1,2], Е. И. Часовских[1]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Статья посвящена области защиты программного обеспечения. Целью работы является выявление наиболее эффективных методов защиты программ от несанкционированного распространения. В интересах этого производится обзор и критериальное сравнение методов защиты. Результаты сравнения представлены в табличном виде, определены наиболее подходящие решения. Продолжением работы будет расширение методов защиты и списка критериев для получения более полных и точных результатов сравнительного анализа.

защита ПО, программное обеспечение, несанкционированное распространение, несанкционированный доступ.

Введение

В условиях разрастания рынка программного обеспечения (далее – ПО) и потребления аналогичных программных средств клиентами для производителей и дистрибьютеров данной области растет и потребность в обеспечении контроля за правомерным распространением и использованием произведенного продукта. В связи с этим появляется множество вариантов защиты интеллектуальной собственности, сертификации программного кода и усложнения воровства его алгоритмов [1]. Данная статья направленна на выявление наиболее удачных решений путем их сравнительного анализа по ряду выделенных критериев.

Средства защиты

Приведем далее кратко обзор наиболее распространенных решений для недопущения несанкционированного распространению программных продуктов.

С_1. Электронный ключ

Статья [2] посвящена вопросу защиты от несанкционированного использования ПО на основе аппаратных и программных ключей с помощью ПО «Электронный ключ». Данная технология защиты от несанкционированного использования ПО базируется на построении модели запрос-ответ, в которой запросы отправляются из открываемого приложения или системы и адресуются к некоторому ранее созданному ключу. Процесс завязан на создании и проверке соответствия, созданного ЭЦП. Данный способ является кроссплатформенным, а решение может использоваться не только для защиты от нелегального использования, но также для защиты программного кода от изучения или копирования. Решение является довольно простым и недорогим вариантом для реализации, что гарантирует легкость в обслуживании, дистрибуции, тестировании и модернизации; однако это может стать и минусом, так как теми же возможностями будет обладать и потенциальный злоумышленник.

С_2. VMProtect

Статья [3] посвящена технологии защиты от анализа и взлома программного обеспечения – «VMProtect». В статье рассматривается вариант применения нескольких технологий таких как: виртуализация, мутация, в также их совместное применение. Описанный метод мутации кода ПО является потомком обфускации кода. Также возможно применение технологии виртуализация путем исполнения выделенного участка кода не напрямую в процессоре, а в программном окружении. Приведенный вариант

применим в системах, позволяющих осуществлять виртуализацию, что несколько ограничивает выбор платформ. Мутация кода является действенным методом защиты от анализа кода, не сильно нагружающим систему, но при анализе опытным реверсором может быть недостаточно действенной. Виртуализация является более мощным механизмом защиты кода, но сопоставимо сильно нагружает систему при виртуализации множества отдельных частей кода. Одной из особенностей данной технологии является добавление в код ПО водяных знаков [4], которые в свою очередь позволяют определить владельца программы. Данная технология предоставляет несколько вариантов версий защиты с применением дополнительных функций.

C_3. IntelliLock

Статья [5] посвящена технологии IntelliLock используемой для контроля лицензирования приложений. Данный способ защиты основывается на идее легкости и гибкости генерации зашифрованных файлов ПО. Пользователь также может интегрировать лицензирование в сторонние программные системы. IntelliLock использует RSA шифрование для создания мастер-ключа, который генерируется на выбранных параметров, например: дата окончания лицензии, количество дней действия лицензии, количество возможных запусков программы, время работы программы. Необходимыми условиями применения технологии являются следующие: ПК с микропроцессором класса Pentium; операционные система (далее – ОС) Windows 98/98SE/ME/NT 4.0/2000/2003/XP/Vista; NET Framework 2.0 или выше. Технология является удобным решением для тех производителей, которые хотят предоставлять своим клиентам пробные версии программ. Однако, продукт имеет ряд проблем при запуске пробной версии, а поддержку продукта нельзя назвать удовлетворительной.

C_4. Software key system

Статья [6] посвящена решению от компании Software key system по управлению лицензиями. Защита приложений основана на принципе выбора контролируемых параметров лицензирования для автоматизации процесса; например, возможно ограничивать версии ПО, сроки подписки, назначать условия продления и отмены подписки. При применении данного решения ПО может быть активировано с помощью простого двухстороннего процесса – запроса и ответа. При генерации запроса используется идентификационный слепок компьютера. Ответ содержит в себе зашифрованный файл лицензии с дополнительными параметрами и подтверждённым слепком компьютера. Решение является кроссплатформенным и поддерживает целый набор ОС. Продукт удобен как для тех, кто не знаком с программированием, так и для IT-специалистов (для осуществления более тонкой

настройки). Одной из особенностей данного решения является вариант развертывания системы лицензирования на облачной инфраструктуре [7].

C_5. Desaware

Статья [8] посвящена системе лицензирования Desaware, позволяющей контролировать полный ее процесс. В решении основным принципом защиты является многоуровневость и разнообразие предлагаемых методов, объединяемых в систему. Разработчику дается на выбор несколько способов защиты своего ПО; например, часть ПО, взаимодействующая с серверной частью, может отправлять запросы к частному, арендованному или облачному серверу. Разработчик может управлять пользовательским интерфейсом, алгоритмом аутентификации клиента, изменять информацию в лицензионном сертификате, интегрировать лицензии существующие системы, применять обфускацию кода ПО. Конкретной платформы или требований для решения не указано, поэтому можно считать данную систему кроссплатформенной. Плюсами решения является разнообразие способов лицензирования и контроля, возможность интегрирования сертификатов в уже существующие системы. Минусом является высокая цена. Особенностью решения является объединение методов лицензирования в единую систему для упрощенной настройки контроля ПО.

Сравнительный анализ

Для проведения сравнительного анализа рассмотренных программных средств были выведены следующие критерии (включая их возможные значения):

К_1) цена продукта: подписка, полный пакет;

К_2) тип реализации: программная или аппаратная, смешанная;

К_3) технология: сертификат, шифрование кода, виртуализация обфускация;

К_4) простота использования: 3 балла – готовый пакет для установки, 2 балла – после установки нужна дополнительная настройка, 1 балл – необходима дополнительная доработка или внедрение в устройство;

К_5) нагрузка продукта на целевую систему при выполнении операций по защите: 3 балла – практически не нагружается, 2 балла – нагрузка может считаться умеренной, 1 балл – испытывает существенную нагрузку;

К_6) охват поддерживаемых программно-аппаратных систем: 3 – любые, 2 – большинство, но с исключениями, 1 – только выделенные;

К_7) в каких государственных пределах разработано ПО: 3 балла – полностью отечественное, 2 балла – отечественное на основе импортного или с открытым исходным кодом [9], 1 балл – полностью импортное.

К_8) наличие пробной версии: 1 балла – есть, 0 балл – нет.

Согласно введенным критериям, был проведен сравнительный анализ, результаты которого были занесены в таблицу 1. В последней строке таблице приведена сумма численных критериев (т. е. К_4–К_8) для каждого из продукта.

ТАБЛИЦА 1. Критериальное сравнение решений

	C_1	**C_2**	**C_3**	**C_4**	**C_5**
К_1	1500 р.+ цена ПО	139–1599$	нет	49; 99; 199 $/месяц	$1500
К_2	Програм-мно- аппа-ратная	Программно-аппаратная	Программная	Про-граммная	Программная
К_3	Сертификат	Виртуализа-ция, обфуска-ция	Сертификация, шифрование	Сертифи-кация	Сертифика-ция, обфуска-ция
К_4	2	1	3	3	3
К_5	2	1	2	3	3
К_6	3	2	2	3	3
К_7	2	1	1	1	1
К_8	1	1	1	1	1
Сумма	10	6	9	11	11

Результаты

Анализ критериального сравнения (табл. 1) позволяют сделать следующие вывода. Во-первых, можно выделить два наиболее удачных решения: С_4 и С_5. Во-вторых, ни одно из решений не получило по К_7 максимальный балл, что говорит об недостатке отечественных разработок в сфере защиты ПО или их малой известности. И, в-третьих, значения по К_2 у решений совпали, поскольку все они имеют пробную версию; это говорит о возможности провести базовое тестирования решения при его выборе.

Вывод

В рамках текущего исследования был проведен обзор наиболее популярных решений по защите ПО от несанкционированного распространения. Последующее критериальное сравнение решений позволило условно выделить наиболее подходящие из них – Desaware и Software key system. Также, полученная сравнительная таблица позволит делать обоснованный выбор решений исходя из требования организаций.

Продолжением исследования должно стать расширение количества исследуемых решений и составление большего количества критериев для более точной оценки предложенных вариантов защиты ПО.

Список используемых источников

1. Буйневич М. В., Васильева И. Н., Воробьев Т. М., Гниденко И. Г., Егорова И. В., Еникеева Л. А. и др. Защита информации в компьютерных системах: монография. СПб. : СПбГЭУ, 2017. 163 с.
2. Цыцура К. С., Потоловский А. И. Технология защиты от несанкционированного использования программного обеспечения «Электронный ключ» // Актуальные проблемы авиации и космонавтики. 2016. Т. 1. N 12. С. 664–666.
3. VMProtect Software Protection: официальный сайт программного продукта [Электронный ресурс]. URL: https://vmpsoft.com/ (дата обращения 27.03.2022).
4. Коржик В. И., Старостин В. С., Флаксман Д. А., Разработка метода использования цифровых водяных знаков для защиты от атаки клонирования бумажных сертификатов // Труды учебных заведений связи. Т. 7. N 2. 2021. С. 79–84.
5. IntelliLock: официальный сайт программного продукта [Электронный ресурс]. URL: https://www.eziriz.com/intellilock.htm (дата обращения 27.03.2022).
6. Software key system: официальный сайт программного продукта [Электронный ресурс]. URL: https://www.softwarekey.com/ (дата обращения 27.03.2022).
7. Мещеряков С. В., Щемелинин Д. А., Израилов К. Е. Принципы организации и мониторинга облачных мультисервисных систем. СПб. : СПбПУ, 2022. 165 с.
8. The Desaware Licensing System: официальный сайт программного продукта [Электронный ресурс]. URL: https://desaware.com/ (дата обращения 27.03.2022).
9. Левин И. Прогноз ландшафта открытого исходного кода в 2023 году // БИТ. Бизнес & Информационные технологии. 2022. N 10 (123). С. 34–35.

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АВТОМАТИЧЕСКОГО РАНЖИРОВАНИЯ УЯЗВИМОСТЕЙ ПО ИХ ТЕКСТОВОМУ ОПИСАНИЮ

К. Е. Израилов[1,2], А. Ю. Ярошенко[3]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[3]Департамента информационных технологий и связи МЧС России

Работа посвящена поиску уязвимостей в интерфейсах транспортной инфраструктуры Умного города. Одной из актуальных задач исследования является автоматическое определение и ранжирование уязвимостей для выбора порядка их нейтрализации. Притом, в качестве исходных данных об уязвимостях берется только их текстовое описание, данное человеком вручную. Для этого оказывается возможным применять различные модели и методы машинного обучения. Описывается ход и результаты проведенного эксперимента для российской базы данных уязвимостей. Делается сравнение

результативности следующих классификаторов: ExtraTreeClassifier, Svm.SVC, MLPClassifier, ExtraTreesClassifier, RandomForestClassifier. Полученная F-мера в среднем показала значение ~0.65, что можно считать удовлетворительным, хотя и требующим доработки.

информационная безопасность, уязвимости, ранжирование, Умный город.

Введение

Умный город считается одной из самых передовых интеллектуальных концепций современного мира. Однако кроме очевидных преимуществ она несет и ряд существенных угроз. Так, ошибки информационного мира могут являться причиной проблем и физического. Наиболее актуально это для подсистем Умного города, связанных с функционированием сложных устройств или участием в них человека. Например, уязвимости программного обеспечения встроенных устройств могут приводить не только к сбою в работе сервисов, но и к финансовым потерям или же человеческим жертвам. Одной из таких подсистем, в которой проблема безопасности стоит наиболее остро, является транспортная инфраструктура. Особенностью же инфраструктуры может считаться постоянное взаимодействие составляющих ее компонент (людей, автомобилей, умных дорожных знаков и т. п.) через специализированные интерфейсные устройства. Однако уязвимостям в последних уделяется недостаточное количество внимания по причине их малой изученности, а также из-за попыток внедрения в практическое использование еще не до конца отлаженных продуктов (в погоне за экономической выгодой). Таким образом, цель текущего исследования можно обозначить как *обеспечение безопасности людей, транспортных средств и объектов инфраструктуры за счет обнаружения уязвимостей интерфейсов «человек – искусственный интеллект» в транспортной инфраструктуре Умного города*. Для этого требуется разработать не только соответствующий метод поиска, за которым логично последует оперативная нейтрализация уязвимостей, но и определить способ выбора порядка противодействия [1, 2, 3]. Одна же из основных задач ставится как *метод автоматического ранжирования уязвимостей*, которая позволит обоснованно выбирать те уязвимости, которые необходимо нейтрализовывать в первую очередь.

Прототип ранжирования

Гипотеза, лежащая в основе метода автоматического ранжирования уязвимостей транспортной инфраструктуры Умного города заключается в составлении их описания экспертом и применении методов машинного обучения для автоматического определения уровня опасности уязвимостей (что является продолжением предыдущих авторских исследований [4]). Так, уязвимости с наиболее высоким уровнем должны быть обнаруживаться

и нейтрализовываться в первую очередь. Для проверки гипотезы был разработан прототип ранжирования, который в качестве описания использовал информацию из базы данных уязвимостей от ФСТЭК. База на сегодняшний день содержит описание и характеристики около 45 тысяч уязвимостей. Одной из характеристик уязвимостей является «Уровень опасности», который может принимать 4 следующих значения: низкий, средний, высокий и критический. Принцип работы прототипа как раз и заключался в попытке определения уровня опасности уязвимости по ее описанию, для чего было применено машинное обучение.

Формализация описания уязвимостей обеспечивалась применением техники TF-IDF (аббр. от англ. Term frequency-Inverse Document Frequency), основанной на оценке важности слова в документе [5]. Принцип действия техники заключается в придании большего значения словам, которые часто встречаются в данном описании, но реже в остальных. Использование TF-IDF позволило перейти от человеко-ориентированного текстового описания уязвимостей к их формальному – в виде весов каждого из слов [6]. Для определения уровня опасности использовались следующие классические модели и методы машинного обучения [7]: ExtraTreeClassifier, Svm.SVC, MLPClassifier, ExtraTreesClassifier, RandomForestClassifier. Прототип был реализован на языке Python с применением библиотек Pandas, NumPy, re, Collections, matplotlib, scikit-learn, Transformers.

Эксперимент

Для проверки гипотезы были осуществлены эксперименты с разработанным прототипом и базой данных уязвимостей. Оценка качества работы классификации определялась с помощью F-меры (гармонического среднего между точностью и полнотой). Результаты применения прототипа для базы данных уязвимостей ФСТЭК и указанных классификаторов приведены в таблице 1.

ТАБЛИЦА 1. Результаты классификации уровня опасности уязвимостей по их текстовому описанию

Классификатор	F-мера	Рейтинг
ExtraTreeClassifier	0,65084312	1
Svm.SVC	0,622730598	4
MLPClassifier	0,605578312	5
ExtraTreesClassifier	0,649937352	2
RandomForestClassifier	0,632009897	3

Результаты оценок работы прототипа по определению уровня опасности уязвимостей позволяют сделать следующие выводы. Во-первых,

наилучшим классификатором оказался ExtraTreeClassifier, представляющий собой сильно рандомизированный древовидный классификатор. Во-вторых, наихудшие значения показал MLPClassifier, являющийся многослойным перцептроном. И, в-третьих, разница между наилучшим и наихудшим классификатором составляет 7,5 % ($\frac{0{,}045264808}{0{,}605578312} = 0{,}0747464152910417$), что говорит о достаточной близости всех полученных оценок.

Выводы

В исследовании была проведена проверка гипотезы о возможности определения некоторых важнейших характеристик уязвимостей по их текстовому описанию. На данный момент качество такой классификации можно считать удовлетворительным, хотя и требующим существенных улучшений. Так, в других экспериментах применение техники Word2Vec [8] для зарубежных баз данных уязвимостей и специализированных токенизаторов показало существенно лучшие результаты (F-мера составила примерно 0,89).

Продолжением исследования должно стать повышение качества классификации, увеличение числа уровней опасности, определение других характеристик уязвимостей, а также применение описанного подхода для более сложных объектов информационной безопасности [9].

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-29-06099.

Список используемых источников

1. Буйневич М. В., Ахунова Д. Г., Ярошенко А. Ю. Комплексный метод решения типовой задачи риск-менеджмента в инфологической среде (на примере ранжирования требований пожарной безопасности). Часть 1 // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2020. N 3. С. 88–99.

2. Буйневич М. В., Ахунова Д. Г., Ярошенко А. Ю. Комплексный метод решения типовой задачи риск-менеджмента в инфологической среде (на примере ранжирования требований пожарной безопасности). Ч. 2 // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2020. N 4. С. 78–89.

3. Ярошенко А. Ю. Предпосылки к необходимости непрерывного ранжирования требований пожарной безопасности // Национальная безопасность и стратегическое планирование. 2021. N 3 (35). С. 100-105.

4. Izrailov K.E., Buinevich M.V., Kotenko I.V., Yaroshenko A.Y. Identifying characteristics of software vulnerabilities by their textual description using machine learning // World Automation Congress (Taipei, Taiwan, 1-5 august 2021). 2021. PP. 186–192. DOI: 10.23919/WAC50355.2021.9559470.

5. Яцко В. А. Достоинства и недостатки взвешивания терминов по формуле TF*IDF // В мире научных открытий. 2013. N 6 (42). С. 229–244.

6. Савченко Т. Ю. Обработка естественного языка для использования в машинном обучении: частотная векторизация, TF-IDF, Word2Vec // Аллея науки. 2018. Т. 4. N 6 (22). С. 1000–1002.

7. Pchelin A. V., Kononov N. A., Serova V. S., Bunova E. V., Marchenko A. D., Shevchenko A. Y. Analysis of machine learning models by solving the text data classification problem // Journal of Computational and Engineering Mathematics. 2021. V. 8. N 2. PP. 33–45.

8. Мишенин А.Н., Нефедова Е.А. Анализ тональности текстов с использованием технологии Word2Vec // Естественные и математические науки в современном мире. 2016. N 7 (42). С. 89-97.

9. Kotenko I., Izrailov K., Buinevich M. Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches // Sensors. 2022. Vol. 22. Iss. 4. PP. 1335. DOI: 10.3390/s22041335

УДК 621.391
ГРНТИ 81.93.29

АНАЛИЗ СЕТЕВОГО ТРАФИКА В СОВРЕМЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ

О. Б. Ильина[1], О. П. Купчиненко[1], А. В. Скоропад[2]

[3]Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного
[2] Филиал ФГУП НИИР-ЛОНИИР

Рассмотрены задачи анализа сетевого трафика, особенности анализаторов трафика, их общие свойства и отличия. Проведен анализ популярных средств мониторинга и анализа сетевого трафика в современной операционной системе специального назначения. Проанализированы возможности графических и консольных утилит для мониторинга, анализа и визуализации сетевого трафика, которые могут помочь выявить проблемы в работе локальной сети.

анализ сетевого трафика, перехват пакетов, мониторинг трафика сети, сниффер, средства анализа сетевого трафика.

Анализ сетевого трафика в операционной системе специального назначения Astra Linux SE является одним из действенных методов обеспечения безопасности сети. Актуальность анализа сетевого трафика растет в связи с развитием сетевых технологий, использованием новых сетевых протоколов и увеличением объема передаваемых по сети данных.

Низкие требования, предъявляемые технологией анализа трафика сети к вычислительным ресурсам, позволяют анализировать большие объёмы сетевого трафика. Эта технология используется и для разграничения доступа

извне к компьютерам и портам внутренней сети. На основе технологии анализа сетевого трафика разработаны сетевые списки контроля доступа ACL (Access Control List) на уровне IP-адресов и портов [1], а также на ее основе функционируют многие сетевые устройства: маршрутизаторы, большинство межсетевых экранов [2, 3] и другие устройства.

Анализ сетевого трафика – это метод, который с помощью захвата и просмотра трафика сети позволяет обнаруживать вредоносные программы, а также проблемы и ошибки различного типа, приводящие к замедленной или ненадежной работе сети. Анализ сетевого трафика используется для идентификации протоколов передачи данных, управления обменом данных и восстановления потоков данных в компьютерных сетях, а также для сбора статистики и решения задач мониторинга вычислительных сетей, который необходим и для предотвращения сетевых атак, и для выявления проблем в работе локальной сети.

Мониторинг трафика сети – это процесс непрерывного автоматизированного наблюдения за некоторыми параметрами трафика для проверки планирования сети и предотвращения негативных событий (неисправных компонентов, а также атак и угроз злоумышленников).

Задачу анализа сетевого трафика можно разделить на независимые подзадачи, которые представлены на рис. 1.

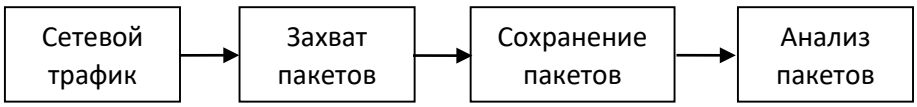


Рис. 1. Подзадачи анализа сетевого трафика

Для анализа сетевого трафика необходимы знания об основах работы сети, так как иначе понять, что найдено в массе собранных пакетов, очень сложно, т. е. анализ сетевого трафика позволяет изучить логику работы сети и перехватить поток данных, которыми обмениваются объекты сети.

Анализатор трафика или сниффер (*sniffer*) – это программное или аппаратно-программное устройство, работающее на канальном уровне модели OSI (*Open Systems Interconnection*) и предназначенное для мониторинга и анализа трафика сети.

Перехват трафика сети осуществляться с помощью режима «прослушивания», который позволяет получать сетевые данные, предназначенные другим сетевым интерфейсам.

Снифферы могут перехватывать весь трафик и сохранять его в двоичном формате, а потом – расшифровывать. Они не используют правила протоколов верхнего уровня модели OSI и обходят механизмы фильтрации, которые используются для интерпретации данных в стеке TCP/IP (*Transmission Control Protocol / Internet Protocol*).

Анализаторы трафика сети обладают следующими свойствами:

- измерения различных показателей трафика в сегменте локальной сети;
- работа с несколькими агентами, которые из разных сегментов локальной сети поставляют перехваченные пакеты;
- фильтрация отображаемых и перехваченных пакетов;
- использование условий начала и завершения процесса захвата сетевых данных;
- одновременная запись пакетов от нескольких сетевых адаптеров, позволяющая сопоставлять процессы, которые происходят в разных сегментах сети.

Различия сетевых анализаторов:

- возможность поддержки графического интерфейса;
- поддерживаемые сетевые протоколы;
- глубина анализа захваченных пакетов;
- возможность настройки фильтров до и после захвата сетевого трафика;
- совместимость с другими программами.

Сетевые анализаторы можно разделить на имеющие графический интерфейс и работающие из командной строки. Но, существуют снифферы и объединяющие эти возможности.

Некоторые анализаторы трафика сети могут захватывать и декодировать пакеты различных сетевых протоколов. Они распознают и поддерживают большое количество сетевых протоколов, могут их описать и декодировать по именам, а также определить, каким приложением порожден сетевой трафик.

Почти все сетевые анализаторы могут выполнять анализ декодированных пакетов. Графический интерфейс позволяет увидеть результаты декодирования пакетов с разной степенью детализации. Существуют снифферы с аналитическими модулями, которые позволяют создавать отчеты о перехваченном сетевом трафике.

Другой особенностью большинства анализаторов трафика является возможность настройки фильтров, как до захвата трафика сети, так и после него, что позволяет выделить из всего трафика пакеты, соответствующие заданным критериям и, таким образом, уменьшить объем перехваченной информации.

Некоторые снифферы обладают возможностью работать с перехваченным трафиком, сохраненным в файл своего формата или формата других сетевых анализаторов. Это позволяет провести более детальный анализ трафика сети.

Основной недостаток анализаторов трафика сети заключается в том, что они предоставляют большой объем сетевых данных, которые очень сложно анализировать.

Операционная система специального назначения Astra Linux SE включает в себя набор как графических, так и консольных утилит для анализа, мониторинга и визуализации сетевого трафика, которые могут помочь выявить проблемы в работе локальной сети.

Рассмотрим средства анализа сетевого трафика в операционной системе специального назначения Astra Linux SE, представленные в таблице 1.

ТАБЛИЦА 1 Средства анализа сетевого трафика

Название	Назначение	Возможности
Tcpdump	Утилита командной строки для сбора данных и анализа сетевого трафика	Просмотр всего (или части) входящего и исходящего трафика определенного хоста. Наблюдение за входящим и исходящим трафиком определенного порта. Слежение за определенной рабочей станцией. Выявление вредоносной рабочей станции. Протоколирование трафика определенной рабочей станции, для последующего анализа. Поиск подозрительного сетевого трафика. Задание интерфейса для «прослушивания». Запись необработанных пакетов в файл. Загрузка правил фильтрации из указанного файла.
Wireshark	Для выявления и решения проблем в сети, для изучения внутреннего устройства сетевых протоколов, для отладки сетевых приложений.	Перехват трафика различных видов сетевого оборудования в режиме реального времени. Показ декодированных пакетов во время перехвата. Возможность подсвечивать захваченные пакеты разных протоколов. Возможность создавать разнообразную статистику. Фильтрация пакетов по множеству критериев. Поиск пакетов по множеству критериев. Запись дампов в несколько файлов. Сохранение и открытие ранее сохраненного сетевого трафика. Импорт и экспорт файлов из других пакетных анализаторов. Возможность следовать за потоком.

Tcpdump – это утилита командной строки с открытым исходным кодом и мощным инструментом анализа, которая используется для сбора данных сетевого трафика. С помощью ее опций можно задать как простые пара-

метры (количество пакетов, которые необходимо перехватить), так и сложные (из заголовков пакетов можно выбрать определенные биты для анализа установленных флагов). Tcpdump имеет сложный язык фильтрации, поэтому для того, чтобы получить набор сетевых данных для анализа, необходимо понимать, как фильтровать данные при сборе.

Для работы анализатору сетевого трафика необходимо перевести сетевую плату в режим прослушивания, в котором она будет перехватывать весь трафик сети, а не только адресованный ей.

Tcpdump выдает содержимое пакетов TCP/IP, проходящих через сетевой интерфейс, на экран или в файл формата pcap. Это не текстовый файл, поэтому для его анализа нужна специальная программа, понимающая данный формат. Но иногда достаточно выводить захваченные сетевые данные на экран, чтобы найти то, что нужно.

Wireshark – это анализатор сетевого трафика с открытым исходным кодом, позволяющий не только захватывать данные сетевого трафика и отображать их в детальном виде, но и предоставлять некоторые инструменты анализа. Он работает на большинстве современных операционных систем.

Одна из главных возможностей Wireshark – это перехват сетевого трафика в режиме реального времени, но он также может работать и с заранее сохраненным сетевым трафиком. Wireshark может перехватывать трафик различных сетевых устройств, в том числе и беспроводных. Он сохраняет данные перехваченного трафика в файл формата pcap или в форматы других сетевых анализаторов.

На сервере с графическим интерфейсом Wireshark может собрать перехваченные данные и проанализировать их. Он содержит множество декодировщиков для различных сетевых протоколов. Если захват трафика выполнялся на компьютере без графического интерфейса, то можно импортировать полученный файл и проанализировать его с помощью Wireshark на другом компьютере, так как для этого файла будут доступны те же инструменты и фильтры, что и для захваченного сетевого трафика.

С помощью рассмотренных средств анализа сетевого трафика можно создать инфраструктуру мониторинга сети. Например, используя планировщик заданий, можно в нужное время с помощью tcpdump запустить сеанс сбора сетевого трафика, записать перехваченные сетевые данные в файл и проанализировать их с помощью wireshark.

Разные виды сетевых проблем, связанных с передачей и получением данных в сети, могут быть быстро определены и исправлены благодаря информации, полученной с помощью вышеперечисленных средств анализа сетевого трафика.

Используя результаты анализа данных сетевого трафика, можно понять, что происходит в сети, найти и устранить неполадки, модернизировать

компоненты сети и оптимизировать ее производительность. Для этого анализ данных выполняется как до, так и после изменений компонентов сети.

Список используемых источников

1. Ильина О. Б., Купчиненко О. П., Скоропад А. В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 2. С 356–360.

2. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу о сетевой безопасности и фильтрации пакетов // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 313–318.

3. Ильина О. Б., Купчиненко О. П., Скоропад А. В. К вопросу обеспечения информационной безопасности сети с помощью фильтрации пакетов // Информационная безопасность регионов России : материалы XI Санкт-Петербургской международной конференции, СПб, 23-25 октября 2019 г. СПб. : СПОИСУ, 2019. Т. 2. С. 434–436.

УДК 004.056
ГРНТИ 81.96

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ОТ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ

Е. А. Ичетовкин, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Для выявления атак на сетевые устройства используют системы обнаружения вторжений. Среди таких систем наиболее перспективными являются системы обнаружения вторжений эвристического типа с компонентами машинного обучения на базе нейронных сетей. Компоненты машинного обучения систем обнаружения вторжений, в свою очередь, могут быть подвергнуты различным атакам, что скомпрометирует их работу и, следовательно, нельзя будет гарантировать корректность результата обнаружения атак. По этой причине одной из наиболее актуальных задач кибербезопасности является анализ методов защиты систем обнаружения вторжений от атак на компоненты машинного обучения.

машинное обучение, нейронные сети, система обнаружения вторжений, защита от атак на компоненты машинного обучения.

Компоненты машинного обучения систем обнаружения вторжений являются составной частью систем обнаружения вторжений [1, 2, 3], выполняющих функцию эвристического анализа сетевого трафика, которая в настоящее время чаще всего реализуется на основе (глубоких) нейронных сетей. Поскольку данный компонент непосредственно участвует в обнаружении атак, злоумышленники могут предпринять попытку атаки на компоненты машинного обучения систем обнаружения вторжений с целью их компрометации.

В предыдущих исследованиях первостепенное внимание при реализации методов обучения компонентов машинного обучения было сосредоточено на повышении точности, полноты и производительности различных алгоритмов обнаружения, а не на их безопасности [4]. С учетом реализации атак на компоненты машинного обучения остро встает проблема защиты от таких атак.

В общем виде место и роль процессов защиты компонентов машинного обучения от атак может быть представлена, как показано на рис. 1. Механизмы защиты должны предотвратить компрометацию компонентов машинного обучения и обеспечить их правильное функционирование в условиях реализации различного набора атак.

Методы защиты компонентов машинного обучения систем обнаружения вторжений, как правило, защищают от ограниченного числа атак, каждый метод имеет свои преимущества и недостатки, и ограничен по возможности применения.

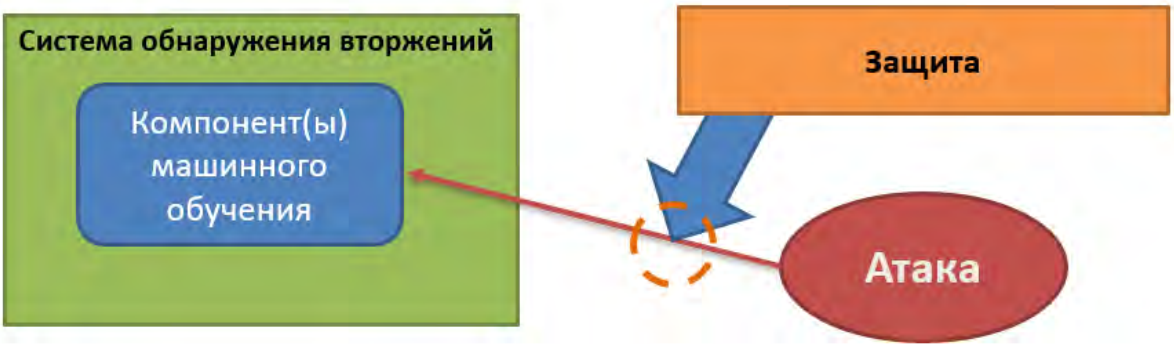


Рис. 1. Место и роль защиты компонентов машинного обучения систем обнаружения вторжений

В общем случае разработчик системы обнаружения вторжений с компонентами машинного обучения сначала вводит состязательные предположения в отношении уязвимостей классификатора. Затем разработчик предлагает контрмеры для защиты классификаторов от злоумышленников.

Рассмотрим ниже несколько методов защиты компонентов машинного обучения от атак, которые могут быть использованы в системах обнаружения вторжений.

В [5] предлагается использование метода защиты компонента машинного обучения, вызывающего *отклонение из-за негативного воздействия.* Метод основан на исключении из выборки образцов, которые имеют большое негативное влияние.

Чтобы количественно измерить влияние на эффективность классификации, сравнивается частота ошибок между исходным классификатором и новым классификатором, который был повторно обучен после добавления вредоносных выборок в исходные данные. Если частота ошибок нового классификатора намного ниже, чем у исходного, то новые добавленные образцы считаются вредоносными данными и удаляются из обучающих данных.

В дальнейшем такой метод может быть усовершенствован в части расчета эффективности при отборе крупномасштабных выборок-кандидатов.

Выделены следующие преимущества данного метода: эффективно удаляет состязательные выборки, которые вводятся в обучающие данные, масштабируется для различных классификаторов. Однако, в [5] не представлено всесторонней оценки производительности в различных сценариях применения данного метода.

Классический метода защиты – *состязательное обучение* – был рассмотрен в [6]. Цель состязательных выборок на этапе обучения состоит в том, чтобы изменить распределение тестовых данных, что приведет к значительному отклонению от распределения обучающих данных.

Затем ложные срабатывания увеличиваются, следовательно, возможным способом защиты от злоумышленников является подгонка распределений тестовых данных путем переобучения моделей, с использованием враждебных образцов.

Таким образом, новые обученные классификаторы могут обнаруживать аномалии на этапе тестирования, в [6] продемонстрировано, что метод может значительно снизить частоту ложных срабатываний моделей обучения в отношении враждебных выборок с 89,4 до 17,9 %.

Преимущества этого метода: метод легко понять и внедрить, он масштабируется для различных классификаторов. Основным недостатком метода является то, что его эффективность зависит от состязательных образцов на этапе обучения.

В [6] проведен анализ метода *дистилляции.* Показано, что этот метод защиты позволяет получить более плавную модель глубокую нейронную сеть (DNN, *Deep Neural Network*) за счет снижения чувствительности к входным возмущениям, а также улучшает способность *DNN* к обобщению и эффективно смягчает состязательные образцы, созданные методом быстрого градиентного спуска (FGSM, *Fast Gradient Sign Method*).

Кроме того, стратегия уменьшения размерности (дистилляции*)* может использоваться для защиты моделей машинного обучения от атак уклонения.

Эта стратегия была направлена на повышение устойчивости классификаторов за счет уменьшения размерности выборочных признаков. Экспериментальные результаты подтвердили, что стратегия эффективна для защиты нескольких типов моделей машинного обучения, таких как SVM (*support vector machines*) и DNN.

Основным недостатком, отмеченным авторами, является то, что метод недостаточно эффективен для защиты от состязательных образцов.

В [7] производилась оценка *ансамблевого метода* защиты компонента машинного обучения. Метод основан на использовании ансамблевой структуры, которая эффективно объединяет несколько DNN для защиты от атак на компонент машинного обучения. Кроме того, такой подход можно масштабировать для интеграции нескольких методик защиты.

Основное преимущество метода в том, что он гибок для интеграции нескольких классификаторов или различных методов защиты, одновременно с этим отмечается, что метод не устойчив к состязательным образцам с возможностью переноса.

В [7] также произведена оценка метода *дифференцирования,* основанного на обеспечении конфиденциальности данных посредством шифрования. Результаты расчета дифференцированной (отдельной) выборки данных не чувствительны к изменению одной записи данных. Таким образом, риск утечки конфиденциальной информации после добавления новой записи данных контролируется в очень небольшой области.

По сравнению с обычными моделями сохранения конфиденциальности, дифференцирование имеет следующие два преимущества: Модель предполагает, что злоумышленник имеет полное знание о записях данных, за исключением целевой записи, при таком допущении модели не нужно учитывать степень осведомленности злоумышленника. Модель построена на прочной математической основе. При этом нужно учитывать, что метод негативно влияет на производительность классификаторов.

В [8] оценивается метод защиты компонента машинного обучения, основанный на *гомоморфном шифровании.* Показано, что этот метод обеспечивает безопасность данных и приватную среду, но при этом приводит к значительным расходам на вычисления.

В соответствии с [8] методы защиты можно разделить на две подгруппы:

- методы для обнаружения состязательных примеров,
- методы для повышения устойчивости классификатора к состязательным примерам, без явных попыток их обнаружения.

Каждый метод защиты либо зависит от конкретной атаки (требуются состязательные примеры), либо не зависит от атаки (работает против всех типов атак). Предполагается, что в исследованиях методов защиты от атак на компоненты машинного обучения основное внимание должно быть уделено методам защиты, не зависящим от атаки, или формированию комплексного подхода к защите, сочетающего несколько методов защиты, поскольку методы защиты, зависящие от атаки (например, состязательное обучение), обеспечивают очень узкую защиту от растущего разнообразия атак.

Заключение

В статье обоснована актуальность защиты компонента машинного обучения систем обнаружения вторжений, и рассмотрены отдельные методы защиты. Представлен качественный анализ различных методов защиты с их преимуществами и недостатками. По результатам исследования сделан вывод о необходимости проведения сравнения различных методов защиты и формирования комплексного подхода к защите, основанного на использовании комбинации различных методов защиты. Направлениями дальнейшего исследования являются разработка методики защиты систем обнаружения вторжений от атак на компоненты машинного обучения, формирование архитектуры компонентов защиты и программная реализация подсистемы защиты систем обнаружения вторжений от атак на компоненты машинного обучения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. N 11. С. 993–1001.

2. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference “Simulation in wider Europe”. ECMS 2005. Riga, Latvia, 1–4 June 2005. PP. 533–543.

3. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. 2018. Vol. 6. PP. 72714–72723. DOI: 10.1109/ACCESS.2018.2881998.

4. Rosenberg I., Shabtai A., Elovici Y., Rokach L. Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain // ACM Comput. Surv. 54, 5, Article 108 (May 2021). PP. 1–57.

5. Liu Q., Zhao W., Li P., Cai W. A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View // IEEE Access, February 2018. PP. 12103–12117.

6. Pitropakis N., Giannetsos T., Anastasiadis E. A taxonomy and survey of attacks against machine learning // IEEE Access. November 2019. PP. 1–45.

7. Carlini N., Wagner D. Towards evaluating the robustness of neural networks // IEEE Symp. Secur. Privacy, San Jose, CA, USA. May 2019. PP. 39–57.

8. Papernot N., McDaniel P., Jha S., Fredrikson M., Celik Z. B., Swami A. The limitations of deep learning in adversarial settings // IEEE Eur. Symp. Secur. Privacy (EuroSP), Saarbrucken, Germany, Mar. 2016. PP. 372–387.

УДК 004.056
ГРНТИ 81.96

АНАЛИЗ АТАК НА КОМПОНЕНТЫ МАШИННОГО ОБУЧЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Е. А. Ичетовкин, И. В. Котенко

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

При мониторинге кибербезопасности крайне важно, чтобы системы обнаружения вторжений, использующие компоненты машинного обучения, могли адекватно выполнять свое предназначение - обнаруживать присутствие злоумышленников на ранней стадии атаки, оперативно локализовать угрозы и контролировать соблюдение регламентов информационной безопасности. Однако нельзя гарантировать адекватное выполнение функций обнаружения вторжений, если компоненты машинного обучения сами подвергаются атакам (так называемым состязательным атакам). Для выработки методов противодействия таким атакам, необходимо провести анализ атак на компоненты машинного обучения систем обнаружения вторжений. Данная статья посвящена данной проблематике.

машинное обучение, нейронные сети, атаки на компоненты машинного обучения.

Системы обнаружения вторжений (СОВ) – аппаратно-программные системы сетевой безопасности, предназначенные для выявления компьютерных атак и аномалий [1, 2, 3]. Инструменты СОВ могут использоваться отдельно или же в составе межсетевых экранов. Первые системы для обнаружения вторжений использовали сигнатурный анализ, также называемый анализом на основе правил. Существенный недостаток таких систем заключался в непригодности защиты от новых или неучтенных в правилах атак. Из-за этих недостатков начали использовать эвристический анализ [4].

В последние годы для эвристического анализа используют методы машинного обучения на базе нейронных сетей. Использование эвристического анализа позволяет обнаруживать новые, ранее неизвестные атаки или любую другую активность, не попавшую ни под какую конкретную сигнатуру.

Например, при работе с зашифрованным трафиком *HTTPS* продемонстрировано превосходство СОВ с компонентами машинного обучения (*ML* СОВ) по сравнению с сигнатурной СОВ *Suricata* [4].

Однако не смотря на свое преимущество, компоненты машинного обучения систем обнаружения вторжений могут быть подвержены атакам со стороны злоумышленника.

В [5] приводится такая классификация атак:

1) по цели атакующего:

- атаки, направленные на нарушение конфиденциальности;
- атаки, направленные на нарушение целостности – классификатор на основе машинного обучения ошибочно классифицирует образец;
- атаки, направленные на нарушение доступности – система машинного обучения становится недоступной;

2) по знаниям атакующего:

- «*черный ящик*», не требует никаких знаний о модели;
- «*серый ящик*», требует ограниченной степени знаний о целевом объекте;
- «*белый ящик*», атакующий знает об архитектуре модели и даже о параметрах, используемых для обучения модели;
- «*прозрачный ящик*», атакующий обладает полным знанием о системе, включая как знания белого ящика, так и знания о защите. Такая атака, способная обойти защитный механизм;

3) по фазе (этапу):

- *атака на этапе обучения* – эта атака направлена на введение уязвимостей во время фазы обучения;
- *атака на этапе вывода* – атака направлена на поиск и последующее использование уязвимостей на этапе классификации;

4) по объектам воздействия (изменяемым признакам):

- статистика файлов данных PCAP, содержащих данные пакетов, передаваемых в сети;
- поля заголовка PCAP-файлов (например, IP или UDP);
- поля заголовка PE (*Portable Executable*, «переносимый исполняемый», т. е. формат исполняемых файлов всех 32- и 64-разрядных Windows-систем);
- строки PE-файла;
- бинарное содержимое PE-файла;
- вызовы API (во время динамического анализа PE-файла);
- слова в содержании письма электронной почты;
- символы в URL.

Эффективность каждой атаки обусловлена используемыми методами реализации атаки, выбранными злоумышленником. Среди атак на компоненты машинного обучения систем обнаружения вторжения выделяется множество основных классов методов реализации атаки [5]:

- метод, основанный на оптимизации;
- метод быстрого градиентного спуска (FGSM, *Fast Gradient Sign Method*). FGSM - это одношаговый алгоритм, который генерирует возмущения в направлении градиента потерь;
- итеративный метод наименее вероятного класса (Iterative Least Likely Method, ILLM). Выбирая наименее вероятный класс для каждого примера, он дает представление о наихудшем сценарии для алгоритма;
- метод глубокого обмана (*DeepFool).* DeepFool ищет кратчайшее расстояние для пересечения границы решения, используя итеративную линейную аппроксимацию классификатора и ортогональную проекцию на него точки выборки;
- якобианский анализ (JSMA, *jacobian saliency map attacks*). Насыщая несколько пикселей в заданном изображении до их максимальных или минимальных значений, JSMA может привести к тому, что модель ошибочно классифицирует результирующее враждебное изображение как указанный ошибочный целевой класс.

У каждого из методов реализации атаки есть свои сильные и слабые стороны. Например, *метод, основанный на оптимизации*, обладает такими достоинствами [6], как минимальное возмущение, возможность генерации высококачественных состязательных образцов. Недостатками данного метода являются большое время реализации и сложность масштабирования до больших наборов данных.

Преимуществами *метода быстрого градиентного спуска (FGSM)* является [7] более высокая скорость, чем у методов, основанных на оптимизации, и возможность генерации высококачественных состязательных примеров. Основной недостаток этого метода - возмущение не является оптимальным по своему воздействию.

На производительность *итеративного метода наименее вероятного класса* влияет количество итераций [8], преимуществом метода является возможность реализации более тонких возмущений, чем у FGSM.

В работе [9], было показано, что *метод глубокого обмана* не гарантирует, что сгенерированные состязательные выборки достаточно хороши для атаки, однако если предполагается, что нейронные сети полностью линейны, метод имеет достаточно высокую эффективность.

Якобианский анализ (JSMA) [5] имеет следующие преимущества: атакующий может точно настроить возмущение, атакующий может обеспечить приемлемый компромисс между количеством и качеством состязательных

образцов. Недостатки этого метода: целевые сети должны быть сетями прямого распространения, сложность вычислений высока при обработке данных большой размерности.

Таким образом, описанные выше методы реализации атак имеют как преимущества, так и недостатки, в частности, основанные на оптимизации FGSM и итерационные методы хороши для создания высококачественных атакующих выборок, но требуют больше времени, особенно для больших наборов данных. С другой стороны, методы, основанные на глубоком обучении, например, DeepFool и JSMA, учитывают множество факторов при создании враждебных выборок, таких как вычислительная мощность, количество и качество требуемых выборок. Такой разброс в параметрах атак показывает потребность в более глубоком количественном сравнительном анализе и изучении методов атакующего воздействия на компонент машинного обучения системы обнаружения вторжений.

Заключение

В рамках данной статьи рассмотрена проблема исследования атак на компоненты машинного обучения систем обнаружения вторжений, поскольку СОВ с таким компонентом, в перспективе, имеют преимущество над сигнатурными системами обнаружения вторжений. Произведен анализ актуальных работ, посвященных атакам на компоненты машинного обучения систем обнаружения вторжения. Представлена классификация атак на компоненты машинного обучения систем обнаружения вторжений. Выделены основные методы реализации атак, произведен их обобщенный сравнительный анализ. В результате анализа сделан вывод о будущих направлениях исследований: разработка модели атак на компоненты машинного обучения систем обнаружения вторжений; разработка модели и алгоритмов защиты систем обнаружения вторжений с компонентом машинного обучения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. N 11. С. 993–1001.

2. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference “Simulation in wider Europe”. ECMS 2005. Riga, Latvia, 1–4 June 2005. PP. 533–543.

3. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. 2018. Vol. 6. PP. 72714–72723. DOI: 10.1109/ACCESS.2018.2881998.

4. Намиот Д. Е., Ильюшин Е. А., Чижов И. В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. Vol. 10, No. 9. PP. 135–147.

5. Rosenberg I., Shabtai A., Elovici Y., Rokach L. Adversarial Machine Learning Attacks and Defense Methods in the Cyber Security Domain // ACM Comput. Surv. 2021. N 54, 5. Article 108 (May 2021). 36 p.

6. Pitropakis N., Giannetsos T., Anastasiadis E. A taxonomy and survey of attacks against machine learning // IEEE Access. November 2019. PP. 1–45.

7. Liu Q., Zhao W., Li P., Cai W. A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View // IEEE Access. February 2018. PP. 12103–12117.

8. Carlini N., Wagner D. Towards evaluating the robustness of neural networks // Proc. IEEE Symp. Secur. Privacy, San Jose, CA, USA. May 2019. PP. 39–57.

9. Papernot N., McDaniel P., Jha S., Fredrikson M., Celik Z. B., Swami A. The limitations of deep learning in adversarial settings // Proc. IEEE Eur. Symp. Secur. Privacy (EuroSP), Saarbrucken, Germany. Mar. 2016. PP. 372–387.

УДК 004.05
ГРНТИ 49.33.35

АНАЛИЗ ПЕРСПЕКТИВ ИНТЕГРАЦИИ БЛОКЧЕЙН ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ 5G

И. О. Казаченко, Д. В. Кушнир

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье поднимается вопрос необходимости интеграции технологии блокчейн в сети пятого поколения. В работе имеется краткое описание концепции технологии блокчейн, а также затронуты преимущества интеграции блокчейна в качестве главного механизма обеспечения информационной безопасности в сетях пятого поколения в целом, и для отдельных технологий в частности.

блокчейн, 5G, информационная безопасность, облачные вычисления, граничные вычисления, слайсинг.

Перед глобальным развертыванием и внедрением сетей пятого поколения необходимо однозначно решить такие вопросы безопасности как: надежность сети в целом, сохранение, неизменность передаваемых данных и конфиденциальность. Также важно отметить, что технологии сотовой связи пятого поколения будут поддерживать новые модели предоставления

услуг конечному пользователю, и, таким образом, еще больше усугубят проблемы безопасности. В частности, контроль решения вопроса безопасности в 5G является более комплексным и сложным из-за различных типов и огромного количества подключенных устройств, следовательно, архитектуры и отработанных алгоритмов безопасности, унаследованных от сетей более ранних поколений, недостаточно. В связи с этим, на данный момент проводится большое количество исследований, направленных на повышение эффективности процесса обеспечения информационной безопасности в сетях пятого поколения, а также на выявление или создание технологий, способствующих повышению эффективности данного процесса.

Одной из таких технологий, получивших массовое распространение с конца 2008 года, является технология блокчейн, представляющая из себя децентрализованную, неизменяемую и прозрачную базу данных. Таким образом, в данной статье поднимается вопрос перспектив интеграции блокчейна в платформу 5G, с целью повышения уровня безопасности сети в целом, а также отдельных технологических решений, в частности.

Общая концепция блокчейна

Концепция блокчейна основана на архитектуре одноранговой сети, в которой информация о транзакциях гибко управляется всеми участниками сети и не контролируется каким-либо централизованным органом. Другим словами, блокчейн представляет из себя последовательный набор блоков, каждый следующий блок в котором включает в качестве хэшируемой информации значение хэш-функции от предыдущего блока (рис. 1).

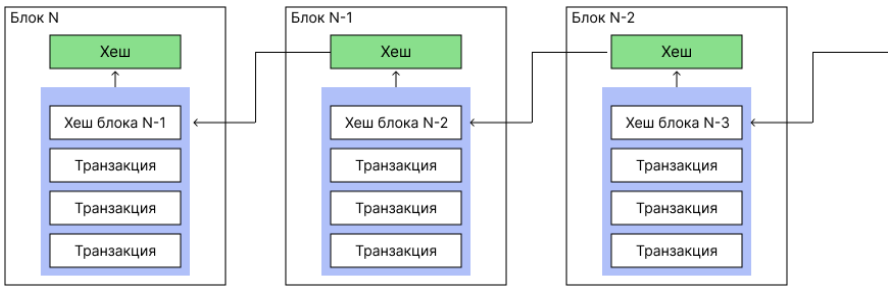


Рис. 1. Структура блокчейна

Фундамент одноранговой сети обеспечивает высокий уровень децентрализации блокчейна, что позволяет размещать базы данных не в определенном центральном устройстве, а распределять данные между всеми участниками сети. Такой подход, позволяет обеспечить высокую отказоустойчивость и безопасность базы данных, хранящейся на блокчейне, исключая влияние одноточечных сбоев в сети [1].

Обновление информации в таких децентрализованных базах данных, как правило, происходит следующим образом: после того, как абонент инициировал какую-либо транзакцию, информация попадает в сеть блокчейн-инфраструктуры, состоящую из тысяч компьютеров, затем все децентрализованные базы данных подтверждают входящий запрос, а подтвержденная транзакция включается в цепочку ранних операций, процесс завершается сообщением от всех хранилищ о подтверждении транзакции (рис. 2).

Рис. 2. Примитивная схема функционирования блокчейн-технологии

Из схемы выше можно определить основные компоненты рассматриваемой технологии:

- серия блоков, где каждый последующий блок связан с предыдущим с помощью хеша;
- распределенный реестр или база данных, которая реплицируется каждому участнику сети. Этот реестр записывает и хранит транзакции, которые создаются пользователями и обеспечивает консенсус между участниками в процессе работы;
- консенсус или набор правил, обеспечивающий согласие между всеми участниками сети на счет текущего состояния данных в сети;
- смарт-контракты, представляющие из себя запрограммированные ранее задачи, которые автоматически выполняются при наступлении каких-либо событий [2].

Блокчейн как способ повышения общего уровня безопасности сети

Описанные ранее качества технологии блокчейна, а именно децентрализация, конфиденциальность, неизменяемость, контролируемость и прозрачность, потенциально позволят повысить безопасность платформы 5G.

Другими словами, в отличие от обычных систем управления базами данных, которые часто используют централизованный сервер для выполнения аутентификации, предоставления доступа и обеспечения механизмов безопасности, блокчейн со смарт-контрактами может осуществлять децентрализованную проверку доступа пользователей, используя вычислительные мощности всех законных участников сети. Это делает услуги 5G (т. е. совместное использование спектра данных и распределенных ресурсов) очень устойчивыми к изменениям потока данных в целом.

Благодаря смарт-контрактам, которые обеспечивают очень гибкие эффективные механизмы контроля доступа пользователей с помощью правил доступа и интеллектуальной логики кодирования, блокчейн потенциально представляет новые решения для аутентификации в сотовых сетях 5G. Вместо того, чтобы полагаться на внешнюю инфраструктуру открытых ключей, контракты могут автоматически проверять подлинность доступа пользователей, обнаруживать угрозы и не допускать обеспечения вредоносного доступа из сетей автономным образом, не раскрывая пользовательскую информацию. Кроме того, путем публикации пользовательских данных в книге учета, блокчейн-платформы обеспечивают надежную защиту данных.

Как итог, блокчейн способен обеспечить полный контроль и надежную передачу личных данных при обмене по сети, что уникально по сравнению со всеми традиционными подходами.

Внедрение блокчейна в технологии сетей пятого поколения

Ключевые особенности блокчейна позволят устранить концепцию централизованного управления сетью путем децентрализации сетевой инфраструктуры, где не требуются сторонние органы управления. Таким образом, потенциальное интегрирование технологии блокчейн может поддерживаться ключевыми технологиями, обеспечивающими поддержку платформы 5G, включая облачные вычисления, пограничные вычисления, виртуализацию сетевых функций и нарезку сети [3]. Исходя из этого, далее представляется обзор преимуществ интеграции блокчейна в данные технологии и процессы:

- Облачные вычисления

В облачных вычислениях блокчейн может использоваться для создания платформы проверки между устройствами интернета вещей, базовым блоком (Baseband Unit, BBU) и производителем, где информация о доступе пользователя хранится в неизменном виде в цепочке, в то время как смарт-контракты будут использоваться для выполнения автоматической аутентификации пользователя.

Выделяют два основных преимущества от использования блокчейна в облачных сетях 5G. Во-первых, концепция облачного управления на основе блокчейна избавляет от централизованного контроля в базовой сети и предлагает децентрализованное справедливое соглашение, что позволяет избавиться от единой точки отказа и значительно повышает доверие к системе. Во-вторых, применяя децентрализованный блокчейн без участия третьих сторон, основанная на блокчейне стратегия облачных вычислений может обеспечить оптимальное использование ресурсов и сэкономить большое количество сигналов и затрат на подключение.

- Граничные вычисления

С помощью блокчейна сетевые возможности пограничных сетей могут быть оптимизированы. Как и в облачных вычислениях, блокчейн может использоваться для создания распределенной и надежной системы аутентификации и обеспечения обмена информацией между различными пограничными платформами.

В системе данные об аутентификации и информация о доступе пользователя могут надежно храниться в блокчейне, который также способен автоматически отслеживать действия мобильных терминалов (устройств) без необходимости центральных органов управления. В частности, также используются смарт-контракты для выполнения перехвата доверенного контента в пограничной вычислительной сети.

Также, внедрение технологии блокчейна в пограничные вычисления позволит обеспечить более эффективный перенос вычислительных мощностей на периферию, за счет предоставления надежного хранения данных в пограничных вычислительных системах.

- Виртуальные сетевые функции

Блокчейн может облегчить работу технологии Network Function Virtualization (NFV) в трех основных аспектах. Во-первых, обеспечение простой и гибкой оркестровки сервисов Virtual Network Function (VNF) для лучшего управления сетью. Во-вторых, блокчейн может обеспечить развертывание сетевых функций и защиту их целостности, как от внутренних атак, так и от внешних угроз, то есть вредоносных модификаций виртуальных машин и Denial of Service (DoS) атак. Также, блокчейн может выполнять аудит данных и мониторинг состояния системы во время процесса сетевого взаимодействия.

- Слайсинг

Блокчейн предоставляет возможности для обеспечения безопасности управления в разделенных сетях пятого поколения. Блокчейн можно использовать для создания надежных сквозных сетевых срезов и предоставления их поставщикам, для обеспечения возможности управлять своими ресурсами. Кроме того, подход, основанный на блокчейне, может обеспечить

динамический контроль надежности ресурсов и улучшить целостность и достоверность информации, которой обмениваются устройства в ненадежных мобильных сетях.

Таким образом, в данной статье были описаны преимущества интеграции технологии блокчейн в сети пятого поколения. Явные преимущества рассматривались как в целом для сетей пятого поколения, так и для различных технологий, реализованных в данной платформе и имеющих потенциал к интеграции блокчейн-технологии, в частности. Рассмотренный тип интеграции является достаточно перспективным и многообещающим.

Список используемых источников

1. Kushnir D., Kovtsur M., Muthanna A., Kistruga A., Akilov M., Batalov A. Developing instrument for investigation of blockchain technology // Studies in Computational Intelligence. 2022. Vol. 1030. PP. 123–141.

2. Chaer A. et al. Blockchain for 5G: Opportunities and challenges // 2019 IEEE Globecom Workshops (GC Wkshps). IEEE, 2019. PP. 1–6.

3. Yue K. et al. A survey of decentralizing applications via blockchain: The 5g and beyond perspective // IEEE Communications Surveys & Tutorials. 2021. Vol. 23. N 4. PP. 2191–2217.

УДК 656.7.025
ГРНТИ 55.47.07

ОБЗОР МЕТОДОВ ДЛЯ ОСУЩЕСТВЛЕНИЯ АВТОМАТИЧЕСКОЙ БЕЗОПАСНОЙ ПОСАДКИ БВС НА РАЗЛИЧНЫЕ ПЛОЩАДКИ

И. А. Кайсина, В. С. Кузнецов, А. М. Тунгускова, А. В. Шкляев

Ижевский государственный технический университет имени М. Т. Калашникова

В статье рассматриваются методы, для осуществления безопасной посадки беспилотных воздушных судов с целью доставки груза. В качестве груза можно рассматривать: продукты питания, медикаменты, посылки, различные небольшие товары из магазинов и т. д. На основе анализа методов и алгоритмов выбраны алгоритмы технического зрения для дальнейшей реализации на испытательном стенде и проведения ряда экспериментальных работ.

аэрологистика, беспилотное воздушное судно, безопасная посадка, доставка груза, полезная нагрузка, системы технического зрения.

Беспилотные воздушные суда (БВС) используют во многих секторах экономики – лесном и сельском хозяйстве, нефтегазовой отрасли, строительстве, геодезии, ЖКХ. Чаще всего это легкие БВС с максимальной взлетной массой до 30 кг. Они нужны для аэрофотосъемочных работ и получения цифровых пространственных данных.

Следующий этап развития рынка беспилотных систем – аэрологистика и доставка грузов. По данным Gartner, к 2026 году для доставки товара до потребителя в мире будут использовать около 1 млн дронов [1].

Сама идея доставки чего-либо с помощью беспилотника возникла уже достаточно давно и будет являться перспективной в гражданской сфере. Основным преимуществом использования данного транспорта выступает то, что груз можно доставить в любое труднодоступное место. На данный момент уже объявлено несколько крупных конкурсов с целью создания системы, с помощью которой можно безопасно доставить груза на дистанцию не менее 1 000 км [2]. Технологический конкурс «Аэрологистика» предполагает разработку и испытание в экспериментальном правовом режиме комплекса решений, критически важных для начала широкого применения БВС в России в целях перевозки грузов.

Многие научные коллективы уже рассматривают данную задачу. Среди публикаций можно выделить несколько работ, к примеру: в работе [3] представлена реализация алгоритма высокоточной посадки на метку с использованием программируемой камеры OpenMV. Основной задачей являлось получение практических навыков по алгоритмизации автономных полетов дронов с применением дополнительных совместимых модулей. В статье [4] рассмотрен вариант решения задачи автоматического обнаружения взлетно-посадочной полосы на видеоизображениях. В публикации [5] описана структура маркерного изображения, которое может использоваться в качестве обозначения места посадки, также представлен алгоритм обнаружения вершин маркера на изображении с камер.

Способы посадки БВС

Существует несколько способов для точной и безопасной посадки БВС, а именно:

1. Посадка при помощи датчиков

Наиболее распространенной является посадка с использованием GPS (Система глобального позиционирования) и INS (инерциальные навигационные датчики). Недостатком GPS является неточность измерения высоты, именно поэтому с ними используются высотомер и датчик барометрического давления. Помимо этого, сигналы GPS не всегда доступны, поэтому автоматическая посадка не всегда может быть применена.

Помимо этого, существует и посадка при помощи датчиков:

• IR-LOCK – маяк системы точной посадки. Данный датчик предназначен для совместного использования с камерой системы точной посадки. Посадка может быть осуществлена не только в автоматическом режиме, но и в ручном.

• Камера системы точной посадки. Данный датчик применяется вместе с IR-LOCK маяком, а также подходит для безопасной посадки беспилотников на землю.

• Лидары. Благодаря своим уникальным конструкциям, они могут обеспечить стабильное и точное измерение расстояния.

2. Посадка на основе систем технического зрения (СТЗ)

Система технического зрения – это система, которая обеспечивает обнаружение, контроль и анализ объектов по изображениям.

Особенность данной посадки заключается в том, что при помощи СТЗ мы можем осуществлять посадку на подготовленную площадку, например, на автоматизированную станцию взлёта и посадки (АСВП) (рис. 1), на частично подготовленную площадку и не подготовленную площадку.

Рис. 1. Автоматизированная станция взлёта и посадки (АСВП)

Данный метод заключается в обнаружении опорных меток (рис. 2), которые печатаются и используются в качестве ориентира для посадки, данные ориентиры предоставляют собой информацию о местоположении и расстоянии.

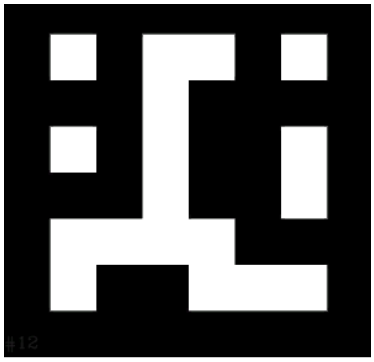


Рис. 2. Опорные метки

Посадка является неотъемлемым этапом использования БВС. На текущий момент мало исследованы алгоритмы и методы посадки на частично подготовленные и неподготовленные площадки ввиду высокой сложности технической реализации. Таким образом, перспективной задачей является разработка методов и алгоритмов для обеспечения безопасной посадки БВС в разных условиях. За входные данные могут быть приняты данные, полученные с камер на борту БВС и обработанные с помощью СТЗ.

Стенд для проведения работ

На данном этапе работ был произведён анализ схожих решений, для этого были проведены патентные исследования, поиск диссертаций по схожей тематике, поиск результатов интеллектуальной деятельности, поиск результатов научно-исследовательских, опытно-конструкторских и технологических работ, а также поиск научных публикаций. Помимо этого, это был разработан примерный стенд для дальнейшей работы. Тест для моделирования включает в себя применение алгоритма, способного отследить определенные маркеры при помощи камеры. В результате была написана программа на языке программирования Python, в которой реализуется алгоритм Camshift, использующий корреляционный метод. Разработанная программа способна распознать маркер при освещенности от 25 люксов на расстоянии 20 метров в HD качестве. На расстоянии более 20 метров требуется подсветка маркера или использование ИК-маяка.

В конечном итоге система может быть собрана на базе БВС мультироторного типа и типа конвертоплан, например, Supercam X4, Supercam X6M2 и Supercam SX350. В качестве полезной нагрузки может быть использована фотокамера, видеокамера, тепловизор, лазерный сканер и т. д.

Заключение

В данной статье было рассмотрено несколько способов посадки, а именно: посадка при помощи датчиков: GPS, INS, IR-LOCK, камера системы точной посадки, лидары и посадка при помощи систем технического зрения. Посадка на основе СТЗ может быть осуществлена на подготовленную площадку, на частично подготовленную и на неподготовленную площадку. Помимо этого, было проанализировано три сценария с методом и посадкой, а также алгоритмы на их основе.

Список используемых источников

1. Смотрите вверх: как в россии рождается беспилотная аэрологистика [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/cmrm/62036c429a7947ce2fc410cc (дата обращения 16.01.2023).

2. Технологический конкурс «аэрологистика» [Электронный ресурс]. URL: https://aero.upgreat.one/ (дата обращения 16.01.2023).

3. Червинко Е. И., Иванов И. А. Реализация алгоритма высокоточной посадки на метку беспилотного летательного аппарата «ПИОНЕР» с использованием программируемой камеры openmv // Экономика и качество систем связи. 2022. N 3 (25). С. 89–94.

4. Логвин А. И., Волков А. В. Алгоритмы автоматического распознавания взлетно-посадочной полосы на видеоизображениях // Научный вестник Московского государственного технического университета гражданской авиации. 2015. N 213 (3). С. 115–117.

5. Трусфус М. В., Абдуллин И. Н. Алгоритм обнаружения маркерных изображений для вертикальной посадки беспилотного летательного аппарата // Труды МАИ. 2021. N 116. С. 13.

УДК 691.391
ГРНТИ 49.03.05

ПЕРЕНОС СООБЩЕНИЙ PTP ПО АРХИТЕКТУРЕ OTN ПРИ НАЛИЧИИ ПРОМЕЖУТОЧНЫХ УЗЛОВ

А. К. Канаев, Ф. А. Прошин

Петербургский государственный университет путей сообщения Императора Александра I

Современные телекоммуникационные сети функционируют на различных уровнях иерархии, обеспечивая высокую пропускную способность на магистральных участках и предоставление любых сервисов пользователям. Технология OTN позволяет достигать необходимых характеристик относительно обработки нагрузки. Данное условие требует обеспечения точной шкалы времени на каждом устройстве, доставляемой с использованием соответствующего протокола обмена метками. На существующих сетях Ethernet наиболее распространён Precision Time Protocol, обеспечивающий высокую точность и простоту настройки. Использование указанного протокола относительно OTN позволит повысить надёжность и стабильность сети. Данная работа направлена на формирование и анализ алгоритма функционирования PTP. Предлагается модель взаимодействия устройств в составе сети. Показано влияние различных этапов обработки на точность результата и появление асимметрии задержек. Характеристики процессов в модели могут редактироваться, позволяют изменять условия функционирования сети.

оптическая транспортная сеть, OTN, синхронизация, PTP, канал синхронизации, OSMC.

Архитектура OTN позволяет передавать любые типы данных в составе нагрузки. Наличие заголовков у блоков различного уровня позволяет передавать управляющую информацию отдельно от информации пользователя. Для переноса информации, относящейся к синхронизации, предназначено поле OTN Synchronization Message Channel (OSMC), которое располагается в заголовке OTU [1]. На рис. 1 показано его местонахождение.

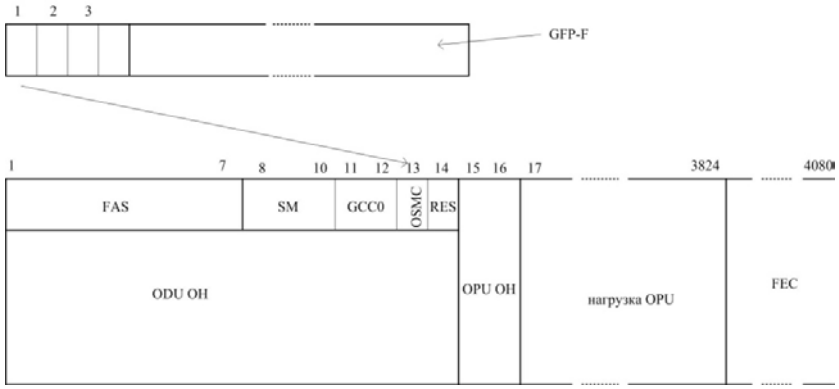


Рис. 1. Канал OSMC

Данный канал может передавать сообщения PTP, SSM или eSSM, которые предварительно инкапсулируются в кадры GFP-F [1]. Канал занимает 1 байт, следовательно, передача одного сообщения PTP, размещаемого в GFP-F, ведётся в составе нескольких блоков OTU. Данная работа предлагает использование этого канала для синхронизации по PTP.

Механизм PTP (IEEE 1588) широко применяется на действующих сетях с коммутацией пакетов, обеспечивая точность менее 1 мкс и выше при аппаратной реализации [2]. Процесс синхронизации состоит из обмена сообщениями между ведущим (*Master*) и ведомым (*Slave*) устройствами. Каждое устройство, которое участвует в обработке PTP, называется часами (*Clock*). На диаграмме показан двухступенчатый процесс при режиме работы «End-to-End». Ведущее устройство передаёт с помощью «Follow_Up» метку t_1 времени отправки сообщения «Sync». Ведомое принимает его и записывает метку t_2. Так как необходимо определить среднюю задержку прохождения, ведомое отправляет запрос «Delay_Request» с меткой времени t_3 его пересылки. При приёме ведущее записывает метку t_4, которая вставляется в сообщение «Delay_Response», посылаемое на ведомое. Далее на основании полученных t_1, t_2, t_3, t_4 определяется средняя задержка по формуле:

$$T_{\text{ср}} = \frac{(t_2 - t_1) + (t_4 - t_3)}{2}.$$

На основании среднего времени прохождения система выполняет корректировку часов по формуле:

$$T_{\text{сдв}} = t_2 - t_1 - T_{\text{ср}}.$$

Описанный процесс необходимо периодически повторять для поддержания шкалы времени на ведомых устройствах. Периодичность обмена может быть различной в зависимости от выбранного профиля и дополнительных настроек.

Как показано на схеме, при определении $T_{\text{ср}}$ считается, что задержка прохождения в прямом и обратном направлениях одинакова. На практике между ведущим и ведомым устройствами располагаются промежуточные узлы, которые не участвуют в обработке меток, добавляя информацию в поле коррекции, но вносят асимметрию в среднюю задержку. Рассмотрим процесс обмена с учётом промежуточных устройств. На рис. 2 приводится упрощённая схема прохождения сообщения по OTN.

Рис. 2. Последовательность прохождения сообщения PTP

Сообщение PTP размещается в кадрах GFP-F в соответствии с [3] и далее передаётся в OTU OSMC. Предполагается, что промежуточные узлы могут считывать сообщение PTP при чтении OTU, внося в поле коррекции

время обработки на данном устройстве. После ODU-коммутации откорректированная метка вставляется в PTP, далее через GFP-F в OSMC и направляется до последующего промежуточного узла. На оконечном сообщение выделяется и считывается необходимая информация. На рис. 3 приводится блок схема процесса синхронизации.

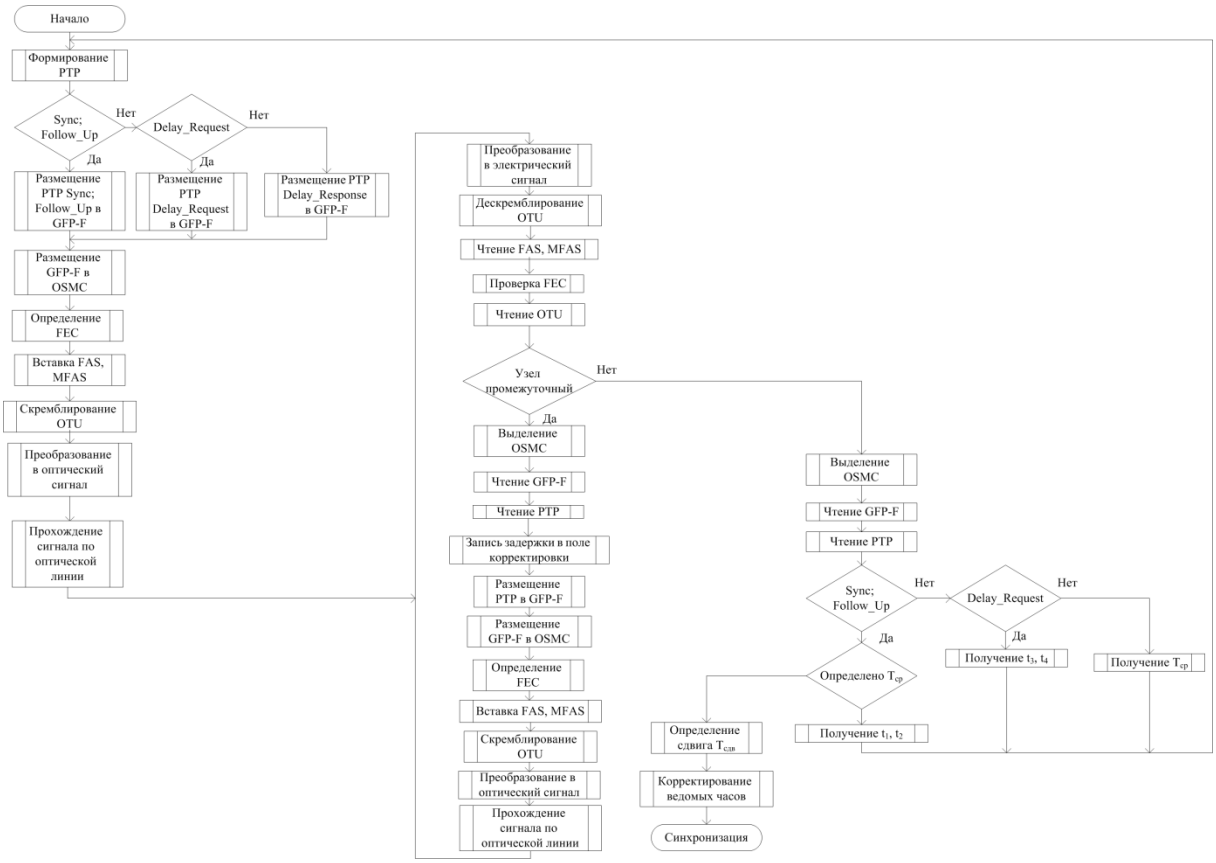


Рис. 3. Алгоритм функционирования PTP в OTN

На основании данного алгоритма выполнено построение модели. Для моделирования выбрана среда моделирования AnyLogic. Предлагается рассмотреть процесс синхронизации в виде модели, где агентами выступают сообщения «Sync», «Delay_Request», «Delay_Response». Каждый процесс соответствует блоку задержки «Delay», задерживающему агента на заданное время. На рис. 4 показана имитационная модель.

Длительность задержек выбрана на основании данных [4, 5]. Модель предполагает, что между ведущим и ведомым устройствами располагаются 5 промежуточных OTN-мультиплексоров с функцией корректировки меток PTP. По результатам моделирования приводятся графики распределения времени прохождения в прямом T_{MS} и обратном T_{SM} направлении, распределения времени обработки на промежуточных коммутаторах в прямом $T_{пром}$ и обратном $T_{промОбр}$ направлении. Расстояние между узлами принято равным

15 км (задержка 5 мкс на 1 км). На рис. 5, 6, 7 показаны результаты моделирования. При моделировании принято, что процессы, вносящие переменную задержку, описываются экспоненциальным распределением. Для каждого эксперимента размещение PTP в GFP-F, считывание PTP из GFP-F выполняется за (30...40) мкс. Эксперимент состоит из 100 реализаций при заданных условиях.

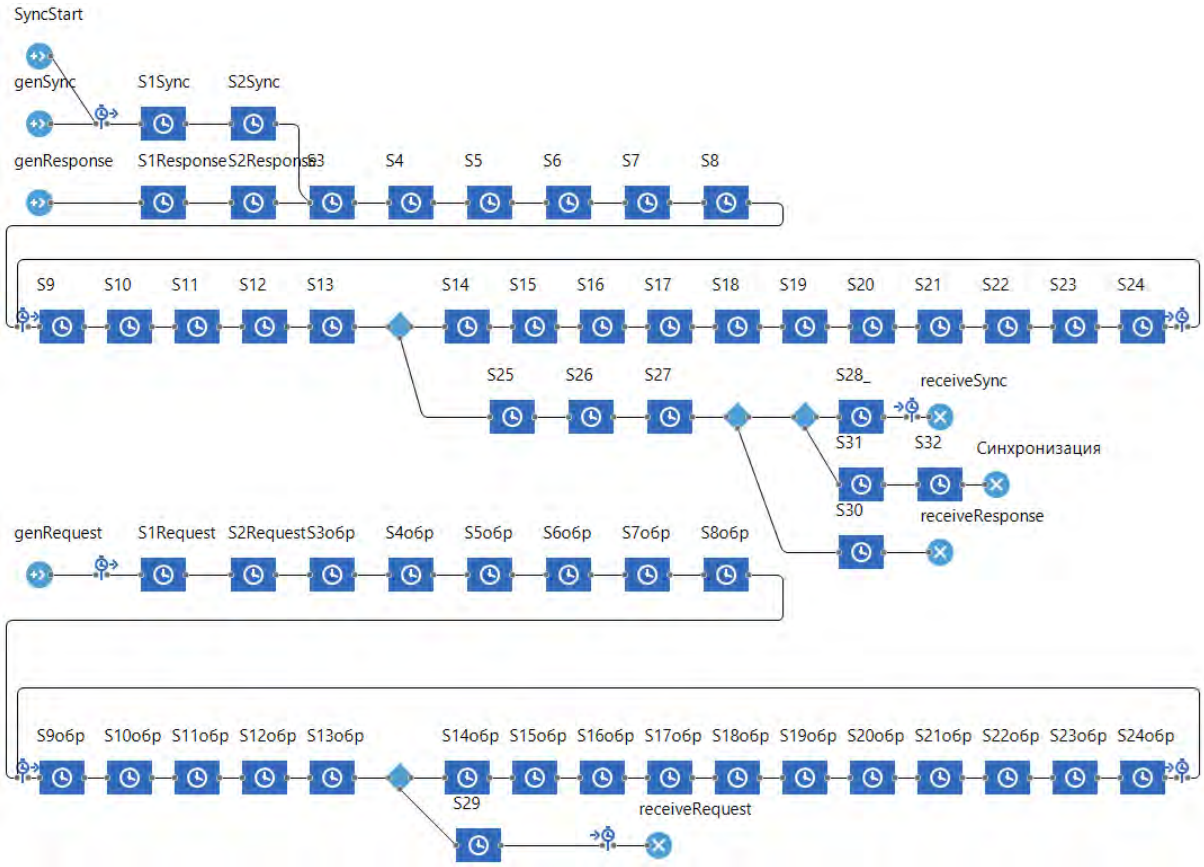


Рис. 4. Имитационная модель в среде AnyLogic

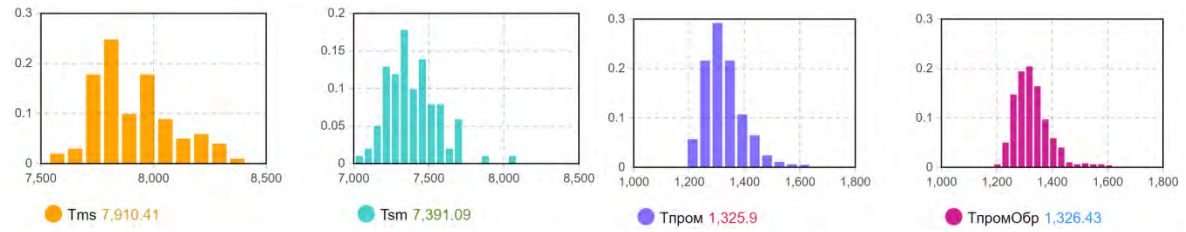


Рис. 5. Распределение времени при FEC (20...30), мкс

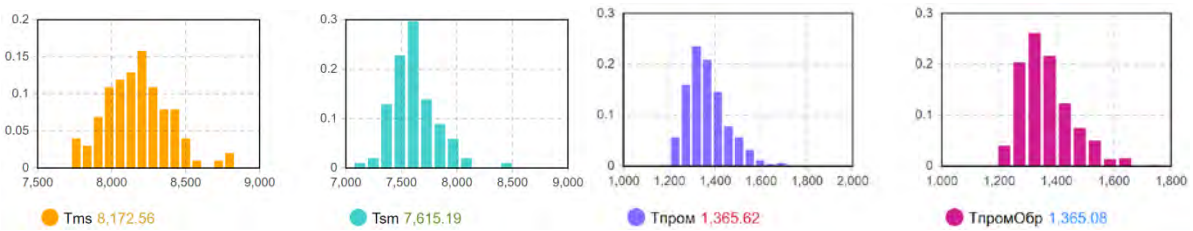


Рис. 6. Распределение времени при FEC (20...50), мкс

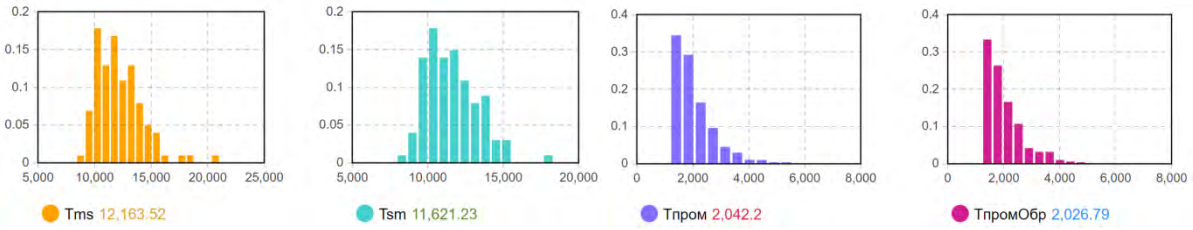


Рис. 7. Распределение времени при задержке вставки GFP-F в OSMC (500...700), мкс

На рис. 5 показаны результаты при использовании опции FEC, задержка на которую принимает значение (20...30) мкс. На рисунке 6 приводятся результаты при возможном усложнении алгоритма FEC, на который потребуется (20...50) мкс. Как показано на графиках, время T_{MS}, T_{SM} различно, то есть наблюдается асимметрия. Среднее время обработки заголовка на промежуточном мультиплексоре примерно равное для прямого и обратного направлений.

На рис. 7 показаны графики при использовании FEC (30...40) мкс с учётом возможной занятости канала OSMC, задержка размещения GFP-F в котором принимается равной (500...700) мкс.

Результаты моделирования показывают, что в общем величина задержки в прямом и обратном направлении различна. Такая асимметрия может вносить значительные погрешности в результаты расчёта $T_{\text{сдв}}$, что на практике приведёт к неточной корректировке часов и снижению точности. Использование опции FEC заметно влияет на величину задержки. Для более сложного алгоритма общая задержка выше, но асимметрия по сравнению с менее мощным FEC находится примерно на одинаковом уровне около 500 мкс. Следовательно, для уменьшения общей задержки возможно применение упрощённых алгоритмов FEC.

При размещении GFP-F в OSMC возможно предусмотреть вариант занятости канала. Так по результатам моделирования при возможном увеличении времени от 500 до 700 мкс общая задержка существенно возрастает. Следовательно, необходимо учитывать возможное влияние этого условия при выборе периодичности опроса.

Как показано на рис. 5, 6, 7 среднее время обработки пакетов PTP на промежуточных узлах примерно одинаково для прямого и обратного направлений, внося примерно постоянную задержку в общее время. Это означает, что OTN-мультиплексоры с поддержкой обработки PTP позволяют эффективно обмениваться устройствам с ведущими часами. Вопрос проработки алгоритма работы с OSMC и структура блока синхронизации для мультиплексора требует дальнейшего исследования.

Список используемых источников

1. Interfaces for the optical transport network ITU-T G.709/Y.1331 (06/2020) / International Telecommunication Union. Geneva : ITU, 2020. 280 p.

2. Weiss A., Kammacher T. Presision Time Protocol for Spectroscope Synchronization, ZHAW, Institute of Embedded Systems, 2015.

3. Precision time protocol telecom profile for phase/time synchronization with full timing support from the network ITU-T G.8275.1/Y.1369.1 (02/2022) – Amendment 3 / International Telecommunication Union. Geneva : ITU, 2022. 68 p.

4. Салифов И. И. Методика оценки сквозной задержки на оптической магистральной сети со сложной архитектурой : дис. канд. техн. наук : 05.12.13 / Салифов Ильнур Илдарович. Екатеринбург, 2012. 253 с.

5. Microsemi MAXX24288 Data Sheet [Электронный ресурс] / Microchip, ноябрь 2016. URL: https://www.microsemi.com/product-directory/ieee-1588-plls-and-software/4669-max24288 (дата обращения 31.03.2023).

УДК 65.011.56
ГРНТИ 50.41.25

ВЫДЕЛЕНИЕ ODA-КОМПОНЕНТОВ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ РАБОЧЕЙ СИЛОЙ (WFM)

С. В. Кисляков[1,2], Е. А. Лочкарев[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]НТЦ АРГУС

В представляемой работе анализируется система «АРГУС Workforce Management» с целью её перевода на новый фреймворк Open Digital Architecture. Были определены группировки бизнес-функций системы в соответствии с ODA Functional Architecture и сопоставлены с бизнес-функциями этой же системы на карте eTOM, выделены ODA-компоненты. Продемонстрировано взаимодействие компонентов, осуществляемое с помощью открытых программных интерфейсов.

открытая цифровая архитектура, ODA-компоненты, программное обеспечение, Workforce Management.

Функциональные возможности АРУГС-WFM

АРГУС Workforce Management (далее «АРГУС WFM») представляет собой систему для управления и оптимизации использования рабочих ресурсов - выездных работников [1].

«АРГУС WFM» разрабатывался на основе eTOM. Далее представлены группировки бизнес-функций, которые являются границей системы по Business Process Framework:

1. Workforce Management Reporting (Отчетность об управлении персоналом) – позволяет получать детальные отчеты по различным аспектам управления персоналом, таким как использование ресурсов, продуктивность и оценка эффективности работы.

2. Workforce Schedule Management (Управление рабочими расписаниями) – помогает создавать гибкие графики работы, учитывая не только требования компании, но и пожелания сотрудников. Также включает возможности для оптимизации расписаний и управления отсутствиями сотрудников.

3. Work Order Analysis (Анализ заказов на работы) – позволяет отслеживать и анализировать выполнение работ, а также эффективность рабочих процессов и затраты на выполнение задач.

4. Work Order Assignments & Dispatch (Назначение и распределение заказов на работы) – обеспечивает автоматическую отправку заказов на работы нужным сотрудникам, учитывая их навыки, опыт и доступность.

5. Work Order Tracking Management (Управление отслеживанием заказов на работы) – помогает контролировать процесс выполнения заказов на работы, включая отслеживание статусов и своевременную информирование о ходе выполнения работ.

6. Workforce Configuration and Setup (Настройка и конфигурирование системы управления персоналом) – обеспечивает настройку системы управления персоналом в соответствии с требованиями компании, включая настройку прав доступа, настройку параметров графиков работы и других настроек.

В открытой цифровой архитектуре бизнес-функции eTOM перераспределились по блокам ODA Functional Architecture (FA). Это одно из основных изменений, привнесенных ODA.

Чтобы построить систему WFM на основе новой концепции, потребуется проанализировать, каким образом ее бизнес-функции перераспределились по FA.

WFM на Функциональной архитектуре ODA

ODA FA состоит из 5 блоков, каждый из которых представляет собой группу бизнес-функций уровня предприятия с набором взаимосвязанных процессов [2].

Бизнес-функции, которые могут быть использованы в формировании бизнес-процессов WFM, сконцентрированы в двух блоках: Production и Party Management.

Производственный блок (Production) отвечает за управление жизненным циклом обслуживания клиентов и ресурсов. Он обеспечивает комплексное управление эксплуатационными функциями, включая установку, развертывание и эксплуатацию технологий.

Блок управления партнёрами и поставщиками (*Party Management*) включает в себя ряд бизнес-функций, которые обеспечивают поддержку всех взаимодействий и данных, связанных с субъектами и объектами, участвующими во взаимодействии с организацией.

Из блока Party Management подходят следующие группировки бизнес-функций:

1. Party Agreement Management – управление оценкой соглашений с контрагентами, включая клиентов. Инициирование и заключение бизнес-соглашений, когда вовлечены одна или несколько других сторон.

2. Sales Development – разработка поддержки продаж и ответа на запросы по новым и существующим продуктам, а также существующим и потенциальным клиентам.

3. Selling – ответственность за управление потенциальными клиентами, оценку и обучение клиентов, а также соответствие ожиданиям клиентов. Управление потенциальными контрагентами, с которыми предприятие может взаимодействовать, такими как потенциальные существующие или новые клиенты и партнеры, для их оценки и обучения, а также обеспечение соответствия их ожиданиям.

Из блока Production подходят следующие группировки бизнес-функций:

1. SM&O Support & Readiness – отвечает за управление инфраструктурой сервиса, обеспечивая наличие необходимой сервисной емкости и готовности поддерживать процессы SM&O (управление, выполнение, обеспечение качества и выставление счетов).

2. RM&O Support & Readiness – управление инфраструктурой ресурсов, чтобы гарантировать наличие и готовность соответствующих ресурсов приложений, вычислительных и сетевых ресурсов, необходимых для поддержки процессов Fulfillment, Assurance и Billing, а также для инстанцирования и управления экземплярами ресурсов, и для мониторинга и отчетности по возможностям и затратам отдельных процессов FAB.

В результате выбраны группировки бизнес-функций ODA FA, которые соответствуют бизнес-функциям анализируемой системы и могут быть использованы в автоматизируемых WFM бизнес-процессах. Например, SM&O Support & Readiness может быть связана с бизнес-функциями WFM под номерами 2, 4, 5 и 6, так как эта группировка функций связана с управлением задачами, персоналом и обеспечением качества. RM&O Support & Readiness соотносится с первой и третьей бизнес-функцией, так как отвечает за мониторинг и отчетность по затратам и возможностям, связанным с процессами WFM. Группировки бизнес-функций из блока Party Management могут быть использованы системой управления рабочей силой в процессах, связанных с любыми взаимодействиями с клиентами, такими как согласование места

и времени встречи или формирование рейтинга специалиста на основе обратной связи клиента по выполненным работам.

ODA-компоненты.

Исходя из выбранных бизнес-функций и определенных блоков ODA FA, необходимо подобрать ODA-компоненты, опираясь на ODA component map [3]:

1. Appointment Management – отвечает за управление назначениями встреч с учетом свободных окон (слотов). В качестве параметров использует время, дату и место встречи [4].

2. Party Problem Management – управление проблемами, о которых сообщает клиент [5].

3. Party management – отвечает за управление данными о клиентах, их идентификацию и аутентификацию. Обеспечивает создание и редактирование профилей клиентов [6].

4. Location Management – отвечает за управление информацией о местоположениях, например адреса, принадлежность к различным зонам и т. д. [7].

На рис. 1 представлен бизнес-процесс обработки заявки на обслуживание, автоматизируемый WFM. В рамках данного бизнес-процесса авторы продемонстрируют, как взаимодействуют компоненты Party Management и Location Management, а рис. 2 показывает, как они могут быть интегрированы в систему.

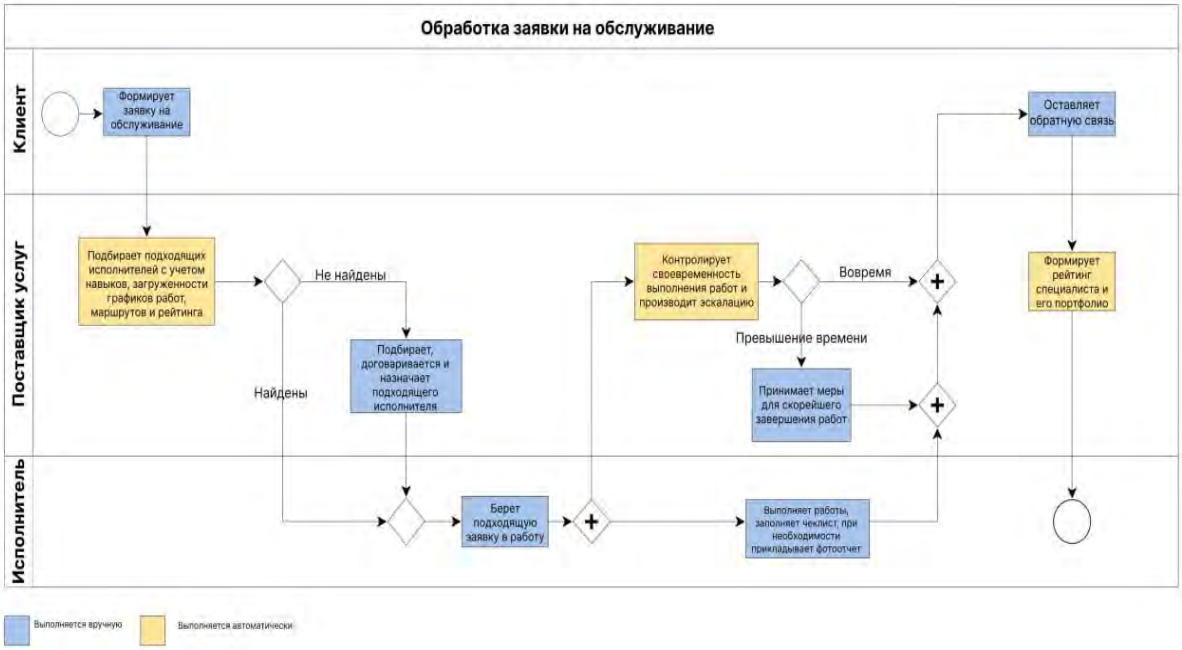


Рис. 1. Бизнес-процесс обработки заявки на обслуживание

Party Management в данном процессе может быть использован для взаимодействия WFM с профилем клиента. Компонент может предоставлять информацию о клиентах. Кроме того, Party Management поддерживает функции по автоматическому связыванию с клиентом для уточнения статуса заявки или об изменениях статуса заявки. Если пользователь сообщает о проблеме, то этот запрос автоматически связывается с его профилем в компоненте Party Management. Location позволяет ссылаться на географическое местоположение, и может быть использован для поиска и проверки адреса клиента. В рамках данного бизнес-процесса, компонент может быть использован для подбора более подходящего исполнителя на основе информации об удаленности адреса клиента.

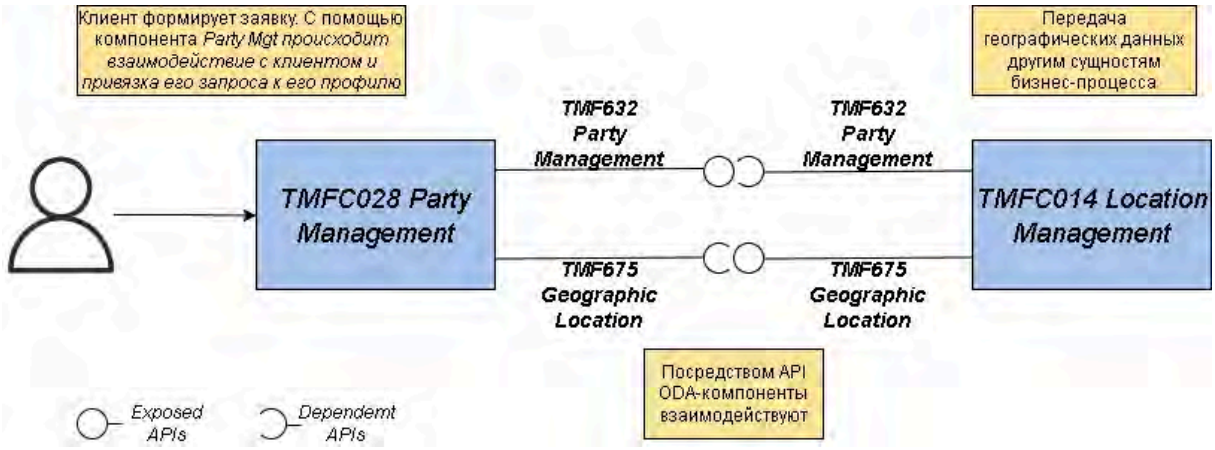


Рис. 2. Взаимодействие компонентов посредством API

Каждый компонент имеет определенные API: dependent (зависимые API, т. е. те, которые могут потребовать другие компоненты для взаимодействия) и exposed (предоставляемые, т. е. те, которые доступны из компонента для взаимодействия с другими). Чтобы ODA-компоненты могли взаимодействовать, необходимо сопоставить dependent API одного компонента с exposed API другого.

Вывод

Открытая цифровая архитектура, как новый фреймворк, предложила стандартизированные программные компоненты с разработанными для них API. Выбор этих ODA-компонентов определяется бизнес-процессом, который необходимо автоматизировать, и наличием API, имеющим определенную функциональность. Для автоматизации бизнес-процесса (рис. 1) понадобится больший набор компонентов. В силу ограниченности объёма, здесь приведены лишь два компонента, позволяющие пояснить принцип их выбора и взаимодействия. В ближайших работах планируется описать весь набор компонентов для автоматизации выбранного бизнес-процесса.

Список используемых источников

1. Продукты и решения // argustelecom URL: https://argustelecom.ru/ (дата обращения 13.11.2022).
2. IG1167 ODA Functional Architecture Exploratory Report v6.0.0 // tmforum.org URL: https://www.tmforum.org/resources/standard/ig1167-oda-functional-architecture-exploratory-report-v6-0-0/ (дата обращения 01.03.2023).
3. ODA Components // oda-directory.labs.tmforum.org URL: https://oda-directory.labs.tmforum.org/component-map (дата обращения 27.02.2023).
4. Appointment Management // tmforum.org URL: https://oda-directory.labs.tmforum.org/component-map/production/Appointment%20Management (дата обращения 03.03.2023).
5. Party Problem Management // tmforum.org URL: https://oda-directory.labs.tmforum.org/component-map/party-management/Party%20Problem%20Management (дата обращения 03.03.2023).
6. TMFC028 Party Management v1.1.0 // tmforum.org URL: https://www.tmforum.org/resources/technical-specification/tmfc028-party-management-v1-1-0/ (дата обращения 03.03.2023).
7. TMFC014 Location Management v1.0.0 // tmforum.org URL: https://www.tmforum.org/resources/technical-specification/tmfc014-location-management-v1-0-0/ (дата обращения 03.03.2023).

УДК 65.011.56
ГРНТИ 50.41.25

ВЫДЕЛЕНИЕ ODA-КОМПОНЕНТОВ ДЛЯ СИСТЕМ УЧЁТА СЕТЕВЫХ РЕСУРСОВ NETWORK RESOURCE INVENTORY

С. В. Кисляков[1,2], Д. И. Сухомлинов[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]НТЦ АРГУС

Мир управления инфокоммуникациями движется в сторону переформатирования подходов к разработке систем поддержки операций и бизнеса. Осуществляется плавный переход концепции NGOSS/Frameworx к открытой цифровой архитектуре построения информационных систем автоматизации. Одной из ключевых идей ODA является деление «монолитного» программного обеспечения на небольшие самодостаточные программные компоненты.

В работе за основу взята система учёта сетевых ресурсов «АРГУС NRI». Для перевода системы NRI использованы принципы открытой архитектуры ODA. В работе выделены основные компоненты системы NRI, их описание и необходимые API для взаимодействия с другими компонентами. Показан пример соединения компонентов для системы учета сетевых ресурсов между собой.

Open Digital Architecture, OSS/BSS, ODA-компоненты, Network Resource Inventory, Open API.

Система «АРГУС NRI» нацелена автоматизировать процессы учета, обработки и анализа информации по линейно-техническим объектам, сооружениям и услугам с помощью современных информационных технологий [1].

Функциональность системы отражена группировками функций программных приложений на рис. 1. Формулировки взяты из Карты приложений телекоммуникационной компании (*TM Forum Telecom Application Map*, TAM).

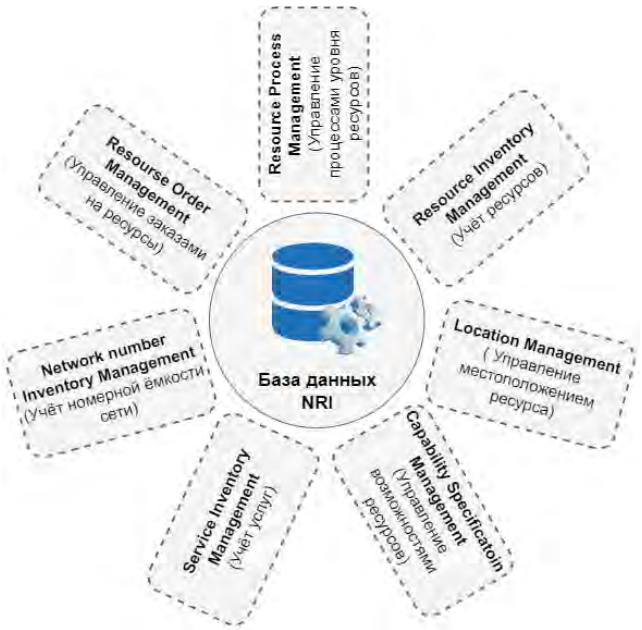


Рис. 1. Функциональные возможности «АРГУС NRI»

Представим монолитную систему в виде ODA-компонентов. Для выделения компонентов для системы NRI обратимся к карте ODA-компонентов [2].

Каждый компонент имеет набор обязательных и необязательных API, их количество зависит от функций и возможностей определенного компонента. Помимо этого, каждый ODA-компонент содержит в себе два вида программных интерфейсов: открытые (*exposed*) и зависимые (*dependent*). Открытые API – программные интерфейсы доступные для определенного компонента. На этом этапе мы перечисляем ресурсы и операции без дополнительных возможностей. Зависимые API необходимы для того, чтобы обеспечить работу предоставленных программных интерфейсов, также компонент может потребовать использование этого набора необходимых API. Для соединения компонентов между собой, необходимо отталкиваться

от автоматизируемых бизнес-процессов и учитывать наличие одинаковых открытых (exposed) и зависимых (dependent) с API (рис. 2).

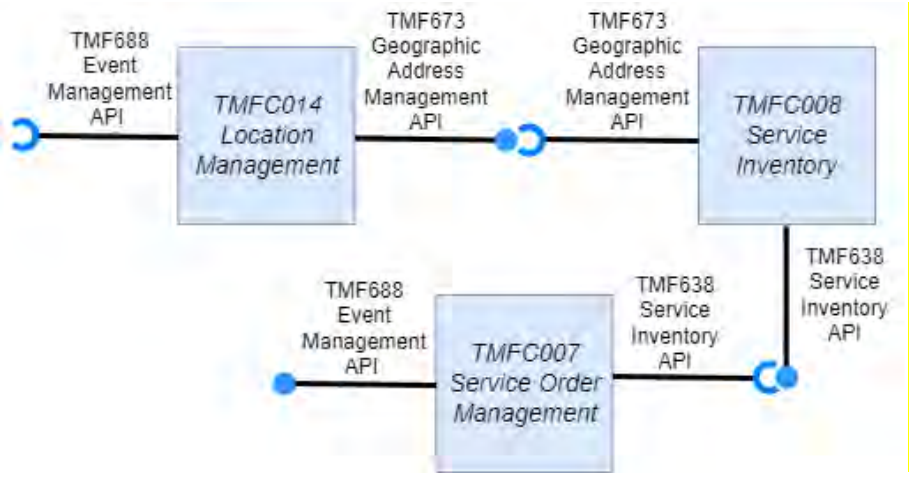


Рис. 2. Фрагмент соединения ODA-компонентов для системы NRI

Компоненты ODA, выделенные под систему NRI, представлены в таблице 1. В таблице выделены блоки, содержащие в себе подходящие компоненты и обязательные программные интерфейсы для этих компонентов, необходимые для взаимодействия между собой.

ТАБЛИЦА 1. Компоненты ODA, представляющие систему NRI

Название компонента	Краткое описание функциональности	API, необходимые для взаимодействия компонентов
Production Block		
Service Inventory	Отвечает за Учёт услуг и контроль свободных ресурсов под услуги. Проверка, которую необходимо выполнить при создании/обновлении элементов учета – это соответствие информации с каталогом услуг [3].	TMF638 Service Inventory можно использовать для запроса экземпляров услуг для клиента через портал самообслуживания или оператор технической поддержки может запрашивать экземпляры услуг от имени клиента, в случае запроса или жалобы со стороны клиента.
Resource Inventory	Отвечает за учет инфраструктуры сетей и имеющихся на ней ресурсов, объектов, включая запасы, детали, производственные активы, которые принадлежат организации и удерживаются	API Resource Inventory можно использовать для учета ресурсов. Resource Inventory API может вызываться Resource

Название компонента	Краткое описание функциональности	API, необходимые для взаимодействия компонентов
Production Block		
	для дальнейшего использования [4]. Компонент Resource Inventory во многом схож с компонентом Service Inventory.	Order Management для создания нового экземпляра ресурса/ обновления существующего экземпляр ресурса в Resource Inventory.
Location Management	Отвечает за организацию сбора данных о местоположении, связанных с производством, в единую структурированную информационную модель для определения разрешенных ресурсов, связанных с производством (например, HLR, HSS) [5]. Location Management упрощает хранение информации о местоположении объекта, связанного с производством, отвечает за отслеживание, управление, добавление регистрации и назначение адреса для ресурса.	TMF673 Geographic Address Management может проверять адрес, введенный клиентом, используемый как часть процесса регистрации заказа. Позволяет получать местоположение, а также географические объекты, связанные с адресом, такие как район, улица, дом.
Service Order Management	Управление заказами на обслуживание (SOM) – это точка входа в домен продукта [6]. Он отвечает за предоставление услуг для клиентов (CFS) на ресурсах, включающие в себя сетевое оборудование и сервисные платформы.	TMF 641 Service Ordering Management может изменять позиции заказа на обслуживание для переключения в деактивированное состояние существующей услуги. Создание сервиса с функцией, модификация существующей услуги для изменения значения характеристики и вспомогательного ресурса.
Intelligence Management		
Resource Performance Management	Управление производительностью ресурсов будет реализовывать функции отслеживания, анализа производительности ресурсов поставщика услуг [7]. Целью компонента является управление конфигурацией ресурсов и взаимосвязь между ними.	На сегодняшний день обязательный API в документации TM Forum отсутствует. Но мы можем сказать, что обязательный API для данного компонента поможет компаниям оптимизировать использование компьютерных ресурсов, повысить производительность и

Название компонента	Краткое описание функциональности	API, необходимые для взаимодействия компонентов
Production Block		
		уменьшать затраты на инфраструктуру.

Заключение

Для адаптации системы «АРГУС NRI» к TM Forum ODA выделены компоненты, поддерживающие требуемую функциональность системы NRI. Реализация системы на основе ODA-компонентов позволит сделать более гибким ИТ-ландшафт оператора, а у разработчика систем появятся компоненты, которые можно использовать не единожды в своих продуктах и решениях. В настоящем исследовании представлена начальная стадия построения ИТ-системы на основе компонентного подхода. В дальнейшем, отталкиваясь от автоматизируемых бизнес-процессов, планируется сформировать полный перечень необходимых компонентов в систему учёта сетевых ресурсов и их связей.

Список используемых источников

1. Продукты и решения // argustelecom. URL: https://argustelecom.ru/ (дата обращения 13.11.2022).

2. ODA Components // tmforum.org. URL: https://oda-directory.labs.tmforum.org/component-map (дата обращения 15.03.2023).

3. TMFC008 Service Inventory v1.2.0 // https://www.tmforum.org/. URL: https://www.tmforum.org/resources/technical-specification/tmfc008-service-inventory-v1-2-0/ (дата обращения 07.03.2023).

4. TMFC012 Resource Inventory v1.0.0 // https://www.tmforum.org/. URL: https://www.tmforum.org/resources/technical-specification/tmfc012-service-inventory-v1-0-0/ (дата обращения 07.03.2023).

5. TMFC014 Location Management v1.0.0 // https://www.tmforum.org/. URL: https://www.tmforum.org/resources/technical-specification/tmfc014-location-management-v1-0-0/ (дата обращения 07.03.2023).

6. TMFC007 Service Order Management v1.0.0 // https://www.tmforum.org/. URL: https://www.tmforum.org/resources/standard/tmfc007-service-order-management-v1-0-0/ (дата обращения 09.03.2023).

7. Resource Performance Management // https://www.tmforum.org/. URL: https://oda-directory.labs.tmforum.org/component-map/intelligence-management/Resource%20Performance%20Management (дата обращения 09.03.2023).

УДК 004.056.53
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПОДХОДОВ К АНАЛИЗУ ЧИПСЕТОВ WLAN С ЦЕЛЬЮ ВЫЯВЛЕНИЯ АППАРАТНЫХ УЯЗВИМОСТЕЙ

А. Ю. Киструга, М. М. Ковцур, Р. И. Шарапов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича.

В настоящее время огромное количество людей использует технологии беспроводной передачи данных, в частности Wi-Fi. Соединение через такие сети очень удобно, и по этой причине в них передается огромное количество данных. В результате, одна из самых главных задач заключается в обеспечении защиты этих данных, особенно это актуально для корпоративных сетей, где защита конфиденциальной информации очень важна. Broadcom – один из крупнейших мировых поставщиков чипсетов для беспроводных устройств. Поскольку чипы данного производителя настолько широко распространены, они могут стать легкой добычей для злоумышленников, и любая обнаруженная в них уязвимость рассматривается как представляющая высокий риск. В целях противодействия активности злоумышленника следует иметь возможность определить уязвимости, которыми обладает конкретный чипсет. Для их выявления требуется применять определённые подходы к анализу указанных чипсетов, которые и исследуются в данной работе.

аппаратные уязвимости, исследование чипсетов, Wi-Fi-exploit, broadcom, прошивка, reverse-engineering.

Аппаратные уязвимости чипсетов WLAN несут огромную опасность для многих устройств. Например, недавно была обнаружена уязвимость в SoC Marvell Avastar 88W8897 (Wi-Fi + Bluetooth + NFC), присутствующей в Sony PlayStation 4 (и ее версии Pro), планшете и ноутбуке Microsoft Surface (+Pro), Xbox One, Samsung Chromebook и смартфонах (Galaxy J1) и Valve SteamLink, которая позволяет дистанционно манипулировать устройством без взаимодействия с пользователем.

В целях выявления аппаратной уязвимости необходимо проанализировать код, записываемый в ПЗУ (Постоянное Запоминающее Устройство) и ОЗУ (Оперативное Запоминающее Устройство) чипсета WLAN. Для получения содержимого ПЗУ используются возможности доступа к памяти микросхемы драйвера хоста через PIO (Программный ввод-вывод), однако для достижения этой цели потребуется изменить драйвер. Это нужно для выполнения команд, необходимых для записи содержимого ПЗУ, что обеспечит возможность дальнейшего его анализа. Если рассматривать чипы производства компании Broadcom, то для них можно найти множество утилит

для взаимодействия со специфичным драйвером bcmdhd. Сама компания Broadcom предоставляет одну из таких утилит командной строки под названием dhdutil [1, 2].

В целях получения содержимого, загружаемого в оперативную память ядра, необходимо скопировать данные, передаваемые микросхеме при её включении. Следовательно, прочитав код инициализации в драйвере хоста, можно найти файл, содержащий полную информацию, записываемую в ОЗУ [1]. Следующим шагом после сбора данных из ОЗУ и ПЗУ является объединение этих данных в один файл, с целью их анализа в интерактивном дизассемблере IDA. Модель файла показана на рис. 1.

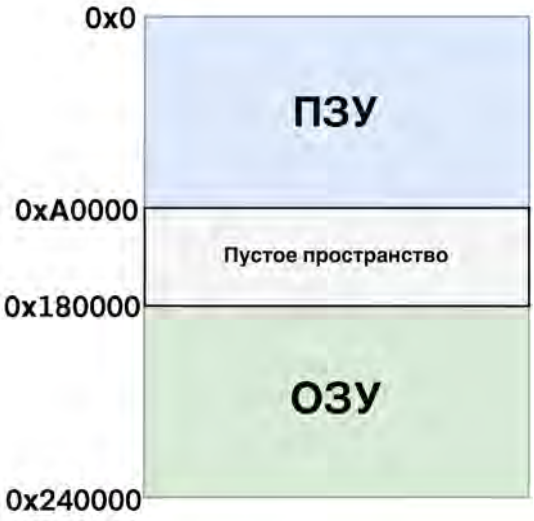


Рис. 1. Общие данные из ПЗУ и ОЗУ

Объемы ОЗУ и ПЗУ в микросхемах WLAN достаточно малы, что приводит производителей к необходимости прикладывать огромные усилия для оптимизации структуры хранения только самых важных данных.

При изучении полученных данных идентифицируются строки, содержащие имена функций и другие подсказки, которые помогают определить и понять базовый код.

Изучив ранее изданные другими исследователями информацию об уязвимостях, можно прийти к выводу, что большинство из них связаны с неправильным использованием значения длины информационного элемента [1, 2, 3]. Информационный Элемент (IE) представляет собой структуру данных в формате TLV (Tag-Length-Value), используемую в кадрах управления IEEE 802.11. Эти IE используются для переноса любых данных, необходимых либо станции, либо точке доступа. В результате анализа подходов других исследователей, обнаружилось, что многие из них описывают работу с TLV. На рис. 2 представлен пример строчек кода [2].

```
typedef struct bcm_tlv {
        uint8_t id;
        uint8_t len;
        uint8_t data[1];
} bcm_tlv_t;
```

Рис. 2. Структура, возвращающая функцию bcm_parsec_tlvs

Одними из самых простых в эксплуатации и анализе считаются уязвимости, представляющие собой heap buffer-overflow (переполнение буфера

структуры данных) [2]. Однако, несмотря на то что эти уязвимости считаются одними из самых простых в эксплуатации, для полного функционирования эксплойта все же может потребоваться дополнительная подготовка.

При анализе чипа Broadcom последние несколько байт содержимого ОЗУ, загруженных в чипсет, содержат строку с версией прошивки, где можно изучить ревизию чипа, дату компиляции прошивки, список тегов. Каждый тег представляет функцию, поддерживаемую образом программы [2].

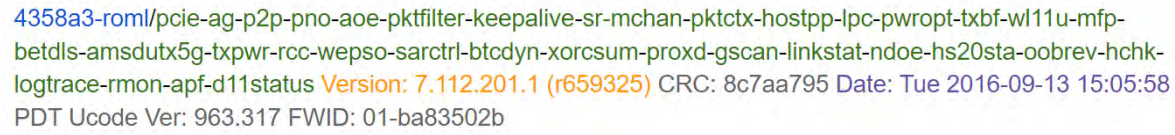


Рис. 3. Строка с информацией о версии прошивки Nexus 6P

Для примера, на рис. 3 в строке версии можно увидеть все функции, которые поддерживает модель данного телефона. Далее, для анализа нужно изучить функции стандарта IEEE 802.11 и определить, с какими функциями злоумышленник может проводить манипуляции [2].

Согласно изученным работам следующим основным шагом является поиск всех вызовов, где манипулируют информационными элементами, а также нахождение всех перекрестных ссылок, вызывающих эти функции и выделение всех мест, где они встречаются. Определив все места вызова, можно найти несколько уязвимостей, которые уже были описаны другими исследователями связанных с обработкой IE [1]. Некоторые функции являются просто оберткой, которая ищет совпадения IE с определенным OUI (Уникальный идентификатор организаций). Такая же функция есть и в ПЗУ прошивки. Проанализировав найденные уязвимости, можно сделать вывод, что они могут быть вызваны при обычном подключении к сетям [4].

Для Nexus 6P злоумышленник сможет воспользоваться уязвимостью, относящейся к реализации Tunneled Direct Link Setup (TDLS) (бесшовный способ более быстрой потоковой передачи мультимедиа и других данных между устройствами, уже находящимися в одной сети Wi-Fi). Соединение TDLS одноранговым узлам в сети Wi-Fi позволяет обмениваться данными в обход Точки Доступа (ТД), тем самым позволяя снизить нагрузку на ТД. Факт поддержки устройством функции TDLS виден благодаря меткам «betdls» и «tdls». Как можно увидеть в телефоне Nexus 6P эта функция поддерживается, а также она поддерживается в большинстве флагманов Samsung. Прочитав информацию о TDLS в стандарте 802.11, можно определить, с какой стороны атакующий сможет манипулировать чипсетом Broadcom [4]. Определив, что сначала функция выполняет некоторые про-

верки, что запрос является допустимым, она запрашивает внутренние структуры данных, чтобы убедиться, что соединение TDLS действительно установлено с нужным узлом. Также функция «wlc_tdls_cal_mic_chk» проверяет, что длина RSN IE (*Robust Security Network Information Element* (поле переменной длины)) не превышает длину буфера, удалось выяснить, что она не может проверить, что последующие IE переполняют буфер. Таким образом, можно сделать вывод, что ввод большого значения длины RSN IE приведет к тому, что интервал ожидания и быстрого перехода IE будут скопированы за пределы границ установленной длины. В последствии, определив максимальную длину функции SSID (символьное название Wi-Fi сети) 32 байта, и удаленно выставив значения более 32 байт, злоумышленник сможет вызвать heap buffer-overflow (переполнения буфера данных), что приводит к удаленному отказу в обслуживании Wi-Fi [5].

В заключении можно отметить, что исследование подходов к анализу чипсетов WLAN с целью выявления наличия аппаратных уязвимостей является важным направлением в области безопасности беспроводных сетей. Благодаря этому исследованию, можно получить дополнительную информацию о потенциальных уязвимостях и проблемах безопасности, связанных с беспроводными сетями. В статье рассмотрены методы и подходы к анализу чипсетов WLAN для выявления общих черт аппаратных уязвимостей, которые могут эксплуатироваться злоумышленниками. Их реализация позволяет злоумышленнику получить несанкционированный доступ к чипсету, манипуляции с ним, а также к перехвату или нарушению целостности передаваемых данных в Wi-Fi среде.

Список используемых источников

1. Reverse-engineering Broadcom wireless chipset // Quarkslab's blog. URL: https://blog.quarkslab.com/reverse-engineering-broadcom-wireless-chipsets.html (дата обращения 02.02.2023).

2. Over The Air .Vol. 2, Pt. 1: Exploiting The Wi-Fi Stack on Apple Devices // Project Zero. URL: https://googleprojectzero.blogspot.com/2017/09/over-air-vol-2-pt-1-exploiting-wi-fi.html (дата обращения 05.02.2023).

3. Over The Air. Vol. 2, Pt. 2: Exploiting The Wi-Fi Stack on Apple Devices // Project Zero. URL: https://googleprojectzero.blogspot.com/2017/10/over-air-vol-2-pt-2-exploiting-wi-fi.html (дата обращения 05.02.2023).

4. Киструга А. Ю., Ковцур М. М., Петров М. П., Шабанов В. П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 561–564.

5. Сахаров Д. В., Красов А. В., Ушаков И. А., Бирих Э. В. Моделирование защищенной масштабируемой сети предприятия с динамической маршрутизацией на основе IPV6 // Защита информации. Инсайд. 2020. N 1 (91). С. 51–57.

УДК 004.056
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ АТАК НА БЕСПРОВОДНЫЕ СЕТИ СТАНДАРТА IEEE 802.11 С РЕЖИМОМ АУТЕНТИФИКАЦИИ WPA3-SAE

А. Ю. Киструга, Н. И. Крыщенко, А. А. Миняев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Безопасность беспроводных сетей стандарта IEEE 802.11 связана с множеством особенностей их структуры и применяемой конфигурации, в которую также входит версия выбранного на устройстве протокола безопасности. В данной статье исследуется эффективность проведения нескольких видов атак на беспроводную точку доступа и клиентов, применяющих режим безопасности WPA3-SAE и смешанный режим WPA2-PSK/WPA3-SAE для аутентификации соединения. Рассматриваются такие атаки как флуд пакетами ассоциации и деаутентификации клиента, а также эксплуатируется уязвимость смешанного режима безопасности. Производится сравнение подверженности режимов безопасности перечисленным атакам с учётом различных версий протокола безопасности, используемых клиентом при подключении к сети Wi-Fi в переходном режиме.

безопасность беспроводных сетей, WPA3-SAE, атака downgrade, атака association flood, атака deauthentication.

Беспроводные сети стандарта 802.11 имеют широкое применение в организациях и домашних сетях по причине удобства применения, заключающегося в обеспечении мобильности пользователей и простой настройке. Однако наравне с проводными, сети Wi-Fi являются объектом для перехвата данных и атак, произвести которые возможно даже без прохождения аутентификации по определённому протоколу безопасности, применяемому на точке доступа. Таким атакам подвержены управляющие кадры, которые позволяют устанавливать и поддерживать соединение в Wi-Fi сети. То есть, не имея никаких сведений о пароле и, соответственно, возможности подключиться к беспроводной сети, можно нарушить её работу, имея при этом лишь программные инструменты для перехвата трафика в беспроводной сети по радиоэфиру и передачи в сеть сгенерированных злоумышленником пакетов.

Новейшей спецификацией безопасности Wi-Fi является WPA3[1], использующей описанный в стандарте IEEE 802.11, но ранее не применяемый метод аутентификации устройств SAE (*Simultaneous Authentication*

of Equals) для предотвращения эксплуатации уязвимостей предыдущей спецификации – WPA2-PSK. Хотя WPA3 включает обязательное использование функции защиты управляющих кадров PMF (*Protected Management Frames*) при подключении клиента, не все виды кадров проверяются на подлинность. Что касается смешанного режима WPA2-PSK/WPA3-SAE, иначе называемого WPA3-SAE Transition Mode, – PMF не является обязательной для поддержки клиентом, что уже может являться дополнительной предпосылкой для влияния атак на работу сети.

Схема организации локальной сети, в которой проводилось исследование атак, представлена на рис. 1. Присутствует легитимный клиент и точка доступа производителя Keenetic, поддерживающая режимы WPA3-SAE и WPA2-PSK/WPA3-SAE. Передаваемый между клиентом и точкой доступа трафик находится в зоне досягаемости злоумышленника, где он имеет возможность перехвата данных посредством анализатора трафика и использования утилит для генерирования кадров, необходимых для проведения атак.

Рассмотрим одну из самых распространённых атак типа отказа в обслуживании – деаутентификацию беспроводного клиента [2], заключающуюся в генерировании и отправке в радиоэфир большого количества кадров типа deauthentication. В ходе исследований было обнаружено, что имплементация WPA3 на конечной станции не гарантирует полной защиты от атаки флуда фреймов деаутентификации. Например, адаптер ASUS USB-N13 при выполнении данной атаки продолжает терять связь с точкой доступа (рис. 2), что открывает дополнительные возможности для проведения downgrade-атаки, так как позволяет более эффективно осуществлять атаку Evil Twin в адрес станций, которые уже подключены к легитимной точке доступа по WPA3.

Рис. 1. Схема стенда сети

Time	Source	Destination	Protocol	Info
32.582719	Keenetic_1f:52:fe	ASUSTekC_68:cc:73	802.11	Deauthentication, SN=58, FN=0, Flags=........
33.027548	ASUSTekC_68:cc:73	Keenetic_1f:52:fe	802.11	Deauthentication, SN=59, FN=0, Flags=........
33.643216	ASUSTekC_68:cc:73	Keenetic_1f:52:fe	802.11	Disassociate, SN=598, FN=0, Flags=.p.....
33.768904	ASUSTekC_68:cc:73	Keenetic_1f:52:fe	802.11	Authentication, SN=599, FN=0, Flags=........
33.769696	Keenetic_1f:52:fe	ASUSTekC_68:cc:73	802.11	Authentication, SN=3300, FN=0, Flags=........
33.772547	ASUSTekC_68:cc:73	Keenetic_1f:52:fe	802.11	Reassociation Request, SN=600, FN=0, Flags=........, SSID="Keenetic-5501"
33.774742	Keenetic_1f:52:fe	ASUSTekC_68:cc:73	802.11	Reassociation Response, SN=3301, FN=0, Flags=........
35.234397	Keenetic_1f:52:fe	ASUSTekC_68:cc:73	802.11	Deauthentication, SN=60, FN=0, Flags=........

Рис. 2. Дамп трафика при атаке деаутентификации

Следующей проведённой атакой является association flood [3, 4], то есть флуд пакетами authentication и association request для имитации подключения новых клиентов с поддельными MAC-адресами. Точка доступа отвечала на каждый запрос пакетом association response и, соответственно, каждый поддельный клиент учитывался в таблице ассоциаций (рис. 3), влияя на качество подключения к сети: возникали проблемы с загрузкой веб-страниц, клиент полностью отключался от сети Wi-Fi, а загруженность центрального процессора точки доступа составляла 50–90 % в зависимости от количества пересылаемых в сеть пакетов.

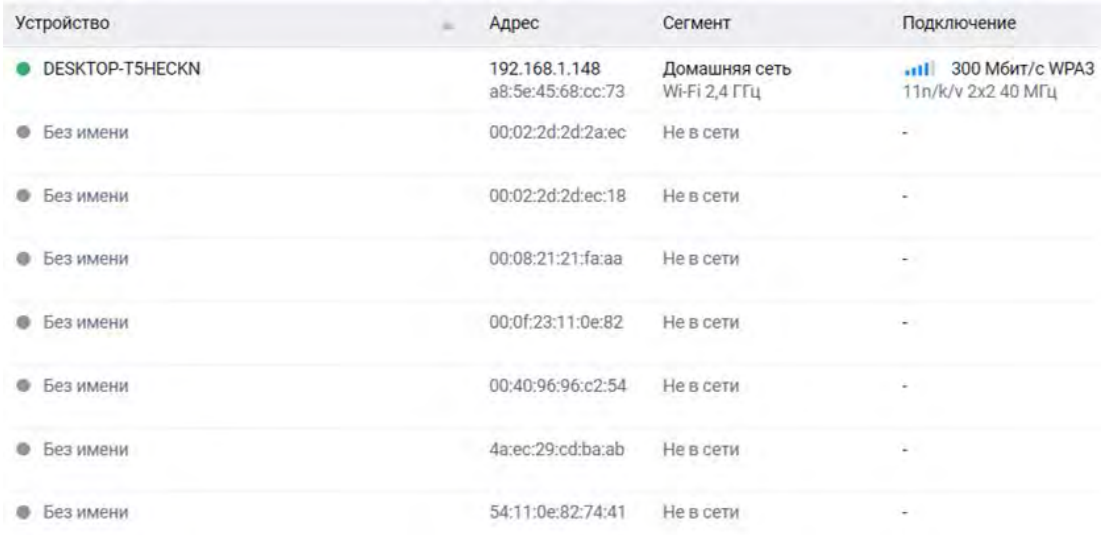


Рис. 3. Переполнение таблицы ассоциаций точки доступа при атаке флудом запросов ассоциации

Как видно из таблицы 1 (см. ниже), атаки проводились при трёх различных условиях: клиент и точка доступа использовали WPA3; клиент использовал WPA2 либо WPA3, а точка доступа при этом смешанный режим WPA2/WPA3. Можно сделать вывод о том, что подавляющее большинство режимов безопасности точки доступа, включающих стандарт WPA3, было подвержено атакам deauthentication и association flood – они приводили к отключению клиента от сети либо не позволяли выходить в сеть Интернет, а также перегружали процессор точки доступа. Атака деаутентификации не считается однозначно успешной для режима WPA3, так как дополнительно проведённые исследования показали устойчивость клиентских устройств к данной атаке в силу корректной настройки функции PMF.

По причине того, что в настоящее время WPA3 только начинает внедряться в современные устройства, подавляющее большинство устройств использует стандарт WPA2. Это стало поводом для разработки смешанного режима аутентификации WPA2+WPA3, благодаря которому устройства, поддерживающие только режим WPA2, могли бы осуществлять соединение с сетью Wi-Fi наравне с клиентами, которым уже доступен режим WPA3.

ТАБЛИЦА 1. Эффективность проведения атак с учётом различных режимов безопасности

Вид атаки	Режим безопасности точки доступа и клиента		
	Точка доступа и клиент с WPA3-SAE	Точка доступа с WPA2-PSK+WPA3-SAE, клиент с WPA2	Точка доступа с WPA2-PSK+WPA3-SAE, клиент с WPA3
Флуд запросами ассоциации	+	+	+
Деаутентификация	–*	+	+

Серьёзной уязвимостью переходного режима WPA3-SAE Transition Mode является возможность подключения клиента с режимом WPA3 к созданной злоумышленником поддельной точке доступа с режимом WPA2 и похожими настройками с целью выявления зашифрованного пароля методом перебора по словарю. Такая атака получила название downgrade [5], алгоритм её реализации заключался в следующем:

1) Клиент ввёл пароль от сети в режиме WPA3 при подключении к точке доступа с режимом WPA2+WPA3.

2) Злоумышленник осуществил атаку флуда пакетами ассоциации либо деаутентификации клиента и, зная SSID сети, создал поддельную точку доступа с таким же названием, но только доступным режимом WPA2, вынуждая клиента считать точку доступа легитимной.

3) При попытке подключения к поддельной точке доступа, используя режим WPA2, в ответ на первое сообщение клиент передал второе сообщение 4-х стороннего рукопожатия, содержащее сгенерированную им случайную последовательность SNonce.

4) Злоумышленник перехватил пакеты рукопожатия (рис. 4), на основе которых провелась атака по словарю и был подобран пароль, применяемый при подключении клиента к подлинной точке доступа по алгоритму WPA3-SAE.

```
CH  1 ][ Elapsed: 54 s ][ 2022-11-27 12:59 ][ WPA handshake: AE:92:56:6F:DB:6A

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

50:FF:20:1F:52:FE  -34 100      536       32    0   1  270   WPA3 CCMP   SAE  Keenetic-5501
AE:92:56:6F:DB:6A  -36   1      536        8    0   1   54   WPA2 TKIP   PSK  Keenetic-5501
64:64:4A:9A:E1:CF  -84   6       79        1    0   2  130   WPA2 CCMP   PSK  Mechanic
88:C3:97:67:04:9C  -82   0        6        0    0   1  130   OPN              xiaomi-repeater-v3_mia
70:8B:CD:C6:93:18  -84  80      454      332    6   1  195   WPA2 CCMP   PSK  Aleksandr
98:DA:C4:B7:93:2E  -89  12       99        0    0   1  270   WPA2 CCMP   PSK  TP-Link_932E
```

Рис. 4. Перехваченное рукопожатие клиента и поддельной точки доступа

Тем самым, клиент, аутентифицированный по протоколу WPA3 подвержен тому, что его пароль может быть взломан методом перебора, несмотря на то что изначально используемый алгоритм SAE призван исключить данную атаку.

В ходе проведённого исследования можно сделать вывод, что несмотря на усовершенствованные характеристики стандарта WPA3, безопасность сети всё ещё остаётся под угрозой в силу незащищённости большинства управляющих кадров, организующих соединение между точкой доступа WLAN и клиентом, а также возможности возврата к более уязвимому протоколу. Без использования дополнительных методов защиты [6, 7, 8, 9, 10] беспроводные сети с рассматриваемым стандартом нельзя считать однозначно устойчивыми к нарушению их функционирования и взломам. Успешность проведения атак деаутентификации или флуда запросами ассоциаций даёт возможность злоумышленнику в дальнейшем провести более серьёзные атаки, например, после деаутентификации клиента подключить его к поддельной точке доступа с аналогичными параметрами для получения возможности перебора пароля пользователя по словарю и кражи, передаваемых им по сети данных.

Список используемых источников

1. Wi-Fi Alliance. 2022. WPA3 Specification Version 3.1. URL: https://www.wi-fi.org/file/wpa3-specification (дата обращения 03.02.2023).

2. Киструга А. Ю., Ковцур М. М., Петров М. П., Шабанов В. П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 561–564.

3. Ворошнин Г. Е., Ковцур М. М., Киструга А. Ю., Докшин А. Д. Исследование устойчивости оборудования Mikrotik к атаке association flood на беспроводную сеть семейства IEEE 802.11 // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 10 / СПОИСУ. СПб., 2021. С. 354–358.

4. Юркин Д. Ю., Ворошнин Г. Е., Ковцур М. М., Мисливский Б. С. Исследование влияния атак ARP inject и association flood в беспроводных сетях на базе оборудования Mikrotik // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 1. С. 44–48.

5. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. URL: https://eprint.iacr.org/2019/383 (дата обращения 06.02.2023).

6. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 734–739.

7. Kovtsur M., Minyaev A., Khramtsov D., Abramenko G. Investigation of attacks and methods of protection of wireless networks during authorization using the IEEE 802.1X protocol // ACM International Conference Proceeding Series. 5, The Premier Conference on Smart

Next Generation Networking Technologies. Сер. "ICFNDS 2021 – 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies". 2021. PP. 555–561.

8. Дешевых Е. А., Конюхов В. М., Крылов К. Ю., Ушаков И. А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПб. : СПбГУТ, 2015. Т. 1. С. 310–313.

9. Kovtsur M. M., Muthanna A., Karelsky P., Kozmyan A., Voroshnin G., Al-Khafaji H. M. R. IPTV Access Methods with RADIUS-Server Authorization // Journal of Information Technology Management. 2022. Vol. 14. N 2. PP. 80–89.

10. Крыщенко Н. И., Миняев А. А., Ковцур М. М. Обзор методических рекомендаций по конфигурированию защищённой WLAN сети // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции. Санкт-Петербург, 2022. С. 554–555.

УДК 004.056
ГРНТИ 81.93.29

ОНТОЛОГИЯ МОДЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. В. Клишин[1], А. А. Чечулин[2]

[1]Национальный исследовательский университет ИТМО
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Целью данной работы является систематизация имеющихся знаний о моделях информационной безопасности, представленных в стандартах и научных исследованиях путем выявления основных понятий и унификации моделей для решения проблемы трудоемкости: анализа, выбора актуальной для информационной инфраструктуры предприятия модели информационной безопасности; оценки текущего уровня информационной безопасности предприятия.

В работе: выявляются основные понятия и их свойства, используемые в документах по информационной безопасности, описывающих модели информационной безопасности; формируются связи между понятиями; начато формирование онтологии моделей информационной безопасности, описанных в нормативно-правовых актах.

модель информационной безопасности, уровень информационной безопасности, стандарт, онтология, понятия моделей информационной безопасности, процессы информационной безопасности.

В настоящее время в сфере информационной безопасности (далее – ИБ) насчитывается большое количество моделей ИБ, основанных на нормативно-правовых актах (далее – НПА), стандартах и научных исследованиях.

Согласно исследованию организации Compliance Forge [1] на международном рынке ИБ насчитывается более 180 НПА и стандартов, описывающих модели ИБ.

В случаях, когда выбор подходящей модели не определен требованиями законодательства и регуляторов отрасли, то подбор актуальной для предприятия модели ИБ является трудоемкой задачей. Выбор необходимой модели также может потребоваться для компенсирования мер, не рассматриваемых в моделях, определенных требованиями нормативно-правовых актов. Наличие большого количества моделей ИБ формирует проблему при их использовании и поднимает вопрос выбора, актуальной для предприятия, модели или мер ИБ. Для решения данной проблемы требуется систематизировать знания о моделях путем их унификации и выявления основных понятий. Формирование общего словаря понятий актуально для специалистов по ИБ, которым требуется проводить оценку соответствия ИБ защищаемой системы требованиям нормативно-правовых актов и стандартов. Актуальность данной работы обусловлена важностью роли модели ИБ в обеспечении ИБ.

Целью данной работы является систематизация имеющихся знаний о моделях ИБ, представленных в стандартах и научных исследованиях путем выявления основных понятий и унификации моделей.

Для выявления основных понятий, используемых в моделях, были проанализированы работы по ИБ, перечисленные на рис. 1.

Рис. 1. Документы по информационной безопасности, описывающие модели

Как правило модели имеют структуру, состоящую из мер ИБ, которые необходимо реализовать для достижения требуемого уровня ИБ, сгруппи-

рованных по общим признакам – критериям. Документ по ИБ может содержать в себе описание нескольких моделей, в зависимости от актуальных и рассматриваемых в данном документе угроз и рисков ИБ.

По итогам анализа документов с описанием моделей ИБ, представленного в статье «Анализ стандартов обеспечения информационной безопасности» [2], были выявлены следующие понятия, представленные в таблице 1.

ТАБЛИЦА 1. Понятия моделей и их определения

Понятие	Определение
Аудитор	Объект, осуществляющий оценку соответствия текущего уровня ИБ организации модели ИБ
Свидетельство	Объект, полученный по итогам проведения операции
Стандарт	Документ описывающий модель ИБ
Модель ИБ	Требования к совокупности технических и организационных мер по обеспечению ИБ
Цель	Финальный результат, на который преднамеренно направлен процесс
Процесс ИБ	Повторяющаяся последовательность действий, направленная на достижение цели и состоящая из мер ИБ
Подпроцесс ИБ	Итог декомпозиции процесса на менее трудоемкие процессы, каждый из которых имеет собственную цель
Операция	Итог декомпозиции процесса или подпроцесса на функции, выполняемые каким-либо объектом над субъектом инфраструктуры предприятия
Структурное подразделение	Орган управления определенным участком деятельности организации, с назначением его ответственным за реализацию определенных операций. Структурное подразделение может быть, как субъектом, так и объектом
Средство/ Инструмент	Объект, при помощи которого осуществляется операция
Объект	Субъект, над которым осуществляется операция

По итогам определения понятий были выявлены их соотношения между собой и сформирована онтология понятий моделей ИБ, представленная на рис. 2 (см. ниже).

По итогам анализа онтологии понятий моделей было выявлено, что в моделях используется процессный подход к обеспечению ИБ, в котором определяются процессы обеспечения ИБ, которые могут быть декомпозированы на менее трудоемкие процессы (подпроцессы) и операции, ответственность за выполнение которых возлагается на определенное структурное подразделение.

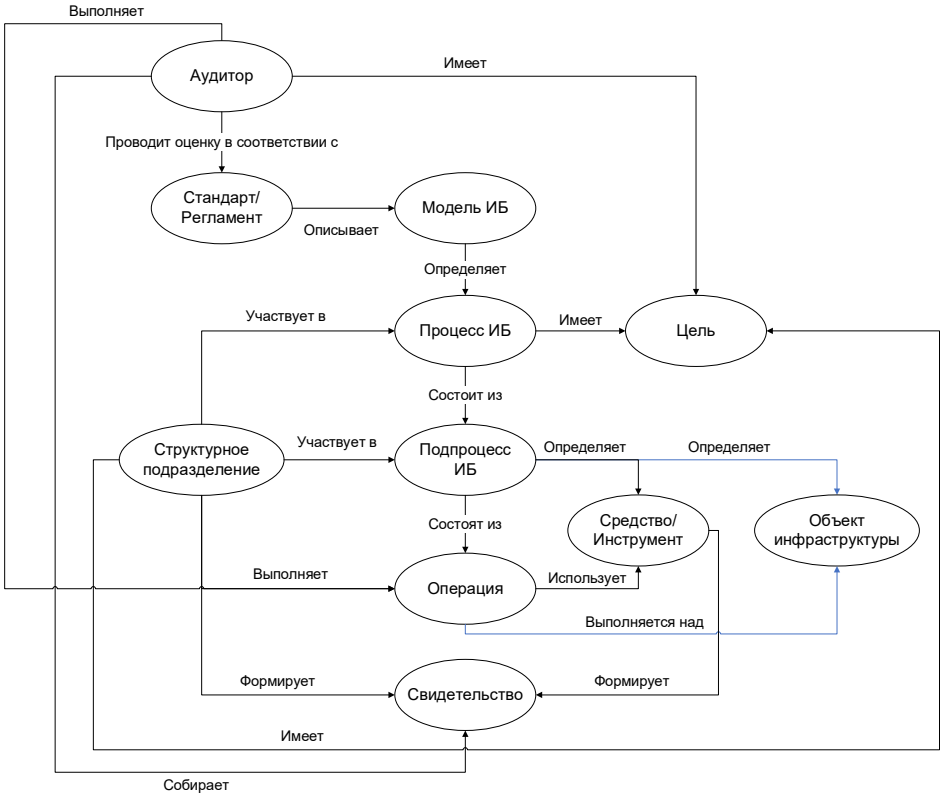


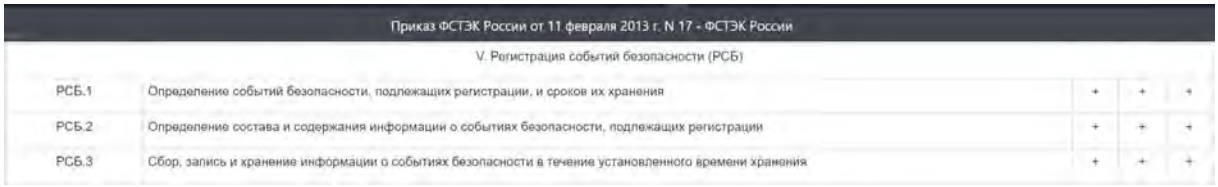
Рис. 2. Онтология понятий моделей информационной безопасности

Для апробирования выявленных понятий и их связей была частично сформирована онтология моделей, основанных на требования приказов ФСТЭК России № 17 [3] и № 239 [4], путем создания экземпляров понятий. На рис. 3 представлено графическое отображение онтологии моделей, представленных требованиями [3] и [4]. Данная онтология сформирована при помощи программы Protégé и включает в себя все выявленные понятия, экземпляры понятий в объеме равном менее 2 %, их связи и свойства.

Рис. 3. Онтология моделей приказов ФСТЭК России № 17 и № 239

По итогам формирования онтологии моделей было обнаружено скрытое знание.

В [3] есть критерий, который описывает меры, лежащие в основе процесса регистрация событий безопасности. Как показано на рис. 4 данный процесс разбит на подпроцессы.



Приказ ФСТЭК России от 11 февраля 2013 г. N 17 - ФСТЭК России

V. Регистрация событий безопасности (РСБ)

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+

Рис. 4. Критерий «РСБ» приказа ФСТЭК России № 17

В [4] данного критерия нет, но есть критерий, который описывает меры, лежащие в основе процесса аудита безопасности. Данный процесс включает в себя подпроцесс под названием «Регистрация событий безопасности» как показано на рис. 5.

Приказ ФСТЭК России от 25 декабря 2017 г. N 239 - FSTEC Russia

V. Аудит безопасности (АУД)

АУД.0	Регламентация правил и процедур аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2	Анализ уязвимостей и их устранение	+	+	+
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4	Регистрация событий безопасности	+	+	+

Рис. 5. Критерий «АУД» приказа ФСТЭК России № 239

Исходя из полученной информации можно сделать вывод, что процесс аудита безопасности, включает в себя процесс регистрации событий безопасности, подпроцессы которого описанный в [3]. Таким образом процесс регистрации событий безопасности можно отнести как к [3], так и к [4].

Также основываясь на данном знании можно определить из каких операций должны состоять подпроцессы и сформировать похожие операции для других подпроцессов. Исходя из анализа процесса регистрации событий можно сделать заключение, что подпроцесс должен включать в себя не только технические операции, такие как использование средств защиты информации, но организационные.

В рамках данной работы были выполнены следующие задачи: проведен литературный обзор в части требований к моделям ИБ; осуществлен анализ моделей ИБ, рассмотренных в стандартах и научных исследованиях; проведена систематизация полученных знаний путем формирования онтологических понятий, свойств и их соотношений; начата разработка онтологического представления стандартов.

Результаты данной работы позволили выявить общие элементы моделей ИБ, что позволит использовать полученную информацию для уменьшения трудозатрат при формировании используемой предприятием модели ИБ путем автоматизации.

Список используемых источников

1. Secure Controls Framework: официальный сайт. URL: https://www.securecontrols-framework.com/.

2. Клишин Д. В., Чечулин А. А. Анализ стандартов обеспечения информационной безопасности // Системы анализа и обработки данных. 2023. N 1 (89). С. 37–54. DOI: 10.17212/2782-2001-2023-1-37-54.

3. Приказ об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: от 11 февраля 2013 г. № 17. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702.

4. Приказ об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации: от 25 декабря 2017 г. № 239. URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239.

УДК 377,378
ГРНТИ 14.85

ВОПРОСЫ ОЦЕНКИ КАЧЕСТВА ПРОГРАММНЫХ СРЕДСТВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

И. С. Ковалев[1], О. И. Пантюхин[2], В. В. Пащенко[1], Б. В. Солодухин[1]

[1]Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Оценка качества программных средств автоматизированных систем различного назначения является сложным процессом, основу которого составляет выбор показателей качества. Особенностью разработки программных средств является необходимость строгого соблюдения государственных стандартов как в области качества программного обеспечения, так и в области разработки автоматизированных систем.

программное обеспечение, программные средства, оценка качества, государственный стандарт, показатели качества.

В условиях развязанной против Российской Федерации тотальной гибридной (санкционной) войны, которая ведется во всех сферах, а также ухода мировых компаний – разработчиков программного обеспечения (ПО) и информационных технологий с российского рынка необходимо предпринимать собственные усилия для победы в конкурентной борьбе и повышении компьютерной (кибернетической) безопасности органов государственной власти, силовых ведомств, финансовых организаций государства и отдельных пользователей ПО. В связи с этим усиливается необходимость

в повышении качества выпускаемого программного обеспечения, чтобы выиграть конкурентную борьбу. Многие компании начали инвестировать достаточно больше финансовых средств в повышение качества своих программных продуктов, в них стали появляться отделы по контролю за качеством и вводиться новые технологии разработки и тестирования программных средств (ПС).

Оценка качества выпускаемой продукции в целом, и программных средств в частности, является одной из главных задач как разработчиков, так и заказчиков ПС. Ведь от правильности выбранных подходов к определению показателей качества и своевременности предпринятых действий по их оценке безусловно зависят итоговые затраты, а также сроки завершения работ по выпуску разрабатываемых продуктов. Кроме того, при аттестации автоматизированных систем управления главными, доминирующими являются показатели уровня развития функций управления, методов управления и аппарата управления. Высокие показатели автоматизированных систем в значительной степени зависят от качества используемых технических и программных средств.

В настоящее время основные вопросы оценки качества ПС определены в соответствующих руководящих документах Российской Федерации [1]: ГОСТ 28806-90 [2]; ГОСТ 28195-89 [3]; а при разработке программных изделий специального назначения необходимо руководствоваться ГОСТ Р 51189-98 [1].

При обосновании оценки качества (ОК) ПС необходимо использовать определения основных понятий качества ПС [2].

Исходя из принципов системности и технологической полноты [1] необходимо на ранних стадиях разработки определить характеристики, показатели и критерии оценки качества, разрабатываемого ПС. С этой целью обычно составляется общий список свойств ПС, характеризующих его качество, устанавливаемый государственными стандартами.

ГОСТ 28195-89 вводит следующую номенклатуру частных показателей качества и характеризуемые ими свойства программного средства: показатели надежности, кибербезопасности, сопровождения, удобства применения, эффективности, универсальности и корректности.

Оценка качества ПС выполняется в течение всего жизненного цикла средства от создания до модификации или списания:

- при формировании (планировании) показателей качества ПС;
- при контроле качества на отдельных этапах разработки;
- при контроле качества в процессе производства ПС;
- при проверке эффективности модификации ПС на этапах сопровождения и эксплуатации [2, 3].

В настоящее время все большее значение придается обеспечению безопасности данных, хранимых и обрабатываемых в автоматизированных

системах, поскольку накопленный в мировой практике опыт программирования и специфика программного обеспечения допускают возможность создания и размещения в ПС различного рода включений, в том числе и диверсионного назначения, к которым относят компьютерные вирусы и программные закладки.

Преступники могут использовать легальный и теневой Интернет, где предлагают многие виды запрещённых товаров и большинство нелегальных услуг. В теневом Интернете (Даркнете) предлагаются инструменты для криминальных действий (вредоносное программной обеспечение, программы-вымогатели, средства поддержки фишинга, анализаторы трафика, устройства для кражи данных с кредитных карт и распределённые атаки DDoS – «отказ в обслуживании». Хакерские программы постоянно совершенствуются и отличаются большим разнообразием. Агентство Европейского Союза по кибербезопасности каждый год сообщает об обнаружении сотен тысяч новых штаммов вредоносных программ.

При разработке требований к ПС на ранних стадиях жизненного цикла необходимо конкретизировать перечень свойств ПС с учетом его назначения и требований областей применения. При разработке концепции ПС следует выбрать и обосновать критерии оценки качества. Далее перечень показателей качества и критерии их оценки указывают в разделе «Требование к программе или программному изделию» технического задания.

При разработке программы и методики проведения испытаний необходимо определить методику оценки качества ПС по указанному в техническом задании перечню показателей.

Основную часть данного процесса составляют определение методики оценки качества для конкретного программного средства, установление критериев его оценки, измерение значений показателей и другие. Однако, правильный выбор показателей является первым и необходимым условием для разработки качественного продукта.

Такому подходу обучают студентов магистратуры, бакалавриата и специалитета при изучении дисциплин по направлению программной инженерии в ведущих технических вузах страны, Санкт-Петербурга, например, на кафедрах СПбГУТ и Военной академии связи.

Список используемых источников

1. Пантюхин О. И., Бочкарёв Д. А., Вакалюк А. И. Выбор показателей для оценки качества программных средств специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 2. С. 102–105.

2. ГОСТ 28806-90. Качество программных средств. Термины и определения. Сб. ГОСТов. М. : Стандартинформ, 2005.

3. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. М. : Издательство стандартов, 1989.

4. Пантюхин О. И., Вакалюк А. И., Бауман В. В., Севастьянов С. И. Вопросы создания системы обеспечения разработки, сопровождения и распространения программных средств требуемого качества // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г.: Материалы конференции / СПОИСУ. СПб., 2019.

УДК 621.396.4
ГРНТИ 50.37.03

АНАЛИЗ ОСНОВНЫХ ХАРАКТЕРИСТИК КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ

И. С. Ковалев, И. Б. Паращук, А. А. Смирнов

Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Проведен анализ роли и места программного обеспечения в структуре процесса автоматизированного управления современными инфокоммуникационными сетями. С учетом анализа действующих отечественных и международных стандартов сформулированы ключевые характеристики качества программных средств в интересах управления сложными объектами такого класса. Рассмотрены возможные показатели, позволяющие получать качественные и количественные оценки качества программного обеспечения для автоматизированного управления современными инфокоммуникационными сетями.

программное обеспечение, автоматизированное управление, инфокоммуникационные сети, характеристики качества, показатель качества.

Автоматизированное управление современными инфокоммуникационными сетями (ИКС) находится в постоянном динамическом развитии, очень быстро совершенствуется по сравнению с другими областями рынка систем управления элементами сетей, сетевыми решениями и рынка систем поддержки принятия решений по сетевому мониторингу [1, 2, 3, 4, 5].

Наряду с аппаратными средствами, ключевым, на наш взгляд, компонентом, непосредственно влияющим на устойчивость, непрерывность, оперативность и безопасность автоматизированного управления современными ИКС, является программное обеспечение процессов такого класса. При этом

программное обеспечение для управления инфокоммуникационными сетями подразумевает взаимоувязанную совокупность актуальных программных решений, например, для автоматизированных систем управления доменами ИКС, реализующих сетевые функции, а также для современных высокопроизводительных сетевых контроллеров и маршрутизаторов, работающих практически в реальном масштабе времени [6, 7].

Программное обеспечение для автоматизированного управления инфокоммуникационными сетями, с точки зрения оценки его качества, представляют собой традиционные, классические программные средства. В этой связи методология теоретической и экспериментальной оценки качества программного обеспечения такого класса, на наш взгляд, должна основываться на имеющихся отечественных и международных стандартах в области оценки качества программных средств. В частности, в рамках отечественных стандартов впервые были определены базовые понятия в этой области [8, 9, 10].

Этими и некоторыми зарубежными стандартами, например, [11] и [12], узакониваются основные определения в области оценки качества программных средств, номенклатура показателей качества и возможные методы их расчета. В частности, определено понятие «качество программного средства», которое представляет собой комплекс всех свойств программного средства, которые обусловливают его пригодность к удовлетворению заранее заданных (или подразумеваемых) требований с точки зрения его соответствия назначению.

Кроме того, анализ указанных отечественных и зарубежных стандартов в данной области позволяет сгруппировать и систематизировать номенклатуру характеристик качества программных средств. В состав данной номенклатуры предлагается включить ряд характеристик, которые, с учетом изучения как российских, так и международных стандартов, в достаточной мере (с достаточной мерой полноты) описывают качество программного обеспечения (ПО) и образуют базу для анализа качества программного обеспечения в интересах автоматизированного управления современными инфокоммуникационными сетями.

Ключевыми характеристиками качества программных средств для автоматизированного управления современными ИКС, на наш взгляд, должны служить:

набор функциональных опций программного обеспечения, которые описывают базовый комплект признаков (атрибутов), относящихся к сути множества реализуемых функций (которые реализуют установленные или предполагаемые потребности для автоматизированного управления современными ИКС) и их конкретным свойствам;

надежность, как совокупность признаков ПО, относящихся к его способности сохранить требуемую степень качества при конкретных условиях функционирования и за определенный интервал времени;

прагматичность (полезность), как сочетание признаков ПО, относящихся к диапазону и масштабу работ, необходимых для практического применения данных программных средств по назначению и возможного оценивания плодотворности такого применения должностными лицами, ответственными за функционирование подсистем автоматизированного управления современными ИКС;

получаемый эффект во взаимосвязи с затратами (эффективность), как сочетание признаков ПО, относящихся к соотношению между степенью (величиной интегрированного показателя) качества функционирования программного обеспечения для автоматизированного управления современными ИКС и объемом используемых для этого вычислительных и аппаратных ресурсов;

поддержка (сопровождаемость), как сочетание признаков ПО, относящихся к диапазону и масштабу работ, необходимых для проведения модификации программных средств в интересах автоматизированного управления современными ИКС;

переносимость на различные аппаратные платформы (программная мобильность), как совокупность признаков ПО, относящихся к его способности быть кросс-платформенным, т. е., быть без ущерба перенесенным из одного аппаратного окружения в иное;

модульность ПО, как совокупность признаков ПО, относящихся к его способности к замене и совершенствованию одних своих сервисов без изменения других сервисов, что позволяет постепенно, шаг за шагом расширять ПО для автоматизированного управления современными ИКС, начиная с минимальной конфигурации программных средств;

масштабируемость, как сочетание признаков ПО, относящихся к его способности к пропорциональному увеличению производительности при добавлении аппаратных ресурсов и, как следствие, при росте вычислительной мощности подсистемы автоматизированного управления современными ИКС;

транспарентность (открытость), как совокупность признаков ПО, относящихся к возможности его свободного публичного распространения, обусловленной доступностью исходных кодов и их способностью изменяемся, что позволяет разрабатывать сложные аппаратно-программные подсистемы, например, подсистемы автоматизированного управления современными ИКС, с минимальными временными и иными ресурсными затратами на их создание, т. к., ключевые функции этих подсистем могут быть реализованы на базе открытых, готовых и, зачастую, уже апробированных программных решений.

Анализ основных характеристик качества ПО для управления современными инфокоммуникационными сетями, и, в частности, детальный анализ работы [13], позволил сгруппировать в гипотетические характеристические множества (на основе рассмотренных характеристик), предложить и обозначить некоторые показатели качества, позволяющие получать качественные и количественные оценки.

Например, к показателям качества ПО для автоматизированного управления современными ИКС, на наш взгляд, можно отнести: пригодность ПО, правильность (безошибочность), способность к взаимодействию, согласованность, защищенность, стабильность, устойчивость к ошибке, восстанавливаемость, понятность для пользователя, обучаемость, простота использования, показатели изменения во времени, показатели затрат ресурсов, анализируемость кода, изменяемость (модифицируемость), устойчивость, тестируемость, адаптируемость, простота внедрения, соответствие аппаратной платформе и взаимозаменяемость [13].

Таким образом, рассмотрены роль и место программного обеспечения в структуре процесса автоматизированного управления современными инфокоммуникационными сетями. С учетом анализа действующих отечественных и международных стандартов сформулированы ключевые характеристики качества программных средств в интересах управления сложными объектами такого класса. Рассмотрены возможные показатели, позволяющие получать качественные и количественные оценки качества программного обеспечения для автоматизированного управления современными инфокоммуникационными сетями.

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. СПб. : Питер, 2021. 1005 с.

2. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост NGN. СПб. : БХВ Петербург, 2014. 160 с.

3. Авраменко В. С., Беззубов О. В., Беляев С. В. и др. Технологии и средства построения инфокоммуникационных систем специального назначения. Часть II : учебник / Под общ. ред. И. Б. Саенко. СПб. : ВАС, 2021. 416 с.

4. Легков К. Е. Новые принципы построения автоматизированных систем управления современными инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли**.** 2015. N 1. С. 38–41.

5. Башкирцев А. С., Митрофанов Е. А., Паращук И. Б. Автоматизированные системы управления телекоммуникационными сетями: обзор и анализ современных требований // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28–30 октября 2020г.: Материалы конференции. Часть 1 / СПОИСУ. СПб. : 2020. С. 63–65.

6. Булдакова Р. А. Программное обеспечение ЦСК: Методические указания по выполнению практических работ. Екатеринбург : УрТИСИ «СибГУТИ», 2005. 49 с.

7. Жмуров В. Д., Паращук И. Б., Саяркин Л. А. Некоторые подходы к анализу надежности программного обеспечения автоматизированных систем управления сетями

связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция (АПИНО-2018) : сб. науч. ст. в 4-х ч. СПб. : СПбГУТ, 2018. Т. 4. С. 234–239.

8. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. М. : ИПК Издательство стандартов. 1989. 31 с.

9. ГОСТ 28806-90. Качество программных средств. Термины и определения. М. : ИПК Издательство стандартов. 1990. 8 с.

10. ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов. М. : Стандартинформ, 2015. 36 с.

11. International Standard ISO/IEC TR 9126-2:2003. Software engineering Product quality. Part 2: External metrics. JTC 1/SC 7. 2003. 94 p.

12. International Standard ISO/IEC 25010:2011(E). Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models. JTC 1/SC 7. 2011. 44 p.

13. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. М. : ИПК Издательство стандартов. 2004. 12 с.

УДК 004.056
ГРНТИ 81.93.29

АТАКИ С ИСПОЛЬЗОВАНИЕМ УЯЗВИМОСТИ СВЯЗАННОЙ СО СРЕДСТВОМ ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО УДАЛЕННОГО ДОСТУПА KASPERSKY VPN SECURE CONNECTION И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИМ

А. А. Ковалева, А. П. Куликовская,
А. А. Саркисян, Е. С. Холоденок, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье приведено описание ряда уязвимостей, связанных с работой информационных систем. В данной статье применялся анализ уязвимостей и атак, выполненный при помощи эксплуатации данных уязвимостей. Приведены примеры атак, выполненных с помощью эксплуатации данных уязвимостей. В статье так же описаны меры противодействия данным уязвимостям. На основании описанного в данной статье можно сделать вывод, что к наиболее распространенным причинам возникновения уязвимостей, как правило, относят: ошибки при проектировании и использовании программного обеспечения; несанкционированное внедрение и последующее использование ПО; внедрение вредоносного ПО; человеческий фактор. Своевременное реагирование

на появление определенных уязвимостей и следование рекомендациям по их устранению способствуют поддержанию общего уровня информационной безопасности на должном уровне.

информационная безопасность; уязвимость, кибератака, информационная система, мониторинг.

В современном мире совершается большое число цифровых преступлений. К ним можно отнести распространение вредоносного программного обеспечения, кражу реквизитов банковских карт, взлом паролей. Для противодействия преступлениям в сфере цифровых технологий применяется цифровая криминалистика или наука, направленная на получение, обработку и анализ данных, расположенных на электронных носителях [1].

Электронные доказательства имеют решающее значение для расследований в области цифровой криминалистики [2]. Одним из основных источников пользовательских данных является образ памяти исследуемого устройства. Память устройства содержит информацию о запущенных процессах, учётных данных, сетевых соединениях, сообщениях из чатов [3].

Для доступа к ресурсам компьютера могут потребоваться особые команды, недоступные обычному пользователю. Например, в операционной системе Windows существуют различные права и привилегии пользователей. Они вводят ограничения на выполнение некоторых системно-ориентированных команд и доступ к данным [4]. Однако используя уязвимости операционной системы, можно повысить привилегии пользователя и получить права администратора. С помощью прав администратора можно получить доступ к гораздо большему набору команд и защищённым данным. Своевременное обнаружение и противодействие такого рода уязвимостям, способствует повышению общего уровня информационной безопасности используемой информационной системы [5].

В результате мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках от 8 августа 2022 г. была опубликована информация об уязвимости средства организации защищенного удаленного доступа Kaspersky VPN Secure Connection. Уязвимости был присвоен регистрационный номер CVE-2022-27535 [6].

Уязвимость средства организации защищенного удаленного доступа Kaspersky VPN Secure Connection связана с возможностью удаления произвольных файлов в системе. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии путем создания специально сформированной символической ссылки на критическую папку в системе и удаления ее с помощью функции «Удалить служебные данные и отчеты» [8].

Цель любой эскалации привилегий – это получение токена доступа, который создается привилегированными пользователями [9]. В общем случае, в ОС Windows это стандартные пользователи, которые называются: “Administrator” и “System”. Именно их токены открывают двери к любой информации, которая есть в операционной системе [10].

С помощью, описанной выше уязвимостей был проведен ряд известных и официально задокументированных атак. В Telegram-канале (https://t.me/cybersecs), курируемом Владиславом Хорохориным, опубликована информация о разработке нового программного обеспечения (ПО) для создания помех самолетам и радиолокационному оборудованию, применяемому в специальной военной операции на территории Украины. Сообщается, что указанное ПО использует технологию SDR (программно-определяемые радиосистемы, Software-defined radio) и предназначено для создания радиопомех путем имитации активности ПВО или радиосвязи [11].

В Telegram-канале (https://t.me/cybersecs), курируемом Владиславом Хорохориным, также была опубликована информация о взломе официального Интернет-портала правовой информации (http://pravo.gov.ru/), а также Telegram-канала указанного Интернет-портала (@pravo_govru). В результате взлома на главной странице сайта был размещен баннер хакерской группировки Cyber.Anarchy.Squad и DumpForums, а в телеграм-канале опубликована противоправная информация, дискредитирующая действия российских вооруженных сил [12].

В Telegram-канале (https://t.me/itarmyofukraine2022) с начала дня 8 августа 2022 года продолжается координация DDoS-атак на различные сайты и ресурсы России. В качестве целей приводятся несколько Интернет-ресурсов [13]:

- https://conf.corpmsp.ru; 185.11.196.100 (443/tcp);
- https://fas2.tconf.rt.ru; 195.19.97.107 (443/tcp);
- https://fas1.tconf.rt.ru; 195.19.96.223 (443/tcp);
- https://fas3.tconf.rt.ru; 195.19.96.191 (443/tcp);
- https://fas4.tconf.rt.ru; 195.19.97.6 (443/tcp).

Эксплуатирования данных уязвимостей может привести к нарушению конфиденциальности информации, расположенной в различных информационных ресурсах [14]. К примеру, в социальной сети Twitter (*https://twitter.com/youranontv*) опубликована информация о наличии в открытом доступе базы данных российских пользователей и компаний, работающих в Великобритании. Файл содержит 14 тыс. строк, включающих: фамилию, имя, дату рождения, адрес проживания, наименование организации, место расположения организации [15].

В социальной сети Twitter (*https://twitter.com/anon_nekas*) опубликована информация о наличии в открытом доступе базы данных электронных

писем правительства Саратовской области. Файл содержит более 2,8 тыс. электронных писем [16].

В социальной сети Twitter (https://twitter.com/anonymoush1span) опубликована информация о наличии в открытом доступе документов группы компаний «СКАНЭКС» (г. Москва), занимающейся разработкой, производством и внедрением технологий для приема, обработки и хранения спутниковых снимков. Архив, размером 11 Гб, содержит различные документы компании [17].

В Telegram-канале (*https://t.me/data1eaks*) опубликована информация о наличии в открытом доступе второй части общей базы данных клиентов компании «Oriflame». Файл содержит 5,5 млн строк, включающих: Ф.И.О., пол, дата рождения, адрес эл. почты, номер телефона, адрес проживания [18].

В качестве мер противодействия данной уязвимости можно привести ограничение доступа пользователей к функциям «Удалить все служебные данные и отчеты» или «Сохранить отчет на вашем компьютере». Так же необходимо обновить Kaspersky VPN Secure Connection до 21.6 или более поздней версии.

Важно отметить, что сами по себе уязвимости информационной безопасности не опасны. Они лишь открывают возможности для осуществления угроз ИБ. К наиболее распространенным причинам возникновения уязвимостей, как правило, относят: ошибки при проектировании и использовании программного обеспечения; несанкционированное внедрение и последующее использование ПО; внедрение вредоносного ПО; человеческий фактор. Своевременное реагирование на появление определенных уязвимостей и следование рекомендациям по их устранению способствуют поддержанию общего уровня информационной безопасности на должном уровне.

Список используемых источников

1. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. N 10. С. 36–40.

2. Щеглов А. Ю., Щеглов К. А. Математические модели и методы формального проектирования системы защиты информационных систем: учеб. пособие. СПб. : Университет ИТМО, 2015. 93 с.

3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика и информационная безопасность : Сборник трудов межрегиональной конференции и Санкт-Петербургской международной конференции, Санкт-Петербург, 24–26 октября 2018 года. Вып. 6. СПб. : Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2018. С. 236–240.

4. Волкогонов В. Н., Гельфанд А. М., Пестов И. Е., Поляничева А. В. Программное обеспечение мониторинга сети организации на основе системы zabbix // Свидетельство о регистрации программы для ЭВМ 2020617706, 10.07.2020. Заявка № 2020616735 от 29.06.2020.

5. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференция : сб. науч. тр. в 4-х т. СПб. : СПбГУТ, 2019. С. 329–334.

6. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. N 3 (88). С. 38–46.

7. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. N 1. С. 47–58.

8. Красов А. В., Левин М. В., Фостач Е. С. Проблемы обеспечения безопасности облачных вычислений // Информационная безопасность регионов России (ИБРР-2017) : Материалы конференции, Санкт-Петербург, 01–03 ноября 2017 года. СПб. : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 520–522.

9. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 3. С. 26–32.

10. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. N 1. С. 70–76.

11. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. N 11. С. 39–47.

12. Виткова Л. А., Иванов А. И., Сергеева И. Ю. Исследование и разработка методик оценки рисков облачных ресурсов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 1. С. 152–155.

13. Виткова Л. А., Глущенко А. А., Сахаров Д. В., Чмутов М. В. Выбор оптимального метода оценки эффективности перехода к облачной архитектуре // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 168–171.

14. Виткова Л. А., Иванов А. И. Обзор актуальных угроз и методов защиты в сфере облачных вычислений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 179–182.

15. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации // Инновационные технологии, экономика и менеджмент в промышленности. сборник научных статей по итогам XII международной научной конференции. НПП Медпромдеталь. Волгоград, 2021. С. 203–204.

16. Миняев А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 1. С. 29–33.

17. Пестов И. Е., Кошелева С. А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества : сборник научных статей по итогам круглого стола со всероссийским и международным участием, Москва, 15–16 декабря 2021 года. N 8. Москва : Общество с ограниченной ответственностью «КОНВЕРТ», 2021. С. 113–115.

18. Пестов И. Е., Алехин Р. В., Руденко С. А., Федоров П. О. Исследование воздействия DDoS-атаки на виртуальную машину при наличии и отсутствии технологии firewall // Теория и практика обеспечения информационной безопасности : сборник научных трудов по материалам всероссийской научно-теоретической конференции, Москва, 03 декабря 2021 года. Москва: Московский технический университет связи и информатики, 2021. С. 263–269.

19. Пестов И. Е. Методика противодействия угрозам нарушения информационной безопасности инстансов и облачной инфраструктуры, основан на описании атак и методов противодействия им, используя теории графов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция : сб. науч. тр. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 742–746.

УДК 004.56
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОС ДЛЯ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ

Р. К. Коломийцев, Р. Б. Петрив

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Тестирование безопасности направлено на выявление недостатков в информационных системах, и может производиться в удаленных и малообслуживаемых сегментах сетей с использованием программно-аппаратных зондов, в качестве программного обеспечения которых используются специализированные операционные системы с открытым исходным кодом. В работе проведен анализ операционных систем, описаны их достоинства и недостатки.

тестирование безопасности, операционные системы, программно-аппаратный зонд, одноплатные платформы.

Использование сборок ОС Linux для криминалистики и тестирования безопасности содержат в своем составе и могут быть дополнены специализированными программными инструментами, которые позволяют обнаружить потенциально слабые места в ИТ-инфраструктуре и принять адекватные меры по укреплению периферии сети.

Проведение сравнительного анализа различных специализированных систем на базе Linux позволит определить их эффективность и удобство для тестирования безопасности, в том числе:

- определение сильных и слабых сторон различных операционных систем на базе Linux в отношении функций и инструментов безопасности;
- выбор подходящей ОС на базе Linux для тестирования безопасности в зависимости от конкретных потребностей организации или клиента;
- помощь организациям или клиентам в принятии обоснованных решений об использовании наиболее безопасной ОС в их ИТ-инфраструктуре;
- создания программно-аппаратных зондов для тестирования и мониторинга безопасности сетевой инфраструктуры.

Kali Linux – одна из самых популярных операционных систем на базе Linux, предназначенная для тестирования безопасности [1].

Достоинства:

- наличие подробной документации и технической поддержки со стороны разработчиков;
- широкий спектр инструментов для анализа сети, эксплуатации и взлома паролей;
- регулярные обновления и исправления для устранения уязвимостей в системе безопасности;
- Kali может быть легко установлен на различных платформах.

Однако имеется несколько недостатков:

- может быть непросто настроить для конкретных нужд;
- могут быть сложности с запуском некоторых приложений на слабых машинах;
- популярность делает его мишенью для злоумышленников, которые знают о его уязвимостях (в частности, программно-аппаратных зондов на его основе).

Parrot Security OS – также основан на Debian и предоставляет широкий спектр инструментов безопасности для тестирования на проникновение, цифровой криминалистики и оценки уязвимостей [2].

Достоинства:

- настраиваемый и простой в использовании. Удобен для пользователей, которые привыкли работать с графическим интерфейсом;
- защищен по умолчанию с помощью целого ряда функций и инструментов безопасности (I2P, Tor, криминалистический режим (не монтирует

какие-либо системные жесткие диски или разделы и не влияет на хост-систему, что делает его более скрытым, чем в обычном режиме);

- регулярно обновляется и исправляется с целью устранения уязвимостей в системе безопасности.

Недостатки:

- ограниченная поддержка некоторых аппаратных средств и программного обеспечения. Отсутствует 32-х битная версия;
- меньшее сообщество пользователей по сравнению с другими операционными системами на базе Linux;
- может не подойти для начинающих, так как требует определенного уровня технических знаний.

BackBox – это дистрибутив Linux на базе Ubuntu, который поставляется с предустановленным набором инструментов безопасности [3].

Достоинства:

- удобный интерфейс с чистым и современным дизайном;
- широкий спектр инструментов безопасности для тестирования на проникновение, сетевого анализа и цифровой криминалистики;
- регулярные обновления и исправления для устранения уязвимостей в системе безопасности.

Недостатки:

- имеются проблемы совместимости с рядом приложений для безопасности, прежде всего сканерами уязвимостей;
- не имеет такого же уровня поддержки сообщества и разработки, как другие операционные системы на базе Linux;
- не такая настраиваемая и модульная, как другие операционные системы на базе Linux, что ограничивает ее пригодность для более продвинутого тестирования безопасности. Могут потребоваться дополнительные настройки для оптимизации под конкретные потребности тестирования безопасности.

BlackArch Linux – поставляется с более чем 2000 предустановленными средствами безопасности [4].

Достоинства:

- широкий спектр инструментов безопасности для сетевого анализа, тестирования веб-приложений и эксплуатации;
- большое и активное сообщество пользователей для поддержки и развития;
- регулярные обновления и исправления, применяемые для устранения уязвимостей в системе безопасности.

Недостатки:

- ограниченная поддержка некоторых аппаратных средств и программного обеспечения;

- не подходит для начинающих, так как требует определенного уровня технических знаний – большая часть работы проводится в терминале;
- более удобен для запуска с внешнего носителя.

В таблице 1 приведен сравнительный анализ операционных систем. По итогам проделанной работы было выявлено:

- все ОС с открытым кодом;
- все ОС без гарантии, не всегда полная поддержка, но наибольшая база знаний по использованию у Kali;
- все ОС можно собрать самостоятельно, но некоторые инструменты для сборки уже могут оказаться недоступны;
- у Kali на текущий момент наибольшая поддержка одноплатных вычислительных платформ.

ТАБЛИЦА 1. Сводная таблица операционных систем

Название	Платформы	Основан	Графическая оболочка	Год выпуска	Последнее обновление
Kali Linux	x64, x86, ARM, Rasp Pi	Debian	Xfce, KDE, GNOME	2013	2022.4 (06.12.2022)
Parrot OS	x64, ARM, Rasp Pi	Debian	MATE, KDE, Xfce	2013	5.2 (15.02.2023)
BackBox	x64	Ubuntu	Xfce	2010	8 (15.11.2022)
BlackArch	x64	Arch Linux	Xfce	2012	2021.09.01 (16.07.2021)

Из проведенного анализа можно сделать выводы:

- В разработке прототипов программно-аппаратных зондов для тестирования безопасности, в зависимости от задачи и функционала, могут быть использованы сборки на основе всех рассмотренных ОС. Однако, принимая во внимание цель создания серийных и тиражируемых устройств, необходимо ставить задачу сбора специализированных дистрибутивов на основе отечественных систем, у которых есть поддержка и соответствующая сертификация.
- Необходимо обеспечивать поддержку, адаптировать, разрабатывать новые средства тестирования безопасности по аналогии с имеющимися.

Из вышесказанного не стоит делать вывод, что нужно немедленно делать выбор в пользу одной из имеющихся или новых ОС. Важно иметь возможность построения отечественного аналога и также подобных ключевых инструментов, как например Metasploit. Все рассмотренные ОС, опыт их разработки и использования стоит изучать, чтобы применять их для решения стратегических задач создания отечественных продуктов.

Список используемых источников

1. Gururaj H. L. et al. Analysis of Cyber Security Attacks using Kali Linux //2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE, 2022. PP. 1–6.

2. ul Hassan S. Z., Muzaffar Z., Ahmad S. Z. Operating Systems for Ethical Hackers-A Platform Comparison of Kali Linux and Parrot OS // International Journal. 2021. Vol. 10. N 3.

3. Uygur S. U. Penetration testing with BackBox. Packt Publishing Ltd, 2014.

4. Толкачева Е. В., Муромцев А. С. Сравнительный анализ инструментов расследования инцидентов информационной безопасности в составе операционных систем Kali Linux и Arch Linux // Архитектурно-строительный и дорожно-транспортный комплексы: проблемы, перспективы, инновации. 2021. С. 803–807.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.55
ГРНТИ 28.21.19

ИССЛЕДОВАНИЕ АТАКИ НА ЧИСЛОВОЙ ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ОСНОВЕ МАЖОРИТАРНОЙ ОБРАБОТКИ БИТ СЫРОГО КЛЮЧА, ПЕРЕХВАТЫВАЕМЫХ НАРУШИТЕЛЕМ

В. И. Коржик, А. С. Лапшин, Д. А. Разумов, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается числовой протокол распределения ключа между двумя пользователями, соединенными каналом с постоянными параметрами, состоящим и протокола формирования бит сырого ключа и протокола преимущественного улучшения основного канала с двумя итерациями. Исследуется атака на протокол, заключающаяся в том, что нарушитель не использует двухэтапное декодирование передаваемых блоков, а применяет одноэтапное мажоритарное декодирование бит сырого ключа, перехваченных в течение двух итераций протокола ПУОК. На основе моделирования найдены вероятности ошибки ключевой последовательности у легального пользователя и нарушителя. Проведены оценки сложности реализации такой атаки.

криптография, распределение ключей, нарушитель.

В работах [1, 2, 3, 4] приведено описание протокола распределения ключа по постоянным каналам и получены оценки его эффективности.

В настоящей работе исследуется атака на протокол, которая при определенных обстоятельствах может привести к существенному снижению его эффективности.

Протокол включает в себя несколько подпротоколов [3, 4]:

- Протокол формирования сырого ключа;
- Протокол преимущественного улучшения основного канала (ПУОК) (2 итерации):
- Протокол ухудшения двух каналов (УДК) (v итераций);
- Процедура повышения достоверности формируемого ключа путем помехоустойчивого кодирования;
- Процедура усиления секретности.

В любом протоколе формирования ключа между двумя пользователями A и B в присутствии нарушителя E обычно рассматривают два канала:

- основной канал от *A* к *B*, назовем его основным каналом и обозначим вероятность ошибки в нем – p_m;
- отводной канал или канал перехвата от корр. *A* к нарушителю *E* с вероятностью ошибки в нем p_e.

Как было показано ранее [5], последние две процедуры будут успешными, если в основном и отводном каналах будет выполнены условие

$$p_m < p_e . \quad (1)$$

Рассмотрим далее протокол, в котором достигается выполнение этого условия.

В обмене участвуют два пользователя (*A* и *B)*, связанные бесшумным каналом связи с постоянными параметрами типа Интернет (рис. 1). Каждый из пользователей генерирует случайные независимые двоичные последовательности γ_A и γ_B с вероятностями: $P\{\gamma_A = 0\} = P\{\gamma_B = 0\} = 1 - p$, $P\{\gamma_A = 1\} = P\{\gamma_B = 1\} = p$.

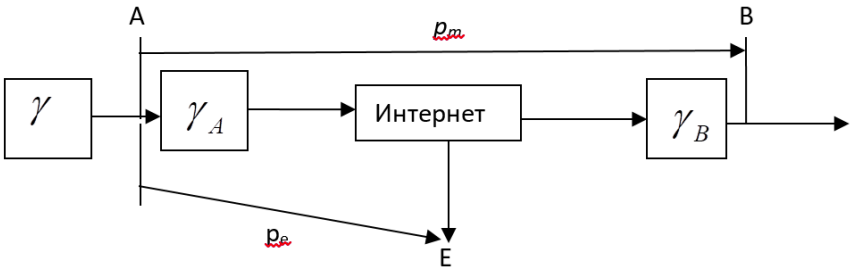


Рис. 1. Общая схема выполнения протокола

Пользователь *A* передает случайную последовательность $\bar{\gamma}$: $P\{\gamma = 0\} = P\{\gamma = 1\} = 1/2$ по каналу. Пользователь B получает последовательность символов $\tilde{\gamma} = \gamma \oplus \gamma_A \oplus \gamma_B$. Нарушитель E подключен к Интернет и перехватывает последовательность бит $\hat{\gamma} = \gamma \oplus \gamma_A$.

Не сложно показать, что вероятности ошибок p_m *и* p_e в каналах A→B и A→E равны

$$p_m = 2(1-p)p\,,\ \ p_e = p\,. \qquad (2)$$

Вероятности ошибки переданного γ бита у легального пользователя и нарушителя показаны в (табл. 1, колонки 2 и 3).

Как видно, последовательность бит $\hat{\gamma}$ у нарушителя имеет меньшую вероятность ошибки, чем у легального пользователя, поэтому необходимо использование дополнительных протоколов, обеспечивающих выполнение соотношения (1). Таким протоколом является протокол преимущественного улучшения основного канала (ПУОК)

Данный итеративный протокол выполняется посредством преобразований, представленных на рис. 2.

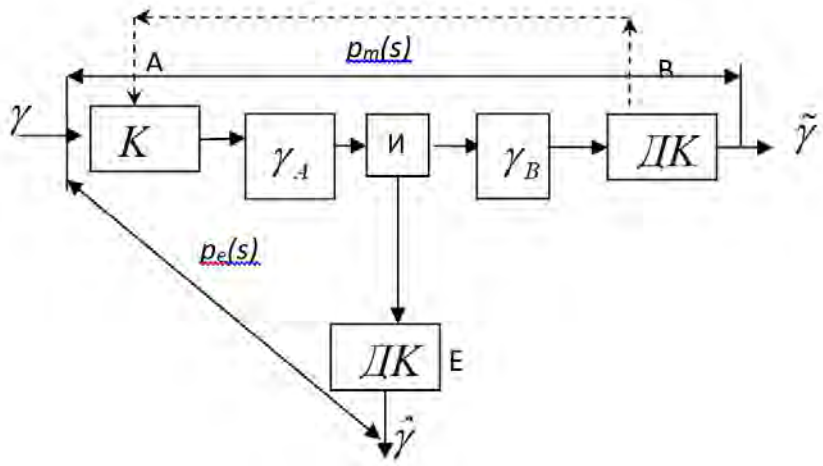


Рис. 2. Схема выполнения ПУОК (К – кодер, ДК – декодер)

По каналу A→B передаются случайные биты γ, которые на передаче кодируются (s,1)-кодом повторения, а на приеме в точках B и E декодируются, в результате получаются биты $\tilde{\gamma}$ и $\hat{\gamma}$ (рис. 2). Декодирование в B осуществляется по правилу: блок принимается и декодируется, если состоит из всех нулей или из всех единиц (другие блоки стираются). E декодирует блок который не стерли A и B мажоритарно. Доказательство оптимальности такого декодирования приведено в [3].

Обозначим:

$p_m(s)$ – вероятность ошибки ($\tilde{\gamma} \oplus \gamma = 1$) в канале A→B после применения кодирования;

$p_e(s)$ – вероятность ошибки ($\hat{\gamma} \oplus \gamma = 1$) в канале A→E после применения кодирования;

$p1_{\alpha\beta}$ – вероятности совместных событий ($\alpha = \hat{\gamma} \oplus \gamma,\ \beta = \tilde{\gamma} \oplus \gamma$), в каналах A→E и A→B после применения кодирования. $\alpha = 0(1)$ – отсутствие (наличие) ошибки декодирования у E, $\beta = 0(1)$ – отсутствие (наличие) ошибки декодирования у B.

Получены следующие формулы для вероятностей ошибок в каналах в каналах A→E и A→B с применением кодирования (для нечетного s) [4].

$$p1_m(s) = p1_{01} + p1_{11},\quad p1_e(s) = p1_{10} + p1_{11} \tag{3}$$

$$p1_{00} = \sum_{i=0}^{\lfloor s/2 \rfloor} C_s^i (1-p)^{2(s-i)} (p)^{2i} / P_{acc},\qquad p1_{10} = \sum_{i=\lceil s/2 \rceil}^{s} C_s^i p^{2i} (1-p)^{2(s-i)} / P_{acc},$$

$$p1_{01} = p1_{11} = \frac{2^{s-1}(p(1-p))^s}{P_{acc}},$$

$P_{acc} = p_m^s + (1-p_m)^s$ – вероятность приема блока из s нулей или из s единиц.

Можно строго показать, что ни при каком p и ни при каком s нельзя получить выполнение условия $p_m < p_e$.

Применим протокол ПУОК еще раз (рис. 3).

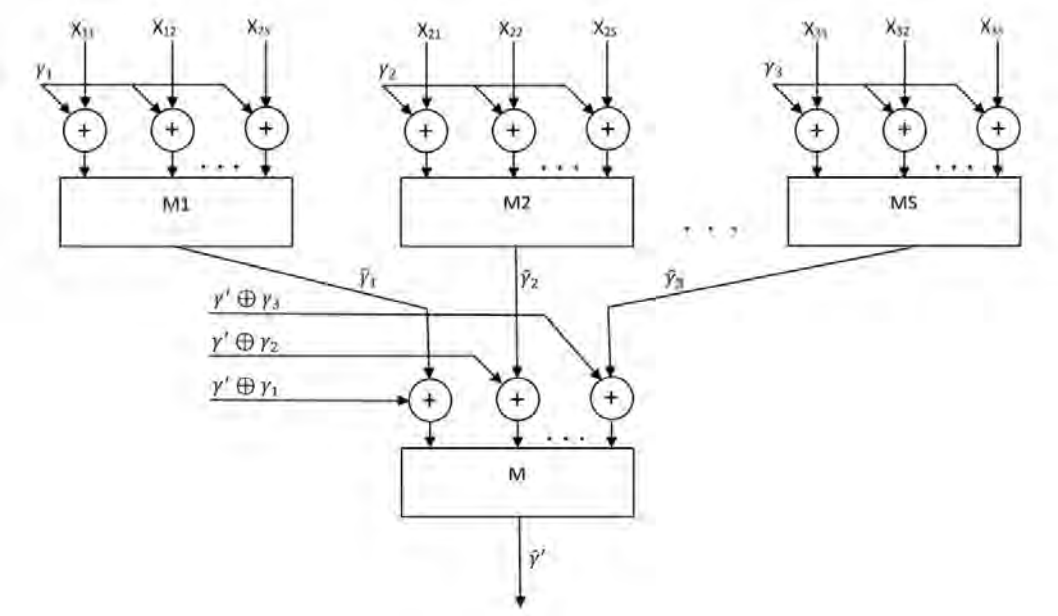


Рис. 3. Схема выполнения двухступенчатого протокола ПУОК

В этом случае в протоколе ПУОК первой ступени используем s мажоритарных декодеров, на каждый из которых поступают биты $\gamma_i \oplus \mathrm{x_{i1}}, \gamma_i \oplus \mathrm{x_{i2}}, \ldots, \gamma_i \oplus \mathrm{x_{is}}$, i = 1,2,…,s, где i – номер декодера. На выходах мажоритарных декодеров получаем биты $\widehat{\gamma_1}, \widehat{\gamma_2}, \ldots, \widehat{\gamma_s}$. Эти биты суммируются с блоками, поступающими от кодера второй ступени $\bar{u} = \gamma' \oplus \gamma_1,\ \gamma' \oplus \gamma_2, \ldots, \gamma' \oplus \gamma_s$, где $\gamma' = (0,1),\ p(\gamma') = 0.5$. После суммирования получаем

блок $\gamma' \oplus \gamma_1 \oplus \hat{\gamma}_1, \gamma' \oplus \gamma_2 \oplus \hat{\gamma}_2, \ldots, \gamma' \oplus \gamma_s \oplus \hat{\gamma}_s$, который подается на мажоритарный декодер второй ступени. На выходе декодер получаем бит $\hat{\gamma}'$.

Для второй итерации ПУОК получены соотношения:

$$p2_m(s) = p2_{01} + p2_{11}, \quad p2_e(s) = p2_{10} + p2_{11}, \tag{4}$$

где $p2_{\alpha\beta}$ – вероятности совместных событий ($\alpha = \hat{\gamma} \oplus \gamma,\ \beta = \tilde{\gamma} \oplus \gamma$), в каналах A→E и A→B после применения кодирования. $\alpha = 0(1)$ – отсутствие (наличие) ошибки декодирования у E, $\beta = 0(1)$ – отсутствие (наличие) ошибки декодирования у B. (Индекс 2 – вторая итерация ПУОК).

Для нечетного s выражения для вероятностей совместных событий после второй итерации ПУОК имеют вид

$$p2_{00} = \sum_{i=0}^{\lfloor s/2 \rfloor} C_s^i p1_{00}^{s-i} p1_{10}^i / P2_{acc}, \qquad p2_{10} = \sum_{i=\lceil s/2 \rceil}^{s} C_s^i p1_{10}^i p1_{00}^{s-i} / P2_{acc},$$

$$p2_{01} = \sum_{i=0}^{\lfloor s/2 \rfloor} C_s^i p1_{01}^{s-i} p1_{11}^i / P2_{acc}, \qquad p2_{11} = \sum_{i=\lceil s/2 \rceil}^{s} C_s^i p1_{11}^i p1_{01}^{s-i} / P2_{acc},$$

$P2_{acc} = p1_m^s(s) + (1 - p1_m(s))^s$ – вероятность приема блока из s нулей или из s единиц во второй итерации.

В таблице 1 приведены вероятности ошибки в приеме бита ключа у легального пользователя и нарушителя после первой и второй итерации при s = 3.

Как видим из таблицы, после второй итерации протокола ПУОК, достигается условие (1). И, следовательно, могут быть далее реализованы процедуры кодирования и усиления секретности,

Рассмотрим далее следующую атаку нарушителя (рис. 3).

Нарушитель наблюдает s блоков, передаваемых от A к B в ходе первой итерации ПУОК: $\gamma_i \oplus x_{i1}, \gamma_i \oplus x_{i2}, \ldots, \gamma_i \oplus x_{is}$, i = 1,2,…,s. Получает блок $\bar{u} = \gamma' \oplus \gamma_1, \gamma' \oplus \gamma_2, \ldots, \gamma' \oplus \gamma_s$, передаваемый от A к B во второй итерации, дублирует s раз каждый бит этого блока и суммирует полученные биты с битами, перехваченными при приеме первой итерации: ПУОК . В итоге получает:

$$\begin{array}{l} \gamma' \oplus \gamma_1, \gamma' \oplus \gamma_1, \ldots, \gamma' \oplus \gamma_1 \quad \gamma' \oplus \gamma_2, \gamma' \oplus \gamma_2, \ldots, \gamma' \oplus \gamma_2 \cdots \gamma' \oplus \gamma_s, \gamma' \oplus \gamma_s, \ldots, \gamma' \oplus \gamma_s \\ \oplus \\ \gamma_1 \oplus x_{11}, \gamma_1 \oplus x_{12}, \ldots, \gamma_1 \oplus x_{1s}, \gamma_2 \oplus x_{21}, \gamma_2 \oplus x_{22}, \ldots, \gamma_2 \oplus x_{2s} \cdots \gamma_s \oplus x_{s1}, \gamma_s \oplus x_{s2}, \ldots, \gamma_s \oplus x_{ss} \\ \hline \gamma' \oplus x_{11}, \gamma' \oplus x_{12}, \ldots, \gamma' \oplus x_{1s}, \quad \gamma' \oplus x_{21}, \gamma' \oplus x_{22}, \ldots, \gamma' \oplus x_{2s} \cdots \gamma' \oplus x_{s1}, \gamma' \oplus x_{s2}, \ldots, \gamma' \oplus x_{ss} \end{array}$$

Видим, что полученный блок соответствует блоку (s^2,1)-кода и может быть декодирован мажоритарно. Таким образом, нарушитель может не проводить двухэтапное декодирование s блоков по s бит каждый, а сразу выполнить декодирование блока длиной s^2 бит, что соответствует одноэтап-

ному мажоритарному декодированию. Но поскольку одноэтапное декодирование не может обеспечить выполнение условия (1), атака достигает цели. В таблице 1 показаны вероятности $p_m(s^2 = 9)$ и $p_e(s^2 = 9)$, что подтверждает сделанный выше вывод.

ТАБЛИЦА 1. Вероятности ошибок для легального пользователя и нарушителя при выполнении двухэтапного протокола ПУОК при s = 3 и одноэтапного ПУОК при s = 9

Вероятности ошибок протокола ФСК			ПУОК1 (s =3)		ПУОК 2 (s = 3)		ПУОК 1 (s = 9)	
P	p_m	p_e	p_m	p_e	p_m	p_e	p_m	p_e
0.05	0.095	0.05	$1.155\cdot10^{-3}$	$6.005\cdot10^{-3}$	$1.548\cdot10^{-9}$	$2.340\cdot10^{-9}$	$1.548\cdot10^{-9}$	$7.939\cdot10^{-10}$
0.1	0.18	0.1	0.010	$5.671\cdot10^{-3}$	$1.183\cdot10^{-6}$	$1.179\cdot10^{-6}$	$1.183\cdot10^{-6}$	$6.243\cdot10^{-7}$
0.15	0.255	0.15	0.039	0.022	$6.448\cdot10^{-5}$	$5.377\cdot10^{-5}$	$6.448\cdot10^{-5}$	$3.510\cdot10^{-5}$
0.2	0.32	0.2	0.094	0.056	$1.131\cdot10^{-3}$	$8.614\cdot10^{-4}$	$1.131\cdot10^{-3}$	$6.378\cdot10^{-4}$
0.25	0.375	0.25	0.178	0.112	$9.977\cdot10^{-3}$	$7.274\cdot10^{-3}$	$9.977\cdot10^{-3}$	$5.871\cdot10^{-3}$
0.3	0.42	0.3	0.275	0.185	0.052	0.037	0.052	0.032
0.35	0.455	0.35	0.368	0.265	0.165	0.120	0.165	0.109
0.4	0.48	0.4	0.440	0.346	0.327	0.251	0.327	0.237
0.45	0.495	0.45	0.485	0.425	0.445	0.384	0.445	0.374

Список используемых источников

1. Korzhik V., Starostin V., Yakovlev V., Kabardov M., Gerasimovich A., Zhuvikin A. Information Theoretically Secure Key Sharing Protocol Executing with Constant Noiseless Public Channels // Mathematical problems of cryptography. 2021. Vol. 12, N 3. PP. 31–47.

2. Yakovlev V., Korzhik V., Akhmetsina M., Zhuvikin A. Key Sharing Protocol Using Exchange by Integers over Public Noiseless Channels Between Users that Provides Security executing without Cryptographic Assumption // The 31th Conference of Open Innovations Association FRUCT, Helsinki Finland, 27-29 April 2022. PP. 363–379.

3. Yakovlev V., Korzhik V., Starostin V., Lapshin A., Zhuvikin A. Channel Traffic Minimizing Key Sharing Protocol Intended for the Use over the Internet and Secure without any Cryptographic Assumptions // Proceedings of the 32st Conference of Open Innovation Association, FRUCT, 2022. 2022 November, Vol. 32, PP. 300–307.

4. Яковлев В. А., Коржик В. И. Протокол распределения ключей по постоянным каналам на основе совместного применения неинтерактивных протоколов обмена данными // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 2. С. 604–608.

5. Yakovlev V., Korzhik V., Morales-Luna G. Key distribution protocols based on noisy channels in presence of an active adversary // Conventional and new versions with parameter optimization". IEEE Transactions on Information Theory. 2008. Vol. 54. N. 6. PP. 2535–2549.

УДК 004.056.53
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ ОСНОВНЫХ АСПЕКТОВ, НЕОБХОДИМЫХ ПРИ СОЗДАНИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Н. А. Косов, И. И. Петров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье представлены и охарактеризованы важные моменты разработки политики информационной безопасности, рассмотрены простейшие способы повышения эффективности защиты предприятий и действия злоумышленников, которые могут привести к краху предприятия. Особое внимание уделено политикам, неотъемлемо связанными с политикой информационной безопасности и затронуты изменения в две тысячи двадцать втором году.

информационная безопасность, политика информационной безопасности на предприятии, политика полномочий, политика контроля доступа, иерархическая структура.

В эпоху информационных технологий формулировка термина информационной безопасности стала весьма расплывчата. Так, на данный момент информационная безопасность представляет собой комплекс мер, оборудования и/или программного обеспечения, которые защищают конфиденциальность, целостность и доступность данных. Другими словами, это практика защиты конфиденциальной информации.

Политика информационной безопасности (далее политика ИБ) обеспечивает целостность, доступность, защиту и конфиденциальность данных, так же сводит к минимуму риск инцидентов безопасности

Стоит отметить, что политики ИБ, (на предприятии может быть несколько. Например, политики разных отделов и т. п.,) обобщают состояние безопасности организации и объясняют, как организация защищает информационные ресурсы и активы. Они способствуют быстрому реагированию на запросы третьих сторон о предоставлении информации со стороны клиентов, партнеров и аудиторов [1].

Политика безопасности может быть настолько широкой, насколько её разработчик захочет. Всё, что связано с информационной безопасностью и безопасностью связанных с ней физических активов, подлежащими исполнению в полном объеме.

Как и в любых других отраслях, перед разработкой политики информационной безопасности нужно подготовиться [2]. Для начала необходимо

провести оценку индивидуального отношения к рискам компании её владельцев и менеджеров. Затем исследовать всевозможные вероятные уязвимости, сюда входят как относящиеся к персоналу, так и к технике или объектам. Когда обнаружение опасностей дало результат, нужно провести оценку соответствующих рисков.

Первый этап при создании политики ИБ – это цель. Она может включать в себя: создание общего подхода к ИБ, обнаружение и предотвращение нарушения ИБ (неправильное использование сетей, данных, приложений и компьютерных систем) [3]. Так же следует поддерживать репутацию организации и соблюдение этических и юридических обязанностей и, самое главное, нужно уважать права клиентов, в том числе то, как реагировать на запросы и жалобы о несоблюдении. Так же необходимо указать какие аудитории выходят за рамки политики (например, сотрудники другого бизнесподразделения, которые отдельно управляют безопасностью, могут не входить в сферу действия политики).

Не стоит забывать и о политике полномочий и контроля доступа.

В иерархической структуре старший менеджер может быть наделен полномочиями решать, какими данными можно делиться и с кем. Политика безопасности может содержать разные термины для старшего менеджера и младшего сотрудника. В политике должен быть указан уровень полномочий над данными и информационными системами для каждой организационной роли.

С помощью политики сетевой безопасности, компания/предприятие или иная структура может предоставлять пользователям доступ к своим сетям и серверам только через уникальные логины, которые требуют аутентификации, такие как: пароли, биометрические данные, идентификационные карты и другое. Организация должна отслеживать все свои системы и записывать все попытки входа в систему.

Для обеспечения должного уровня безопасности и для удобства использования политика ИБ должна классифицировать данные по категориям, которые могут включать «совершенно секретно», «секретно», «конфиденциально» и «общедоступно». При классификации данных политика ИБ должна гарантировать, что конфиденциальные данные не могут быть доступны лицам с более низким уровнем допуска, должна защитить важные данные и помочь избежать ненужных мер безопасности для менее важных данных.

Распространение политики ИБ среди сотрудников, проведение учебных занятий/семинаров – всё это необходимо для того, чтобы проинформировать сотрудников о процедурах и механизмах безопасности, включая меры защиты данных, меры защиты доступа и классификацию конфиденциальных данных.

Злоумышленником может стать каждый, даже непреднамеренно, поэтому следует уделить особое внимание атакам с помощью социальной инженерии, политике чистого рабочего стола, политике приемлемого использования Интернета, в том числе и его ограничение, защите компьютеров с помощью блокировки, уничтожению документов, которые больше не нужны предприятию.

Определив минимальные стандарты, применимые к выбранному программному обеспечению для шифрования, необходимо составить политику шифрования и политику резервного копирования данных, которая определяет правила и процедуры создания резервных копий данных. Это неотъемлемый компонент общей стратегии защиты данных, обеспечения непрерывности бизнеса и аварийного восстановления.

Следует назначить персонал для проведения проверок доступа пользователей, обучения, управления изменениями, управления инцидентами, внедрения и периодических обновлений политики безопасности. Их обязанности должны быть определены как часть политики безопасности на предприятии.

Неправильная классификация информации и данных может нарушить программу безопасности. Так же необходимо создать план реагирования на инциденты безопасности, он поможет вовремя инициировать соответствующие действия по исправлению ситуации во время инцидентов безопасности.

Российские индивидуальные предприниматели и юридические лица, которые на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, работающие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а так же российские юридические лица и индивидуальные предприниматели, которые обеспечивают взаимодействие вышеуказанных сетей или систем должны принять во внимание изменения в ГОСТ по ИБ и АС в 2022 году, которые затронули и системы менеджмента ИБ.

С 01.01.2022 взамен ГОСТ Р ИСО/МЭК 27001-2006 вступила в силу обновлённая редакция одного из основополагающих стандартов в области риск-ориентированного управления информационной безопасностью – ГОСТ Р ИСО/МЭК 27001-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», утвержденный Приказом Росстандарта № 1653-ст от 30.11.2021 [4].

Было установлено, что с 1 января 2025 года вступив в силу запрет на использование средств защиты информации, произведённых в недружественных странах либо производители которых находятся под юрисдикцией таких государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Простейшие способы повышения эффективности защиты предприятий:

– Перевоспитать сотрудников в отношении фишинга и спама.

Сложные атаки по электронной почте часто могут быть неотличимы от реальных электронных писем.

– Ограничить раскрытие конфиденциальной информации.

Необходимо заблокировать все секретные или ключевые корпоративные данные. Никогда не поздно оценить или усилить дополнительными уровнями аутентификации отдельные элементы относящиеся к безопасности предприятия.

– Повторить проверку средств контроля безопасности.

Предприятия должны оценить риски для критически важных активов, а затем выбрать подходящие средства контроля безопасности для внедрения. Это могут быть физические средства контроля, такие как обнаружение и предотвращение несанкционированного доступа к физическим объектам, системам или активам, или логические средства контроля, такие как наличие средств контроля безопасности на брандмауэрах и многое другое.

Действия злоумышленников, которые могут привести к краху предприятия:

– Разведка.

На этапе разведки злоумышленник собирает информацию о целевой организации. Они могут использовать автоматические сканеры для поиска уязвимостей и слабых мест, которые могут быть взломаны.

– Вторжение.

На этапе вторжения злоумышленники пытаются проникнуть внутрь периметра безопасности. Злоумышленники обычно внедряют вредоносное ПО в систему, чтобы закрепиться.

– Эксплуатация.

На этапе эксплуатации злоумышленники ищут дополнительные уязвимости или слабые места, которые они могут использовать в системах организации.

– Повышение привилегий.

На этапе повышения привилегий целью злоумышленника является получение привилегий для дополнительных систем или учетных записей.

– Боковое перемещение.

На этапе бокового перемещения злоумышленники подключаются к дополнительным системам и пытаются найти наиболее ценные активы организации.

– Запутывание.

На этапе запутывания злоумышленник пытается замести свои следы.

– Отказ в обслуживании.

На этапе отказа в обслуживании (DoS) злоумышленники пытаются нарушить работу организации. Обычно цель состоит в том, чтобы отвлечь сотрудников службы безопасности и оперативного персонала, позволяя злоумышленникам достичь своей реальной цели, которая заключается в извлечении данных.

– Эксфильтрация.

На этапе эксфильтрации продвинутый злоумышленник, наконец, попадает в цель, получая в свои руки наиболее конфиденциальные данные организации.

В заключение хотелось бы сказать, что системная работа в области информационной безопасности требует внимания не только специальных подразделений, но и финансовых, и бухгалтерских служб, руководства компании. Все сотрудники, которые лично заинтересованы в успешности её реализации, должны быть вовремя уведомлены о целях и задачах. Такая система как система мотивации призвана помочь с успешным внедрением политики информационной безопасности. Вследствие этой системы, в процесс оказываются вовлечёнными почти все части компании. Её отрасли должны быть заинтересованы в исполнении предписаний.

В условиях крупной компании поставленная задача становится трудновыполнимой. Стоит обратить внимание на все, от начального момента согласования и до внедрения, затем последующей сертификации и аттестации. В условиях XXI века нельзя отрицать важность и всю пользу решения такой задачи.

В данной исследовательской работе были рассмотрены основные аспекты, которые необходимы при создании политики информационной безопасности на предприятии. Так же было обращено внимание на изменения в ГОСТ по ИБ и АС в 2022 году, которые затронули и системы менеджмента ИБ. Были описаны простейшие способы повышения эффективности защиты предприятий и действия злоумышленников, которые могут привести к краху предприятия.

Предприятие, которое должным образом не относиться к своей информационной безопасности, рискует своим существованием.

Список используемых источников

1. Малюк А. А. Введение в информационную безопасность : учебное пособие для вузов. М. : Горячая линия – Телеком 2019. 288 с. С. 25–29.

2. Политика компании в области информационной безопасности № П3-11.01 П-01 версия 2.00. Утверждена Решением Совета директоров ПАО «НК «Роснефть» «31» марта 2020 г. Протокол от «03» апреля 2020 г. № 19 Введена в действие «21» апреля 2020 г. Приказом ПАО «НК «Роснефть» от «21» апреля 2020 г. №233. С. 8-12

3. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. N 2. С. 59–68.

4. ГОСТ Р ИСО/МЭК 27001-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», утверждённый приказом Росстандарта № 1653-ст от 30.11.2021. С. 3-7.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом С. Н. Шемякиным.

УДК 004.056
ГРНТИ 49.33.35

АЛГОРИТМ ПРИЧИННО-СЛЕДСТВЕННОЙ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНОГО ГРАФО-ОРИЕНТИРОВАННОГО ПОДХОДА

И. В. Котенко, Д. А. Левшун

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Инструменты аналитики безопасности киберфизических систем, в частности функционирующих в таких важных областях как промышленность, энергетика, медицина и других, должны обеспечивать непрерывный мониторинг защищенности. Информация о текущем состоянии безопасности системы, как правило, регистрируется в виде событий безопасности. В данном исследовании предлагается алгоритм причинно-следственной корреляции событий безопасности в киберфизических системах на основе интеллектуального графо-ориентированного подхода. Алгоритм включает в себя формирование графа последовательностей событий безопасности на основе интеллектуального анализа данных. Экспериментальная оценка предложенного алгоритма проведена с использованием набора данных промышленной киберфизической системы.

события безопасности, корреляция событий безопасности, графы событий.

Современные инструменты защиты киберфизических систем (КФС), предназначенные для обнаружения вторжений, вредоносных программ, аномалий и уязвимостей, генерируют большое количество данных аналитики безопасности [1, 2, 3]. Помимо необходимости обработки возрастающего объема информации, для аналитиков безопасности проблемой остается сопоставление гетерогенных событий безопасности и восстановление их последовательности. В общем значении событие безопасности представляет собой идентифицированное состояние системы, службы или сети, которое указывает на потенциальное нарушение политики информационной безопасности (ИБ), отказ средств защиты или неизвестную ситуацию, имеющую отношение к безопасности [4].

Определение причинно-следственных взаимосвязей между событиями безопасности может помочь как идентифицировать текущую угрозу, так и прогнозировать возможные атаки на систему. Основополагающую роль при этом играет корреляция событий безопасности, которая позволяет выявить контекст между независимыми событиями [5]. Можно выделить три основных группы методов корреляции событий: на основе сходства, на основе причинно-следственных связей и на основе поиска паттернов [6]. В настоящее время перспективным направлением видится гибридизация различных подходов к корреляции для повышения функциональности и нивелирования недостатков отдельных методов.

Главной задачей данного исследования является разработка алгоритма причинно-следственной корреляции событий безопасности на основе интеллектуального графо-ориентированного подхода. Графовые модели позволяют представлять знания в виде сети, которая состоит из узлов, изображающих определенные объекты (события, состояния системы, шаги атаки), и ребер, описывающих отношения этих объектов. Часто исследователи рассматривают такую модель в качестве графа атак, где переходы между узлами представляют собой атакующие действия с некоторыми весами, такими как вероятность или критичность. В данном исследований в качестве узлов графа предлагается использовать центроиды кластеров событий безопасности, а в качестве ребер – переходы между кластерами, описываемые изменениями признаков событий. Кластеризация событий безопасности позволяет выявить схожесть отдельных событий между собой без наличия предварительных знаний, а также снизить объем информации для последующего причинно-следственного анализа.

Под центроидом кластера понимается репрезентативный для определенного кластера вектор признаков события безопасности $c = \{x_1, x_2, \ldots, x_n\}$, где x_i – значение i-того признака, n – количество признаков события (длина вектора). Последовательность векторов c_a и c_b при этом можно представить как множество $r_{ab} = \{(x_{1a}, x_{2b}), \ldots, (x_{na}, x_{nb})\}$, где x_{ia} –

значение *i*-го признака для вектора c_a, x_{ib} – значение *i*-го признака для вектора c_b. Такому переходу также может быть назначен вес $w \in \mathbb{R}$, который соответствует частоте перехода за заданный отрезок времени h, и может быть получен путем статического анализа последовательности событий.

Обозначим данный граф как:

$$G = (C, R, h, f),$$

где $C = \{c_1, \ldots, c_k\}$ – набор центроидов кластеров событий в виде узлов графа длиной; k – число кластеров; $R = \{r_1, \ldots, r_d\}$ – множество возможных переходов между центроидами длиной d; h – длина временного окна для статистического анализа событий; f: $(R, h) \rightarrow \mathbb{R}$ – функция, отображающая ребра в их веса.

Подобный граф может строится как для всего потока входящих событий, так и для определенных состояний безопасности на этапе обучения. Под множеством категорий состояний безопасности Y при этом может пониматься как бинарное множество $Y = \{0, 1\}$, где 0 – метка нормального состояния, а 1 – метка наличия атаки или аномалии, так и множество $Y = \{y_0, y_1, \ldots, y_m\}$, где y_0 – нормальное состояние, а $y_1 \ldots y_m$ – множество атак. Построение графа событий безопасности, относящихся к определенному типу атаки, позволяет представить различные этапы атаки. Такой процесс особенно важен для обнаружения многошаговых атак.

Алгоритм причинно-следственной корреляции событий безопасности на основе интеллектуального графо-ориентированного подхода можно разделить на следующие этапы.

1. Предобработка потока событий безопасности. Данный этап включает в себя преобразование потока входящих событий в матрицу E^t размерности $l \times n$, где l – количество событий, n – количество признаков события, а также нормализацию данных путем масштабирования значений признаков. События матрице E^t упорядочены во времени и могут быть представлены как $e_t = \{x_{t1}, x_{t2}, \ldots, x_{tn}\}$, где x_{ti} – значение *i*-го признака в момент времени t.

2. Анализ схожести событий на основе кластеризации данных. Алгоритм кластеризации μ позволяет преобразовать матрицу событий E^t в последовательность центроидов кластеров $C^t = \{c_{t1}, \ldots c_{tl}\}$, где $c_{ti} = \mu(e_{ti})$. Множество всех уникальных кластеров для заданного состояния системы описывается как $C = \{c_1, \ldots, c_k\}$.

Для анализа схожести событий прилагается использовать метод кластеризации BIRCH [7]. В качестве метрики схожести между событиями при этом используется евклидово расстояние между их векторами в виде набора признаков. BIRCH позволяет осуществлять иерархическую кластеризацию на наборах данных большого размера, а также не требует знания точно количества кластеров, в отличии от *k*-средних и спектральной кластеризации, и лучше обрабатывает шумы в данных по сравнению с алгоритмами DBSCAN и OPTICS [8].

3. Построение матрицы переходов между кластерами событий на основе статистического анализа последовательностей событий. В данной матрице W с размерностью $k \times k$, где k – количество кластеров, каждый элемент w_{ab} соответствует частоте появления последовательности центроидов c_a, $c_b \in C$ за отрезок времени h. Это значение определяется путем применения к последовательности C^t скользящего временного окна с единичным шагом и вычисления среднего количества появлений заданной последовательности двух событий.

4. Построение графа последовательностей событий безопасности. Для любой пары центроидов $c_a \in C$ и $c_b \in C$ строятся пара вершин, если вес соответствующего элемента матрицы W не равен нулю. Переход между событиями описывается как $r_{ab} = \{(x_{1a}, x_{2b}), \ldots, (x_{na}, x_{nb})\}$. Множество возможных переходов определяется как R.

Приведем пример построения графа событий безопасности на наборе данных Electra, который моделирует поведение тяговой подстанции, используемой для высокоскоростной железной дороги [9]. Набор включает в себя события нормального поведения системы и 6 типов атак. Каждое событие описывает 9 параметров передачи данных в системе, которые выступают в качестве признаков.

На основе предложенного алгоритма был реализован программный прототип на языке Python. В качестве входных данных используется 3 000 000 строк событий. Нормализация осуществляется при помощи масштабирования значений признаков на отрезок [0, 1]. Для кластеризации использовался алгоритм BIRCH с установленным порогом 0.05, который определяет наименьшее значение радиуса кластера, полученного путем слияния новой выборки данных и ближайшего кластера. Анализ схожести событий в выборке позволил выявить **80** кластеров.

На рис. 1 представлены полученные направленные графы для атаки «человек посередине» (MITM_UNALTERED) и модификации ответов (RESPONSE_ATTACK). Подписи узлов соответствуют меткам кластеров событий безопасности. Для упрощения изображения подписи весов ребер опущены. Можно отметить, что некоторые кластеры событий могут быть отнесены более, чем к одной атаке. Например кластеры 19–32 включаются как в граф RESPONSE_ATTACK, так и MITM_UNALTERED. Это позволяет выделять общие этапы между различными состояниями. В то же время, на выборке не были обнаружены общие кластеры между нормальным поведением и атаками.

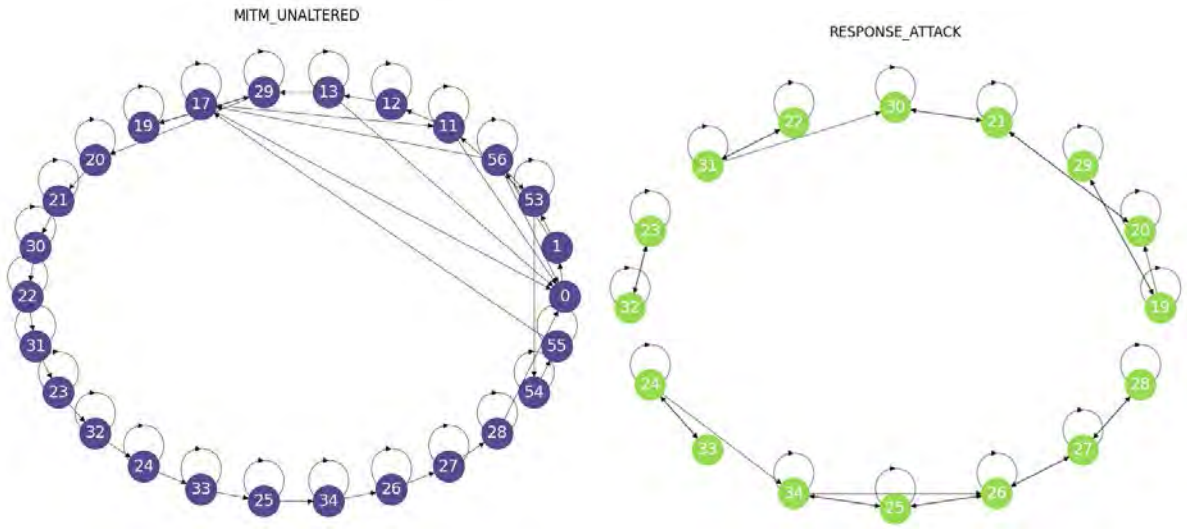


Рис. 1. Графы событий безопасности для атак набора данных Electra

Переходы между узлами графа можно описать в следующем формате:

```
{'r11_12':
          {'features': [
                      {'address': {'from': 0.06739, 'to': 0.11405}},
                      {'data': {'from': 1e-05, 'to': 0.99993}}]
}}
```

В данном формате «*rA_B*» обозначает переход от узла «A» к узлу «B». В списке «*features*» перечисляются наименования параметров с меняющимся значением с указанием начального значения («*from*») и последующего («*to*»). Параметр «*address*» содержит адрес памяти для выполнения операции чтения/записи, «*data*» – передаваемые или получаемые данные.

Таким образом, предложенный алгоритм причинно-следственной корреляции событий безопасности на основе интеллектуального графо-ориентированного подхода позволяет формировать модели для обнаружения и прогнозирования последовательностей событий. В дальнейшей работе планируется расширение предложенного алгоритма для поиска частых паттернов в рядах событий. Также данный алгоритм планируется включить в гибридную систему корреляции событий безопасности.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. N 11. С. 993–1001.

2. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access, 2018, Vol. 6. PP. 72714–72723.

3. Котенко И. В., Федорченко А. В., Саенко И. Б., Кушнеревич А. Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. N 5 (23). С. 2–16.

4. ISO/IEC 27001:2022. Information technology-Security techniques – Information security management systems– Requirements // ISO/IEC International Standards Organization. 2022.

5. Vlahakis G., Apostolou D., Kopanaki E. Enabling situation awareness with supply chain event management // Expert Systems with Applications. 2018. Vol. 93. PP. 86–103.

6. Levshun D., Kotenko I. A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities // Artificial Intelligence Review. 2023. PP. 1–44.

7. Zhang T., Ramakrishnan R., Livny M. BIRCH: an efficient data clustering method for very large databases // ACM sigmod record. 1996. Vol. 25. N 2. PP. 103–114.

8. Nayyar A., PuriV. Comprehensive analysis & performance comparison of clustering algorithms for big data / /Review of Computer Engineering Research. 2017. Vol. 4. N 2. PP. 54–80.

9. Gómez Á. L. P., Maimó L. F., Celdrán A. H., Clemente F. J. G., Sarmiento C. C., Masa C. J. D. C., Nistal R. M. On the generation of anomaly detection datasets in industrial control systems // IEEE Access. 2019. Vol. 7. PP. 177460–177473.

УДК 004.056.5
ГРНТИ 81.93.29

СОДЕРЖАНИЕ И ОСОБЕННОСТИ КЛЮЧЕВЫХ СТАДИЙ РАЗРАБОТКИ МЕТОДОВ И МОДЕЛЕЙ ОБРАБОТКИ ДАННЫХ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ В ВЕДОМСТВЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЯХ

И. В. Котенко[1,2], И. Б. Паращук[1,3], И. Б. Саенко[1,3]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Рассмотрены содержание и сущность ключевых стадий разработки моделей, методов и алгоритмов интеллектуальной аналитической обработки больших массивов гетерогенных данных об инцидентах кибербезопасности в ведомственных инфокоммуникационных сетях. Исследованы особенности и обоснованы применяемые при решении подобных задач методические приемы, математические методы и частные технологии

искусственного интеллекта, позволяющие повысить достоверность и оперативность принятия решений по защите информационных, телекоммуникационных и других критически важных ресурсов в сетях и системах такого класса.

инцидент, аналитическая обработка данных, кибербезопасность, метод, модель, искусственный интеллект, инфокоммуникационные сети.

Бурное и энергичное развитие информационных и сетевых технологий, осуществляющееся в настоящее время и сопровождаемое крупными достижениями в построении киберфизических систем, включая сети IoT, IIoT, системы «Smart Home», квантовые и «зеленые» вычисления, приводит не только к появлению новых пользовательских прикладных программных систем, но и к лавинообразному росту количества и уровня угроз кибербезопасности, особенно, в области критических информационных инфраструктур, к которым относятся и ведомственные инфокоммуникационные сети (ИКС) [1].

В этой связи особую актуальность для обеспечения кибербезопасности ведомственных ИКС, как старого, так и нового поколения, приобретают, на наш взгляд, модели, методы и алгоритмы интеллектуальной аналитической обработки (ИАО) больших массивов гетерогенных данных (БМГД) об инцидентах кибербезопасности в инфокоммуникационных сетях, методы и алгоритмы обнаружения уязвимостей и атак в сетях такого класса, а также алгоритмы мониторинга, оценки и прогнозирования их информационной безопасности [2, 3].

Поэтому важной является разработка и экспериментальное исследование новых, инновационных моделей, методов и алгоритмов аналитической обработки больших массивов гетерогенных данных об инцидентах кибербезопасности в ведомственных ИКС. Причем при создании таких методов и алгоритмов, упор должен быть сделан, на наш взгляд, на использование современных технологий искусственного интеллекта, поскольку в нынешних условиях, только такой подход, соответствующий специфике сегодняшних реалий, позволит обеспечить выполнение требований по точности обнаружения как известных, так и неизвестных кибератак, требований по оперативности и достоверности обработки данных об инцидентах кибербезопасности в ведомственных ИКС [4, 5, 6].

При этом предполагается, что ключевыми стадиями разработки методов, моделей и алгоритмов ИАО БМГД об инцидентах кибербезопасности в ведомственных ИКС могут и должны стать шаги, ориентированные на такие актуальные инциденты и позволяющие оценивать уровень угроз, визуализировать результаты и принимать решения по защите, например:

– стадия исследований и построения методов, моделей, методик и алгоритмов обнаружения (с использованием имитационного и графо-ориентированного моделирования) в реальном времени инцидентов типа «атака» на ведомственные ИКС [7];

– стадия разработки моделей, методик и алгоритмов обнаружения в реальном времени противоестественной (аномальной) активности и нарушений критериев и политик кибербезопасности ведомственных ИКС с использованием методов ИАО БМГД об инцидентах;

– стадия создания моделей, методик и алгоритмов оперативной оценки уровня угроз и степени кибербезопасности информационных, телекоммуникационных и других критически важных ресурсов ИКС на основе ИАО БМГД об инцидентах;

– стадия формулировки и построения методик и алгоритмов оперативного анализа и управления рисками кибербезопасности ведомственных ИКС на основе ИАО БМГД об инцидентах – в интересах оценки состояния, поддержки принятия решений, объективного и оперативного расследования таких инцидентов;

– стадия разработки моделей, методик и алгоритмов оперативной визуализации БМГД об инцидентах кибербезопасности – в интересах оценки состояния, поддержки принятия решений, объективного и оперативного расследования таких инцидентов;

– стадия исследований и построения методов, моделей, методик и алгоритмов принятия решений по защите ИКС на основе ИАО БМГД об инцидентах кибербезопасности.

С точки зрения содержания рассмотренных ключевых стадий разработки методов, моделей и алгоритмов ИАО БМГД об инцидентах кибербезопасности в ведомственных ИКС, особого вниманию, на наш взгляд, заслуживает начальный этап – стадия разработки методов, моделей, методик и алгоритмов обнаружения в реальном времени инцидентов типа «атака» на ведомственные сети. В рамках этой стадии, с учетом планируемого использования имитационного и графо-ориентированного моделирования, предлагается вначале определиться с исходными данными, т. е., выбрать и проанализировать один или несколько датасетов в конкретной предметной области – процессе функционирования ведомственной ИКС.

Далее осуществляется выбор для программной реализации одной из имитационных, графо-ориентированных моделей и сравнительный анализ релевантных библиотек и их функций для реализации выбранной модели [7]. Затем предусматривается разработка методики обнаружения в реальном времени атак на основе имитационного и графо-ориентированного

моделирования, использующих построенные модели и алгоритмы, обобщение методики под возможные другие разновидности моделей и алгоритмов обнаружения атак на ведомственные ИКС. В итоге, на данной стадии предлагается сформулировать предложения по архитектуре и экспериментальному стенду с учетом особенностей реализации компонента обнаружения атак, в т. ч. предложения по встраиванию компонента обнаружения атак в общую архитектуру кибербезопасности ведомственных ИКС, определению интерфейсов с другими компонентами данной архитектуры.

Содержания иных ключевых стадий разработки методов, моделей и алгоритмов ИАО БМГД об инцидентах затрагивает вопросы формулировки описательной модели угроз кибербезопасности в ведомственных ИКС, разработки частных методов и алгоритмов обнаружения уязвимостей в сетях такого класса на основе мультиаспектного подхода, SQL-уязвимостей (SQL-инъекций) и атак, киберинсайдеров, а также использования краулера (программного поискового робота) для формирования датасета для безопасности данных в ИКС. Вторая и последующие стадии процесса разработки методов, моделей и алгоритмов ИАО БМГД об инцидентах посвящены формированию и экспериментальному исследованию моделей, методов и алгоритмов мониторинга, оценки и прогнозирования уровня кибербезопасности в ведомственных ИКС. Создаются и проверяются на практике модели и алгоритмы интервального анализа кибербезопасности в ведомственных ИКС, модель и метод инвариантного оценивания и прогнозирования состояния кибербезопасности [8].

С использованием методов машинного обучения и краулера создан и апробирован методологический подход к мониторингу периметров защищенности ведомственных ИКС и анализу инцидентов кибербезопасности. На основе мобильных робототехнических устройств и сенсоров мобильных терминалов пользователей предложен подход к реализации проактивного мониторинга состояния кибербезопасности ведомственных беспроводных сенсорных ИКС. В качестве частных объектов исследования, зачастую входящих в состав ведомственных ИКС, рассматриваются сети Интернета вещей, мобильные сети, а также беспроводные сенсорные сети, причем использованы профили типовых устройств ведомственных ИКС, а в рамках исследования использованы методы машинного обучения, статистического анализа и обработки нечетких множеств.

Таким образом, рассмотрены содержание и сущность ключевых стадий разработки моделей, методов и алгоритмов интеллектуальной аналитической обработки больших массивов гетерогенных данных об инцидентах кибербезопасности в ведомственных ИКС. Исследованы особенности и обоснованы применяемые при решении подобных задач методические приемы, математические методы и частные технологии искусственного интеллекта,

позволяющие повысить достоверность и оперативность принятия решений по защите информационных, телекоммуникационных и других критически важных ресурсов в сетях и системах такого класса.

Работа выполнена при финансовой поддержке РНФ (проект 21-71-20078) в СПб ФИЦ РАН (СПИИРАН).

Список используемых источников

1. Гребешков А. Ю. Вычислительная техника, сети и телекоммуникации : учебное пособие для вузов. М. : ГЛТ, 2016. 190 с.

2. Полтавцева М. А. Агрегация и нормализация гетерогенных данных в системах мониторинга информационной безопасности и обнаружения вторжений крупномасштабных промышленных КФС // Труды ИСП РАН. 2020. Том 32, Вып. 5. С. 131–142.

3. Паращук И. Б., Царамов М. В., Сафонов Д. В. Анализ основных требований к процедурам поиска и навигации в больших объемах информации, циркулирующей в региональных телекоммуникационных сетях // Юбилейная XV-я Санкт-Петербургская Международная конференция «Региональная информатика-2016 (РИ-2016)». Материалы конференции. СПб. : СПОИСУ, 2016. С. 114–115.

4. Kotenko I., Doynikova E., Fedorchenko A. Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security Assessment Tasks // EAI/Springer Innovations in Communication and Computing, 2020. PP. 79–116.

5. Саенко И. Б., Кушнеревич А. Г., Котенко И. В. Реализация платформы распределенных параллельных вычислений для сбора и предварительной обработки больших данных мониторинга в киберфизических системах // Международный конгресс по информатике: Информационные системы и технологии (CSI ST-2016). Материалы международного конгресса. Республика Беларусь, Минск, 24-27 октября 2016 г. С. 641–645.

6. Котенко И. В., Саенко И. Б., Браницкий А. А., Паращук И. Б., Гайфулина Д. А. Интеллектуальная система аналитической обработки цифрового сетевого контента для защиты от нежелательной информации // Информатика и автоматизация (Труды СПИИРАН). 2021. Вып. 20 (4). С. 755–792.

7. Десницкий В. А. Подход к обнаружению атак в реальном времени на основе имитационного и графо-ориентированного моделирования // Информатизация и связь. 2021. N 7. С. 30–35.

8. Котенко И. В., Паращук И. Б. Информационные и телекоммуникационные ресурсы критически важных инфраструктур: особенности интервального анализа защищенности// Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2022. N 2. С. 33–40.

УДК 004.043
ГРНТИ 81.93.29

МЕТОДИКА АВТОМАТИЗИРОВАННОГО СБОРА КРИМИНАЛИСТИЧЕСКИХ ДАННЫХ В ПРОЦЕССАХ THREAT HUNTING

И. В. Котенко[1], И. А. Попков[2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В процессе Threat hunting задействован ретроспективный анализ хостовых и сетевых телеметрий в рамках выбранной гипотезы компрометации инфраструктуры. Применение методов криминалистического сбора информации может расширить спектр анализируемых данных. В работе предлагается методика автоматизированного выборочного сбора криминалистических данных для повышения информативности хранящихся в SIEM-данных. Рассматривается сбор таких данных, как MFT-таблицы, дампы трафика, оперативной памяти и системных вызовов на основании аномальности ранее происходивших на хосте событий.

мониторинг событий информационной безопасности, проактивное обнаружение инцидентов, проактивный поиск угроз, форензика.

Введение

Одной из важнейших задач кибербезопасности является анализ защищенности защищаемых систем [1, 2, 3]. По данным ежегодного отчета Mandiant [4] среднее время между проникновением злоумышленника в инфраструктуру и обнаружением этого проникновения (dwell time) составляет 21 день. Помимо этого, для региона EMEA (Европа, Ближний Восток и Африка) процент внешних уведомлений об инцидентах составляет 62 %, а внутренних – 38. Это значит, что злоумышленники могут неделями или даже месяцами находиться в инфраструктуре организации, не замеченными внутренними системами обнаружения.

Безусловно, проникновения в инфраструктуру оставляют цифровые следы, однако их количество и качество не позволяют однозначно отделить легитимное поведение систем от нелегитимного [5]. Среднее значение dwell time в индустрии постепенно уменьшается, отчасти благодаря внедрению подхода Threat Hunting [6]. В русскоязычных источниках [7] под понятием Threat Hunting принято понимать процесс проактивного и итеративного анализа телеметрии, собираемой с конечных точек и сетевых сенсоров с целью выявления угроз, обошедших используемые в сети превентивные средства

защиты. Данный процесс базируется на предположении, что злоумышленник уже находится в защищаемой инфраструктуре, и защищаемая система частично или полностью скомпрометирована.

Этапы Threat hunting

Принято выделять 4 этапа проведения Threat Hunting, образующих цикл: создание гипотезы проникновения, инструментальное исследование, выявление новых шаблонов поведения, техник, тактик и процедур, а также автоматизированный анализ [8]. В рамках выстраивания матрицы Threat Hunting, связывающей цикл Threat Hunting с этапами Hunting Maturity Model [9], цикл дополняется этапом сбора данных.

Сбор данных для проведения Threat Hunting

Современной практикой сбора данных для проведения Threat Hunting можно считать сбор следующих наборов данных [7]:

1) события активности процессов;
2) данные сканирования оперативной памяти;
3) данные инвентаризации точек автозапуска;
4) события ОС (операционной системы);
5) листинг определенных каталогов, которые могут быть использованы атакующими или вредоносным ПО для хранения своих исполняемых файлов;
6) периодические снапшоты результатов работы отдельных утилит;
7) данные NetFlow;
8) метаданные загружаемых из интернета файлов;
9) метаданные HTTP-активности;
10) метаданные SSL- / TLS-трафика;
11) метаданные DNS-трафика;
12) метаданные LDAP-трафика;
13) метаданные Kerberos-трафика;
14) метаданные SMB / DCE RPC;
15) метаданные файлов, передаваемых внутри сети по SMB;
16) метаданные электронных писем, сведения о файлах и ссылках, получаемых по электронной почте.

Пункты 2, 3, 5, 6, 7 и 9 сложны в реализации, требуют реализации эффективных подходов и инструментов, использующих методы форензики. Исходя из этого, актуальным направлением дальнейшего развития Threat Hunting является расширение этих подходов и полноценный сбор данных наряду с использованием традиционных журналов безопасности [10].

Анализ существующих решений

На данный момент исследователи уже предлагают использование криминалистических данных в целях Threat Hunting [11, 12].

Однако, основными проблемами сбора криминалистических данных остаются:

– сбор данных во время Threat Hunting сессии – постфактум относительно анализируемых в рамках гипотезы событий;

– большой объем хранимой и передаваемой информации;

– нормативное обеспечение регулярного сбора такого рода данных;

– побуждение злоумышленника к маскировке при обнаружении им процессов сбора телеметрий;

– определение аномальности событий, предшествующих сбору.

Частичным решением данных проблем может стать автоматизированный сбор криминалистических данных на основании аномальности происходивших на узле событий.

Методика автоматизированного сбора криминалистических данных

Для автоматизации сбора криминалистических данных в момент происшествия аномальных событий на узлах сети необходима модернизация архитектуры конвейера сбора событий безопасности с вовлечением следующих компонентов [13, 14, 16]:

– агентов сбора криминалистических данных;

– EDR (endpoint detection and response solution);

– брокеров данных;

– компонентов SIEM-системы;

– дополнительных средств анализа данных.

Методика заключается в выполнении следующей последовательности операций, определяющих сбор криминалистических данных с узлов:

1) установка агентов сбора криминалистических данных на критичных хостах;

2) определение потоков / расписаний передачи данных;

3) выявление корреляционных правил запуска процедур автоматизированного сбора;

4) установка жизненного цикла данных;

5) корректировка правил запуска с учетом применимости собранных данных в циклах Threat Hunting.

Корреляционные правила настраиваются на основании недостаточности оснований для открытия полноценного инцидента и ценности для ретроспективного анализа (по модели Paris [5]). Другими словами, корреляционное правило SIEM-системы со специально подготовленным тегом должно

запускать сбор криминалистических данных без уведомления оператора центра управления безопасностью (Security Operation Center, SOC).

Данные, собранные таким способом, входят в набор анализируемых во время сессий Threat Hunting. В случае, если данные, собранные корреляционными правилами, не вошли в анализируемый набор событий в рамках нескольких сессий Threat Hunting, корреляционное правило может быть скорректировано для большей эффективности.

Криминалистические данные нуждаются в особом жизненном цикле в отличие от остальных данных в SIEM-системе. Такие данные могут быть сразу архивированы, так как доступ к ним будет получен только в рамках сформированной гипотезы. Срок хранения таких данных должен быть увеличен в связи с потенциальной необходимостью расследования протяженных во времени атак.

Заключение

Для повышения эффективности проведения Threat Hunting и, соответственно, сокращения среднего времени обнаружения проникновений в рамках предложенной методики было выдвинуто предложение об избирательном сборе криминалистических данных на основании аномальности событий, произошедших ранее на связанных узлах сети. Предполагается, что предложенный способ и методика сбора данных позволят увеличить информативность анализируемых специалистом Threat Hunting данных и не приведут к чрезмерному увеличению собираемых данных. В последующих исследованиях предполагается уточнить предлагаемую методику, провести ее реализацию и эксперименты.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. 2005. Vol. 3685. PP. 311–324.

2. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. N 2. С. 7–24.

3. Kotenko I., Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security Events // Lecture Notes in Computer Science. 2014. Vol. 8407. PP. 462–471.

4. Special Report Mandiant M-TRENDS 2022. URL: https://www.mandiant.com/m-trends

5. Adam Bateman. The PARIS Model. URL: http://threathunter.guru/blog/the-paris-model/

6. Domaintools, 2021. Threat Hunting Report. URL: https://www.domaintools.com/wp-content/uploads/2021-Threat-Hunting-Report.pdf

7. Охота за угрозами: зачем она нужна. Bi.Zone. Материалы конференции CyberPolygon 2020. URL: https://cyberpolygon.com/ru/materials/threat-hunting-why-might-you-need-it/

8. A Framework for Cyber Threat Hunting. WhitePaper. URL: https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf

9. Bianco D. J. A Simple Hunting Maturity Model, 2015. URL: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

10. Javeed D., Khan M. T. An Efficient Approach of Threat Hunting Using Memory Forensics // International Journal of Computer Networks and Communications Security. May 2020. Vol. 8, No. 5. PP. 37–45.

11. Rasheed H., Hadi A., Khader M. Threat Hunting Using GRR Rapid Response // 2017 International Conference on New Trends in Computing Sciences (ICTCS), Amman, Jordan. 2017. PP. 155–160.

12. Klinkhamhom C., Boonyopakorn P. Threat Hunting for Digital Forensic Using GRR Rapid Response with NIST Framework // 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), Phuket, Thailand. 2022. PP. 177–180.

13. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. N 2. С. 57–68.

14. Котенко И. В., Саенко И. Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук. 2014. Т. 84. N 11. С. 993–1001.

15. Котенко И. В., Полубелова О. В., Саенко И. Б., Чечулин А. А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности. 2012. Т.8, N 2. С. 100–108.

16. Котенко И. В., Федорченко А. В., Саенко И. Б., Кушнеревич А. Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. N 5 (23). С. 2–16.

УДК 004.043
ГРНТИ 81.93.29

АНАЛИЗ АКТУАЛЬНЫХ НАПРАВЛЕНИЙ ИССЛЕДОВАНИЙ В ОБЛАСТИ THREAT HUNTING

И. В. Котенко[1], И. А. Попков[2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Threat Hunting – это цикличный процесс, включающий в себя группу взаимосвязанных процессов по управлению угрозами, охватывающих различные сферы обеспечения

информационной безопасности организации. В статье проводится анализ наиболее важных с точки зрения текущих трендов этапов проведения Threat Hunting – инвентаризации инфраструктуры, формирования гипотез проникновения, сбора и корреляции телеметрических данных, а также документирования результатов. В статье для каждого из этих этапов выделяются актуальные исследовательские проблемы и направления их решения.

мониторинг событий информационной безопасности, проактивное обнаружение инцидентов, проактивный поиск угроз.

Введение

Согласно [1] Threat Hunting представляет собой проактивный поиск угроз, в основном ручной процесс с элементами автоматизации, в котором аналитик использует свои знания и навыки для проверки больших объемов информации на наличие индикаторов компрометации, согласно заранее определенной гипотезе о наличии угрозы.

Целью Threat Hunting заявляется обнаружение не зафиксированных вторжений в защищаемую инфраструктуру. Очевидно, параметрами этой деятельности могут служить: процент обнаруженных атак из репрезентативной выборки, среднее время между первичным доступом злоумышленника к инфраструктуре и его обнаружением, этап атаки (например, по модели *Unified Kill Chain* [2]), на котором было обнаружено вторжение.

История Threat Hunting

Впервые подход Threat Hunting был предложен Ричардом Бейтлихом в статье Become a Hunter в журнале Information Security Magazine в 2011 году [3]. В этой работе автор адаптировал понятие «hunter-killer», взятое из терминологии ВВС США, под контекст корпоративных центров управления безопасностью (Security Operation Center, SOC). Благодаря этой аналогии автор впервые описал данный подход к поиску угроз информационной безопасности (*Threat Hunting* в оригинальной статье).

Значительный вклад в развитие подхода Threat Hunting также был внесен Девидом Бьянко в работах «The Pyramid of Pain» и «A Simple Hunting Maturity Model» в 2013 и 2015 годах соответственно [4, 5]. В этих статьях автор предложил более конкретные методы к модернизации обычных SOC для целей проведения Threat Hunting.

Типы Threat Hunting

Специалисты выделяют следующие типы Threat Hunting [6]:

1) *Threat Hunting на основе собранных данных (data-driven Threat Hunting)*. Данный подход основан на выделении аномалий в потоке собираемых данных и выдвижении гипотезы Threat Hunting на основании найденных

аномалий. Обнаруженные на этапе формирования гипотезы данные становятся отправной точкой на этапе исследования;

2) *Threat Hunting на основе Threat Intelligence (intel-driven Threat Hunting)*. Данный подход предлагает формировать гипотезу Threat Hunting на основании свежих полученных данных Threat Intelligence. Подход может приносить пользу в случае, если поток данных Threat Intelligence сопоставим с моделью рисков организации;

3) *Threat Hunting на основе TTP-модели (techniques, tactics and procedures driven Threat Hunting)*. Данный подход является наиболее универсальным, так как он не использует индикаторы компрометации для формирования гипотезы. Однако, по этой же причине его использование затруднено на этапе исследования, так как специалистам приходится самостоятельно предполагать реализацию выбранную TTP-модель и на ее основании проводить поиск.

Данные типы не являются взаимоисключающими и могут совмещаться на практике для повышения эффективности проводимого поиска угроз и инцидентов.

Актуальные проблемы Threat Hunting

На основании проанализированных работ в области исследования Threat Hunting можно выделить наиболее актуальные на данный момент исследовательские проблемы:

– эффективность корреляции при высоких значениях EPS (events per second) [7, 8];

– точность детектирования APT-атак на ранних этапах вторжения [9,10];

– подготовка команды специалистов Threat Hunting [11];

– использование методов форензики в целях Threat Hunting [12, 13];

– Threat Hunting с помощью выявления паттернов поведения в потоке событий [14, 15, 16];

– обмен информацией о Threat Intelligence в целях Threat Hunting [17, 18];

– эмуляция злоумышленника для генерации гипотез Threat Hunting [19, 20, 21].

Актуальные направления исследований

Исходя из проанализированных проблем, можно выдвинуть несколько наиболее актуальных направлений исследований в области Threat Hunting:

– интеллектуальная инвентаризация активов в целях Threat Hunting - полный набор данных об инфраструктуре позволяет обогащать со-

бытия информационной безопасности данными об активах, задействованных в инциденте. Эту информацию можно собирать силами самих узлов инфраструктуры, подстраиваясь под платформу узла и типы хранимых на нем данных;

– сбор и корреляция нестандартной хостовой и сетевой телеметрии. Обнаружить атаку на инфраструктуру можно не только с помощью журналов информационной безопасности, но и по набору второстепенных данных. Такими данными могут стать: данные форензики, телеметрии состояния и доступности узлов, слепки конфигураций, сетевой трафик. Расширение диапазона собираемых данных позволяет обнаруживать незафиксированные в журналах действия злоумышленника в инфраструктуре;

– методы формирования гипотез Threat Hunting. Аналогично системы помощи принятия решений в информационной безопасности – процесс Threat Hunting нуждается в системе формирования гипотез. Даже частичная автоматизация этого процесса способна повысить качество и разнообразие предлагаемых гипотез, что, в свою очередь, способно повлиять на скорость обнаружения атаки в рамках этой гипотезы;

– автоматизация процессов документирования процессов Threat Hunting. Составление отчетов по проведению Threat Hunting хоть и предполагает творческий подход, все еще оставляет большой спектр работы по унификации и ускорению данного процесса.

Заключение

Подход к поиску угроз и инцидентов информационной безопасности Threat Hunting, появившийся чуть больше 10 лет назад, уже приносит практические результаты многим организациям по всему миру, но все еще оставляет большой фронт проблем для исследования. В статье представлен анализ текущих исследований в области Threat Hunting, и выдвинуты предложения по частичному решению актуальных для этого подхода проблем. Детальное описание и апробацию предложенных подходов предполагается представить в последующих исследованиях.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

Список используемых источников

1. Lukova-Chuiko N., Fesenko A., Papirna H., Gnatyuk S. Threat Hunting as a Method of Protection Against Cyber Threats // International Conference "Information Technology and Interactions". CEUR Workshop Proceedings. 2020. PP. 103–113.

2. Pols P. Unified Kill Chain White Paper Version 1.3, 2023. URL: https://www.unified-killchain.com/assets/The-Unified-Kill-Chain.pdf

3. Bejtlich R. Become a Hunter // Information Security Magazine. 2011. URL: https://www.academia.edu/6842108/Become_a_Hunter

4. Bianco D. The Pyramid of Pain, 2013. URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

5. Bianco D. A Simple Hunting Maturity Model, 2015. URL: http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

6. Wang Z. A systematic literature review on cyber threat hunting // ArXiv, 2013. abs/2212.05310.

7. Kotenko I., Gaifulina D., Zelichenok I. Systematic Literature Review of Security Event Correlation Methods // IEEE Access. 2022. N 10. PP. 43387–43420.

8. Котенко И. В., Федорченко А. В., Саенко И. Б., Кушнеревич А. Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // Вопросы кибербезопасности. 2017. N 5 (23). С. 2–16.

9. Khalid A., Zainal A., Maarof M. A., Ghaleb F.A. Advanced Persistent Threat Detection: A Survey // 3rd International Cyber Resilience Conference (CRC). 2021. PP. 1–6.

10. Joloudari J. H., Haderbadi M., Mashmool A., Ghasemigol M., Band S. S., Mosavi A. H. Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning, // IEEE Access. 2021. N 8. PP. 186125–186137.

11. Wei J. A Laboratory for Hands-on Cyber Threat Hunting Education // The Colloquium for Information System Security Education (CISSE). June, 2019. PP. 1–19.

12. Javeed D., Khan M. T., Ahmad I., Iqbal T., Badamasi U. M., Ndubuisi C. O., Umar A. An Efficient Approach of Threat Hunting Using Memory Forensics // International Journal of Computer Networks and Communications Security. May 2020. Vol. 8, No. 5. PP. 37–45.

13. Klinkhamhom C., Boonyopakorn P. Threat Hunting for Digital Forensic Using GRR Rapid Response with NIST Framework // 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC). 2022. PP. 177–180.

14. Homayoun S., Dehghantanha A., Ahmadzadeh M., Hashemi S., Khayami R. Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence // IEEE Transactions on Emerging Topics in Computing. 2018. N 8. PP. 341–351.

15. Khan M. S., Richard R., Molyneaux H., Cote-Martel D., Elango H.J., Livingstone S., Gaudet M., Trask D.V. Cyber Threat Hunting: A Cognitive Endpoint Behavior Analytic System // Int. J. Cogn. Informatics Nat. Intell. 2021. N 15. PP. 1–23.

16. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring based on Big Data Processing and Machine Learning // IEEE Access. 2018. Vol. 6. PP. 72714–72723.

17. Krauss O., Papesh K. Analysis of Threat Intelligence Information Exchange via the STIX Standard // International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). 2022. PP. 1–6.

18. Gao P., Shao F., Liu X., Xiao X., Qin Z., Xu F., Mittal P., Kulkarni S. R., Song D. X. Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence. // IEEE 37th International Conference on Data Engineering (ICDE). 2021. PP. 193–204.

19. Kotenko I. Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet // 19th European Simulation Multiconference “Simulation in wider Europe”. ECMS 2005. Riga, Latvia, 1–4 June 2005. PP. 533–543.

20. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. N 2. С. 7–24.

21. Ajmal A. B., Shah M. A., Maple C., Asghar M. N., Islam S. M. Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. // IEEE Access. 2021. N 9. PP. 126023–126033.

УДК 53.082.54
ГРНТИ 29.31.29

ИЗМЕРЕНИЕ ПАРАМЕТРОВ МЕХАНИЧЕСКИХ КОЛЕБАНИЙ ПРЕЦИЗИОННЫХ КВАРЦЕВЫХ РЕЗОНАТОРОВ

Е. В. Кравец

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Задача исследования амплитуды и частоты колебания поверхности кварцевого генератора возникает при проектировании и разработке новых конструкций. В работе рассматриваются оптические интерференционные схемы определения амплитуды механических колебаний, оценивается диапазон возможных измерений. На основе проведенного анализа предлагается для измерения амплитуды колебаний поверхности кварцевого резонатора применить оптический метод измерений с использованием интерферометра с гетеродинированием оптического пучка. Сдвиг частоты оптического сигнала производится с помощью акустооптического модулятора света.

кварцевый резонатор, интерферометр, акустооптический модулятор.

Введение

Основой создания устройств стабилизации частоты и других высокостабильных частотозадающих устройств СВЧ для связной и навигационной аппаратуры являются кварцевые резонаторы.

Основные электрические и эксплуатационные характеристики резонаторов во многом определяются особенностями механических колебаний пьезоэлектрического элемента. Механические колебания твёрдых тел обусловлены распространением в них упругих деформаций и вызванных ими соответствующих акустических волн. При этом частота, спектральная плотность фазового шума и стабильность частоты резонаторов существенно зависят от вида механического колебания пьезоэлемента и параметров и качества исполнения электродов [1, 2, 3, 4, 5, 6].

Одной из наиболее сложных проблем, возникающих при разработке кварцевых резонаторов, является определение оптимальных геометрических размеров пьезоэлементов, обеспечивающих высокую добротность и моночастотность, что, в свою очередь, связано с идентификацией многочисленных мод колебаний.

Амплитуда колебаний поверхности прецизионных кварцевых резонаторов не превышает единиц нанометров, поэтому основным методом иссле-

дования распределения акустических колебаний по поверхности пьезоэлементов является лазерная интерферометрия. При этом потенциальная чувствительность оптических методов достигает долей ангстрем [5, 6].

Оптические схемы регистрации колебаний

Пространственные распределения амплитуды смещений могут быть измерены оптическим методом на основе использования интерферометра Майкельсона (рис. 1) [5, 6]. Интермодуляционная составляющая сигнала фотоприемника содержит компоненту, которая позволяет определить амплитуду колеблющейся по гармоническому закону поверхности:

$$S(t) \sim \cos(m \cdot \sin(\Omega t + \varphi_0) + \varphi),$$
$$m = 2 \cdot \frac{2\pi}{\lambda} \cdot A, \quad (1)$$
$$\varphi = \frac{\omega}{c} \cdot (z_2 - z_1),$$

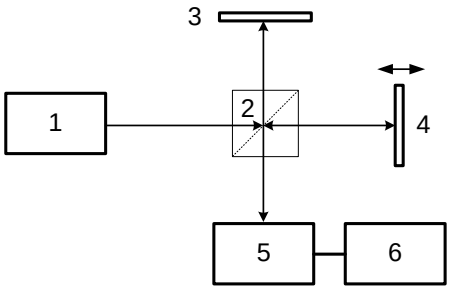


Рис. 1. Схема интерферометра Майкельсона: *1* – лазер, 2 – светоделительное зеркало, *3* – неподвижное зеркало, *4* – кварцевый резонатор, *5* – фотоприемник, *6* – блок обработки

где z_1 и z_2 – оптический ход пучков: опорного и сигнального соответственно, A – амплитуда изменения разности хода пучков, Ω – частота колебания кварцевого резонатора, φ_0 – начальная фаза колебания.

Спектр выходного сигнала фотоприемника (1) зависит от начальной разности фаз φ интерферирующих пучков:

$$S(t) = J_0(m) \cdot \cos\varphi - \sum_{l=1}^{\infty} 2J_{2l-1}(m) \cdot \sin\varphi \cdot \sin((2l-1) \cdot (\Omega t + \varphi_0)) +$$
$$+ \sum_{k=1}^{\infty} 2J_{2k}(m) \cdot \cos\varphi \cdot \cos(2k(\Omega t + \varphi_0)) \quad . \quad (2)$$

Выражение (2) показывает существенное влияние на спектр выходного сигнала разности фаз φ между оптическими пучками. Таким образом, классическая схема интерферометра Майкельсона требует согласования фазовых фронтов опорной и сигнальной волн, что затрудняет проведение измерений.

Для измерения распределения амплитуд по поверхности кварцевого резонатора может быть использована оптическая схема на основе интерферометра Майкельсона с акустооптическим модулятором [5, 6, 7].

Оптическую схему интерферометра Майкельсона можно упростить, используя в качестве опорного пучок, отраженный от одной из граней акустооптического модулятора. Оптическая схема, реализующая такой метод, представлена на рис. 2.

Интермодуляционная составляющая сигнала, получаемого на фотоприемнике, с точностью до амплитудного множителя может быть представлена в виде:

$$s(t) \sim \cos(\omega_A \cdot t + m \cdot \sin(\Omega t + \varphi_0) + \varphi),$$
$$m = 2 \cdot \frac{\omega}{c} \cdot A, \qquad (3)$$
$$\varphi = \frac{\omega}{c} \cdot (z_2 - z_1),$$

где ω_A – частота генератора (6), обеспечивающего частотный сдвиг выходного сигнала.

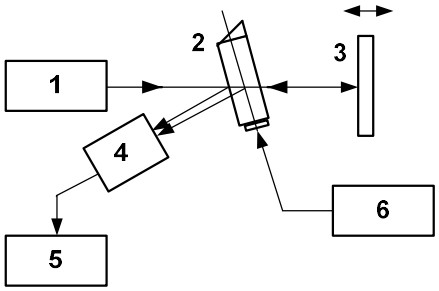


Рис. 2. Схема интерферометра с акустооптическим модулятором: *1* – лазер, *2* – акустооптический модулятор, *3* – кварцевый резонатор, *4* – фотоприемник, *5* – блок обработки, *6* – генератор

В отличие от схемы интерферометра Майкельсона без акустооптического модулятора начальная разность фаз пучков φ не влияет на амплитудные составляющие спектра сигнала:

$$S(t) = J_0(m) \cdot \cos(\omega_A t + \varphi) +$$
$$+\sum_{k=1}^{\infty} 2J_{2k}(m) \cdot \cos((\omega_A + 2k\Omega) \cdot t + \varphi) + \sum_{k=1}^{\infty} 2J_{2k}(m) \cdot \cos((\omega_A - 2k\Omega) \cdot t + \varphi) + \qquad (4)$$
$$+\sum_{l=1}^{\infty} 2J_{2l-1}(m) \cdot \cos((\omega_A + (2l-1) \cdot \Omega) \cdot t + \varphi) - \sum_{l=1}^{\infty} 2J_{2l-1}(m) \cdot \cos((\omega_A - (2l-1) \cdot \Omega) \cdot t + \varphi).$$

При условии $m \ll 1$ в спектре сигнала почти отсутствуют гармоники высоких порядков, а полезный сигнал можно считать монохроматическим. Кроме того приблизительно известна частота колебаний поверхности резонатора. Указанные условия позволяют определить амплитуду колебаний, а также избавиться от влияния интенсивности опорного и сигнального пучков, путем определения отношений амплитуд несущей и первой компоненты в спектре сигнала:

$$\frac{J_1(m)}{J_0(m)} \approx \frac{m}{2} \cdot (1 + \frac{m^2}{8} - \frac{5 \cdot m^4}{192} + ...)$$
$$m \approx 2 \cdot \frac{U_1}{U_0} \qquad (5)$$

В соответствии с выражениями (3) и (5) амплитуда колебаний резонатора может быть определена следующим образом:

$$A = \frac{\lambda}{2\pi} \cdot \frac{U_1}{U_0}. \qquad (6)$$

Представляет интерес определить длину волны источника монохроматического излучения λ. Предлагается определить оптимальное значение исходя из условия равенства интенсивность взаимодействующих пучков интерферометра.

Оптический сигнал в плоскости фотоприемника состоит из двух компонент, одна из которых формируется путем отражения от грани акустооптического модулятора 2, а вторая– за счет прохождения сквозь акустооптический модулятор 2, отражения от поверхности кварцевого резонатора 3 (рис. 2) и дифракции в модуляторе 2:

$$\alpha_1 = \left(\frac{n-1}{n+1}\right)^2, \qquad \alpha_2 = \left[1-\left(\frac{n-1}{n+1}\right)^2\right]^4 \cdot \eta \cdot R_{Au}, \tag{7}$$

где n – показатель преломления материала акустооптического модулятора (TeO_2), η – эффективность акустооптического взаимодействия (в зависимости от уровня управляющего сигнала в модуляторе η = 0,4–0,8).

Результаты расчетов, представленные в таблице 1, показывают, что использование лазеров с длиной волны менее 550 нм нецелесообразно, так как коэффициент отражения R_{Au} от поверхности электрода кварцевого резонатора имеет значение < 0,4 [8, 9].

С учетом дисперсии и спектрального коэффициента отражения для источника с длиной волны λ = 650 нм коэффициенты интенсивности опорного и предметного луча составляют соответственно $\alpha_1 = 0{,}15$, $\alpha_2 = 0{,}175$.

ТАБЛИЦА 1. Энергетические коэффициенты пропускания оптической системы при различной длине волны лазерного источника излучения

λ, нм	n	R_{Au}	α_1	α_2
<500	2,3	0,4	0,171	0,071
550	2,3	0,85	0,171	0,4
645	2,26	0,98	0,15	0,175
1150	2,2	0,98	0,14	0,175

Предложенный способ оценки амплитуды колебаний кварцевого резонатора ограничивается условием отсутствия в спектре сигнала боковых компонент высших порядков. При условии $m \leq 0{,}1$ и λ = 650 нм амплитуда колебания кварцевого резонатора не должна превышать 5 нм, что соответствует колебаниям поверхности прецизионных кварцевых резонато-

ров. При индексе фазовой модуляции $m > 0{,}1$ наряду с основной парой боковых гармоник появляются высшие спектральные компоненты, что не позволяет применять данный способ обработки выходного сигнала.

Список используемых источников

1. Lepetaev A. N., Khomenko I. V., Kosykh A. V. Numerically-analytical calculation method for vibration amplitude distributions of inharmonic modes of double rotated cuts thickness-shear resonators // Proceedings of 2007 IEEE Ultrasonics Symposium. New York : Institute of Electrical and Electronics Engineers. 2007. PP. 1393–1396.

2. Хоменко И. В. Результаты исследования термостатированного кварцевого генератора с двухмодовым возбуждением резонатора ТД-среза на численно-аналитической модели // Омский научный вестник. 2008. N 3 (70). С. 115–121

3. Vig, J. R. Quartz crystal resonators and oscillators. For frequency control and timing applications : A tutorial. USA, NS : Development & Engineering Center Fort Monmouth, 2000. 493 p

4. Ложников А. О., Ермоленко С. В. Исследование спектра колебаний кварцевых резонаторов двухповоротных срезов с улучшенной моночастотностью // Техника радиосвязи : Научн.-техн. сб. 2016. Вып. 2 (29). С. 101–108.

5. Вороховский Я. Л., Молоток В. В., Клудзин В. В., Пресленев Л. Н. Измерение амплитуды упругих смещений кварцевого резонатора // Информационно-управляющие системы. 2009. N 6. С. 63–66.

6. Whitman R. L., Laub L. J., Bates W. J. Acoustic surface displacements on a wedge-shaped transducer using an optical probe technique // IEEE Transactions on Sonics and ultrasonics. 1968. Vol. 15. PP. 186–189.

7. Базыкин С. Н. Информационно-измерительные системы для измерения линейных перемещений // Современные наукоемкие технологии. 2016. N 9. С. 373–377.

8. Физические свойства парателлурита [Электронный ресурс]. URL: http://acousto-optics.phys.msu.ru/page-TeO2-ru.html (дата обращения 21.12.2022).

9. Золотарев В. М., Морозов В. Н., Смирнова Е. В. Оптические постоянные природных и технических сред: справочник. Л. : Химия. Ленинградское отделение, 1984. 214 с.

УДК 004.451.24
ГРНТИ 81.93.29

ВНЕДРЕНИЕ МЕХАНИЗМОВ КОНТЕЙНИРИЗАЦИИ В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. А. Кравцова, А. С. Учинин, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире быстро развивающихся технологий механизмы виртуализации приобрели важную роль среди компьютерных технологий. С понятием виртуализа-

ции неразрывно связано технология контейнеризации. Актуальность применения контейнеризации объясняется оптимизацией работы и тестирования приложения, быстротой их масштабирования и развертывания. Цель статьи заключается в описании механизма контейнеризации, его работы и особенностях, методах защиты контейнеров.

контейнеризация, виртуализация, Linux, Astra Linux, Docker, cgroups, namespaces.

Введение

Контейнеризация – метод виртуализации, при котором возможна поддержка нескольких изолированных экземпляров пространства пользователя, а не одного. Данная технология предотвращает сбои и проблемы связанные с совместимостью различных версий программ, зависимостей и т. д. В рамках контейнеризации рассматривается понятие «контейнер», который подразумевает файлы необходимые для хранения приложений со всеми компонентами. Контейнер индивидуален и автономен.

Основная часть

Понятие контейнеризация

Для того, чтобы понять, что представляет из себя механизм контейнеризации, рассмотрим понятие «виртуализации». База для механизма контейнеризации исходит из виртуализации. Виртуализация представляет собой возможность создания на одном физическом устройстве нескольких вычислительных сред, которые разделяют между собой вычислительные ресурсы данного физического устройства [1]. В свою очередь, контейнеризация и виртуализация имеют ряд отличий:

- Виртуализация – представление на уровне физического оборудования, в то время как контейнеризация – представление на уровне приложения. Другими словами, при виртуализации создается полностью отдельная операционная система. При контейнеризации используется ядро операционной системы той машины, на которой открывается контейнер.
- Контейнеры легче, быстрее разворачиваются, требуют меньше оперативной памяти и мощностей, т. е. менее ресурсоемки [2].

Контейнеризация – это метод виртуализации, который позволяет осуществлять изолированный от основной ОС запуск приложений и содержащий все зависимости, конфигурационные и исполняемые файлы необходимые для работы программы или пользователя, находящегося в контейнере. Контейнеры имеют жизненный цикл – после закрытия контейнера, вся информация внутри него стирается, поэтому для сохранения значимых данных, они выводятся во внешнюю ОС.

Данная технология позволяет изолированно от ОС запускать приложения и разрешать конфликты, которые могут появиться в случае, например,

когда версия ПО или библиотеки не подходит под данную версию программы. Благодаря ей существует возможность транспортировки сред - контейнер упаковывает абсолютно все необходимые данные, которые нужны для запуска, это позволяет легко переносить контейнеры из одних рабочих сред в другие. Контейнеры независимы друг от друга, это значит, что если в одном контейнере возникнет ошибка, то это не повлияет на другой.

Алгоритм внедрения контейнеризации

Linux имеет встроенные механизмы контейнеризации – Namespaces и Cgroups

Linux namespace – это абстракция над ресурсами в операционной системе, обеспечивающая изоляцию процессов друг от друга. Если раньше процессы обращались напрямую к ресурсам, то с появлением namespaces, все запросы проходят через этот дополнительный слой абстракции. В любой данный момент времени любой процесс принадлежит ровно одному экземпляру namespace каждого типа, это обеспечивает независимость пространств имен друг от друга [3].

Существуют следующие пространства имён:

- **Mount** – абстракция над пространством имен для файловых систем. Mount контролирует видимые некоторому процессу точки монтирования, т.е. когда процесс находится внутри какого-то пространства имен, он может видеть только те точки монтирования, которые принадлежат данному пространству [3].
- **Network** – абстракция над сетью, которая позволяет процессу внутри некоего пространства имен видеть сетевые интерфейсы, IP-адреса, таблицы маршрутизации и т. д. Данная абстракция отграничивает сетевые ресурсы хоста, от сетевых ресурсов контейнера, но при этом обеспечивает туннель между разными пространствами сети.
- **IPC** – данная абстракция обеспечивает изоляцию утилит межпроцессного взаимодействия, т.е. процессы из пространства имен IPC изолированы от чтения или записи ресурсов из других пространств имен.
- **PID** – абстракция над пространством номеров процессов обеспечивает изоляцию ID процессов, изоляция дерева системных процессов, что значит, что процессы, принадлежащие разным пространствам имен, могут иметь один и тот же PID.
- **User** – абстракция над пространством пользователей, которая изолирует ID пользователей и групп и служит для отображения UID и GID.
- **UTS** (*UnixTimeSharing*) – абстракция над пространством hostname и NIS. Данная абстракция изолирует имя хоста системы для данного пространства имен, что позволяет контейнерам иметь собственные доменные и контейнерные имена.

Появление такого механизма как Cgroups было связано с решением вопроса ограничения ресурсов для изолированных процессов.

Cgroups – это процессы с наложенной изоляцией вычислительных ресурсов со стороны ядра Linux.

Механизм реализует следующие возможности:

- Ограничение использования физической и виртуальной памяти;
- Расстановка приоритетов групп для выделения разного количества процессорного ресурса и пропускной способности подсистемы ввода-вывода;
- Анализ затрат тех либо иных ресурсов группой;
- Изолированность групп друг от друга таким образом, что одной группе недоступны процессы, сетевые соединения и файлы другой.

Помимо встроенных механизмов контейнеризации существуют также и другие механизмы, не встроенные в систему, но с открытым исходным кодом и возможностью установки и адаптации их к системе. Один из таких механизмов – Docker. Данный механизм позволяет создавать и развертывать контейнеры, автоматизировать их работу, контролировать жизненный цикл. Docker может быть установлен как на Astra Linux Common Edition, так и на Astra Linux Special Edition, но в зависимости от версии – специальной или обычной установка будет отличаться [4].

Astra Linux SE – это ОС, основанная на Astra Linux Common Edition и, кроме того, включающая в себя ряд отличий и доработок, способствующих лучшей защищенности информации [5]. Система изоляции пространств имен приложений Docker в AL SE поддерживает два режима работы:

1. привилегированный режим – контейнерная служба Docker осуществляется с правами суперпользователя (*root*);

2. непривилегированный (*rootless*) режим – контейнерная служба Docker выполняется в пользовательском пространстве имён. При использовании этого режима служба контейнеризации работает как суперпользователь только с точки зрения приложения в контейнере, а служба контейнеризации и контейнеры не получают прав суперпользователя в хостовой ОС.

В Astra Linux защищенность контейнеров обеспечивается мандатным контролем целостности, таким образом дополнительно изолируя контейнеры. В Astra Linux SE Docker представлен как пакет docker.io, его можно установить с помощью менеджера пакетов Synaptic или из командной строки в **привилегированном режиме** командой: sudo apt install docker.io

Для использования Docker в **непривилегированном режиме** в дополнение к пакету docker следует установить пакет rootless-helper-astra:

sudo apt install docker.io rootless-helper-astra

Установка Docker на Astra Linux CE не так тривиальна (табл. 1.).

ТАБЛИЦА 1. Установка Docker на Astra Linux Common Edition

Сначала задаётся пароль пользователя root	sudo passwd
Осуществляем переход в root	sudo su
Устанавливаем необходимые пакеты	apt-get install apt-transport-https ca-certificates curl gnupg-agent software-properties-common -y
Добавляем репозиторий, для этого открываем список репозиториев и вносим репозиторий	nano /etc/apt/sources.list deb[arch=amd64] https://download.docker.com/linux/debian stretch stable
Добавляем ключ репозитория	curl -fsSL https://download.docker.com/linux/debian/gpg sudo apt-key add -
Обновляем пакеты	apt-get update
Устанавливаем Докер	apt-get install docker-ce docker-ce-cli containerd.io -y

Помимо этого, для того, чтобы защитить контейнеры в механизме Docker, нужно учесть следующие характеристики:

- **Квоты ресурсов** – позволяют оптимизировать и ограничить объем ресурсов памяти и ЦП, доступных для контейнера.
- **Риск получения несанкционированного доступа** при запуске от имени root. В данном случае стоит придерживаться принципа наименьших привилегий, т. е. пользователю изначально предоставляется минимальный доступ. Именно поэтому в Docker не прописан запуск по умолчанию от имени root.
- **Безопасность реестров**. В данном случае можно использовать межсетевой экран или контролировать доступ на основе ролей.

Заключение

В связи с рассмотренными выше механизмами контейнеризации, можно сказать, что контейнеризация является весьма удобным методом изолированной отладки и тестирования приложений, при котором влияния на основную систему оказано не будет, ввиду того, что все необходимый компоненты (код, библиотеки, системные инструменты и т. д.) пакуются в один образ в контейнере, данный контейнер изолируется от всех других контейнеров и не влияет на их работу в случае возникновения ошибок.

Список используемых источников

1. Багомедова А. Р., Ушаков И. А., Цветков А. Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 58–63.

2. Суворов А. М., Цветков А. Ю. Исследование атак типа переполнение буфера в 64-х разрядных Unix подобных операционных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании 2018. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2018. СПб. : СПбГУТ, 2018. С. 570-573.

3. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы. Ч. 1. СПб. : СПбГУТ, 2015. 62 с.

4. Таргонская А. И., Цветков А. Ю. Разработка защищенного веб-интерфейса для управления устройствами в сети // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 734–739.

5. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 657–662.

УДК 004.056
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ БОЛЬШИХ ДАННЫХ

В. А. Кравцова, И. А. Ушаков
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Методы совершения кибератак становятся более сложными с каждым днем. Варианты защиты, разработанные на основании сигнатур, становятся ненадёжны. Решения для обнаружения аномалий поведения в сети отслеживают корпоративные сети на предмет аномального поведения, чтобы обнаруживать новые угрозы и своевременно принимать меры. Большой объем вычислений и постоянные изменения в распределении сетевых данных усложняют анализ данных и обнаружение аномального поведения внутри них. Из этого можно сделать вывод, что решения для работы с большими данными стали неотъемлемой частью работы по осуществлению защиты информации. В этой статье будут рассмотрены исследования аномалий сетевого трафика с использованием больших данных.

аномалии, вторжение, большие данные, нейронные сети.

Введение

Огромный объем информации, с которым работает каждый пользователь сети, вынуждает искать новые подходы к построению защищенной инфраструктуры. Для описания процесса обработки и хранения структурированных и неструктурированных записей о всех событиях, происходящих

в системе, используется термин Большие Данные (БД). БД могут использоваться для анализа и выявление аномалий в сетевом трафике. При работе с БД следует учитывать вариативность нормы с течением времени (*novelty anomaly*) [1]. Для различных систем понятия нормы и аномалии будут разниться, поэтому модель базового поведения системы необходимо разрабатывать индивидуально, учитывая взаимодействия ее элементов.

Основная часть

Большие данные часто классифицируют по пяти измерениям (рис. 1).

Рис. 1. Измерения больших данных

Только путем анализа всех больших данных могут быть достигнуты точные и своевременные знания, необходимые для предоставления качественных решений. Преимуществами использования средств обнаружения аномалий в сетевом трафике на основании больших данных являются отсутствие необходимости постоянного контроля со стороны человека и распознавание раннее неизвестных комплексных атак. Вовремя обнаруженные сбои или уязвимости системы смогут быть быстро решены и уберегут организацию от крупных финансовых потерь.

Сложность работы с аномалиями в сетевом трафике обуславливается тем, что злоумышленники могут маскировать атаки, предполагая, как

должна выглядеть базовая модель поведения системы. Наличие шума в данных может быть распознано как аномалия, однако таковым являться не будет, что приведет к ложному срабатыванию системы.

При работе с БД все аномалии можно разделить на несколько типов (рис. 2):

- точечные аномалии, выражающиеся резким всплеском на фоне остальных данных.
- контекстные аномалии, когда при неравномерном распределении данных выявляются атрибуты, которые сигнализируют об отклонении от гибкой нормы.
- групповая аномалия, когда в единичных, отличающихся от нормы, данных можно рассмотреть взаимосвязь [2].

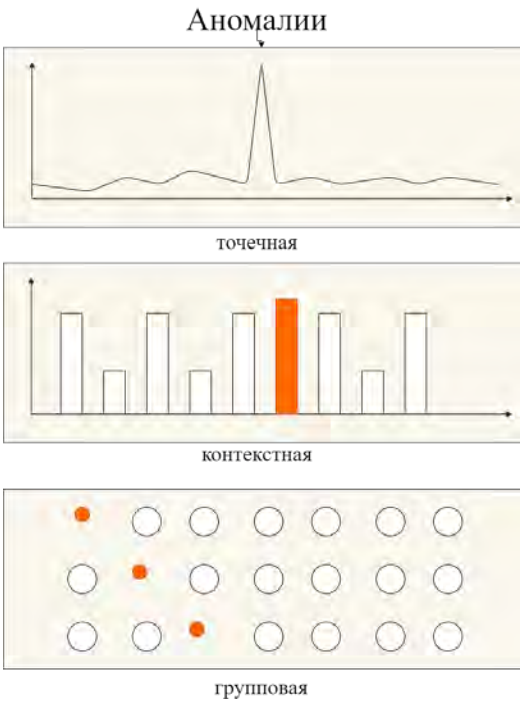


Рис. 2. Типы аномалий

Существует несколько подходов к обучению системы обнаружения аномалий на основе машинного обучения: с учителем, частично с учителем, без учителя. Основное различие между этими подходами заключается в использовании помеченных наборов данных. Обучение с учителем использует помеченные входные и выходные данные, а алгоритм обучения без учителя – нет.

Для наиболее успешной идентификации сетевых событий при разработке модели обнаружения необходимо учесть IP-адреса, порты, протокол, объем переданных данных. Далее собранные события можно либо использовать для обучения нейронной сети, либо объединить одним из методов машинного обучения для отнесения их к инцидентам информационной безопасности. Здесь могут использоваться такие методы как метод реконструкции, вероятностный метод, метод кластеризации, метод расстояния и плотности.

1. Вероятностный метод основан на определенных вероятностных предположениях о возникновении событий. Точки оцениваются по отношению к их распределению вероятностей. Экземпляры с очень низкой вероятностью идентифицируются как аномалии.

2. Метод расстояния и плотности оценивает точки по отношению к окружающей их среде. Если в области вокруг одной точки достаточно похожих точек, они оцениваются как обычные. Это сходство данных обычно

представлено расстоянием между точками данных. Алгоритм *k*-ближайших соседей работает по этому принципу.

3. Метод кластеризации осуществляет группировку похожих объектов и структур. Экземпляры разбиты на группы таким образом, чтобы данные внутри группы были максимально похожи, но данные разных разделов максимально отличались друг от друга. Экземпляры, которые не могут быть отнесены ни к одной группе, классифицируются как аномалии.

4. Метод реконструкции пытается обнаружить закономерности в данных, чтобы иметь возможность восстановить сигнал без шума. Известными алгоритмами, принадлежащими к этим методам, являются анализ основных компонентов (PCA) и репликаторные нейронные сети (RNN).

При использовании одного из методов машинного обучения модель обнаружения аномалий становится более устойчивой, чем при модели на основе нейронных сетей, которая может быть не готова к серьезным отклонениям от обучающих данных.

Можно выделить несколько методов распознавания аномалий, такие как классификация, когда реализация данного метода основана на предположении о том, что нормальное поведение системы может определяться одним или несколькими классами. Таким образом, экземпляр, не принадлежащий ни к одному из классов, является отклонением. Поиск аномалий проходит в два этапа: обучение и распознавание. Классификатор обучается на массиве маркированных данных, далее определяется принадлежность к одному из известных классов. В противном случае экземпляр помечается, как аномалия [3].

Статистический анализ. При использовании этого подхода исследуется процесс, строится его профиль (модель), который затем сравнивается с реальным поведением. Если разница в реальном и предполагаем поведении системы выше установленного порога, делается вывод о наличии отклонений.

Спектральные методы находят аппроксимацию данных, используя комбинацию атрибутов, которые передают большую часть вариативности в данных.

В таблице 1 рассмотрено сравнение методов распознавания аномалий.

ТАБЛИЦА 1. Методы распознавания аномалий

Метод	Результат	Режим распознавания	Работа без предварительного обучения
Классификация	Метка	С учителем, частично с учителем	Нет
Кластеризация	Метка	С учителем, частично с учителем	Нет

Метод	Результат	Режим распознавания	Работа без предварительного обучения
Статистический анализ	Степень	Частично с учителем	Нет
Метод расстояния и плотности	Степень	Без учителя	Да
Спектральные методы	Метка	Без учителя, частично с учителем	Да

Заключение

Поскольку утечка данных представляет значительный риск для соблюдения требований, многие организации используют детектор аномалий как часть своей стратегии обеспечения соответствия требованиям. Требования соответствия SOC 2 включают инструменты обнаружения аномалий безопасности как жизненно важный элемент операций по обеспечению безопасности. Модели обнаружения аномалий могут отслеживать текущие успехи мер безопасности и обеспечивать безопасное хранение, доступ и перемещение данных. Кроме того, эти типы средств обнаружения аномалий используют журналы и предлагают возможности создания отчетов для демонстрации аномалий данных во время аудитов безопасности. Это снижает риск нарушения нормативных требований и законов о конфиденциальности данных.

Проект реализуется победителем грантового конкурса для преподавателей магистратуры 2021/2022 Стипендиальной программы Владимира Потанина, номер договора ГСГК-049/22 от 26.05.2022.

Список используемых источников

1. Ушаков И. А., Исмоилов Ф. Х., Фёдорова А. Э., Манкаев Р. М., Деркач А. Ю. Обнаружение аномалий в сетевом трафике, используя методы машинного обучения // Актуальные вопросы современной науки и образования : сб. ст. XX Международной научно-практической конференции. В 2-х ч. Пенза, 20 июня 2022 года. Часть 1. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 96–98.

2. Terzi D. S., Terzi R. and Sagiroglu S. "Big data analytics for network anomaly detection from netflow data" // 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey. 2017. PP. 592–597.

3. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. N 2 (45). С. 207–243.

УДК 004.624
ГРНТИ 81.93.29

ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ СЕТЕВЫХ СОЕДИНЕНИЙ НА ОСНОВЕ ОТЕЧЕСТВЕННОГО ОБОРУДОВАНИЯ

В. А. Кравцова, И. А. Ушаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

VPN-соединения необходимы не только для удалённой работы и анонимизации трафика, но и для организации зашифрованного обмена данными в рамках широких сетей различных предприятий. Драйверами индустрии VPN-шлюзов будут устройства интернета вещей, технологии 5G. Новыми нишами для средств криптографической защиты могут стать АСУ ТП и предприятия добывающей промышленности. В связи со сложившейся в мире обстановкой также возникает необходимость в использовании для этих целей устройств российского производства.

криптошлюз, VPN, VRRP, туннелирование, IPSEC, IKE.

Цель: Построение VPN-соединения на основе отечественного оборудования.

Задачи:

1. Сравнение криптошлюзов «Инфотекс» и «S-terra CSP».
2. Макетирование VPN-туннеля с помощью программно-аппаратного комплекса российского вендора.

Основная часть

VPN-шлюзы (также криптографические шлюзы, криптошлюзы, криптомаршрутизаторы) – программно-аппаратные комплексы, используемые для криптографической защиты трафика, передаваемого по каналам связи, с помощью шифрования пакетов по различным протоколам.

Согласно опросу издания Anti-malware.ru, крупные компании используют криптографические шлюзы либо для организации удалённого доступа *(Client-to-Site* VPN), либо для построения site-to-site VPN (рис. 1).

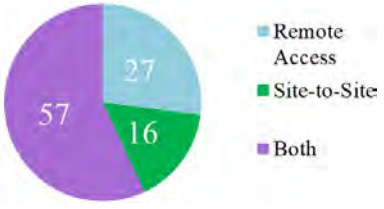


Рис. 1. Использование криптографических шлюзов

Несмотря на то, что для построения обоих типов VPN используются одинаковые программные и программно-аппаратные решения,

между ними есть значительная разница. При Remote-Access устройство удаленного пользователя отвечает за шифрование и расшифровку отправляемых и получаемых данных. VPN формата Site-to-Site обеспечивают безопасное подключение двух или более локальных сетей в разных физических местах. При использовании Site-to-Site VPN криптошлюз одной удаленной локальной сети связывается со шлюзом другой локальной сети (или сети штаб-квартиры) для создания защищенного туннеля [1].

В России основными потребителями криптошлюзов являются государственные учреждения, а также организации, являющиеся операторами персональных данных. Использование криптошлюзов в АСУ ТП обусловлено требованиями к защите информации в подобных системах согласно ФЗ № 187, приказу ФСТЭК № 31. Это позволяет говорить о серьезной перспективе данного направления для производителей СКЗИ в части развития своих продуктов.

Таким образом, можно сделать вывод о необходимости использования криптошлюзов для обеспечения кибербезопасности РФ.

Рассмотрим особенности некоторых отечественных криптошлюзов подробнее. Для сравнения были выбраны продукты компаний «Инфотекс» и «S-terra CSP» (табл. 1) [2].

ТАБЛИЦА 1. Сравнение S-terra GATE и VipNet HW

Параметр	S-terra GATE	VipNet HW
Класс защиты	ФСБ: КС1, КС2, КС3 ФСТЭК: МЭ 4 класса	ФСБ: КС3 ФСТЭК: МЭ 4 класса
Совместимость с другими производителями	поддерживается	не поддерживается
ОС	Debian GNU/Linux 9	Windows, ОС Linux
Поддерживаемые ГОСТ	ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015	ГОСТ 34.12-2015. ГОСТ 34.13-2015.
Мониторинг доступности удаленного узла	Dead Peer Detection (DPD) протокол	Не поддерживается на сертифицированной версии
Способ получения ключевой пары	Генерация с помощью утилит криптопровайдера, входящих в состав продукта, с выдачей CER Генерация внешним PKI сервисом с доставкой на сменных ключевых носителях Генерация внешним PKI сервисом с доставкой через PKSC#12 (RSA)	Генерация с помощью утилит криптопровайдера, входящих в состав продукта, с выдачей CER В процессе создания пользователей ViPNet

Параметр	S-terra GATE	VipNet HW
Интеграция с СОВ	ПК «С-Терра СОВ. Версия 4.3»	Внедрение СОВ в версии HW5
Отказоустойчивость и балансировка нагрузки	VRRP RRI	VRRP

Таким образом, С-Терра шлюз выгодно выделяется на отечественном рынке, потому, можно перейти к реализации практической части с применением криптошлюза С-Терра Шлюз 4.3 [3].

В соответствии с целью была разработана следующая схема (рис. 2).

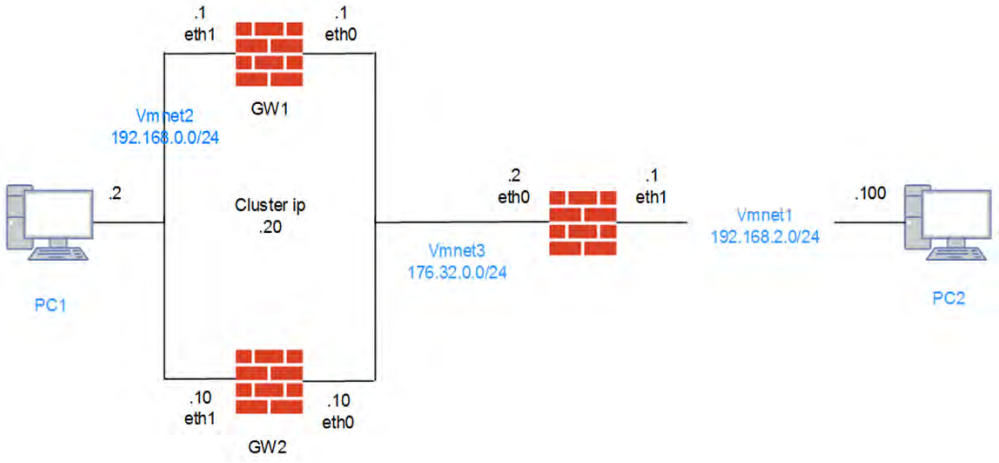


Рис. 2. Схема стенда

Из шаблона виртуальной машины (ВМ) устанавливаются 3 шлюза безопасности. Добавляются сетевые интерфейсы перед импортированием (*VMnet*). На каждом шлюзе при первом включении проводится обновление карты интерфейсов. Далее шлюз инициализируется командой initialize. Эта процедура включает настройку генератора случайных чисел для получения более сложного ключа безопасности, а также ввод лицензии продукта. Инициализация завершается запуском IPsec демона, иногда требуется перезагрузка. Настраиваются интерфейсы согласно схемы, работа протокола VRRP: приоритет шлюзов, таймер информационных пакетов и маршрут по умолчанию. В качестве маршрута по умолчанию используется внешний IP адрес соседнего шлюза.

Настройка VPN-туннеля начинается с задания параметров протокола IKE: шифрование, хэш-функция шифрования и способ аутентификации. Указывается набор преобразований для IPsec. Описывается трафик, который планируется защищать, подсети клиентских устройств. Создаются криптографические карты, access-листы.

Для работы туннеля необходимо загрузить сертификаты. Создается запрос на локальный сертификат, добавляется запрос на удостоверяющий центр по ссылке https://www.cryptopro.ru/certsrv/certrqxt.asp. Полученные сертификаты (корневой и локальный) доставляются на шлюз и импортируются в базу продукта. Проверка списка отозванных сертификатов отключается, без этого сертификаты на шлюзе будут не активны.

На данном этапе конфигурация VPN-туннеля, а также отказоустойчивого кластера завершена.

Заключение

Проверка на GW3, что соединение идет через GW1 (рис. 3).

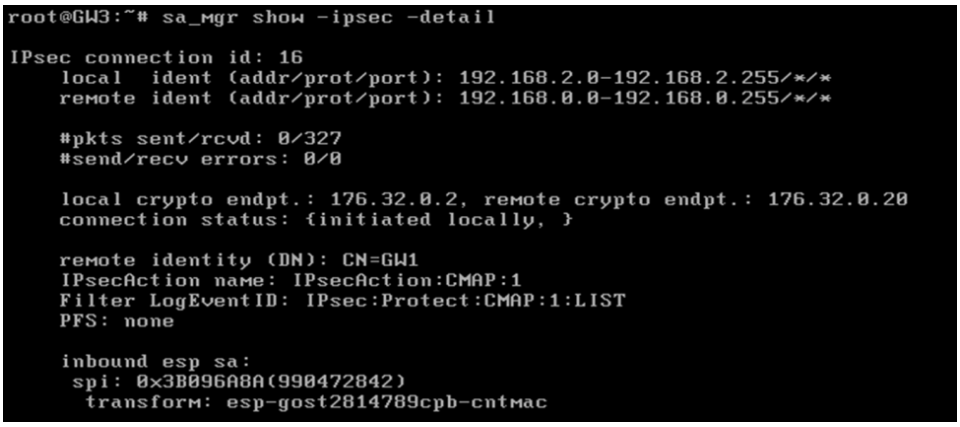


Рис. 3. Проверка IPsec туннеля, вывод детальной информации

Создание трафика между конечными устройствами и отключение GW1 (рис. 4).

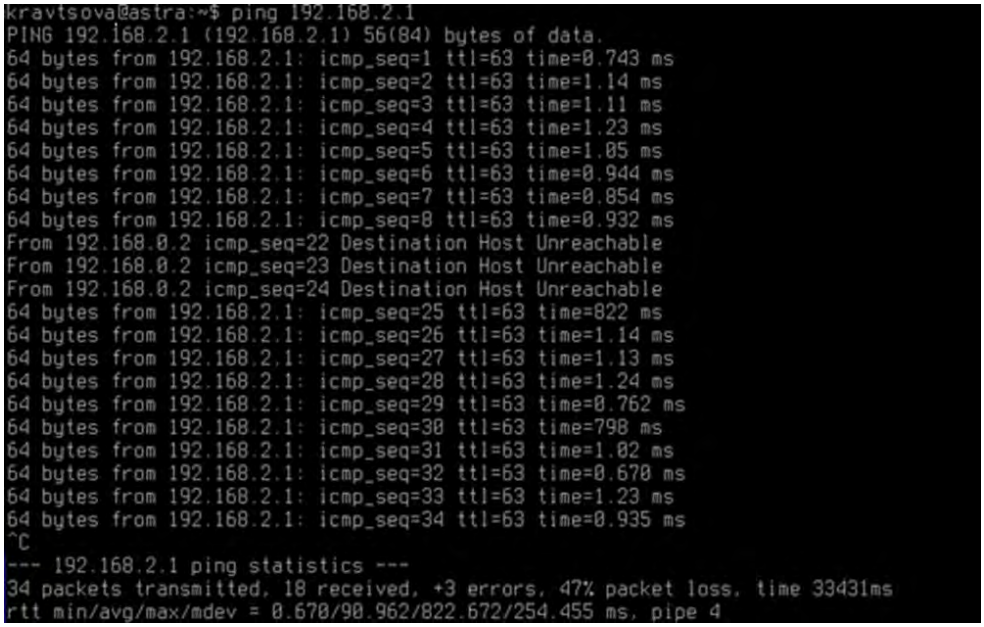


Рис. 4. Генерация трафика между устройствами внутри туннеля VPN

В результате видно, что за время переключения на резервную ноду было потеряно 16 пакетов. Просмотр того, что соединение идет через GW2 (рис. 5).

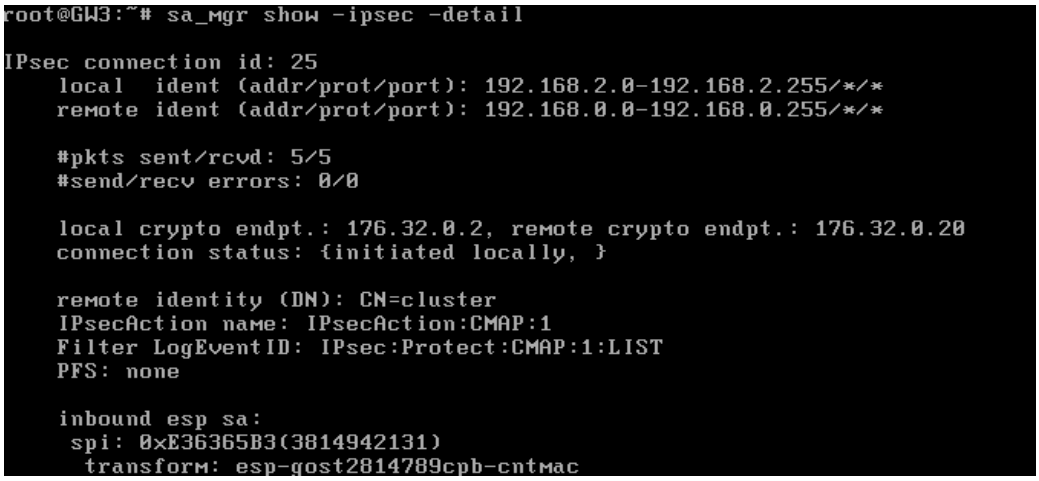


Рис. 5. IPsec туннель построен на кластер, шлюз GW1 выключен

Проверка сертификатов на шлюзах (рис. 6).

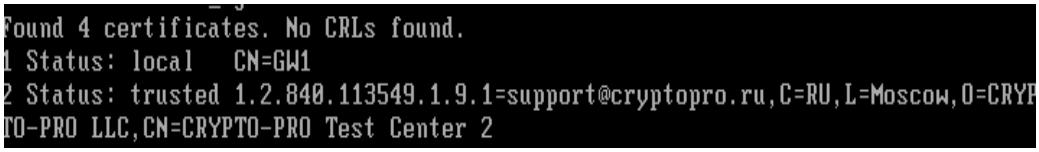


Рис. 6. Сертификаты на шлюзе GW1

Заключение

Интеграция подобного решения на объект КИИ возможна уже в текущий момент, а переход к обязательному импортозамещению с первого января 2025 года согласно «Указу Президента Российской Федерации от 30.03.2022 № 166» пройдёт без проблем с организацией инфраструктуры.

Список используемых источников

1. Лоханько Н. О., Ушаков И. А., Чехутский В. С. Использование Openflow как решения для поставщиков услуг VPN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х томах, СПб. : СПбГУТ, 2018. Т.1. С. 578–581.

2. ViPNet Coordinator HW [Электронный ресурс] // ViPNet. 2023. URL: https://infotecs.ru/product/setevye-komponenty/vipnet-coordinator-hw/ (дата обращения 01.03.2023)

3. С-Терра Шлюз 4.3 [Электронный ресурс] // С-Терра. 2023. URL: https://www.netacad.com/ru/courses/packet-tracer (дата обращения 26.02.2023)

УДК 004.772
ГРНТИ 49.38.49

СЕТЕВАЯ СТЕГАНОГРАФИЯ НА ОСНОВЕ ФОНТАННЫХ КОДОВ

А. В. Красов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе представляется метод создания стеганографического канала при помощи фонтанного кода. Фонтанный код используется для передачи широковещательного трафика в каналах с неизвестным уровнем потерь. Поскольку при потере несущего пакета теряются и части секретного сообщения, надежная передача обеспечивается за счет использования второго фонтанного кода. Таким образом возможно создавать многоуровневые стеганографические каналы, которые могут быть использованы в широковещательных сетях. Данный метод открывает возможность обхода систем эшелонированной защиты, а также может быть использован для доставки секретных сообщений группе лиц.

сетевая стеганография, фонтанный код, канал скрытого хранения данных в сети, многоуровневая стеганография.

В настоящее время отрасль информационной безопасности становится все более значимой в мире. Множество личных данных, данные предприятий и корпораций, прочая информация – все это находится в сети. Техника стеганографии предполагает сокрытие секретной информации в обычном, не секретном файле или сообщении так, чтобы она не была обнаружена. Затем секретная информация извлекается из обычного файла или сообщения в месте назначения, что позволяет избежать обнаружения. Стеганография – это дополнительный шаг, который можно использовать вместе с шифрованием для сокрытия или защиты данных.

Фонтанные коды [1] используются для кодирования и передачи пакетов в ненадежных сетях. Принцип их работы заключается в названии: на основе исходного файла генерируется огромное множество закодированных блоков, которые “бьют в сеть”, как фонтан. Плюсом данного метода являются низкие накладные расходы, так как для передачи (или хранения) фиксированного набора из p исходных пакетов одинакового размера по каналу с заметной потерей пакетов исходные пакеты кодируются путем объединения данных пакетов в невероятно бесконечное количество кодированных пакетов, а приемник декодирует кодированные пакеты в исходные пакеты. Кодирование осуществляется таким образом, что из любого p (или чуть

больше) закодированных пакетов можно полностью восстановить набор исходных пакетов. Таким образом, нет необходимости в канале управления от получателя к отправителю для пакетов подтверждения.

Поскольку беспроводные сенсорные сети используются также для работы с конфиденциальными данными, злоумышленник может быть заинтересован в компрометации одного узла (или нескольких) и утечке некоторых данных. Типичным средством для этого является использование стеганографического канала в коммуникации сенсорного узла с узлом сети [2]. В данном случае представляется канал, который скрывается в LT-коде [3] в качестве конкретной реализации фонтанного кода. Тайный канал использует паттерн случайного состояния/модуляции [4] для введения скрытых данных. Поскольку на него будет влиять потеря пакетов в несущей сети, он должен использовать некоторые средства для учета этого. Это, в свою очередь, открывает интересную возможность для многоуровневой стеганографии [4], поскольку второй канал скрытия может быть использован в этом фонтанном коде. Так как многоуровневая схема является однородной, существуют только практические ограничения на количество уровней, т. е. пропускная способность в определенный момент будет слишком мала для реализации дополнительного скрытого канала с фонтанным кодом.

Примером работы является следующее. Предположим, что отправитель хочет передать набор из p исходных пакетов pi, где $i \in P$, при $|P| = p$ (для упрощения вводится, что $P = \{0,1, ..., p - 1)$. Все пакеты являются битовыми строками одинакового размера. Отправитель кодирует исходные пакеты в последовательность кодированных пакетов следующим образом. Для кодированного пакета ej выбирается степень j в соответствии с распределением степеней $\Omega(d)$. Затем, подмножество $Dj \subseteq P$ размера $|Dj| = dj$ выбирается случайным образом (все p подмножества размера dj равновероятны). Закодированный пакет содержит данные $i \in Dj\ pi$, побитовое или поразрядное представление данных исходного пакета, плюс представление подмножества Dj. Декодер знает количество исходных пакетов, которые должны быть переданы. Получив закодированный пакет ej с подмножеством Dj, приемник выполняет следующие шаги [5]:

- Шаг 1: Приемник сохраняет пакет ej, если он еще не видел этот пакет ранее, т.е. если приемник еще не хранил пакет ej' с подмножеством $Dj' = Dj$;
- Шаг 2: Приемник проверяет, есть ли у него уже закодированный пакет ej' с Dj', где Dj' и Dj отличаются только одним элементом $\{k\}$;
- Шаг 3: если пакет есть, то исходный пакет pk может быть восстановлен путем объединения данных $i \in Dj\ pi$ и $i \in D'\ pi$ из разных закодированных пакетов, так как $pi \oplus pi = 0$. Продолжаем cpk (закодированным подмножеством размера 1) с шага 1;
- Шаг 4: Приемник проверяет, может ли он генерировать новые закодированные пакеты из ej и пакетов, которые он сохранил, так, чтобы степень

нового пакета была ниже, чем степень пакетов, из которых он произошел. Для каждого нового сгенерированного пакета приемник снова начинает с шага 1.

Декодер останавливается, если все исходные пакеты были восстановлены, то есть после получения (1 + ϵ) p пакетов с очень высокой вероятностью, для подходящего распределения степеней Ω. Подробнее о реализации декодера см., например, [5].

Для представления подмножества *Dj* можно использовать любой битовый вектор длины *p*, где бит *i* установлен тогда и только тогда, когда $i \in Dj$. Это представление обозначается как BV. В качестве альтернативы, степень *j* может быть передана как двоичное число в log *p* бит1, и подмножество может быть представлено в явном виде. Либо индекс *i* каждого элемента $i \in Dj$ передается в виде двоичного числа, что дает максимум -log2 *p* бит (обозначается как SUB), где *dmax* – максимальная возможная степень. Альтернативно, подходящий набор подмножеств размера *dj* может быть передан в виде двоичного числа (обозначается как ENUM), что дает $\log 2\ dj \le (p \log 2\ p)/2$ бит, т. к. в качестве альтернативы, подходящее подмножество подмножеств размера *dj* можно передать в виде двоичного числа (обозначается как ENUM), в результате чего потребуется $\log 2\ dj \le (p \log 2\ p)/2$ бит, так как $dj \le p/2 < (p/2)p/2$. Обратите внимание, что это ограничение не является жестким. Например, 64 ≈ 1,83 − 1018 < 265, в то время как 3232 = 2160. Более того, если максимальная степень меньше, чем *p*/2, то количество необходимых битов еще меньше. Наконец, все $sp = d \in D\ p$ возможных подмножеств можно перечислить в виде двоичного числа (обозначаемого как ENUMALL) в диапазоне от 0 до *sp* − 1, т. е. с log2 *sp* бит, где *D* – множество возможных степеней.

Выбор представления зависит от обстоятельств. Если сами исходные пакеты велики по сравнению с их числом *p*, например, более 1 000 бит для *p* = 64, то даже хранилище битов *p* log *p* перед отправкой *Dj* кажется небольшими накладными расходами. Однако, если каждый *pi* состоит только из 128 бит, то накладные расходы в 64 бита будут большими. Например, для p = 64 и SUB каждое поле имеет ширину log *p* = 6 бит, за исключением поля степени, которое имеет log (1 + log *p*) = 3 бита. Для ENUM ширина поля индекса равна log 64 = 61 бит, так как большинство подмножеств имеют степень = 32. Смещение 1,956 для ENUMALL с *p* = 16 является суммой *d* = 1,2,4 16. Также вводится новый тип представления числа *Dj*, которое немного больше предыдущих, но обладает дополнительным свойством: если подмножества каждой степени выбраны равновероятными, то все представления множеств *Dj* равновероятны.

Предполагается, что дан LT-код со степенным распределением Ω, выбирающий степень $d \in D$ с вероятностью ρ(*d*), где $D = \{d1, \ldots, d|D|\}$ – мно-

жество возможных степеней *d*, *withd*1 < *d*2 <- - - < *d*|*D*||. Тогда число возможных подмножеств размера d из множества *P* пакетов с размером *p* = |*P*| равно *nd* = *P*/*d*. Предполагается репрезентация ENUM, т. е. степень дается в виде двоичного числа с log2 |*D*| бит, а используемое подмножество задается в виде числа в диапазоне 0 и *d* − 1 в двоичном представлении с log2 *dp* бит – если мы *as-sumed*|*D*| ≤ *p*/2, то это максимальный размер, а подмножества имеют одинаковую длину. Если подмножества одной степени выбираются случайно, независимо и с равными вероятностями, то можно заменить показатели подмножества одной степени на зашифрованное содержимое секретного сообщения. В блочном шифровании обычно используется фиксированное количество битов, поэтому используется только одна степень∗. Поскольку степени не равны 2, можно либо использовать блочное шифрование для близкой степени 2, либо интерпретировать все зашифрованное секретное сообщение как число в степени *n*/*d*. Если оригинальное сообщение может быть восстановлено из любых *p* (1 + ϵ) полученных пакетов, то в среднем ρ(*d*∗) из них будут иметь степень∗ и, таким образом, нести часть секретного сообщения. Следовательно, необходимо выбрать длину секретного сообщения, которая должна быть выбрана соответствующим образом, чтобы требовалось меньше пакетов, и секретное сообщение должно быть способно справиться с потерей пакетов. Последнее может быть достигнуто путем кодирования секретного сообщения LT-кодом. Однако, поскольку закодированное секретное сообщение должно выглядеть случайным, используемый LT-код должен использовать представление, которое также выглядит случайным. В дополнение к выбранному∗ требуется определить общее количество полезных битов в пакете. Для каждого пакета с вырожденным значением∗ можно использовать log *n* ∗ битов, и такие пакеты появляются с вероятностью ρ(*d*∗). Можно попытаться максимизировать произведение ρ(*d*∗) – log *nd*∗; во многих случаях *d*∗ может быть |*D*|, т. е. высшей степенью, но вероятность ρ(*d*) будет очень низкой. Если начать с *p* = 64 и представления ENUM, можно выбрать *d*∗ = 4, так что можно использовать секретное сообщение из 16 пакетов, поскольку ρ (4) > 0,25, и иметь 19 бит на пакет, включая пространство для LT-кодирования. Для такого кодирования используется вариант ENUMALL с интегральными коэффициентами *f,* так что каждое подмножество степени имеет *f* представлений, в результате чего в *n*∗ = *fd* – *nd* и *n*∗ = *d* ∈ *D n*∗, такое, что *n*∗ /*n*∗ ≈ ρ(*d*). Для кодирования в 18 бит значения ρ(*d*) будут соблюдены еще более точно. Поскольку у нас есть 19 битов на пакет секретного сообщения, 3 бита остается для полезной нагрузки, так что всего в секретном сообщении может быть 48 бит. В этом втором LT-коде можно реализовать скрытый канал с *p* = 8, защищенный третьим LT-кодом с репрезентацией ENUMALL (перечисление всех подмножеств в диапазоне от 0 до *d* ∈ *D p*), которому требуется 12 бит, т. е. 4 бита

остаются в качестве полезной нагрузки в каждом пакете, так что общий размер сообщения для этого второго скрытого канала составляет 32 бита.

Таким образом, данный подход представляет собой пример многоуровневой стеганографии [6] и даже допускает более двух уровней. Максимальная вложенность ограничена только уменьшением размера: LT-кодирование на каждом уровне равно размеру пакета на следующем уровне, и таким образом размеры пакетов уменьшаются от уровня к уровню. Однако количество пакетов уменьшается только на первом уровне, так как на следующих уровнях может использоваться кодировка, в которой пакеты всех степеней могут использоваться для переноса части секретного сообщения со следующего уровня.

Список используемых источников

1. Байерс Д., Луби М., Митценмахер М., Реге А. Цифровой фонтанный подход к надежному распределению больших объемов данных // Конференция ACM SIGCOMM 1998 по приложениям, технологиям, архитектурам, и протоколы для компьютерных коммуникаций, Ванкувер, 2–4 сент. 1998 г. Т. 28. С. 56–57.

2. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. Wiley-IEEE Press. February 2016. 296 p. ISBN 978-1-118-86169-1.

3. Штеффен В., Себастьян З., Бернхард Ф., Кристиан Х. Обзор и классификация техник сетевых скрытых каналов на основе паттернов. 2015. 981 с. ISBN 978-0-13-134555-3.

4. Войцех Ф., Войцех М., Щипиорски К. Мультимногоуровневая стеганография: Улучшение скрытой коммуникации в сетях // Журнал универсальной вычислительной техники. 2012. Т. 18. N. 14. С. 1967-1986.

5. Вейвей Л., Гуанцзе Л., Цзянтао Ж., Ювей Д., Дипак Г. Проектирование аналоговых перьевых каналов синхронизации: необнаруживаемость, устойчивость и адаптация к моделям // IEEE Transactions on Information Forensics and Security. 2016. Т. 11. N 4. С. 677–690.

УДК 654.154.6
ГРНТИ 49.39.33

ИСПОЛЬЗОВАНИЕ IP УАТС АГАТ CU В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

А. В. Красов, А. В. Поляничева, А. И. Сафина

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с нынешней политической обстановкой и действующих санкций необходимость импортозамещения в России становится все более актуальной. На российском

рынке существует несколько производителей отечественного оборудования, такие как «Eltex», «Агат РТ», «Мультиком», и др. В рамках данной работы подробно рассматривается программная IP-АТС Агат CU.

IP-телефония, IP-АТС, телекоммуникационное оборудование, импортозамещение.

Введение

Российский рынок телекоммуникационного оборудования в последние годы стремительно развивается. Однако в связи с текущей политической ситуацией и действующими санкциями необходимость импортозамещения в России становится все более актуальной.

Основное внимание в данной статье уделено программным IP-АТС, которые являются важнейшим компонентом современных телекоммуникационных систем. Программная IP-АТС – это телефонная система, которая использует программное обеспечение, работающее на компьютере, для управления входящими и исходящими вызовами. Это экономически эффективное и гибкое решение, которое может быть настроено в соответствии с потребностями различных предприятий [1].

В данной статье подробно рассматривается профессиональная телекоммуникационная платформа – IP УАТС Агат CU, которая объединяет в одном устройстве АТС, запись разговоров и голосовое оповещение [2].

Применение

IP-АТС – это универсальная коммуникационная система, которая может использоваться в широком спектре сфер, включая:

– Малый и средний бизнес: IP-АТС является идеальной коммуникационной системой для малых и средних предприятий, которым необходимо экономически эффективное и масштабируемое решение для удовлетворения их коммуникационных потребностей. Она может использоваться для управления входящими и исходящими вызовами, а также для управления голосовой почтой и другими функциями.

– Центры обработки вызовов: IP-АТС также подходит для центров обработки вызовов, поскольку она предлагает такие передовые функции, как автоматическое распределение вызовов, запись разговоров и голосовое уведомление. Эти функции помогают операторам call-центров более эффективно и результативно управлять своей коммуникационной инфраструктурой.

– Здравоохранение: также IP-АТС может использоваться в учреждениях здравоохранения, таких как больницы и клиники. Она может использоваться для управления входящими и исходящими вызовами, а также для управления голосовой почтой и другими функциями. Кроме того, функция записи вызовов может использоваться для обеспечения качества.

– Образовательные учреждения: IP-АТС может также использоваться в образовательных учреждениях, таких как школы и университеты. Она может использоваться для управления входящими и исходящими вызовами, а также для управления голосовой почтой и другими функциями. Кроме того, функция голосового оповещения может использоваться для экстренных уведомлений и объявлений.

Особенности IP УАТС Агат CU и ее сравнение с аналоговыми IP-АТС

На российском рынке существует несколько производителей отечественного оборудования, таких как «Eltex», «Агат РТ», «Мультиком» и др. Эти производители предлагают ряд телекоммуникационного оборудования и услуг, которые предназначены для удовлетворения потребностей предприятий и потребителей на российском рынке.

Одним из основных преимуществ IP УАТС Агат CU перед аналоговыми IP-АТС являются ее расширенные возможности. IP-АТС Агат CU предлагает такие функции, как запись звонков, голосовое уведомление и автоматическое распределение вызовов, которые недоступны на многих аналоговых IP-АТС. Эти функции могут помочь предприятиям более эффективно и результативно управлять своей коммуникационной инфраструктурой.

Еще одним преимуществом IP-АТС Агат CU является ее масштабируемость. IP УАТС Агат CU – это гибкое и масштабируемое решение, которое может расти вместе с предприятием по мере роста его коммуникационных потребностей. А многие аналоговые IP-АТС имеют фиксированное количество телефонных линий и расширений, что может ограничить возможности предприятия по расширению своей коммуникационной инфраструктуры.

С точки зрения безопасности, IP-АТС Агат CU предлагает передовые функции безопасности, такие как шифрование и аутентификация, которые могут помочь защитить коммуникационную инфраструктуру предприятия от взлома и других угроз безопасности. В отличие от них, некоторые аналоговые IP-АТС могут иметь более слабые функции безопасности или не предлагать их вообще.

Кроме того, IP УАТС Агат CU имеет встроенный VPN-сервер, позволяющий создавать защищенные соединения между офисами и удаленными работниками, а также обеспечивать защищенные соединения для удаленного управления [3].

Чтобы лучше проиллюстрировать различия между IP-АТС Агат CU и аналоговыми IP-АТС, ниже приведена сравнительная таблица 1 некоторых ключевых характеристик данных устройств:

ТАБЛИЦА 1. Сравнительная характеристика АГАТ CU-7212ST [4], Eltex SMG-200 [5] и Максиком MXM500P [6]

Характеристика	АГАТ CU-7212ST	Eltex SMG-500	Максиком MXM500P
Емкость	До 2048 IP-абонентов	До 500 IP-абонентов	До 500 IP-абонентов
Количество одновременных VoIp-соединений	До 100	До 100	До 100
VoIP-протоколы	SIP (RFC 2543, 3261, 3262, 3264, 3311, 4028)	SIP, SIP-T/SIP-I H.323	SIP, IAX2, H.323
Определение номера	AOH; Caller ID (CLIP/FSK(ITU-T V.23, Bell 202)); DTMF	AOH, Caller ID	AOH, Caller ID
Голосовое уведомление	+	-	+
Запись разговоров	+	+	-
Автоматическое распределение вызовов	+	+	-
Функционал call-центра	+	+	-
Количество портов FXS/FXO	До 80/80	До 16/16	До 48/80
LAN-порты	2	4	-
E1-порты	До 1	До 4	До 4
Механизмы безопасности	Шифрование, аутентификация, межсетевой экран, контроль доступа	Шифрование, аутентификация, межсетевой экран, контроль доступа	Шифрование, аутентификация, межсетевой экран, контроль доступа
Интеграция со сторонними приложениями	+	-	-

Анализ предоставленных характеристик позволяет сделать вывод о более высокой эффективности IP-АТС АГАТ CU-7212ST по сравнению с ее аналогами от компаний «Eltex» и «Максиком». В частности, емкость АГАТ CU-7212ST позволяет вместить до 2 048 IP-пользователей, в то время как IP-АТС компаний «Eltex» и «Максиком» обладают емкостью до 500

пользователей. Таким образом, АГАТ CU-7212ST является более масштабируемым и подходящим решением для крупных компаний или организаций.

Однако при выборе IP-АТС необходимо учитывать не только емкость и количество пользователей, но также и другие характеристики, такие как надежность, функциональность, стоимость и т.д. Кроме того, необходимо провести более глубокий анализ функциональных возможностей и технических характеристик каждой из рассматриваемых систем для принятия более обоснованного решения.

Выводы

Системы IP-АТС обеспечивают централизованный и эффективный способ управления каналами связи и улучшают взаимодействие между работниками. С ростом спроса на удаленную работу и виртуальное общение потребность в надежной и безопасной системе IP-АТС высока как никогда.

Таким образом, использование систем IP-АТС является необходимым для современной деловой коммуникации, а актуальность импортозамещения в России предоставляет уникальную возможность для отечественных производителей, таких как «Агат РТ», конкурировать на рынке. IP УАТС Агат CU обеспечивает конкурентное преимущество благодаря своим передовым функциям и механизмам безопасности, что делает ее надежным и безопасным коммуникационным решением для бизнеса в России и за ее пределами.

Список используемых источников

1. Обыдёнкин А. И. Автоматизированная система управления корпоративной телефонной сетью предприятия [Электронный ресурс] // Международный научно-исследовательский журнал: электрон. научн. журн. 2013. URL: https://cyberleninka.ru/article/n/avtomatizirovannaya-sistema-upravleniya-korporativnoy-telefonnoy-setyu-predpriyatiya/ (дата обращения 20.03.2023).

2. АТС серии Агат CU. URL: https://www.netwell.ru/products/ats-serii-agat-cu/ (дата обращения 21.03.2023).

3. Коммутационная платформа Агат CU. URL: https://agatrt.ru/telefonizaciya-predpriyatiya/kommutacionnaya-platforma-agat-cu (дата обращения: 21.03.2023).

4. IP-АТС АГАТ CU-7212ST (Standart). URL: https://agatrt.ru/shop/ip-atc/ip-ats-agat-cu7212s-standart/ (дата обращения 23.03.2023).

5. Офисная IP АТС SMG-500. URL: https://eltex-co.ru/catalog/ip-atc/smg-500/ (дата обращения 23.03.2023).

6. Цифровая IP АТС Максиком MXM500P. URL: https://www.multicom.ru/tsifrovaya-ats-mxm500/ (дата обращения 23.03.2023).

УДК 004.772
ГРНТИ 49.38.49

СРАВНЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

А. В. Красов, А. С. Салита

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В связи с постоянно растущими потребностями в конфиденциальности передаваемой информации производится разработка новых алгоритмов шифрования. Однако конфиденциальную передачу информации можно обеспечить и при помощи методов сетевой стеганогрфии. В данной статье сравнивается эффективность одних их самых распространенных методов сетевой стеганографии – это метод вложений в заголовки пакетов, LACK и RSTEG.

сетевые протоколы, транспортные протоколы, сетевой анализ, сетевая безопасность.

В современном мире очень остро стоит вопрос конфиденциальности информации. В отличие от криптографии, при применении стеганографии нет необходимости в лицензировании и согласовании. Также стеганография позволяет сохранить в тайне участников обмена информацией, и наоборот – отследить участников нелегального распространения данных [1].

На данный момент в нашей жизни всё большее значение играют сетевые технологии, передача информации в которых осуществляется при помощи специальных протоколов. Используя протоколы передачи данных, мы можем также скрытно передавать необходимую информацию. Такой метод, объединяющий собой разные способы, получил название «сетевая стеганография» [3].

Большая часть утечек информации происходит изнутри компании благодаря инсайдерам. Для того, чтобы обойти эшелонированную защиту компаний инсайдеры, прибегают к различным методам, в том числе и к сетевой стеганографии. Яркими примерами сетевой стеганографии являются следующие методы: метод вложения в протоколы IPv4, TCP и UDP, Lost Audio Packets Steganography, Retransmission Steganography, метод стеганографии на основе протокола SCTP [2, 4]. Стоит отметить, что все методы при не грамотном использовании влекут за собой резкое увеличение сетевого трафика на интерфейсе, что детектируется многими средствами мониторинга и обеспечения корпоративной безопасности. Крайне сложным является выявление методов, основанных на изменении структуры передачи пакетов таких как LACK или RSTEG, однако говоря о пропускной способности данных методов стоит отметить, что в большинстве случаев она мала.

Метод вложения в поля сетевых протоколов, может быть обнаружен при помощи статистического анализа трафика используя формулы информационной энтропии по Шеннону, критерий Колмогорова-Смирнова и т. п. Также одним из активных методов может приведение их полей к стандартным значениям, однако данный метод ведет к задержкам сетевых пакетов, что крайне нежелательно, а также может привести к потери трафика в случае трафика IP-телефонии и видеоконференций. Вложение данных в большинство протоколов приводит к искажению передаваемой информации. Поэтому в множестве случаев данный метод можно обнаружить в сетях. Из полей протоколов IPV4, TCP и UDP труднее всего обнаружить вложения в поля Identification протокол IPv4, Sequence Number, Acknowledgement Number, Window Size протокола TCP [5]. Поле Identification может быть легко выявлено при помощи статистического анализа, если в сеть приходит небольшое количество фрагментируемых пакетов. Поля Sequence Number, Acknowledgement Number, Window Size влекут за собой потерю данных и могут быть выявлены при помощи статистического анализа общего количества TCP пакетов.

Следовательно все рассмотренные поля имеют риск выявления высокий, кроме полей Identification, Sequence Number, Acknowledgement Number, Window Size, которые имеют риск выявления средний.

Стоит отметить тот факт, что метод стеганографии LACK может быть легко обнаружен путем ухудшения качества связи между двумя пользователями. Также возможно произвести статистический анализ потерянных пакетов в определённой сети. Для этого необходимо реализовать возможность пасивного наблюдения на основе отчётов RTCP о совокупном количестве потерянных пакетов или наблюдением за потоком RTP по номерам пакетов. Из этих показателей можно сделать вывод о применении метода LACK.

Еще одним способом отслеживания метода LACK яаляется активное наблюдение, анализ всех потоков RTP в сети. В данные наблюдения должны быть основаны на полях SSRC: номер очереди и временная метка. Если будут обнаружены «опаздывающие пакеты», то такие пакеты должны быть отброшены, но такой метод будет также отбрасывать пакеты, которые были задержаны по естественным причинам и могут быть использованы, что несомненно приведет к ухудшению качества связи.

Риск выявления данного метода средний, поскольку требует огромное количество ресурсов на анализ данных пакетов, но при постоянном использовании может быть замечен пользователями.

Повторные передачи в IP-сетях – это «естественное явление», поэтому намеренные повторные передачи, введенные RSTEG, нелегко обнаружить, если они поддерживаются на разумном уровне. Одним из возможных методов обнаружения является статистический стеганализ, основанный на ско-

рости повторной передачи в сети. Если для некоторых соединений TCP скорость повторной передачи значительно выше, чем для других, то может быть обнаружено потенциальное использование RSTEG. Такой метод стеганализа включает мониторинг скорости повторной передачи TCP для всех соединений в подсети.

Существует также другое решение, которое упрощает стеганализ RSTEG применительно к протоколу TCP. Предлагаемый метод стеганализа может быть реализован с помощью «пассивного надзирателя» (*Fisk et al. 2002*) [6, 7]. «Пассивный надзиратель» должен иметь возможность отслеживать весь TCP-трафик, и для каждого TCP-соединения он должен хранить отправленные сегменты в течение заданного периода времени, который зависит от таймера повторной передачи, т. е. пассивный надзиратель должен хранить сегмент до тех пор, пока он не будет подтвержден получателем, чтобы дальнейшая ретрансляция не имела смысла. Когда происходит повторная передача, пассивный надзиратель сравнивает первоначально отправленный сегмент с повторно переданным, и, если полезная нагрузка отличается, обнаруживается RSTEG и сегмент отбрасывается. Однако стоит отметить, что при отслеживании всех TCP сессий необходимо огромное количество ресурсов для хранения и анализа информации.

С другой стороны, следует отметить, что на основании результатов, представленных в Stone and Partridge (2000) [8], до 0,09 % (1 из 1100) сегментов TCP могут быть повреждены из-за сетевой доставки. В результате получателю может быть отправлена искаженная копия сегмента. После получения искаженного сегмента проверка выполняется на основе значения в поле контрольной суммы TCP, и отправителю сообщается о необходимости повторной передачи. Таким образом, в этом сценарии исходный и повторно переданный сегменты будут отличаться друг от друга. Возникновение этого эффекта в IP-сетях маскирует использование RSTEG.

Таким образом данный метод имеет низкую вероятность обнаружения, поскольку обнаружение данного метода требует огромных ресурсов, а искажение пакетов в сети маскирует данный метод.

Список используемых источников

1. Салита А. С., Гетьман Е. М., Красов А. В. Стеганографические вложения в протоколах VoIP // Материалы конференции «Технологии информационного общества». 2022. С. 52–54.

2. Волкогонов В. Н., Гетьман Е. М., Салита А. С. Методы и способы создания стеганогрфических вложений в сетевых пакетах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. С. 178–183.

3. Ульянов Н. П., Яворский Я. В., Колесников А. А., Мартыненко В. В. Классификация стеганографии, понятие об отрицаемой стеганографии // Роль и значение науки в обществе и ее влияние на инновационное развитие : сб. ст. Международной научно-

практической конференции, Таганрог, 07 июля 2022 года. Уфа: Общество с ограниченной ответственностью «ОМЕГА САЙНС», 2022. С. 73–76.

4. Роуленд К. Х. Скрытые каналы в пакете протоколов TCP/IP // Первый понедельник. 1997. Вып. 5. С. 250–256.

5. Мердок С. Дж., Льюис С. Встраивание скрытых каналов в TCP/IP. Скрытие информации. 2005. С. 247.

6. Fisk G., Fisk M., Papadopoulos C., Neil J. Eliminating steganography in Internet traffic with active wardens // 5th International Workshop on Information Hiding, Lecture Notes in Computer Science. 2002. N 2578. PP. 18–35.

7. Fisk G, Fisk M., Papadopoulos C., Neil J. Eliminating steganography in Internet traffic with active wardens, 5th International Workshop on Information Hiding // Lect Notes Comput Sci. 20022578. PP. 18–35.

8. Stone J, Partridge C (2000) When the CRC and TCP checksum disagree // In: Proceedings of SIGCOMM 2000.

UDCC 629.12
SCSTI 20.53.01

SOFTWARE TOOLS FOR INFOCOMMUNICATION NETWORKS AND DATA STORAGE SYSTEMS: FUZZY IDENTIFICATION OF VULNERABILITIES

E. Kryukov**a, A. Smirnov,** I. Parashchuk

Military Communications Academy named after Marshal of the Soviet Union S.M. Budyonny

A methodological approach is considered that allows to describe the signs of vulnerabilities in the software of infocommunication networks and data storage networks, which allows to identify threats. A method for solving problems of identification of objects and processes in the conditions of fuzziness of their observed features is proposed. It is based on eliminating the fuzziness of identifying software vulnerabilities, uses fuzzy and linguistic variables when processing fuzzy knowledge about the characteristics of potential vulnerabilities. It is assumed that this will increase the reliability of software security control.

software tools, threats, vulnerabilities, security, infocommunication network, data storage system, fuzzy sets, identification.

Software tools (SWT) of infocommunication networks (ICN) and data storage systems (DSS) in modern conditions are subject to strict requirements for reliability and security. This is due to the rapid development of ICN and DSS, the introduction of a number of advanced technologies into the field of information and telecommunications (wireless and mobile communications, special networks and D2D communications, ubiquitous sensor networks, Internet of Things, IoE, M2M, NGN, BCN, NGI, FutureNetwork, SDN, OpenFlow, FutureWeb networks,

systems of network robotics, etc.), with the ever-increasing complexity of hardware and software solutions aimed at the practical implementation of these technologies, and with the ever-growing capabilities of potential violators to implement vulnerabilities of SWT for ICN and DSS [1, 2].

At the same time, an important role, from the point of view of vulnerabilities and their exploitation by violators in the interests of reducing the security of data circulating in the control circuits of ICN and DSS, is played by the SWT and program interfaces. Being an important component of modern ICN and DSS, SWT are created, as a rule, by symbiosis of various software objects of the software and information environment. Therefore, they require increased attention in terms of meeting the requirements for protection from current threats to the information security of ICN and storage systems.

The specificity of the study of information security mechanisms of communication networks and data storage systems lies both in the uniqueness of the software objects themselves that implement their work, and in the relative novelty of physical and software vulnerabilities inherent in objects of this class – networks and storage systems. Moreover, the emerging new classes of these vulnerabilities are still poorly understood. The experience of protecting SWT for ICN and DSS from violations exploiting these vulnerabilities is small. At the same time, the vast majority of decisions to identify vulnerabilities in the SWT are made under conditions of uncertainty (fuzziness) of the observed data on the signs of such vulnerabilities. That is why, in our opinion, the tasks related to the development of algorithms for fuzzy identification (identification, detection and categorization) of vulnerabilities in the SWT for ICN and DSS are relevant. The tasks of identifying (detecting and categorizing) anomalous data characterizing the attributes ("symptoms") of potential "holes" in the security of SWT for ICN and DSS in the conditions of the fuzziness of the observed signs of such vulnerabilities can be solved on the basis of methods for processing fuzzy sets [3, 4].

At the same time, possible signs of vulnerabilities of SWT for ICN and DSS are described in detail in [5, 6]. With this in mind, identification (detection and categorization) in conditions of fuzziness can be carried out for five main groups (classes) of vaguely defined signs of vulnerabilities of the ICN and DSS: vaguely defined (observed) signs of code vulnerabilities – vulnerabilities that appeared during the development of software for ICN and DSS; vaguely defined signs of vulnerabilities configurations – vulnerabilities that appeared in the process of setting the configuration (configuration) of the ICN and DSS software; vaguely defined signs of vulnerabilities of the architecture of the SWT for ICN and DSS; vaguely defined signs of organizational vulnerabilities that appeared as a result of the absence (lack) of organizational measures to protect the SWT for ICN and DSS, as well as vaguely defined signs of multifactor vulnerabilities that appeared as a result of the presence of a combination of several previously considered threats of the SWT for ICN and storage systems.

Identification of vaguely defined (observed) signs of vulnerabilities of the SWT for ICN and DSS is carried out with the aim of their unambiguous, reliable detection and categorization. In other words, the ultimate goal is to classify threats and vulnerabilities (based on the results of identifying their signs), for example, to a dangerous, not very dangerous or not dangerous category. This is, in fact, a determination of whether these vulnerabilities are critical (with the greatest degree of danger) for SWT for ICN and DSS, or not. Moreover, the degree of danger of a particular type of vulnerability is considered as a kind of comparative measure that characterizes the vulnerability of the SWT to this vulnerability and its impact on the violation of the security properties of data transmitted through ICN channels and processed in the storage systems.

From the point of view of the problem of identification (identification, detection and categorization) of vulnerabilities of SWT for ICN and DSS in the conditions of source data fuzziness, an approach using concepts, methods and algorithms for describing and processing fuzzy sets is proposed. This approach will allow taking into account the subjective factors introduced by the administrator (auditor) of the security of the ICN and DSS when determining the level of criticality (danger) of threats and vulnerabilities of such a class of SWT. The method of identifying vulnerabilities of the SWT for ICN and DSS in the conditions of fuzzy initial data should implement a procedure for processing a large number of vaguely observed signs of such threats and vulnerabilities, as well as rely on opinions, judgments and diverse, fuzzy (most often, expert) knowledge about the degree of negative consequences in case of successful exploitation of such vulnerabilities by potential violators.

The description of vaguely defined identification attributes ("symptoms") of potential "holes" in the security of SWT for ICN and DSS is a formal description of such objects and phenomena with the help of fuzzy sets and consists in determining those signs of vulnerabilities that allow relatively reliably consider these threats and vulnerabilities to belong, for example, to a dangerous, not very dangerous or not dangerous category. This description can be carried out by presenting knowledge about the degree (depth, level) of belonging of vulnerability features to a specific type. At the same time, expert knowledge should be taken into account, which can be presented both in quantitative (numerical variable) and in linguistic form. Expert fuzzy knowledge is applied and processed based on a numerical measure and on the semantic and syntactic meaning of the concepts used by the expert to isolate from the whole set of signs of threats and vulnerabilities those signs that, in his opinion, characterize the critical (most dangerous) threats and vulnerabilities. Let's consider some aspects of the application of concepts, methods and algorithms for processing fuzzy sets in the tasks of identifying (detecting and categorizing) vulnerabilities of SWT for ICN and DSS in conditions of fuzziness. When describing objects and phenomena using fuzzy

sets in vulnerability identification tasks, it is proposed to use the well-known concepts of fuzzy and linguistic variables, as well as fuzzy numbers. At the same time, a fuzzy variable is described, for example, for our task, for a vaguely defined vulnerability attribute – "a high level of threat using the vulnerability of the control program code". This fuzzy variable is characterized by three values, which in the theory of fuzzy sets are called a cortege [3, 4]:

$$< y, G, \tilde{A} > . \quad (1)$$

Thus, using the expression (1) on the basis of a cortege $< y, G, \tilde{A} >$, a fuzzy variable can be described, where y – is the name of the variable; G – is a universal set, the domain of the variable y; set $\tilde{A}$ – is a fuzzy set on G, describing a fuzzy constraint on the values of the variable g, due to y [4]:

$$\tilde{A} = \bigcup_{g \in G} g \,|\, \mu_g . \quad (2)$$

At the same time, the set $\tilde{A}$ in the theory of fuzzy sets is called the compatibility function of a fuzzy variable. This set describes the semantics of a fuzzy variable, with the variable g being the base variable for y. The set $\tilde{A}$ determines the degree (depth) with which the value of g corresponds to the element y, while the values of the fuzzy variable are numbers. As part of the task of identifying vulnerabilities of the SWT for ICN and DSS, as is customary in the theory of fuzzy sets, we will call the linguistic variable cortege [4]

$$< y, T(y), G, S, N >, \quad (3)$$

where y – is the name of the variable characterizing the degree (depth, level) of belonging of the vulnerability features of the SWT for ICN or DSS to a specific type of critical (most dangerous) threats and vulnerabilities; $T(y)$ – is the term set characterizing the names of linguistic values of y from the universal set G – is the domain of the variable y definition; S – is the syntactic rule, describing the process of obtaining new values of a linguistic variable; N – is a semantic rule that allows each fuzzy variable y to be assigned its meaning $N[y]$.

At the same time, numerical and non-numeric linguistic variables are distinguished in the tasks of identifying vulnerabilities of the SWT for ICN or DSS. A linguistic variable that characterizes the vulnerability of SWT for ICN or DSS is called a numeric variable if its domain of definition G is a subset of real numbers. An example of a non-numeric linguistic variable is the variable "dangerous", which formalizes the concept of "dangerous vulnerability of the SWT for ICN or DSS" with the values "not very dangerous", "dangerous", "very dangerous", "very-very dangerous".

Thus, an approach is proposed that allows us to characterize the application of the theory of fuzzy sets to solve the problems of reliable identification of vulnerabilities of SWT for ICN and storage systems in conditions of fuzziness of the

observed values of the signs of these vulnerabilities. An attempt has been made to show that the procedures for identifying signs of vulnerabilities of SWT for ICN or DSS can be reliably described formally using fuzzy and linguistic variables. This makes it possible to eliminate the uncertainty (such as fuzziness) of the source data that occurs when solving the problems of describing and identifying signs of vulnerabilities of SWT for ICN and DSS in real conditions. Ultimately, this makes it possible to increase the reliability and objectivity of security control of modern infocommunication networks and data storage systems.

References

1. Vostretsova E.V. Fundamentals of information security: a textbook for university students. Yekaterinburg: Ural Publishing House, 2019. 204 p. [in Russian].

2. Mayvold E. Network security. M: KNOW "Intuit", 2016. 571 p. [in Russian].

3. Shahbazova S. N., Sugeno M., Kacprzyk J. Recent Developments in Fuzzy Logic and Fuzzy Sets: Dedicated to Lotfi A . Zadeh. Springer, 1st. ed. 2020. 211 p.

4. Parashchuk I. B., Bobrik I. P. Fuzzy sets in problems of communication network analysis. St. Petersburg: VUS, 2001. 80 p. [in Russian].

5. Parashchuk I. B., Kotenko I. V. On the issue of integrated security of a "smart city" and the problems of countering socio-cyberphysical threats // World Science: Problems and Innovations: collection of articles of the XII International Scientific and Practical Conference. Penza: ICNS Science and Education. 2017. PP. 33–36. [in Russian].

6. Parashchuk I. B., Chechulin A. A. Protection of human-machine interface for intelligent transport environment // Promising directions of development of domestic information technologies (PNROIT2020): Materials of the VI Interregional conference. Sevastopol: SevSU, Vol. 1, 2020. PP. 65–66. [in Russian].

УДК 004.056.53
ГРНТИ 49.33.29

ИСПОЛЬЗОВАНИЕ СИСТЕМ ПРИНУДИТЕЛЬНОГО КОНТРОЛЯ ДОСТУПА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНТЕЙНЕРИЗАЦИИ

Д. Д. Кузнецов, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Контейнеризация уже является неотъемлемой частью нашего мира. Она, помимо всех своих преимуществ и особенностей, несёт в себе опасность и имеет ряд уязвимостей. Ведь практически всегда для работы или запуска контейнерных приложений требуется наличие каких-либо привилегий и использование прав суперпользователя root –

очень частое явление. В этой статье описывается, как системы принудительного контроля доступа на примере SELinux позволяют усилить безопасность контейнеров и создать глубоко эшелонированную защиту.

информационная безопасность, контейнеризация, SELinux, уязвимости.

Контейнеры сейчас являются самым простым способом упаковки приложения со всеми необходимыми зависимостями в модуль, который можно удобно использовать и распространять. Они значительно повышают производительность серверов, за счёт того, что предметом виртуализации является не «голое железо» или гипервизор, а операционная система [1]. Контейнер – это изолированный процесс ОС Linux, он также, как и любой процесс системы ограничен в доступных ему системных ресурсах, превращаясь тем самым в «песочницу» для контейнерного приложения на основе одного хоста. И так как контейнеры – это процессы, то и в плане безопасности они идентичны. Для них необходимо ограничивать полномочия и всегда запускать от непривилегированного пользователя.

Однако у контейнеров имеется множество проблем, среди которых основными являются:

- уязвимости ПО;
- ошибки конфигурации;
- взлом/компрометация образа;
- раскрытие конфиденциальных данных;
- уязвимости сетевых протоколов;
- *root escape* или «побег из тюрьмы».

Способов защиты и изоляции контейнеров существует большое количество, но основным является DAC (*discretionary access control*). К сожалению, для полноценной защиты контейнеров от всех перечисленных мной угроз этого будет недостаточно [2]. Для этого был создан и введён в ядро *Linux* механизм дополнительных модулей безопасности – LSM (Linux security modules).

Linux Security Modules (LSM) предоставляет собой механизм для различных проверок безопасности, которые могут быть подключены новыми расширениями ядра. Хотя эти расширения на самом деле не являются загружаемыми модулями ядра. Вместо этого они выбираются во время сборки через *CONFIG_DEFAULT_SECURITY* и могут быть переопределены во время загрузки. В официальном ядро уже встроены модули безопасности *SELinux, AppArmor*. Проверки LSM вызываются на действия, которые прошли проверку DAC, то есть модули работают параллельно с DAC [3].

Данный механизм имеет очень обширную область применения, но в основном добавляет мандатный контроль доступа, например, как *SELinux*. Ничего не мешает придумать собственную модель безопасности, реализовать

ее в виде модуля и легко внедрить, используя фреймворк. Модулей LSM существует большое множество ввиду возможностей применения, также они постоянно развиваются и разрабатываются новые, с точки зрения работы с контейнерами наиболее важными являются: *SELinux*, *AppArmor*, *Integrity*/IMA (*Integrity Measurement Architecture*) и *SecComp*. У них общий подход, но разная реализация функций. Существует настраиваемый набор правил, который определяет субъекты и объекты, к которым первые имеют доступ. Основное правило всех политик заключается в том, что если что-то явно не разрешено, то оно по умолчанию запрещено [4].

SELinux использует метки в расширенных атрибутах для контроля доступа к файлам. *AppArmor* по аналогии с *SELinux* использует вместо меток абсолютный путь к файлу. Модуль *Integrity* устроен иначе, он контролирует целостность кода системы, подсчитывая и сравнивая контрольные суммы файлов с записанными в расширенных атрибутах эталонными значениями. *SecComp* – яркий пример модуля с другим назначением, его задача – производить фильтрацию системных вызовов по заданному набору правил [5].

SELinux– это дополнительный инструмент изоляции контейнеров и ОС с помощью мандатного управления доступом для каждого пользователя, приложения, процесса или файла. *SELinux* полностью блокирует любые попытки выйти за пределы абстракции пространства имен. Принцип работы *SELinux* достаточно прост, он присваивать метки всем процессам и объектам ОС, из-за чего каждый элемент, используемый в операциях ядра, помечается и классифицируется, и на основе составленных правил ему предоставляется или не предоставляется доступ.

Правила *SELinux* определяют взаимодействие между помеченными процессами и помеченными объектами. Правила, заданные пользователем в политиках, применяются на уровне ядра. Ниже приведён пример работы *SELinux*.

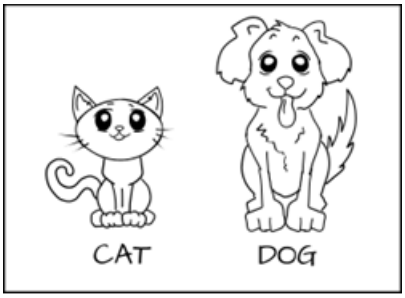


Рис. 1. Типы процессов

На рис. 1 видно, что *cat* и *dog* – это типы процессов, а корм – это класс объектов, с которыми будут взаимодействовать процессы: *cat_chow* и *dog_chow*.

На рис. 2 (см. ниже) задаются разрешение для собаки есть собачий корм: *allow dog dog_chow:food eat*. Аналогично и для кошки: *allow cat cat_chow:food eat*.

По этим правилам процессу cat на уровне ядра будет разрешено есть корм с меткой *cat_chow*, а dog — корм с меткой *dog_chow*. Однако, в случае попыток противодействовать данной политике, например, dog попытается съесть корм *cat_chow*, то ядро заблокирует данное действие.

Данный механизм является контролем по типам, он защищает ОС системы от контейнерных процессов. Контейнерные процессы могут читать

и запускать только файлы из каталога */usr* и записывать данные только в контейнерные файлы. Таким образом, происходит разграничение хоста от контейнеров, но оно не обеспечивает защиту контейнеров друг от друга, ведь все они помечены одним типом. Для такой защиты необходимо обратиться к контролю по меткам – MCS (*Multiple Category System*) [6].

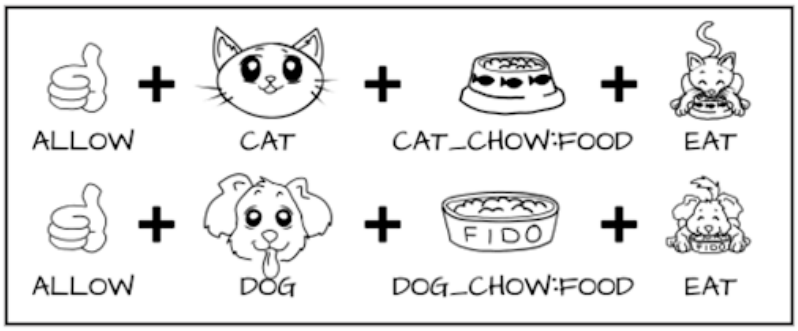


Рис. 2. Правила политики *SELinux*

Присвоение меток MCS работает так, что необходимо настроить набор категорий, являющихся простыми текстовыми метками и добавить в них пользователей. Сначала необходимо настроить категории, а затем добавить в них пользователей, а они уже в свою очередь смогут применять эти метки как считают нужным. MCS также позволяет использовать стандартные метки *SELinux* для управления объектами. Применение MCS помогло защититься от уязвимости CVE-2019–5736, которую обнаружили в 2019 году инженеры Open Shift [7].

Существующие проблемы в области безопасности контейнеров требуют тщательного подхода при проектировании системы. Для поддержания изоляции контейнеров используется множество различных средств: пространства имен, контрольные группы, Linux привилегии, модули безопасности Linux. Хотя при всём при этом полная изоляция не гарантируется, ведь для работы контейнера и приложений внутри него могут требоваться права доступа, которыми может воспользоваться злоумышленник, поэтому текущая ситуация создаёт необходимость в создании и подборе инструментов защиты под задачи конкретных контейнеризированных приложений.

Список используемых источников

1. Bentaleb O. et al. Containerization technologies: Taxonomies, applications and challenges // The Journal of Supercomputing. 2022. T. 78. N 1. PP. 1144–1181.

2. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. С. 657–662.

3. Red Hat documentation, SELinux. [сайт]. URL: https://access.redhat.com/documentation/enUS/Red_Hat_Enterprise_Linux/5/html/Virtualization/sect-VirtualizationSecurity_for_virtualization-SELinux_considerations.html (дата обращения: 03.03.2023).

4. Рузманов Е. Ю., Красов А. В., Цветков А. Ю. Сравнение моделей разграничения прав доступа на основе атрибутов и ролей // Безопасность в профессиональной деятельности: сборник научных статей. СПб., 2021. С. 227–232.

5. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 563–568.

6. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 2. С. 50–56.

7. NIST, CVE-2018-5736. [сайт]. URL: https://nvd.nist.gov/vuln/detail/CVE-2018-5736 (дата обращения 03.03.2023).

Статья представлена заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.057.4
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ СТАНДАРТА IEEE 802.11MC И ЕГО ПРИМЕНИМОСТИ В РАМКАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СЕТИ ПРЕДПРИЯТИЯ

О. И. Кузьмина, А. А. Миняев, Д. В. Сахаров

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современные корпоративные сети могут достигать крупных масштабов. Одновременно с ростом числа пользователей в корпоративных сетях увеличивается и вероятность атаки. Определение местоположения клиентов беспроводных корпоративных сетей является одним из способов создания гео-зон для контроля перемещения сотрудников в заданной территории. Такой подход к обеспечению информационной безопасности позволит предприятию обеспечить необходимый уровень защищенности беспроводной сети. В докладе представлено исследование стандарта IEEE 802.11mc и его применимости в рамках обеспечения информационной безопасности беспроводной сети предприятия. Рассмотрены требования к клиентам сети и беспроводному оборудованию.

беспроводные сети, определение местоположения, LBS, Wi-Fi RTT.

Современное предприятие – это множество взаимодействующих процессов: производственных, логистических, финансовых, маркетинговых, управленческих и т. д. Все они должны работать слаженно и эффективно для того, чтобы предприятие могло успешно конкурировать на рынке и обеспечивать свою прибыльность. Вопросом первостепенной важности является управление и контроль множества параметров. Для оперативного управления процессами предприятия необходима автоматизация. А для работы систем управления необходима надежная инфраструктура.

Использование систем определения местоположения клиентов беспроводной сети предприятия может позволить оптимизировать логистические процессы и улучшить обслуживание клиентов. Например, с помощью таких систем можно отслеживать перемещение товаров на складе и в реальном времени определять, где находится нужный товар. Также можно использовать эти системы для определения местоположения клиентов внутри предприятия и предоставления им персонализированных услуг. Например, клиенты могут получать уведомления о скидках и акциях на товары, которые находятся рядом с ними. В целом, использование систем определения местоположения клиентов беспроводной сети предприятия может помочь повысить эффективность работы предприятия и улучшить обслуживание клиентов.

Системы определения местоположения клиентов беспроводной сети (*Location-Based Services*, LBS) используются для определения местоположения устройств внутри помещений и на открытом воздухе. Они могут использоваться для различных целей, таких как управление доступом к зонам предприятия, навигация внутри зданий, анализ потоков движения и поведения клиентов.

Системы LBS могут использовать различные технологии для определения местоположения, включая GPS, Bluetooth, Wi-Fi и RFID. В случае использования Wi-Fi технологии, системы LBS используют сигналы от беспроводных точек доступа для определения местоположения устройств [1].

Для определения местоположения с помощью Wi-Fi технологии необходимо иметь карту расположения беспроводных точек доступа внутри здания. Эта карта может быть создана путем сканирования сигналов от беспроводных точек доступа и записи их координат. Затем эта карта может быть использована для определения местоположения устройств внутри помещений на основе сигналов от беспроводных точек доступа.

Системы LBS могут использоваться в различных отраслях, таких как розничная торговля, гостиничный бизнес, здравоохранение и образование. Они могут помочь улучшить клиентоориентированность и повысить эффективность бизнес-процессов.

Стандарт IEEE 802.11mc, также известный как Wi-Fi FTM (*Fine Time Measurement*) RTT (*Round-Trip-Time*), разработан для обеспечения более точного определения местоположения устройств беспроводной сети в помещении. Точность данного метода достигает 1–2 м. Для определения расстояния между устройствами и точками доступа в стандарте IEEE 802.11mc используется технология измерения промежутка времени передачи сигнала [2, 3] (*Time of Flight*, ToF) (рис. 1).

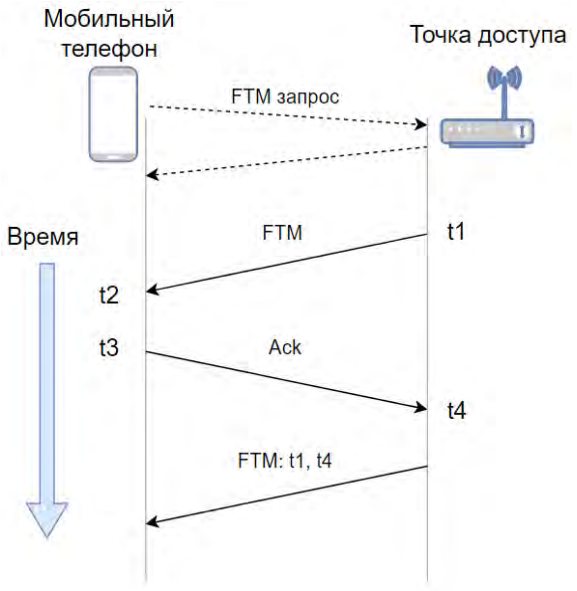


Рис. 1. Принцип измерения расстояния IEEE 802.11mc FTM RTT

При наличии одной точки доступа Wi-Fi доступно только измерение расстояния. При наличии трех или более близлежащих точек доступа появляется возможность определить местоположение устройства с использованием подхода трилатерации [4].

Принцип работы технологии основан на временной задержке приема и передачи сигнала – необходимо учитывать время, необходимое для отправки сигнала, и время, необходимое для получения подтверждения. Система рассчитывает этот промежуток времени, а затем умножает его на скорость света.

$$d = \frac{\big((t4 - t1) - (t3 - t2)\big) * c}{2},$$

где d – расстояние между отправителем сигнала и приёмником, м; t – время, с; c – скорость света, м/с [5].

Пока не все устройства имеют необходимую аппаратную поддержку для этой функции. В настоящее время список сертифицированных маршрутизаторов содержит следующие модели:

- Google Wi-Fi;
- Compulab Wi-Fi Indoor Location Device;
- Google Nest Wi-Fi (*Point or Router*).

Одним из применений этой функции является улучшение сервиса Google "Find My Device". Начиная с Android 9, Google внедрил поддержку Wi-Fi RTT.

Многие модели смартфонов с операционной системой Android 9 или более поздней версии могут рассчитывать расстояние до точек доступа. Следующие мобильные устройства поддерживают технологию Wi-Fi RTT: Xiaomi, LG Corporation, Samsung, Google Pixel, Poco X2, Sharp Aquos [6].

Функция Wi-Fi RTT в Android 9 позволяет поддерживающим устройствам измерять расстояние до других устройств: будь то точки доступа или устройства Wi-Fi Aware. Эта функция, основанная на протоколе IEEE 802.11mc, позволяет приложениям использовать повышенную точность определения местоположения.

Для защиты конфиденциальности своих пользователей Google рандомизирует MAC-адрес, используемый во время транзакций Wi-Fi RTT. Без рандомизации MAC-адресов злоумышленники могли бы использовать Wi-Fi RTT для слежки за пользователями смартфонов и отслеживания их местоположения [7, 8, 9].

Применение стандарта IEEE 802.11mc может быть полезно для обеспечения безопасности в предприятии. Например, его использование может позволить управляющим системой безопасности получать более точную информацию о местонахождении устройств в беспроводной сети предприятия. Это может помочь в реагировании на потенциальные угрозы безопасности и предотвращении несанкционированного доступа к информации [10, 11, 12].

Кроме того, использование стандарта IEEE 802.11mc может быть полезно для управления доступом к различным зонам предприятия. Например, система безопасности может быть настроена таким образом, чтобы она автоматически блокировала доступ к определенным зонам, если устройство клиента находится в неположенном месте, или за пределами контролируемой зоны.

Однако, следует отметить, что использование стандарта IEEE 802.11mc может быть ограничено наличием соответствующего оборудования и программного обеспечения. Кроме того, его применение может потребовать дополнительных затрат на настройку и поддержку системы безопасности.

Стандарт IEEE 802.11mc может быть полезным инструментом для обеспечения безопасности в беспроводной сети предприятия, но его применение должно быть оценено в контексте конкретных потребностей и возможностей предприятия.

Список используемых источников

1. Дрепа В. Е., Кузьмина О. И., Миняев А. А. Разработка модели системы определения местоположения беспроводных клиентов сетей семейства IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т. 1. С. 428–433.

2. IEEE 802.11 wireless local area networks. URL: https://www.ieee802.org/11/ (дата обращения 15.03.2023)

3. Дрепа В. Е., Киструга А. Ю., Ковцур М. М. Точность определения местоположения Wi-Fi клиента в свободном пространстве при использовании индикатора уровня принимаемого сигнала // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-

Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. СПб. : Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2022. С. 549–550.

4. Дрепа В. Е., Кистpуга А. Ю., Ковцур М. М., Кузьмина О. И., Петров В. А. Исследование метода fingerprinting для определения местоположения беспроводного клиента IEEE 802.11 // Заметки ученого. 2022. N 3-2. С. 137–141.

5. Lopez Pastor, Jose A & Arques, Pedro & Franco-Penaranda, Juan & Garcia-Sanchez, Antonio-Javier & Gomez Tornero, Jose. Wi-Fi RTT-based active monopulse RADAR for single access point localization // IEEE Access. 2021. PP. 1-1. 10.1109/ACCESS.2021.3062085.

6. Android devices that support WiFi-RTT. URL: https://developer.android.com/guide/topics/connectivity/wifi-rtt#supported-devices (дата обращения 15.03.2023)

7. Петрова Т. В., Ковцур М. М., Карельский П. В., Поляничева А. В. Подходы обнаружения беспроводной точки доступа злоумышленника в локальной вычислительной сети // Региональная информатика (РИ-2022) : Юбилейная XVIII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 26–28 октября 2022 года. СПб. : Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2022. С. 572–573.

8. Кистpуга А. Ю., Ковцур М. М., Петров М. П., Шабанов В. П. Методика обнаружения местоположения нарушителя, реализующего атаку деаутентификации на сеть IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. Т.1. С. 561–564.

9. Kovtsur M., Minyaev A., Khramtsov D., Abramenko G. Investigation of attacks and methods of protection of wireless networks during authorization using the IEEE 802.1X protocol // ACM International Conference Proceeding Series. 5, The Premier Conference on Smart Next Generation Networking Technologies. Сер. "ICFNDS 2021 – 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies" 2021. PP. 555–561.

10. Попов А. А., Федорова О. В., Цветков А. Ю. Исследование современных механизмов обеспечения защиты конечных устройств под управлением ОС семейства Linux от атак с использованием rootkit // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2022. N 3. С. 36–43.

11. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning // Studies in Computational Intelligence. 2020. Vol. 868. PP. 350–355.

12. Гельфанд А. М., Казанцев А. А., Красов А. В., Уляшева В. Р. Интернет вещей (IoT): угрозы безопасности и конфиденциальности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 215–220.

УДК 519.876.5
ГРНТИ 28.19.31

СИСТЕМАТИЗАЦИЯ КОМПЬЮТЕРНЫХ МУЗЫКАЛЬНЫХ ТЕХНОЛОГИЙ

А. А. Кутлыярова[1], В. Е. Малахов[2], Г. Г. Рогозинский[2]

[1]Санкт-Петербургский государственный институт кино и телевидения
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассматривается вопрос систематизации области компьютерных музыкальных технологий. Приводится описание систем и выполняемых ими процессов при помощи нотации EDF0. Предлагается классификация по типам объектов и субъектов, участвующих в процессах, а также по типу ядра, выполняющего основные функции.

компьютерные музыкальные технологии, звуковой объект, EDF0.

Введение

Область компьютерных музыкальных технологий (КМТ) уходит своими корнями к истокам электронной музыки, а также к первым экспериментам и инновациям с электронными инструментами на рубеже XX в. Благодаря этому появилась возможность облегчить процесс создания музыкальных композиций и экспериментировать, создавая новые жанры [1].

Учитывая значительное развитие КМТ и появление множества направлений и способов применения КМТ, их следует рассматривать как отдельное научное направление.

Однако, данная область по-прежнему плохо формализована и требует системного подхода для выделения проблем и поиска связи между компонентами КМТ.

Общее описание проблемной области

КМТ представляют собой совокупность различных приложений, таких как синтез и обработка звука, системы генерации композиций, исполнительские системы и автоаранжировщики, ассистивные обучающие системы, цифровые рабочие станции, системы живого кодирования, эксперементальные музыкальные системы, системы извлечения музыкальной информации и системы нотации [2, 3, 4, 5, 6].

В данной статье мы сосредоточимся на следующих системах, представляющих интерес с точки зрения системотехники: системы синтеза звука, системы обработки звука, системы сонификации и генеративные/алгоритмические системы

Предлагается провести анализ КМТ в терминах нотации EDF0 (вход, выход, управление, механизм).

Система синтеза звука

Как показано на рис. 1, в качестве входа управляющих элементов выступают алгоритмы, задающие параметры синтеза звука и события – триггеры, определяющие время начала и завершения синтеза.

Обработка входных параметров производится при помощи интерфейса и алгоритмов обработки триггера, а синтез звука обеспечивает ядро синтеза под управлением алгоритмов синтеза. После завершения процедуры на выход подаётся звуковой объект [7].

В данной системе оператор не влияет на сам процесс синтеза, а может лишь определить входные параметры, триггер и продолжительность воздействия на него.

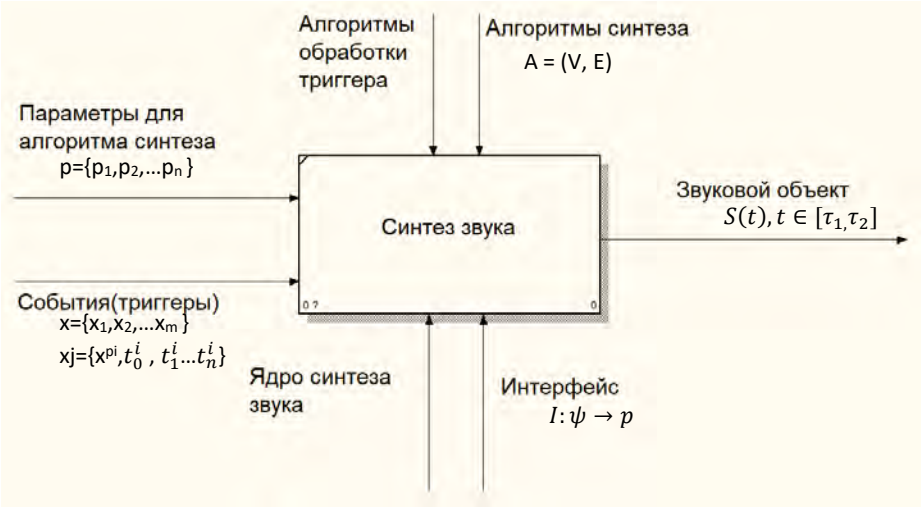


Рис. 1. Общее представление процесса синтеза звука

Система обработки звука

На входе получает звуковой сигнал, который преобразуется на программном уровне при помощи алгоритмов. Обработка входных данных осуществляется при помощи ядра обработки, при этом сам процесс является вариативным, его параметры подаются на входе при помощи интерфейса, а сам процесс можно представить в виде направленного графа, где вершины определяют направление обработки под влиянием этих параметров.

Представленная система принимает входные параметры и на основе заданных значений строит свою дальнейшую работу, при этом воздействие на систему во время её работы минимально.

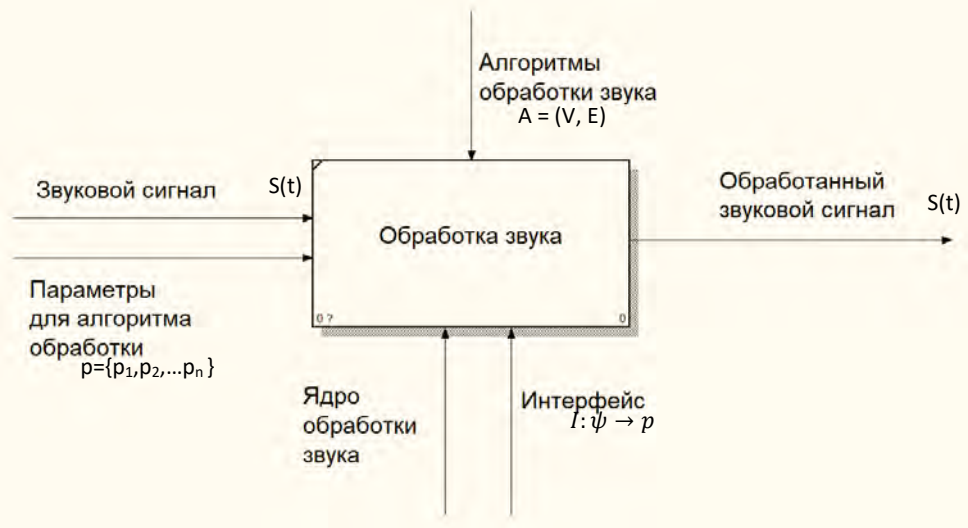


Рис. 2. Общее представление процесса обработки звука

Система сонификации

Сонификация необходима для отображения информации посредством звука. Система включает в себя системы генерации и может быть дополнена системой обработки звуков.

Данная система имеет нелинейную структуру принятия решений и обладает, возможностью реагировать на получаемые извне данные, формируя на их основе результат. В качестве параметров на входе могут выступать данные датчиков или сигналы оператора, в остальном система способна самостоятельно сформировать звуковой сигнал, обработав поступившую информацию при помощи алгоритма [8].

Для систем сонификации управляющими считаются параметры синтеза, которые могут ограничивать набор возможных звуков, а также набор параметров мэпинга, описывающие как система должна сопоставить вводные данные и звук на выходе.

Генеративная/алгоритмическая система

Система является сложной и вариативной. Многие примеры предоставляют обширный набор параметров пользователю для управления вводными данными генерации. Сама система получает на входе через интерфейс исходные данные, содержащие запрос и затем осуществляет генерацию при помощи генеративного ядра на основе уже известных примеров в соответствии запрошенному жанру, настроению или другим значениям параметров, введённых пользователем, после чего на выход передаётся звуковой объект.

Обработка запросов осуществляется при помощи алгоритмов, добавляющих звуки по определённым правилам или же нейросетевыми технологиями способными самостоятельно подбирать решения и создавать из них музыкальную композицию.

Заключение

В ходе работы были рассмотрены системы различных процессов систем КМТ. С помощью описания процессов сделано описание трудноформализированных направлений.

По результатам исследования в области КМТ обнаружено наличие системы с ядром высокого уровня и низкого уровня. Системы с ядром низкого уровня являются базой для систем высокого уровня, входят в их структуру и зачастую представляют собой системы типа «вход-выход», где на процесс работы не оказывается влияния или происходит минимальное воздействие.

Системы с ядром высокого уровня – это системы, состоящие из множества подсистем, они могут изменять параметры внутренних процессов самостоятельно или под влиянием оператора в любой момент времени.

Предложена классификация систем по уровню ядра, по видам входных и выходных данных, по способу управления и управляющим элементам. Полученные результаты позволят провести дальнейшую формализацию проблемной области КМТ.

Список используемых источников

1. Нельсон, Эндрю Дж. Звук инноваций: Стэнфорд и компьютерная музыкальная революция. Бостон: MIT Press, 2015.

2. Горбунова И. Б. Музыкально-компьютерные технологии: лаборатория // ЭНЖ «Медиамузыка». 2012. N 1. URL: http://mediamusic-journal.com/Issues/1_5.html (дата обращения 27.01.2023).

3. Горов Рон. Слушание и написание музыки: профессиональная подготовка современного музыканта. 2-е изд. Гардена, Калифорния: сентябрьская публикация. 2002. С. 212. ISBN 0-9629496-7-1.

4. Коллинз Н., Маклин А., Рорхубер Дж. и Уорд А. Живое кодирование в производительности ноутбука // Organized Sound 2003. N 8 (3). PP. 321–330. doi: 10.1017/S135577180300030X

5. Ван Г. и Кук П. Программирование на лету: использование кода в качестве выразительного музыкального инструмента // Материалы Международной конференции по новым интерфейсам для музыкального выражения (NIME). Нью-Йорк: НИМЭ, 2004.

6. Блэквелл Алан, Маклин Алекс, Ноубл Джеймс, Отто Йохен и Рорхубер Джулиан Сотрудничество и обучение с помощью живого кодирования (Dagstuhl Seminar 13382) // Dagstuhl Reports 3. 2014. No. 9. PP. 130–168.

7. Шеффер Пьер (2002) [1966]. Traité Des Objets Musicaux: Essai Interdisciplines (на французском языке). 2-е / новое изд. Париж: Éditions du Seuil. п. 271. ISBN 978-2-02-002608-6. OCLC 751268549. Перевод на английский см.: Schaeffer, Pierre (2012). В поисках специальной музыки. Перевод: Норт, Кристин; Дэк, Джон. Лондон: Калифорнийский университет. ISBN 978-0-520-26573-8. OCLC 788263789.

8. Крамер Грегори Слуховой дисплей: сонификация, одификация и слуховые интерфейсы. Институт Санта-Фе изучает науку о сложности. Слушания Том XVIII. Ридинг, Массачусетс: Эддисон-Уэсли, 1994. ISBN 978-0-201-62603-2.

УДК 004.056
ГРНТИ 81.93.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕШЕНИЙ ПО ПРОГРАММНО-АППАРАТНОЙ РЕАЛИЗАЦИИ МЕЖСЕТЕВЫХ ЭКРАНОВ НА ОСНОВЕ ОТКРЫТОГО ИСХОДНОГО КОДА

Т. Т. Кутуев, Р. Б Петрив

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

В связи с уходом крупных иностранных компаний-поставщиков сетевого оборудования с отечественного рынка прекращается поддержка приобретенных и используемых продуктов. Следовательно, возникает необходимость в создании межсетевого экрана с возможностью легкого распространения программного обеспечения и поддержкой пользователей. Такой системой может стать решение на базе одноплатных вычислительных платформ с использованием программного обеспечения с открытым исходным кодом.

одноплатный компьютер, свободно распространяемое программное обеспечение, межсетевой экран, программное обеспечение с открытым исходным кодом.

В текущей обстановке крупные компании-поставщики сетевого оборудования покидают рынок, некоторые из компаний частично или полностью прекращают поддержку пользователей, включая аппаратные и программные продукты. Решением данной проблемы может стать свободно распространяемое программное обеспечение с открытым исходным кодом, которое может быть использовано для разработки сетевых устройств на базе различных аппаратных платформ. В рамках данной статьи были рассмотрены четыре возможных решения на базе одноплатного компьютера Raspberry Pi с использованием следующего программного обеспечения:

- IPFire;
- OPNsense;
- OpenWrt;
- Комплексное решение Ubuntu Server + Uncomplicated Firewall.

Используемое оборудование

Для выполнения поставленных задач используется одноплатный компьютер Raspberry Pi 3 модель “B”. Примерный вид устройства представлен на рис. 1.

Рис. 1. Одноплатный компьютер Raspberry Pi 3 с USB-Ethernet адаптером

Характеристики [1, 2] данного компьютера представлены в таблице 1.

ТАБЛИЦА 1. Основные характеристики используемого компьютера

Характеристика	Значение
Процессор	Cortex-A53, ARM, 64-бит, 4 ядра, 1.2 ГГц
Оперативная память	1 Гб, LPDDR2
Сеть	WiFi 802.11n, 10/100 Мбит Ethernet
Хранение данных	MicroSD
Габариты	85×56×17 мм

На данной модели отсутствуют дополнительные сетевые разъемы RJ-45 Ethernet, для создания прототипа использовался адаптер USB – Ethernet. Для загрузки образа системы используется накопитель формата MicroSD.

Используемое программное обеспечение

Для возможности исследования практического применения межсетевых экранов на базе микрокомпьютеров использовалось свободно распространяемое программное обеспечение с открытым исходным кодом.

Преимущества использования такого программного обеспечения:

- Модифицируемость;
- Экономическая выгода;
- Прозрачность кода.

Модифицируемость кода позволяет доработать программное обеспечение в соответствии с задачами. Бесплатное распространение позволяет со-

кратить затраты на программную часть системы. Прозрачность кода позволяет защититься от возможных угроз безопасности, в том числе от скриптовых вирусов и несанкционированного доступа со стороны недобросовестных разработчиков.

Алгоритм установки программного обеспечения

Для установки образов в форматах “.img” и “.iso” используется бесплатная утилита Raspberry Pi Imager, которая позволяет создать съемный носитель с операционной системой.

IPFire

Свободно распространяемое программное обеспечение с открытым исходным кодом на основе Linux, предназначенное для обеспечения безопасности и защиты сети от внешних угроз. Данная система имеет графический Web-интерфейс, а также возможность установки аддонов [3]. Актуальная версия на момент написания данной статьи – 2.27 Core Update 173 от 27 февраля 2023 года.

OpenWrt

Данная операционная система основана на ядре Linux, является одной из самых популярных свободно распространяемых операционных систем для сетевых устройств. Выбор данной системы для прототипа обусловлен изначальной поддержкой процессоров с архитектурой ARM [4]. Одним из преимуществ является наличие графического web-интерфейса. В рамках выполнения задач, рассматриваемых в данной статье, используется OpenWrt версии 23.03.3 от 05 января 2023 года.

OPNsense

Операционная система на основе FreeBSD, которая позиционируется как бесплатное и открытое программное обеспечение для межсетевых экранов и маршрутизаторов. OPNsense не имеет встроенной поддержки архитектуры процессоров на базе ARM [5], в рамках данной работы рассматривался неофициальный форк OPNsense версии 20.1.2 от 06 марта 2020 года.

Ubuntu Server в связке с Uncomplicated Firewall

Ubuntu Server – Linux операционная система, предназначенная для использования в качестве программного обеспечения сервера. Содержит приложения для управления сервером и выполнения задач, связанных с хостингом, обработкой и хранением данных, администрированием сети.

Uncomplicated Firewall - входящий в стандартный набор утилит Ubuntu инструментарий командной строки, являющийся надстройкой над встроенной утилитой iptables.

В рамках данной статьи использовался дистрибутив Ubuntu 22.04 LTS от 21 апреля 2022 года.

Критерии сравнения

- Критерий 1 (К1) – Функционал (основные и дополнительные функции);
- Критерий 2 (К2) – Пропускная способность (Мбит/с);
- Критерий 3 (К3) – Уровень по модели OSI;
- Критерий 4 (К4) – Простота установки (3 балла – встроенное ПО, 2 – требуется установка, 1 – требуется доработка);
- Критерий 5 (К5) – Эффективность (3 балла – возможность использования в корпоративной среде, 2 – средние сети, 1 – только домашние сети или небольшие офисы);
- Критерий 6 (К6) – Масштабируемость (3 балла – более 100 устройств, 2 – более 50 устройств, 1 – от 10 до 50 устройств);
- Критерий 7 (К7) – Мультиплатформенность (3 балла – поддержка 3 и более платформ, 2 – поддержка текущей платформы, 1 – форк)/

В таблице 2 представлено сравнение возможных решений по данным критериям.

Примечание: для измерения пропускной способности использовалась утилита iperf 3, стрелкой вверх указана пропускная способность при передаче с сервера на клиент, стрелкой вниз - с клиента на сервер.

ТАБЛИЦА 2. Сравнительная таблица

Критерий Решение	(К1)	(К2)	(К3)	(К4)	(К5)	(К6)	(К7)	**Итого**
IPFire	Firewall + IPS, IDS, VPN	↑94Мбит/с ↓79Мбит/с	3-4, 7	2	2	2	2	**8**
OpenWrt	Firewall, DHCP, DNS, VPN	↑90Мбит/с ↓87Мбит/с	3-4, 7	2	2	2	3	**9**
OPNsense	Firewall, IPS, IDS, DNS, QoS	↑95Мбит/с ↓84Мбит/с	3-4, 7	1	3	3	1	**8**
Ubuntu UFW	Firewall	↑96Мбит/с ↓74Мбит/с	3	3	1	1	2	**7**

Заключение

Наибольшее количество баллов набрали системы OpenWrt (9 баллов) и IPFire (8 баллов). Решения на базе OpenWrt и IPFire являются универсальными, легко модифицируемыми и производительными системами. Соответственно, для создания прототипа целесообразно использовать именно эти системы. В дальнейшем возможна разработка собственного программного обеспечения на основе представленных решений.

Список используемых источников

1. Upton E.C, Halfacree G. Raspberry Pi User Guide: 4th Edition // Wiley, 2016. 320 p. ISBN 978-1-11-926436-1.

2. Характеристики Raspberry Pi 3 model B [Электронный ресурс]. URL: https://www.raspberrypi.com/products/raspberry-pi-3-model-b/ (дата обращения 20.02.2023).

3. Возможности IPFire (Features) [Электронный ресурс]. URL: https://www.ipfire.org/features (дата обращения 20.02.2023).

4. Официальное руководство пользователя OpenWrt [Электронный ресурс]. URL: https://openwrt.org/docs/guide-user/start (дата обращения 20.02.2023).

5. Официальная документация OPNsense [Электронный ресурс]. URL: https://docs.opnsense.org/ (дата обращения 20.02.2023).

6. Прошивка OpenWRT для роутеров [Электронный ресурс]. URL: https://habr.com/ru/sandbox/160736/ (дата обращения 20.02.2023)

Статья представлена научным руководителем, заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В Красовым.

УДК 004.056.53
ГРНТИ 20.53.17

БЛОКЧЕЙН ОПЕРАЦИИ И АЛЬТЕРНАТИВНЫЕ ТЕХНОЛОГИИ

Д. В. Кушнир, З. В. Михайлова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье представлено описание технологии блокчейн, ее особенностей, компонентов и алгоритмов работы. Также перечислены варианты возможных уязвимостей и угроз компонентов, а также алгоритмов данной технологии и пути их решения в будущем. Далее представлена сравнительная характеристика альтернативной технологии – базы данных и выявлены оптимальные пути использования обеих систем. Далее приведено описание новой технологии Tracechain. В заключении приводится сравнительный анализ блокчейна и технологии TraceChain.

блокчейн, уязвимости блокчейн, смарт-контракт, база данных, TraceChain.

Бизнес и торговля всегда занимали ведущие позиции в экономической политике государства. Важным значением в этих процессах обладают алгоритмы и способы передачи денежных средств и данных, которые, в свою очередь, необходимо обеспечивать конфиденциальностью и безопасностью, с одной стороны, и доступностью для сотрудников или владельцев, с другой стороны.

В качестве альтернативы для хранения существующих платежных данных, автоматизации задач отчетности и аудита в 2008 году была изобретена технология блокчейн.

Блокчейн в дословном переводе означает цепочку блоков, в которой содержатся данные, например, записи о сделках. Особенность таких цепочек заключается в том, что их нельзя изменить либо удалить, а только дополнить новыми данными. Например, если количество некого продукта сократилось, то непосредственно добавляется новая запись о количестве взамен редактирования изначальной ячейки. Блокчейн также обладает технологией распределенных реестров [1]. Суть данной технологии заключается в хранении всей истории сделок и владельцев в едином пространстве на множестве жестких дисков независимых пользователей.

Технология блокчейн обладает следующими особенностями. Децентрализация, а именно распределение характеристик контроля от центрального устройства к сети пользователей. Неизменность, то есть невозможность редактирования данных, что предполагает отсутствие вмешательств в транзакцию после внедрения в реестр. Консенсус, а именно зарегистрированный набор правил для одобрения транзакции.

Технология блокчейн работает по следующему алгоритму. Изначально необходимо произвести запись активов. Далее необходимо произвести консенсус, большее количество пользователей сети заключают, что актив действительный. Следующий шаг заключается в создании блоков. При достижении консенсуса активы записываются в блоки, своеобразные страницы реестра. Также в блоки записывается криптографический хэш, который играет роль цепочки. При изменении блока, изменяется и структура хэша. Таким образом, обеспечивается невозможность изменения данных без внимания пользователей. Блокчейн система предоставляет доступ к крайней копии главного реестра.

По данным National Institute of Standards and Technology (NIST) за прошедшее десятилетие компании, использующие технологию блокчейн лишись более 13,6 млрд долларов из-за кибератак.

Далее следует перейти к рассмотрению основных уязвимостей данной системы.

Первой уязвимостью могут служить криптографические алгоритмы. Блокчейн структуры, такие как Bitcoin предполагают применение алгоритма Elliptic Curve Digital Signature Algorithm (ECDSA). Область применения

ECDSA ограничивается областью применения электронной цифровой подписи, то есть в тех местах, где может потребоваться проверка целостности и авторства сообщения [2]. При создании некоторых видов кошельков и верификации впоследствии пользователю необходимо ввести n-знаковую последовательность символов. Если автоматическая генерация последовательности недоступна в системе, пользователь может сгенерировать случайный ряд значений в сторонних ресурсах.

К следующей уязвимости можно отнести алгоритмы консенсуса Proof of Stake (POS) [3]. Существует вероятность получения мошенниками доступа более чем к половине активов вычислительной мощности сети. Такая угроза может привести к предоставлению контроля над сетью, а именно возможности редактировать историю, проводить операции с большим расходованием и блокировку активов. Мошенники в данном консенсусе нередко создают дополнительную, новую цепочку блоков в сети по длине перекрывающих половину всех блоков, после чего изначальный блокчейн может быть модифицирован. Аналогично, алгоритм Proof of Work (POW) может содержать уязвимость. Существует вероятность атаки 51 %, при которой группа лиц может получить контроль над 51 % вычислительных мощностей.

Другая уязвимость может быть связана с технологией смарт-контрактов [4]. Уязвимости смарт-контрактов влекут за собой серьезные последствия, так как они работают с финансовыми операциями. При изменении составляющих смарт-контрактов мошенниками вернуть их в изначальный вид практически невозможно. Состояние контрактов определяется в зависимости от его переменных, которые могут изменяться при модификации блоков и от функций, описывающих логику. Незнание состояния смарт-контрактов может послужить уязвимостью.

Однако, несмотря на перечисленные уязвимости, данная современная технология развивается в огромном темпе. Таким образом, на сегодняшний день внедряются методы формального анализа и аудита безопасности смарт-контактов.

Значительный спектр возможностей, предоставляемый блокчейном, может быть предоставлен более традиционными технологиями.

База данных – это упорядоченный набор структурированной информации или данных, которые обычно хранятся в электронном виде в компьютерной системе [5].

Далее приведен сравнительный анализ использования распределенного реестра блокчейн технологии и базы данных (табл. 1).

ТАБЛИЦА 1. Сравнительный анализ блокчейн и базы данных

Характеристики	Блокчейн	База данных
Управление и руководство	Ончейн управление (обсуждении вопросов в сети блокчейн). Оффчейн управление (обсуждение вопросов вне системы блокчейн). Децентрализованы.	Контролируются администратором, централизованны.
Архитектура	Многоуровневая (уровни: инфраструктура, данные, сетевой, консенсус, прикладной)	Клиент – сервис
Управление данными	Операции чтение – внесения данных	Операции чтения – внесения данных – модификации – удаления
Целостность и безопасность	Неизменность данный. Высокая безопасность.	Третьи лица могут изменять содержимое базы данных. Низкая безопасность.
Прозрачность	Присутствует, пользователь может сверить данные.	Отсутствует. Пользователи не могут проверить данные без разрешения.
Затраты	Трудна при использовании и реализации, высокая стоимость	Проста в настройке и использовании, низкая стоимость
Производительность	Медленнее	Быстрее
Экономическая эффективность	Для небольших компаний	Для крупных корпораций

Недостатки блокчейн могут быть связаны не столько с самой идеей, сколько с текущими методами его реализации. В настоящий момент разрабатываются пути решения проблемы производительности. Первый способ заключается в задействовании меньшего количества узлов при обработке транзакций. Таким образом, большее количество транзакций можно будет выполнять параллельно. Второй способ заключается в создании уровней связи данных, которые будут отправлять большинство транзакций за пределы цепочки, но в пределах локальной сети, взаимодействуя при перемещении только с блокчейном [6]. Данный алгоритм предполагает создать помимо основного блокчейна новый уровень, который будет предполагать интеграцию со смарт-контрактами. Суть данной технологии заключается в возможности использования основного блокчейна через новый уровень.

Альтернативной, в которой отсутствуют проблемы производительности, может послужить новая российская разработка от компании MetaHash – TraceChain, выпущенная в 2018 году. Ключевым аспектом данной технологии являются математические алгоритмы под управлением искусственного интеллекта, которые предотвращают перегрузку сети. Данная система представляет собой замкнутые кольца, которые, при визуализации, располагаются внутри друг друга. Все потоки данных в данной системе идут от радиуса к центру, далее синхронизируются внутри множества ядер и распределяются по сети. Ядра могут меняться посредством голосования. Ядра полностью децентрализованы, защищены Trust-алгоритмами и перепроверками внешними радиусами. Метод подтверждения транзакций происходит посредством проверки во всех узлах, через которые проходит транзакция на пути к центральным ядрам, посредством данного алгоритма TraceChain система способна обрабатывать до 50 тысяч транзакций в секунду, в то время как блокчейн система способна обрабатывать до 7 транзакций в секунду.

ТАБЛИЦА 2. Сравнительный анализ блокчейн и TraceChain

Характеристики	Блокчейн	TraceChain
Скорость подтверждение транзакции	10 минут	до 3 секунд
Объем транзакций в секунду	до 12	от 50.000 до миллионов
Уровень децентрализации	высокий	высокой

Данное исследование позволяет сделать вывод, что каждая рассматриваемая технология обладает своими преимуществами и недостатками. Для реализации распределенных систем среднего масштаба, но с высоким уровнем безопасности наиболее предпочтительными представляются решения, построенные на основе блокчейна. Для реализации корпоративных проектов с низкой степенью децентрализации адекватным решением будет применение традиционных баз данных. В тоже время для реализации проектов глобальных размеров значительные преимущества предлагает решение TraceChain, несмотря на свою новизну, малую изученность и недостаточную распространенность.

Технологию распределенного реестра следует выбирать индивидуально в зависимости от поставленных задач, бюджета и количества пользователей.

Список используемых источников

1. Системы распределенного реестра [Электронный ресурс] // digital.gov.ru. URL: https://digital.gov.ru/uploaded/files/07102019srr.pdf (дата обращения 05.12.2022).

2. Коржик В. И., Яковлев В. А. Основы криптографии : учебное пособие. Санкт-Петербург : Интермедия, 2017. 312 с.

3. Алгоритм консенсуса Proof-of-Stake [Электронный ресурс] // forklog.com. URL: https://forklog.com/cryptorium/chto-takoe-proof-of-stake-pos (дата обращения 09.12.2022).

4. Башир И. Блокчейн: архитектура, криптовалюты, инструменты разработки, смарт-контракты. М. : ДМК Пресс, 2019. 538 с.

5. Смарт-контракты и вопросы безопасности [Электронный ресурс] // itsec.ru. URL: https://www.itsec.ru/articles/smart-kontrakty-i-voprosy-bezopasnosti (дата обращения 10.12.2022).

6. Решения для масштабирования [Электронный ресурс] // academy.benance.com. URL: https://academy.binance.com/ru/articles/blockchain-layer-1-vs-layer-2-scaling-solutions (дата обращения 12.01.2023).

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ И АППАРАТНЫХ КЛИЕНТОВ БЛОКЧЕЙН-СЕТЕЙ

Д. В. Кушнир, А. А. Нечаев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Широкую популярность технология блокчейн получила именно благодаря криптовалютам. Наряду с возможностями, которые предоставляют криптовалюты, возникают дополнительные проблемы в безопасности использующих их систем. Одним из векторов атак на рассматриваемые системы является поиск уязвимостей в клиентах криптовалют как программных, так и аппаратных. На сегодняшний день известен целый ряд типовых атак на каждый вид клиентов, так и универсальные атаки на оба типа клиентов. Так как клиенты являются неотъемлемой частью практически всех блокчейн систем, то необходимо определить критерии их безопасности и анализ существующих реализаций для определения стойкости любых блокчейн решений.

блокчейн, уязвимость, криптокошелек, программные кошельки, аппаратные кошельки.

Блокчейн – это распределенная децентрализованная база данных, в которую записываются транзакции безопасным и прозрачным образом. Данные в блокчейне хранятся в блоках, каждый блок содержит криптографический хэш предыдущего блока, что затрудняет изменение прошлых транзакций без изменения всех последующих блоков. Одно из применений технологии блокчейн является криптовалюта. Криптовалюта – это цифровая или виртуальная валюта, которая использует криптографию для обеспече-

ния безопасности и работает независимо от центрального банка. Пользователи криптовалют хранят свои монеты на криптовалютных кошельках, о которых и пойдет речь [1].

Существует два вида криптовалютных кошельков:

- Аппаратный крипто-кошелек – это физическое устройство, на котором хранятся закрытые ключи и которое используется для безопасного хранения и управления криптовалютами. Устройство небольшое и портативное, его можно подключить к компьютеру или мобильному устройству.
- Программный крипто-кошелек – а представляет собой цифровое приложение или программу, которая позволяет пользователям хранить, управлять и совершать транзакции со своими криптовалютами. Его можно установить на настольный компьютер или мобильное устройство. Программные кошельки можно разделить на две основные категории: «горячие кошельки» и «холодные кошельки». Горячие кошельки подключены к Интернету и более уязвимы для атак, в то время как холодные кошельки хранят закрытые ключи в автономном режиме, что делает их более безопасными [2].

В вопросах безопасности принято считать, что аппаратные кошельки более предпочтительны. Они хранят закрытые ключи в автономном режиме, что делает их менее уязвимыми для кибератак. Помимо этого, на устройстве могут быть предусмотрены дополнительные меры защиты, такие как доступ по отпечатку пальца или дополнительный пароль. Программные кошельки, в большинстве своем, подключены к интернету, что делает их более уязвимыми к атакам фишинга, вредоносного ПО и атаки типа человек посередине. Несмотря на то, что среди программных кошельков существуют холодные кошельки, они также подвержены сетевым атакам, но на стороне компании-поставщика услуг.

Уязвимости программных криптокошельков

Одним из наиболее значительных рисков безопасности является возможность установки вредоносного программного обеспечения на устройство, на котором установлен кошелек. Это может произойти в результате неосознанной загрузки и установки вредоносных программ пользователем или в результате использования злоумышленником уязвимости в программном обеспечении или операционной системе [3].

Еще одним важным фактором, который следует учитывать, является надежность и сложность пароля, используемого для защиты кошелька. Слабые или легко угадываемые пароли могут быть легко взломаны злоумышленниками, что поставит под угрозу содержимое кошелька [4].

В дополнение к этим факторам также важно учитывать методы социальной инженерии. Одной из самых масштабных атак на кошелёк Phantom

проходил примерно по такому сценарию: хакеры создали копию сайта Phantom и почтовый адрес, похожий на официальный. В тексте письма говорилось, что кошелек должен быть срочно проверен из-за последнего обновления, а в случае отказа от проверки действие учетной записи приостановится. При переходе по ссылке открывалось окно, где была просьба ввести сид фразу, состоящую из 12 или 24 слов. При наличии сид фразы, злоумышленник получает полный доступ к кошельку и всем его средствам [5].

Другой случай кражи данных произошел 8 февраля 2023 года, когда с кошелька Trust Wallet было украдено более 4 миллионов. Преступник представлялся крупным инвестором в крипто проекты, отправлял зараженный PDF файл под видом NDA (Соглашение о неразглашении) или KYC (Документ, подтверждающий личность). После поступления средств на кошелек, вредоносное ПО сообщало преступникам о наличии монет. Согласно расследованию, похожих случаев было несколько, все преступники действовали в похожей манере. Во всех похожих случаях, хакер требовал, чтобы перевод был осуществлен на абсолютно новый, подконтрольный жертве Trust Wallet кошелек, что может быть предметом для поисков уязвимостей со стороны кошелька, однако команда аудиторов не нашла ничего [6].

Уязвимости аппаратных криптокошельков

Одной из распространенных уязвимостей аппаратных криптокошельков являются физические атаки. Злоумышленники могут попытаться получить физический доступ к устройству путем кражи устройства или получения доступа к печатной плате. Это может позволить извлечь закрытые ключи, хранящиеся на устройстве. Например, в 2018 году, в Гонконге у жертвы украли кошелек с 2 миллионами долларов, применив физическую силу. Хакеры использовали специальное оборудование для извлечения приватных ключей из аппаратных кошельков.

Еще одной уязвимостью аппаратных криптокошельков являются атаки по побочным каналам, которые включают использование информации, утекшей из устройства во время нормальной работы. Пример атаки по был продемонстрирован в 2020 году, когда исследователи из Мичиганского университета, что они могут извлечь закрытые ключи из Trezor One. Исследователи использовали технику, которая заключалась в манипулировании напряжением, подаваемым на устройство, чтобы вызвать сбой и извлечь конфиденциальную информацию.

Пользователи аппаратных криптокошельков могут предпринять шаги, чтобы свести к минимуму риск атаки. Клиенты должны убедиться, что они приобретают свое устройство у надежного поставщика, и могут следовать рекомендуемым производителем процедурам безопасности, таким как уста-

новка надежного PIN-кода и сохранение фразы восстановления в безопасном месте [7]. В марте 2018 года компания Ledger обнаружила в своих устройствах уязвимость в прошивке, что позволяло злоумышленникам украсть закрытые ключи и получить доступ к средствам, хранящимся на устройстве. Мошенническое приложение могло нарушить изоляцию между приложениями и получить доступ к конфиденциальным данным, которыми управляют определенные приложения, такие как GPG (Приложение для шифрования), U2F (Приложение двухфакторной аутентификации) или Neo (Приложение для разработки децентрализованных приложений и смарт контрактов) [8].

Определение критериев безопасности

При выборе криптокошелька стоит обращать на всевозможные критерии безопасности. В таблице 1 приведена сравнительная таблица по ключевым параметрам безопасности программных криптокошельков.

ТАБЛИЦА 1. Сравнение программных криптокошельков

Кошелек	Open Source	2FA	Иерархическое детерминирование	Аудиты безопасности	Поддержка мультиподписей	Холодное хранилище
Exodus	Да	Да	Да	Нет	Нет	Нет
Electrum	Да	Да	Да	Да	Да	Да
MyEther-Wallet	Да	Да	Да	Да	Да	Нет
Ledger Live	Нет	Да	Да	Да	Да	Да
Trust Wallet	Да	Да	Да	Да	Да	Нет
Tezor Suite	Да	Да	Да	Да	Да	Нет

Аналогичное сравнение для программных криптокошельков представлено в таблице 2.

ТАБЛИЦА 2 Сравнение аппаратных криптокошельков

Кошелек	Поддерживаемые ОС	Функции безопасности	Open Source	Интерфейс	Поддерживаемые криптовалюты
Ledger Nano X	Windows, Mac, Linux, Android, IOS	Чип, PIN код, кодовая фраза	Да	Bluetooth, USB	1800+
Tezor Model T	Windows, Mac, Linux, Android	Чип, PIN код, кодовая фраза	Да	USB	1000+
KeepKey	Windows, Mac, Linux	Чип, PIN код, кодовая фраза	Частично	USB	40+

Кошелек	Поддерживаемые ОС	Функции безопасности	Open Source	Интерфейс	Поддерживаемые криптовалюты
BitBox02	Windows, Mac, Linux, Android, IOS	Чип, резервная копия MicroSD, кодовая фраза	Да	MicroSD, USB	1000+
Coldcard Mk3	Windows, Mac, Linux	Чип, резервная копия MicroSD, кодовая фраза	Частично	MicroSD, USB	Bitcoin
Ellipal Titan	Windows, Mac, Linux, Android, IOS	Чип, PIN код, кодовая фраза	Нет	QR code, USB	30+

Хотя программные и аппаратные криптокошельки имеют свои уникальные функции безопасности, они не застрахованы от уязвимостей и атак. Программные кошельки уязвимы для атак вредоносного ПО, фишинга и социальной инженерии. Аппаратные кошельки могут подвергаться физическим атакам или атакам на цепочку поставок. Несмотря на эти риски, криптокошельки остаются важным компонентом экосистемы блокчейна, позволяя пользователям безопасно хранить свои цифровые активы и управлять ими. Безопасность криптокошельков является постоянной проблемой в индустрии блокчейнов, и пользователи, разработчики и заинтересованные стороны отрасли должны работать вместе, чтобы усилить меры безопасности и предотвратить атаки.

Список используемых источников

1. Antonopoulos Andreas Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly, 2014. 298 p.

2. Securing Your Wallet [Электронный ресурс] // Bitcoin. URL: https://bitcoin.org/en/secure-your-wallet (дата обращения 24.02.2023).

3. Casey M., Vigna P. The Truth Machine: The Blockchain and the Future of Everything, HarperCollins, 2018. 336 p.

4. Gerard D. Attack of the 50 Foot Blockchain: Bitcoin, Blockchain. Ethereum & Smart Contracts. Createspace, 2017. 182 p.

5. Petitto N. Hacker Impersonates TrustWallet in Crypto Phishing Scam [Электронный ресурс] // Vade. URL: https://www.vadesecure.com/en/blog/hacker-impersonates-trustwallet-in-crypto-phishing-scam (дата обращения 24.02.2023).

6. Adejumo Oluwapelumi, Trust Wallet says user's $4M hack was done via social engineering [Электронный ресурс] // Cryptoslate. URL: https://cryptoslate.com/trust-wallet-says-users-4m-hack-was-done-via-social-engineering. (дата обращения 24.02.2023).

7. Котенко И. В., Ушаков И.А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика "РИ-2016" : Материалы конференции, Санкт-Петербург, 26–28 октября 2016 года. Санкт-Петербург: Политехника-принт, 2016. С. 168–169.

8. Firmware 1.4: deep dive into three vulnerabilities which have been fixed [Электронный ресурс] // Ledger. URL: https://www.ledger.com/firmware-1-4-deep-dive-security-fixes. (дата обращения 24.02.2023).

УДК 004.056.2
ГРНТИ 20.53.19

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ 2P2 СЕТИ BLOCKCHAIN

Д. В. Кушнир, Е. Р. Никонов

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Основу возможностей проектов, базирующихся на технологии blockchain, составляет взаимодействие участников, составляющих P2P сеть, что означает отсутствие обязательного разделения участников по ролям. Узлы сети связаны друг с другом напрямую, каждый из них может выступать как в качестве сервера, так и в качестве клиента. Выполнено исследование построения подобной сети на основе проектирования полноценного узла с реализованными функциями взаимодействия с другими участниками.

blockchain, распределенный реестр, blockchain сеть, защита информации, ключ, подпись.

Под blockchain системой понимается полноценный отдельный узел blockchain сети [1], который содержит в себе все необходимые механизмы хранения, обработки и передачи данных. Экземпляр узла должен быть расширяем и в перспективе пригоден для использования в blockchain сети.

Blockchain сеть является P2P сетью [1, 2], что означает отсутствие серверов, которые обрабатывают и отдают данные, и клиентов, которые используют эти серверы. В подобной сети имеются узлы, каждый из которых является ее полноправным членом, узел – и клиент, и сервер. Узлы сети связаны друг с другом напрямую.

Экземпляр узла blockchain сети разбит на компоненты [1] (рис. 1), каждый из которых выполняет свою функциональную задачу, что позволяет выполнить критерий расширяемости:

1. связующий компонент – Chain.
2. компонент работы с пользователями – Wallet.
3. компонент работы с транзакциями – Transaction.
4. компонент работы с блоками данных – Block.
5. компонент для работы с кэшем – Chainstate.

6. компонент для предоставления неполной копии системы в сети – Merkle Tree.

7. компонент работы с базой данных и предоставления API – DB and API.

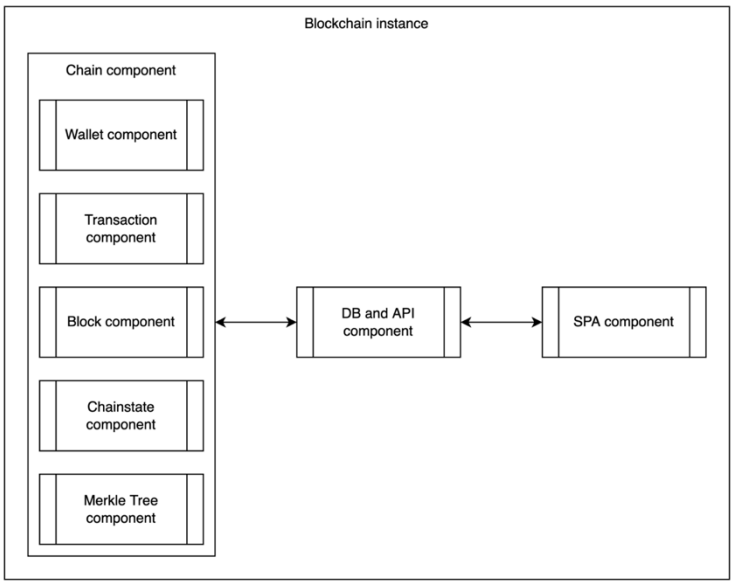


Рис. 1. Экземпляр blockchain системы

Описанный узел использует алгоритм консенсуса Proof of Work (PoW) подобно оригинальным узлам сети Bitcoin [3, 4, 5]. Важными компонентами для построения blockchain сети на основе данного экземпляра являются DB and API и Merkle Tree. Данный экземпляр предоставляет определенное API для взаимодействия с помощью компонента DB and API. Компонент Merkle Tree позволяет проверить принадлежность определенной транзакции, не загружая каждый отдельный блок данных целиком [6].

Несмотря на то, что узлы в такой сети являются полноценными, они могут играть разные роли [7, 8]:

1. *Miner node* – майнер. Узлы подобного типа работают на мощном или специализированном оборудовании, их единственная цель – как можно быстрее добывать новые блоки. Майнеры возможны только в blockchain системах, использующих алгоритм *PoW.*

2. *Full node* – полный узел. Данные узлы проверяют блоки, добытые майнерами (если система использует PoW алгоритм) и проверяют транзакции. Для этого у них должна быть полная копия blockchain системы. Кроме того, полные узлы выполняют такие операции, как помощь другим узлам в обнаружении друг друга. Для сети очень важно иметь много полных узлов, так как именно они принимают решения о действительности блоков или транзакций.

3. *SPV node* – узел упрощенной проверки платежей. Узлы SPV не хранят полную копию blockchain системы, но все же могут проверять определенные транзакции. Узел SPV зависит от полного узла для получения данных, и к одному полному узлу может быть подключено много подобных. Данный узел делает возможным использование кошелька без надобности загружать полную цепочку блоков, чтобы стать полноправным участником blockchain сети.

Используя экземпляр blockchain узла, предлагается разбить blockchain сеть на несколько узлов с разными ролями:

– Центральный узел. К данному узлу будут подключаться все остальные узлы для синхронизации.

– Узел кошелька / пользователя. Смысл данного узла состоит в создании новых транзакций и хранении экземпляра blockchain.

– Узел майнера. Данный узел будет хранить новые транзакции в пуле транзакций. При достижении определенного количества транзакций в пуле узел будет создавать новый блок.

Сценарий работы (рис. 2):

1. Центральный узел создает blockchain экземпляр.

2. Узел пользователя подключается к центральному узлу и загружает весь экземпляр к себе.

3. Узел майнера подключается к центральному узлу и загружает весь экземпляр к себе.

4. Узел пользователя создает транзакцию.

5. Узел майнера получает транзакцию от узла майнера и сохраняет ее в своем пуле памяти.

6. Когда в пуле памяти достаточно транзакций, узел майнера начинает создавать новый блок.

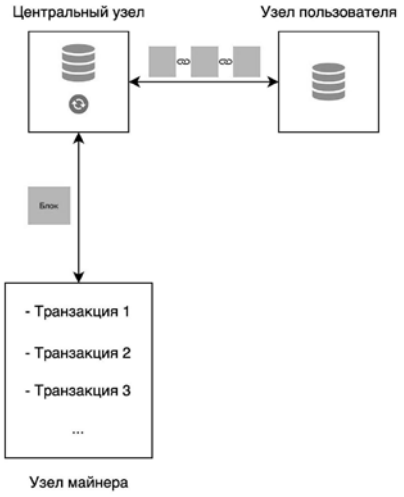


Рис. 2. Сценарий работы *blockchain* сети на основе экземпляра узла

7. После создания нового блока он отправляется на центральный узел.

8. Узел пользователя синхронизируется с центральным узлом.

9. Пользователь узла кошелька проверяет, что его платеж прошел успешно.

Каким образом узел пользователя знает, к какому центральному узлу подключаться? Жесткое связывание адресов является ошибкой с точки зрения безопасности. Вместо связывания адресов куда лучше использовать DNS-сервера, которые знают адреса некоторых центральных узлов (рис. 3).

Каким образом общаются узлы между собой? Узлы общаются между собой посредством сообщений VERSION (рис. 4), которые содержат в себе поля Version, BestHeight и AddrFrom. Version поле нужно для предоставления информации о версии сети, поле BestHeight необходимо, чтобы сравнивать количество блоков между узлами и если они не равны, то блок с меньшим количеством скачивает недостающие. Поле AddrFrom предоставляет информации об адресе, с которого пришел запрос.

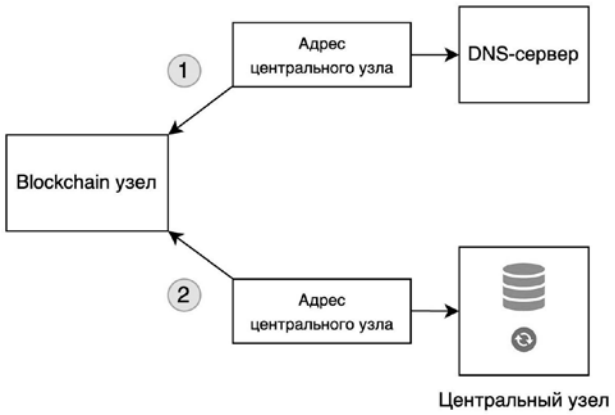


Рис. 3. Взаимодействие узлов с *DNS-серверами*

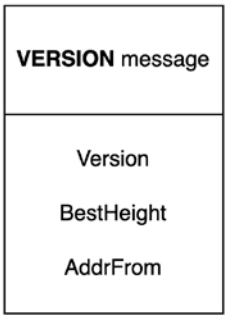


Рис. 4. Сообщение VERSION

Таким образом мы получаем легкую версию blockchain сети на основе экземпляра узла [1]. Имеется возможность расширения ролей в плане использования SPV роли для пользователей, так как экземпляр узла имеет определенный функционал на основе компонента Merkle Tree.

В рамках данной статьи был исследован подход к построению blockchain сети на основе предыдущих наработок [1] в виде полноценного экземпляра узла blockchain сети. Перспективой данной работы является полное практическое воплощение подхода в жизнь с уже существующей blockchain системой [1], усовершенствование сети путем добавления нескольких центральных узлов, добавление SPV роли и тестирование.

Список используемых источников

1. Никонов Е. Р. Особенности проектирования основных компонентов блокчейн системы // Молодежная научная школа кафедры «Защищенные системы связи». 2022. N 4. С. 122–126.

2. Jeffrey A. Tucker. Bit by Bit: How P2P Is Freeing the World // The global community Liberty.me. 2015.

3. White Paper: Proof of Stake vs. Proof of Work [Electronic resource] // BitFury Group. URL: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (date of the application: 20.02.2023).

4. White PaperY Xiao, N Zhang, W Lou, YT Hou: A Survey of Distributed Consensus Protocols for Blockchain Networks [Electronic resource] // BitFury Group. URL: https://arxiv.org/pdf/1904.04098.pdf (date of the application: 20.02.2023).

5. Md Sadek Ferdous, Member, IEEE, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque, Member, IEEE, and Alan Colman: Blockchain Consensus Algorithms: A Survey [Electronic resource] // BitFury Group. URL: https://arxiv.org/pdf/2001.07091.pdf (date of the application 20.02.2023).

6. Деревья и корни Меркла [Электронный ресурс] // Binance academy. URL: https://academy.binance.com/ru/articles/merkle-trees-and-merkle-roots-explained. (дата обращения: 20.02.2023).

7. Geroni D. Blockchain Nodes: An In-Depth Guide [Electronic resource] // 101blockchains. URL: https://101blockchains.com/blockchain-nodes (date of the application 20.02.2023).

8. Going the distance. A blog about blockchains and smart contracts development. [Electronic resource] // Jeiwan. URL: https://jeiwan.net. (date of the application 20.02.2023).

УДК 004.424
ГРНТИ 50.41

ПРОГРАММИРОВАНИЕ КВАНТОВОГО КОМПЬЮТЕРА И ЕГО ЭМУЛЯЦИЯ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. В. Кушнир, Т. А. Платонова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В настоящее время квантовые технологии продолжают активно развиваться. Они требуют новых подходов к реализации привычных задач в области вычислений и коммуникаций. Так, для работы с квантовыми компьютерами были разработаны специальные языки программирования. Кроме того, из-за ограниченности доступа к физическим квантовым технологиям, в настоящее время разработаны инструменты для эмуляции квантовых вычислений. Исследование разработки программ для квантовых компьютеров и работа с эмуляторами проведены на базе языка программирования Python с использованием библиотеки Qiskit. Показана возможность проведения исследований в области квантового программирования для последующего решения задач в области информационной безопасности.

квантовый компьютер, кубит, гейт, квантовые вычисления, языки программирования.

Одним из активно развивающихся направлений являются квантовые вычисления. В отличии от классических вычислений на привычных нам компьютерах, оперирующих с битами, т.е. регистрами в состоянии 0 или 1, квантовые используют кубиты, квантовые суперпозиции состояний 0 и 1. Оперируя кубитами, в отличии от работы битами, мы получаем доступ к работе с экспоненциальным вычислительным пространством по отношению

к количеству задействованных кубит в квантовом компьютере [1]. Это позволяет эффективно решать следующие задачи:

- криптографические: выполнение криптоанализа, шифрование, расшифрование сообщений;
- оптимизации, такие как поиск минимума или максимума функции;
- моделирования свойств материалов и молекул;
- распознавания образов и машинное обучение.

Однако квантовый компьютер не может заменить классический во всех задачах, и его использование ограничено некоторыми техническими и практическими аспектами. В будущем, он будет играть важную роль в решении сложных задач, для которых сейчас не известны эффективные способы решения. Некоторые из ожидаемых приложений квантовых компьютеров включают:

- разработку новых лекарств и медицинских технологий;
- улучшение климатического моделирования и прогнозирования;
- решение задач в области финансовой математики и инвестиций;
- улучшение алгоритмов искусственного интеллекта и машинного обучения.

Кроме того, квантовые компьютеры также могут привести к развитию новых технологий и научных открытий, которые мы не можем сейчас представить.

Пока что не существует полноценного квантового компьютера в том виде, в котором его представляют ученые. Но большие компании (IBM, Google, Microsoft Research, Intel) уже создали множество прототипов таких машин и продолжают процесс их модернизации в погоне за числом кубитов. На данный момент самым мощным квантовым компьютером является созданный в 2022 году IBM Quantum System Two, использующий квантовый процессор IBM Osprey, с 433 кубитами. Google Sucamore процессор на 53 кубита – первый процессор, который по заверениям разработчиков достиг квантового превосходства [2].

Рядовому пользователю получить доступ к такой технологии пока что почти невозможно. Исключением, например, является библиотека Qiskit, которая позволяет запускать программы на квантовом компьютере IBM Q. Однако по заверениям Google, они планируют создать к 2029 году первый коммерческий квантовый компьютер. Если говорить про Россию, то Российский ионный квантовый компьютер на четырех кубитах в скором времени сделают доступным всем желающим через платформу облачных вычислений, которая разработана в Российском квантовом центре [3].

Помимо собственно реализации квантовых компьютеров для работы с ними требуются специальные языки программирования, которые учитывают специфику элементов квантового компьютера, в котором базовыми элементами являются не классические логические операции над двоичными

числами, а гейты. В квантовых вычислениях, гейты – это операции, которые применяются к кубитам для изменения их состояния. Как правило, они представляют собой матричные операции.

Для квантовых ПК разработан целый ряд языков [4, 5]. Одним из первых языков, реализованных для квантового программирования является Quantum computing language (QCL). Он отдаленно напоминает язык C (в отношении синтаксиса и типов данных), и, был создан для изучения концепции программирования на квантовых компьютерах.

Из множества существующих высокоуровневых языков можно выделить несколько самых известных. В 2010 году появился Quipper, он позволил выражать общие понятия, действия и концепции, без углубления в низкоуровневые инструкции и операции. Самым ближайшим аналогом языка Quipper, работающим на обычных компьютерах, является Java.

Пожалуй, самым популярным является Q# – высокоуровневый язык программирования, разработанный в 2017 году, который нивелирует необходимость иметь глубокие знания в квантовой физике. Он несколько похож на C# и предназначен для аппаратного обеспечения, масштабирования для всего спектра квантовых приложений и оптимизации выполнения.

Самым молодым из существующих языков на данный момент является, созданный в 2022 году, Silq. По заверениям разработчиков он производит программы, которые значительно короче, чем те, что написаны на упомянутых выше языках, а также использует гораздо меньше примитивов.

Следующий представитель не относится к высокоуровневым. Исходный код OpenQASM был выпущен как часть программного обеспечения IBM Quantum Information Software Kit (QISKit) для использования с квантовой вычислительной платформой Quantum Experience. OpenQASM имеет общие черты со специализированными языками программирования (такими, как Verilog), используемыми для описания структуры и поведения электронных схем.

Про него поговорим более детально. Вернее, про его версию в виде библиотеки Qiskit для Python [6]. Qiskit – фреймворк для квантовых вычислений с открытым исходным кодом, разрабатываемый исследовательской группой IBM Research, а также сообществом энтузиастов с целью создания ПО для облачных квантовых вычислений. Основная версия Qiskit использует Python в качестве языка программирования, однако доступны также версии для языков Swift JavaScript. Данный фреймворк предоставляет возможность разработки квантового ПО как на высоком уровне абстракции (для пользователей без опыта квантового программирования), так и на низком уровне, близком к машинному коду OpenQASM. Главным преимуществом Qiskit является возможность бесплатно проводить вычисления на суперкомпьютере IBM с предоставлением 5 кубитов.

На рис. 1 приведен пример программы для квантового компьютера, написанный с помощью рассмотренной библиотеки. На рис. 2 продемонстрирована схема, иллюстрирующая алгоритм работы программы. Блок с буквой H обозначает оператор Адамара, второй – гейт контролируемого отрицания CNOT, два оставшихся показывают считывание состояния кубита. Поставленной задачей является демонстрация распределения значений двух кубитов после применения к ним двух простых гейтов.

```
from qiskit import QuantumCircuit, transpile
from qiskit.providers.aer import QasmSimulator

simulator = QasmSimulator()

circuit = QuantumCircuit(2, 2)

circuit.h(0)
circuit.cx(0, 1)
circuit.measure([0,1], [0,1])

compiled_circuit = transpile(circuit, simulator)

job = simulator.run(compiled_circuit, shots=1000)

result = job.result()

counts = result.get_counts(compiled_circuit)
print("\nОбщее количество 00 и 11 :",counts)

circuit.draw()
```

```
Общее количество 00 и 11 : {'11': 506, '00': 494}
```

Рис. 1. Листинг программы

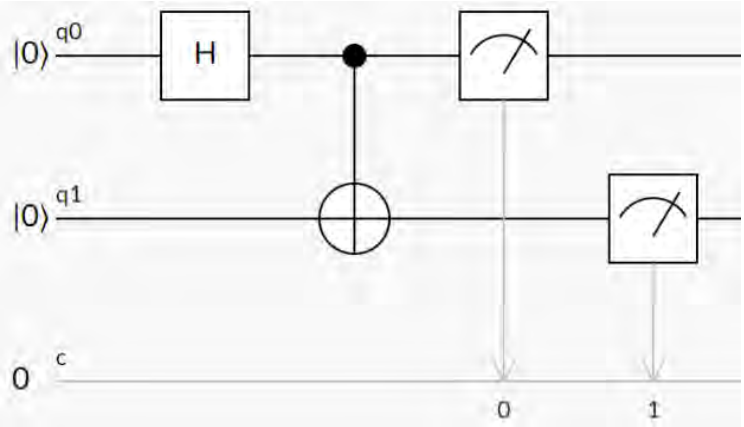


Рис. 2. Схема

После импорта необходимых библиотек, создаются два кубита. Далее к первому применяется оператор Адамара, который действует на кубит по правилу:

$$\widehat{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$
$$\widehat{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

После чего, к обоим применяется оператор CNOT (контролируемое отрицание). Следующим шагом считываются значения обоих кубитов и идет их передача в симулятор. Из него получаем результат и перемещаем его в переменную counts. Далее на экран выводятся результат распределения значения кубитов, сообщение и схема с обозначением гейтов.

Направление квантовых вычислений очень быстро развивается, тем самым представляя угрозу существующим системам шифрования, но подводят нас к новым перспективам в области безопасности, таким как квантовая криптография и новые методы шифрования. Квантовые компьютеры выводят вычисления на новый уровень, а вариативность языков и симуляторов позволяет программистам быстро освоить их и начать работу в новой области. Уже в настоящий момент возможно составление программ для квантовых компьютеров и их выполнение на симуляторах, а в дальнейшем и на реальных квантовых компьютерах.

Список используемых источников

1. Сысоев С. С. Введение в квантовые вычисления. Квантовые алгоритмы: учеб. пособие. СПб. : Изд-во С.-Петерб. ун-та, 2019. 144 с.

2. Google достигла квантового превосходства [Электронный ресурс] // Хабр (habr.com). URL: https://habr.com/ru/news/t/468361/ (дата обращения 10.02.2023).

3. Доступ к российскому квантовому компьютеру предоставят всем желающим [Электронный ресурс] // Наука тасс (nauka.tass.ru). URL: https://nauka.tass.ru/nauka/13315055/ (дата обращения 10.02.2022)

4. Баскаков П. Е., Хабовец Ю. Ю., Пилипенко И. А., Кравченко В. О., Черкессова Л. В. Инструменты для выполнения и эмуляции квантовых вычислений // Вестник НГУ. Серия: Информационные технологии. 2020. Т. 18, N 2. С. 43–53.

5. Как стать программистом квантовых компьютеров [Электронный ресурс] // Proglib (proglib.io). URL: https://proglib.io/p/kak-stat-programmistom-kvantovyh-kompyuterov-2022-08-30 (дата обращения 10.02.2023).

6. Кайзер С., Гранад К., Изучаем квантовые вычисления на Python и Q# : пер. С англ. А. В. Логунова. М. : ДМК Пресс, 2021. 430 с.

УДК 621.391.1
ГРНТИ 49.33.29

АНАЛИЗ МЕТОДОВ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ СЕТЕЙ АВТОТРАНСПОРТА НА ОСНОВЕ СИСТЕМЫ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ.

Т. В. Лаптева, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Подключенные транспортные средства – один из основных анонсированных вариантов использования сотовой системы пятого поколения. Это новая эра коммуникации, которая известна как автомобильные сети и включает в себя множество форм и услуг. Автомобильные сети предоставляют все услуги, связанные с развертыванием автономных транспортных средств и обменом данными между близлежащими транспортными средствами. Такие системы требуют полного охвата, сверхвысокой надежности и доступности, сверхнизкой задержки и высокой гибкости системы в соответствии с Партнерским проектом 3-го поколения и Международным союзом электросвязи. Ознакомление с сетью доступа автомобильной сети для предоставления вычислительных ресурсов на границе сети будет первой частью этой работы. Это уменьшит сквозную задержку, уменьшит перегрузку сети, достигнет более высокой надежности и повысит ее гибкость.

граничные множественные вычисления, сети автотранспорта, интернет вещей.

В результате развития информационных технологий помимо трафика, генерируемого людьми, появляется также трафик, генерируемый устройствами – трафик Интернета вещей. Кроме этого, при повсеместном использовании приложений Интернета вещей (IoT) возникают межмашинные коммуникации и связь между транспортными средствами. В результате чего объем передаваемых данных стремительно увеличивается.

Производители, перед которыми стоит задача поддержки глобально распределенных парков подключенных транспортных средств, столкнутся с проблемами, связанными со сбором и обработкой данных. Решение, предложенное консорциумом автомобильных технологий (AECC), предусматривает возможность выполнять локальную обработку данных, ближе к местоположению систем автомобиля, вместо того чтобы пытаться вернуть данные в несколько централизованных мест [1].

Граничные вычисления с множественным доступом (MEC) широко признаны в качестве ключевой технологии для обеспечения требований к сверхнизким задержкам, а также предназначенных для переноса вычисле-

ний и хранения данных из удаленного облака (общедоступного или частного) ближе к источнику их обработки. Для нового класса «приложений 5G» это часто является острой необходимостью. Размещение таких приложений в традиционном облаке не позволяет удовлетворить строгие требования к задержкам приема-передачи. MEC реализуют возможности облачных вычислений на границе сети.

Автомобильная ассоциация 5G (5GAA) рассматривает пограничные вычисления как одну из ключевых поддерживающих технологий для многих сервисов V2X для подключенного и автоматизированного вождения. Ею разработана рабочая программа «Технология MEC для поддержки автомобильных услуг» (MEC4AUTO). Несмотря на множество остающихся проблем, текущая рабочая программа 5GAA направлена на демонстрацию использования технологии MEC для автомобильных сервисов, например, в системах с несколькими пограничными облаками операторов мобильной сети (MNO), несколькими OEM, несколькими MEC.

Основные характеристики системы множественных граничных вычислений (MEC), которые отличают их от других «пограничных вычислений»: близость к конечным пользователям, сверхнизкая задержка, высокая пропускная способность, доступ в реальном времени к радиосети и контекстной информации, а также осведомленность о местоположении.

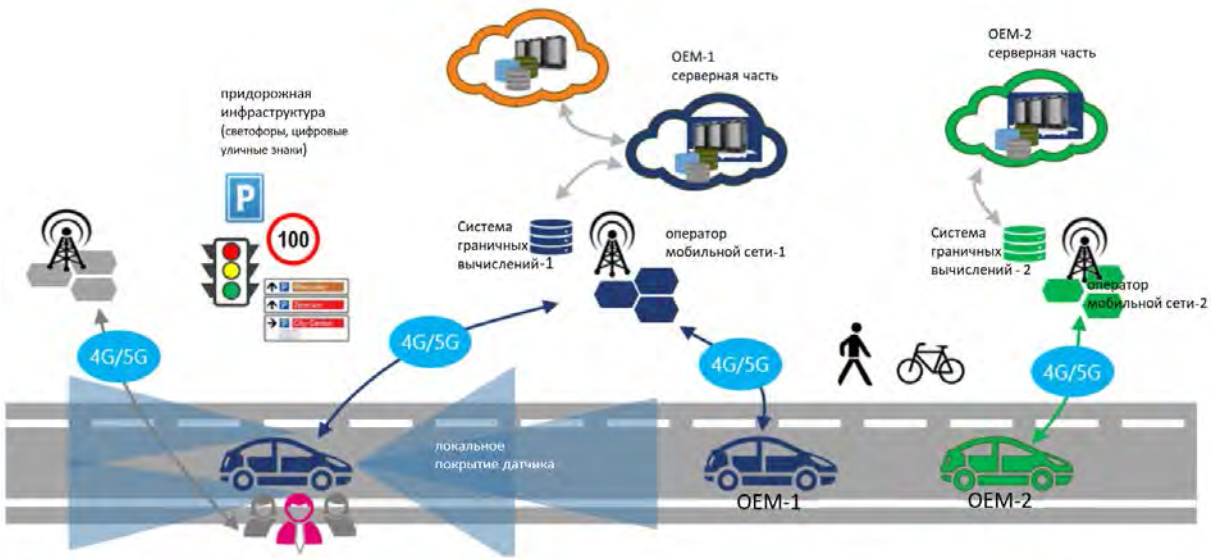


Рис. 1. Поддержка граничных вычислений для автомобильных сценариев (с точки зрения MEC4AUTO)

Автомобильный рынок – один из ключевых вертикальных сегментов, стимулирующих внедрение Edge Computing [2]. На рис. 1 ниже показан типичный автомобильный сценарий «Технология MEC для поддержки автомобильных услуг (MEC4AUTO)», созданный ассоциацией 5GAA, в котором несколько транспортных средств, потенциально принадлежащих разным

производителям автомобилей, и другие устройства (VRU) подключены к придорожной инфраструктуре (RSU) и сотовой сети (RAN). Экземпляры клиентских приложений обычно могут взаимодействовать с серверными приложениями, т. е. в пограничных облаках, удаленных облаках и/или OEM/частных облаках.

В целом, с точки зрения приложений, внедрение Edge Computing представляет собой переход от «традиционной» клиент-серверной модели разработки приложений на трехуровневый сдвиг парадигмы. Фактически, появление Edge Computing (например, MEC) трансформирует эту среду, вводя промежуточный элемент на границе с сетью радиодоступа (RAN) в качестве дополнительной точки присутствия (PoP) MEC (рис. 2), обычно отличной от традиционной удаленной облачной точки присутствия (например, даже на другом континенте). Возможны разные уровни периферийного развертывания, также связанные с разными бизнес-моделями и владельцами облака; во всех таких случаях введение MEC предоставляет разработчику приложений дополнительную гибкость, позволяющую специально проектировать компоненты на границе сети при разработке приложений.

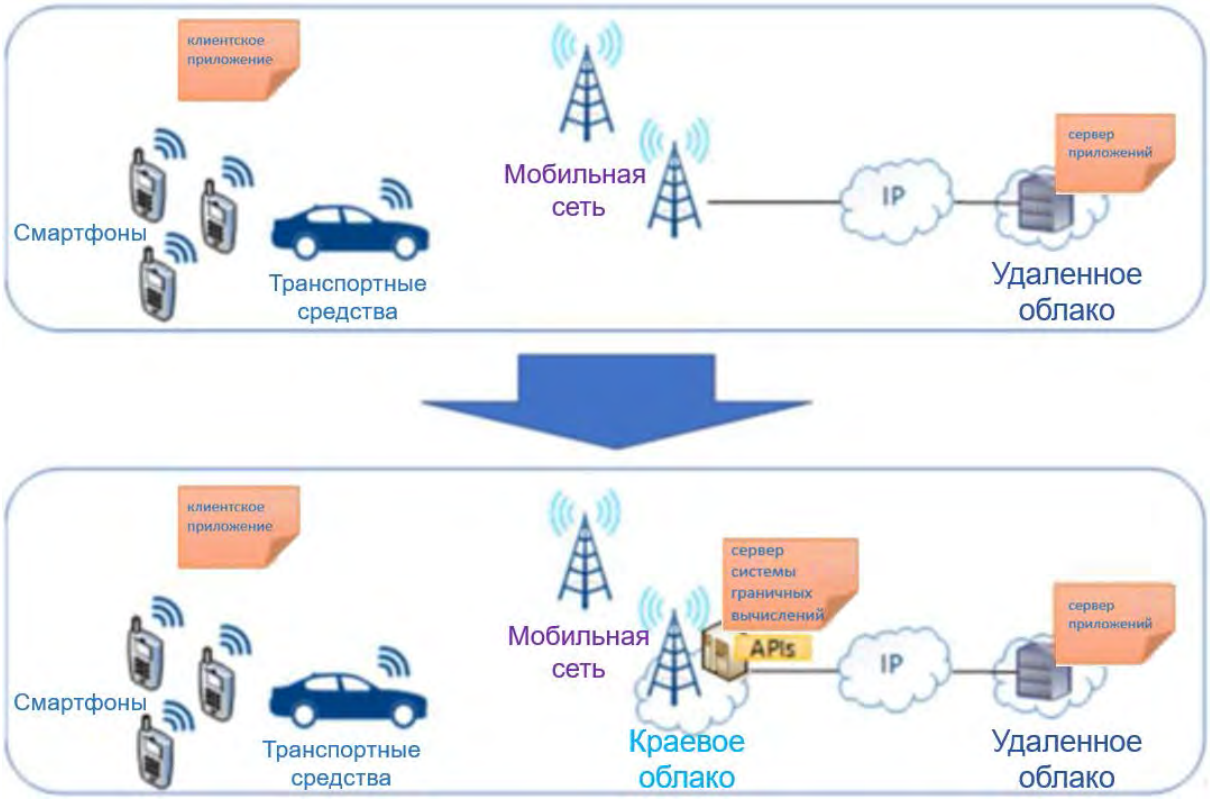


Рис. 2. Пример смены трехуровневой парадигмы с точки зрения разработки приложений

В результате получается новая модель разработки с тремя «местоположениями»: клиент, ближний сервер (на границе облака), дальний

сервер (в удаленном облаке). Местонахождением клиента может быть традиционный смартфон (VRU) или другие вычислительные элементы с беспроводным подключением в автомобиле или опять же придорожная инфраструктура. Более того, эта модель является совершенно новой для большинства разработчиков программного обеспечения не только из-за введения промежуточного экземпляра приложения (на границе), но и из-за возможности приложения MEC потреблять данные и пограничные службы локально, например, предоставляемые через RESTful API платформы MEC, как показано на рис. 2 [2].

В [3] представлены различные варианты развертывания систем MEC в сетях 4G и 5G:

– Подход «натыкайся на провод»: платформа MEC и приложения могут быть развернуты между сетью доступа и базовой сетью. В этом решении низкая задержка поддерживается за счет установки платформы MEC вплоть до базовых станций сети (*ENodeB*, eNB) или в местах, обеспечивающих минимальную задержку.

– Распределенный подход базовой пакетной сети (*Evolved Packet Core*, EPC): платформа и приложения MEC расположены в этом развертывании через усовершенствованную базовую сеть пакетной передачи данных (EPC). Для распределенного подхода EPC возможны различные варианты: хост MEC является внешним по отношению к сети 3GPP, а плоскость данных MEC находится за интерфейсом SGi другой вариант распределенного EPC является развертывание узлов MEC рядом с Serving Gateway (SGW) и PGW EPC [6]. Во втором варианте хост MEC совмещен с локальным выходом (SGW-LBO). В этом случае платформа MEC является доверенным приложением оператора EPC и SGW-LBO может размещаться на платформе MEC.

Для сетей 5G системный оркестратор MEC (MEAO) обменивается информацией с сетью MNO с помощью функции сетевого воздействия или NEF. Система управления MEC, организующая работу хостов и приложений MEC, может динамически решать, где развертывать приложения MEC [4].

Кроме этого, для обеспечения поддержки краевых вычислений применяются две основные технологии виртуализации: на основе гипервизора и контейнера.

С развитием контейнеризации, как одной из технологий поддержки туманных/краевых вычислений, встал вопрос управления распределением вычислительной нагрузки (оркестрации) для обеспечения эффективного использования географически-распределенных ресурсов.

Посредством размещения на узлах сервисов и их оркестрации, обеспечивается эффективная совместная работа вычислительных сервисов для решения задач, возложенных на туманную/граничную среду [5].

Анализ существующих работ

Многие исследователи предлагают использовать пограничные вычисления для решения проблем распределения ресурсов, включая потребление энергии и задержки обслуживания, повышения производительности и надежности сетей автотранспорта.

Ниже представлены основные работы, имеющие отношение к предметной области.

В работе [6] рассматривается подход к распределению граничных ресурсов на основе механизма аукциона, для минимизации потребляемой энергии и снижения времени задержки вычислений. Главное преимущество метода в том, что он не основан на полезности узлов. Таким образом, можно добиться желаемого распределения ресурсов, не зная функций полезности задействованных объектов. Результаты моделирования показали, что предложенный метод превосходит существующие.

В работе [7] представлены исследования для решения научной проблемы построения архитектуры сети транспортных средств для надежной доставки правильных и бескомпромиссных данных в рамках концепции V2X для повышения безопасности участников дорожного движения с использованием технологии блокчейн и мобильных пограничных вычислений. Научная работа предоставляет формализованную математическую модель системы, учитывающую взаимосвязь объектов и информационных каналов V2X, а также энергоэффективный алгоритм разгрузки трафика на сервере MEC.

В работе [8] оценена работоспособность различных припаркованных транспортных средств в совместных пограничных вычислениях для выбора стабильных исполнителей задач и решения проблемы оптимизации планирования ресурсов между припаркованными транспортными средствами и пограничными серверами. Также в этой статье описываются основные объекты и связанные с ними функции в сети, а также предлагается безопасный и надежный протокол для взаимодействия между объектами.

Заключение

Системы граничных вычислений позволяют поддерживать высокий уровень масштабируемости, доставки данных в режиме реального времени и мобильности в автомобильных одноранговых сетях (VANET). Использование комплексного подхода к возможностям MEC, а также таких перспективных методов и технологий как, например, аукционный метод распределения ресурсов с использованием многоагентного подхода и Blockchain позволят в будущем увеличить производительность и надежность сетей автотранспорта.

Список используемых источников

1. Distributed Computing in an AECC System (White Paper) Version 1.0.0, August 18, 2021.
2. 5GAA MEC for Automotive in Multi-Operator Scenarios, Version 1.0, 03.03.2021.
3. 5GAA_XWI2 190090, ‘MEC deployment options in ETSI’, Mitsubishi, November 2019.
4. ETSI White Paper No. 28 MEC in 5G networks, June 2018.
5. Кирсанова А. А., Радченко Г. И., Черных А. Н. Обзор технологий организации туманных вычислений // Вестник ЮУрГУ. Серия: Вычислительная математика и информатика. 2020. Т. 9, N 3. С. 35–63. DOI: 10.14529/cmse200303.
6. Mahmood Omar Abdulkareem, Abdellah Ali R., Muthanna Ammar and Koucheryavy Andrey Distributed Edge Computing for Resource Allocation in Smart Cities Based on the IoT [Электронный ресурс] // NetApp URL: https://www.mdpi.com/2078-2489/13/7/328 (дата обращения 15.03.2023).
7. Vladyko Andrei, Elagin Vasiliy, Spirkina Anastasia, Muthanna Ammar, and Ateya Abdelhamied, Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications [Электронный ресурс] //NetApp URL: https://www.mdpi.com/2079-9292/11/2/173 (дата обращения 11.03.2023).
8. Mohammad Ayoub Khan. Edge Computing Resource Allocation and Optimization Method and Its Application in Internet of Vehicles Environment [Электронный ресурс] // NetApp URL: https://www.hindawi.com/journals/scn/2022/7333068/ (дата обращения 11.03.2023).

УДК 004.05
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В СМЕШАННОМ СЕТЕВОМ ДОМЕНЕ

Н. А. Лебедев, Д. А. Свечников

Академия федеральной службы охраны Российской Федерации

Рассматривается вариант организации защиты информации в смешанном сетевом домене, включающем рабочие станции под управлением ОС Windows и Astra Linux. Предлагаемое решение позволит обрабатывать информацию ограниченного доступа, не содержащей сведения составляющие государственную тайну в автоматизированных системах разных классов защищенности за счет комплексного применения подсистем защиты информации ОС Astra Linux SE, Secret Net Studio, Secret Net LSP и средства доверенной загрузки «Соболь».

информационная безопасность, защита информации, мониторинг, реагирование на инциденты информационной безопасности.

Вопросу своевременности перехода на использование российского программного обеспечения на значимых объектах критической информационной инфраструктуры (КИИ) Российской Федерации уделяется большое внимание. Разработаны и утверждены методические рекомендации и план перехода на использование российского программного обеспечения для государственных и ведомственных информационных систем РФ [1].

Ведущими российскими компаниями накоплен определенный опыт по разработке и сертификации операционных систем (ОС) и программного обеспечения (ПО). На значимых объектах КИИ РФ допускается применение только сертифицированных ФСБ РФ и ФСТЭК РФ ОС и ПО.

Широкое применение получила операционная система специального назначения (ОССН) Astra Linux SE, сертифицированная ФСБ РФ, ФСТЭК РФ, а также Министерством обороны РФ [2]. Современная версия ОСНН – Astra Linux SE 1.7 имеет несколько конфигураций, отличающихся по набору мер защиты информации и функционалу «Базовый», «Усиленный» и «Максимальный».

Вместе с тем, в результате проведенного анализа было выявлено, что базовые средства защиты ОССН Astra Linux SE не в полной мере удовлетворяют требованиям нормативных документов [3, 4], в части реализации мер защиты информации: многофакторная аутентификация; разграничение доступа к управлению BIOS/UEFI; контроль целостности аппаратной конфигурации; фильтрация трафика при сетевом взаимодействии; удаленное управление, мониторинг и реагирование на инциденты безопасности домена.

В настоящее время полный переход на российское ПО и ОС не возможен, так как большая часть ИС функционирует под управлением разнотипных ОС иностранного производства и использует только совместимое прикладное программное обеспечение (например, ОС *Windows*).

На базе разработанного программно-аппаратного стенда проведены исследования задачи обеспечения защиты информации в смешанном сетевом домене, функционирующем под управлением ОС Windows и ОССН Astra Linux SE на базе сертифицированного ПО ООО «Код Безопасности»: ПАК «Соболь», Secret Net Studio в роли «Сервер безопасности» и «Защитные компоненты» на ОС Windows, Secret Net LSP на ОС Astra Linux в роли агента безопасности. Комплексное применение данного ПО на базе ОССН Astra Linux SE позволило расширить меры защиты информации в смешанном сетевом домене.

На всех объектах домена установлен и настроен ПАК «Соболь». Программное обеспечение Secret Net LSP выступает в роли агента безопасности, функционирует в сетевом режиме и, при взаимодействии с серверной частью ПО Secret Net Studio, обеспечивает следующие возможности:

– защиту от внутренних угроз; мониторинг событий безопасности; управление объектами домена; защиту от утечки информации; фильтрацию трафика.

На базе ПО Secret Net Studio развернут «Сервер безопасности», что позволило реализовать для всех объектов домена:

а) *Контроль доступа*: управление доступом пользователей к информационным и системным ресурсам домена.

б) *Мониторинг событий*: регистрация и анализ событий безопасности домена, формирование отчетов об активности пользователей.

в) *Централизованное управление*: управление настройками безопасности всех объектов домена.

Для определения варианта построения СЗИ, имеющего максимальный набор мер защиты информации при ограничениях на стоимость и сложность их реализации сформулирована задача оптимизации. Для ее решения применен показатель защищенности ИС, позволяющий оценить степень выполнения требований безопасности на основе соотношения количества, реализованных в ИС мер защиты информации к максимально возможному количеству мер защиты информации для данного класса защищенности ИС [5]:

$$Y_{tr} = \frac{i_{tr}}{\max_{tr}},$$

где i_{tr} – количество мер защиты информации реализованных в информационной системе $i = \overline{1, n}$, $\max_{tr}$ – максимально возможное число мер защиты информации в ИС с учетом предъявляемых требований и существующих ограничений на стоимость набора мер защиты информации $(C \in [0;1]) \to min$ и сложность реализации решения $(S \in [0;1]) \to min$.

Полученные результаты расчетов представлены в таблице 1.

ТАБЛИЦА 1. Расчеты показателя защищенности информационной системы

Уровень защищенности	Максимальный	Усиленный				
Дополнительные меры защиты	Нет	ПО Secret Net Studio	ПАК Соболь	ПО Secret Net LSP	ПАК Соболь, Secret Net LSP	ПАК Соболь, Secret Net LSP, Secret Net Studio
C	0,99	0,69	0,6	0,67	0,7	0,75
S	0,6	0,65	0,65	0,65	0,7	0,74
Y_{tr}	0,9	0,6	0,78	0,7	0,84	0,99

Таким образом, максимальное значение показателя защищенности ИС при принятых ограничениях на стоимость набора мер защиты информации

и сложность его реализации в смешанном сетевом домене может быть достигнуто за счет совместного применения ОС Astra Linux SE 1.7 (уровень защищенности «Усиленный») при дополнительном применении ПАК Соболь, ПО Secret Net LSP и ОС Windows защищенной ПО Secret Net Studio в ролях «Сервер безопасности» и «Защитные компоненты».

Список используемых источников

1. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.01.2023 № 21 «Об утверждении методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры РФ, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в РФ».

2. Astra Linux Special Edition – операционная система специального назначения. URL: https://astralinux.ru/products/ (дата обращения 15.03.2023).

3. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

4. Решение Коллегии Гостехкомиссии России № 7.2 от 02.03.2001 «Специальные требования и рекомендации по технической защите конфиденциальной информации».

5. Курочкин С. И., Заводцев И. В. Методы оценки уровня защищенности информационных систем // Перспективы развития информационных технологий. 2016. N 29. С. 197–204.

УДК 004.056
ГРНТИ 81.93.29

ПОДХОД К ИМИТАЦИОННОМУ МОДЕЛИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ ДЛЯ АНАЛИЗА КИБЕРФИЗИЧЕСКИХ АТАК

Д. С. Левшун

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Объекты критически важной инфраструктуры являются неотъемлемой частью ключевых сфер экономики и напрямую связаны с обеспечением жизнедеятельности населения. Нарушение функционирования данных объектов приводит не только к финансовому и репутационному ущербу, но и оказывает влияние на экономику в целом. При этом число компьютерных атак на информационные ресурсы стремительно растет. Одним из возможных способов анализа защищенности подобных объектов является

их моделирование. В данной работе предлагается оригинальный подход к имитационному моделированию объектов критически важной инфраструктуры для анализа киберфизических атак. Новизна данного подхода заключается в динамическом анализе атак за счет информации о процессах и ресурсах системы, выявления конфликтов и пограничных состояний, многоагентного моделирования, событийного моделирования, моделирования атакующих с различным уровнем компетенции и правами доступа, моделирования атак и их последствий.

информационная безопасность, критически важная инфраструктура, киберфизическая атака, имитационное моделирование.

В настоящее время системы, использующие технологии Интернета вещей – это неотъемлемая часть любой сферы жизнедеятельности человека, что обусловливает критическую важность обеспечения их защищенности. При этом решить данную задачу в полной мере, как показывает практика в России и за рубежом, пока не удалось.

Последствия отказа критически важных систем, в том числе связанные с деятельностью злоумышленников, включают в себя как финансовый и репутационный ущерб, так и угрозу жизни и здоровью человека [1].

Одним из возможных направлений атаки является использование слабых мест и архитектурных дефектов, наличие которых в подобных системах обусловлено различными факторами. При этом распространенность угроз информационной безопасности в том числе связана с разработкой систем Интернета вещей без участия специалистов в области информационной безопасности с применением слабозащищенных протоколов передачи данных, выходом в сеть Интернет и использованием непроверенного на наличие ошибок кода [2].

Решение данной проблемы является важной задачей, именно поэтому были разработаны и применяются на практике различные подходы к моделированию систем Интернета вещей в интересах анализа атакующих действий, а также выявления нарушений конфиденциальности информации и аномальной активности. А для отображения различных аспектов сложных систем и выявления потенциальной возможности различных атак используются аналитические [3], имитационные [4], полунатурные [5] и гибридные [6] модели, каждая из которых анализирует отдельные аспекты информационной безопасности систем Интернета вещей, в том числе задействованных на объектах критически важной инфраструктуры.

Имитационное моделирование представляет собой создание системы во времени с имитацией различных процессов. При этом может использоваться среда моделирования общего назначения, такая как SIMULINK-Matlab, LabVIEW, Dymola и т. п., или специализированная среда, адаптированная под определенную область. Зачастую, в таких средах работа системы моделируется для определения эффективности функционирования, как

например, в [7] определяются варианты развертывания датчиков беспроводных сенсорных сетей для обеспечения качественного и оптимального покрытия и связи. С точки зрения безопасности имитационное моделирование позволяет учитывать динамическую составляющую при создании сценариев атак. Так анализ данных журналов событий (или логов) является важной задачей, когда речь идет о понимании поведения сложных систем и сетей, и позволяет проводить анализ безопасности, диагностику неисправностей, анализ производительности или обнаружение вторжений. В [8, 9] приводятся генераторы шаблонов журналов событий, которые соответствуют всем строкам журнала в кластере и, следовательно, описывают общие характеристики строк. В [10] исследуются идентификация, моделирование и оценка атак в интеллектуальных сетях и предлагается модель для представления сценариев атак в виде комбинации типов атак, схемы атаки и их временного возникновения. В [11] описан испытательный виртуальный стенд PowerCyber, который объединяет аппаратное и программное обеспечение отраслевого диспетчерского управления и сбора данных (SCADA), а также методы эмуляции и моделирования для обеспечения точной кибер-инфраструктуры электросетей.

Рассмотрим подход к имитационному моделированию объектов критически важной инфраструктуры, предлагаемый в данной работе для анализа киберфизических атак.

В основе имитационного моделирования предлагается использовать графы атак, в рамках которых каждый узел графа анализируемой сетевой системы будет представлять собой отдельный хост или устройство, а каждое ребро – сетевое взаимодействие между ними. Для анализа возможности компрометации каждого узла, предполагается объединение классических методов статического анализа на основе CVSS метрик с динамическими вероятностями успешности применения доступных злоумышленнику CVE. При этом вероятность успешности применения будет зависеть от параметров злоумышленника, доступных атакуемому узлу ресурсов, а также размещенных на нем средств защиты. Для устройств без информации об CVE, предполагается их предположение на основе их конфигурации, что позволит расширить применения подхода на устройства Интернета вещей. Дополнительным параметром для анализа киберфизических атак послужит время, позволяющая оценить скорость продвижения злоумышленника по исследуемой системе в зависимости от используемых мер противодействия. Более того, предлагаемый подход позволит оценить ущерб от вредоносной деятельности.

Список используемых источников

1. Левшун Д. С., Чечулин А. А., Котенко И. В. Жизненный цикл разработки защищенных систем на основе встроенных устройств // Защита информации. Инсайд. 2017. N 4. С. 53–59.

2. Котенко И. В., Чечулин А. А., Левшун Д. С. Анализ защищенности инфраструктуры железнодорожного транспорта на основе аналитического моделирования // Защита информации. Инсайд. 2017. N 6. С. 48–57.

3. Andres-Maldonado P. et al. Analytical modeling and experimental validation of NB-IoT device energy consumption // IEEE Internet of Things Journal. 2019. – Vol. 6. – N 3. – PP. 5691–5701. DOI: 10.1109/JIOT.2019.2904802.

4. Çeken C., Abdurahman D. Simulation modeling of an iot based cold chain logistics management system // Sakarya University Journal of Computer and Information Sciences. 2019. Vol. 2. No. 2. PP. 89–100. DOI: 10.35377/saucis.02.02.598963.

5. Petrenko V. I. et al. Development of Methods and Software Modules Security Assessment Information of Limited Distribution // Innovative Approaches to the Application of Digital Technologies in Education and Research. CEUR Workshop Proceedings. 2019.

6. Riahi A. et al. A systemic approach for IoT security // 2013 IEEE international conference on distributed computing in sensor systems. IEEE, 2013. PP. 351–355. DOI: 10.1109/DCOSS.2013.78.

7. Kaiwartya O. et al. T-MQM: Testbed-based multi-metric quality measurement of sensor deployment for precision agriculture — A case study // IEEE Sensors Journal. 2016. Vol. 16. N 23. PP. 8649–8664.

8. Wurzenberger M. et al. Creating Character-based Templates for Log Data to Enable Security Event Classification // Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. 2020. PP. 141–152.

9. Mudholkar A. et al. Analysis of Automated Log Template Generation Methodologies // Advances in Artificial Intelligence and Data Engineering. Springer, Singapore, 2021. PP. 571–588.

10. Tundis A., Egert R., Mühlhäuser M. Attack scenario modeling for smart grids assessment through simulation // Proceedings of the 12th International Conference on Availability, Reliability and Security. 2017. PP. 1–10.

11. Hahn A. et al. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid // IEEE Transactions on Smart Grid. 2013. Vol. 4. N 2. PP. 847–855.

УДК 621.39
ГРНТИ 49.01.85

НЕПРЕРЫВНОСТЬ И АВТОНОМНОСТЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ – ЭЛЕМЕНТЫ ЕЕ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ

О. М. Лепешкин[1], О. А. Остроумов[1], О. Е. Пирогов[2], И. С. Черных[2]

[1]Санкт-Петербургский государственный политехнический университет
[2]Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Любая система управления сложные технические объекты, критически важные объекты на современном этапе развития техники используют линии, узлы, систему

связи. Одними из свойств системы связи является непрерывность и автономность функционирования системы, характеризующих способность выполнять функции системы, выполнение которых описывается функциональной устойчивостью системы. В работе рассматривается обеспечение функциональной устойчивости сложной технической системы.

критическая информационная инфраструктура, критически важный объект, функциональная устойчивость, непрерывность, автономность, система связи, система управления, задачи, функции.

Развитие техники, различных систем привело к увеличению их возможностей выполнять большее количество функций и задач с лучшим качеством. Наряду с этим, возросла интенсивность воздействий злоумышленников, использующих различные дестабилизирующие факторы влияющих на устойчивое функционирование различных систем, объектов, средств. Возрастание возможностей систем, количества выполняемых ими функций и задач, потребности в них вышестоящей системы, других объектов определяют зависимость от них. Такие объекты и системы становятся критически важными [1, 2, 3]. При этом, критичность обусловлена, в первую очередь, потенциальной возможностью нарушения их функционирования, т. е. не выполнения требуемого количества функций и задач [4, 5]. Последствиями воздействия дестабилизирующих факторов будет возникновение в системе конфликта, обусловленного потребностью системы в получении ресурса, выполнении ее элементом функции или задачи, и реальным состоянием данного элемента, всей системы, в котором она не может их предоставить, выполнить.

Повсеместная цифровизация, использование в различных сферах жизни общества, промышленности технических средств, предназначенных для обработки информации, функционирующих как программно-аппаратное средство, способствуют тому, что наиболее опасным дестабилизирующим фактором являются информационно-технические воздействия [6, 7]. При этом, в данной работе интерес представляет возможность воздействия и его последствия, приводящие к нарушению функционирования системы, объекта.

Под функциональной устойчивостью системы, объекта понимается их способность выполнять свое целевое предназначение и весь требуемый перечень функций и задач за счет требуемого ресурса в установленные сроки, с требуемым качеством в условиях изменяющейся обстановки [5, 8, 9].

Составляющими функциональной устойчивости (ФУ) являются непрерывность (НФС) и автономность функционирования системы (АФС).

$$ФУ = НФС + АФС.$$

Под непрерывностью функционирования системы понимается ее способность выполнять требуемый перечень функций системы в установленные сроки в условиях пополнения ресурса. При этом предполагается, что постоянно имеется возможность затребовать необходимый ресурс и его получить в требуемые для обеспечения выполнения функции сроки. Определение непрерывности функционирования системы можно записать следующим образом:

$$\forall F_{\text{ф}} \forall t_{\text{ф}} \forall F_{\text{ф треб}} \exists A, \lim_{t_{\phi}\to\infty} \lim_{r\to\infty} \lim_{F_{\text{ф}}\to\infty} f(x) = A \left| \begin{array}{c} x = \dfrac{F_{\text{ф}}(r,t)}{F_{\text{ф треб}}} \\ \dfrac{t_{\text{ф}}}{t_{\text{ф треб}}} \to 1 \\ r \in R, r \neq \text{const}, r \geq r_{треб}. \end{array} \right. \quad (1)$$

Под автономностью функционирования системы понимается ее способность выполнять требуемый перечень функций, при условии отсутствия возможности привлекать (пополнять) дополнительные ресурсы. Определение автономности функционирования системы можно записать следующим образом:

$$\forall F_{\text{ф}} \forall t_{\text{ф}} \forall F_{\text{ф треб}} \exists A, \lim_{t_{\phi}\to\infty} \lim_{r\to\infty} \lim_{F_{\text{ф}}\to\infty} f(x) = A \left| \begin{array}{c} x = \dfrac{F_{\text{ф}}(r,t)}{F_{\text{ф треб}}} \\ \dfrac{t_{\text{ф}}}{t_{\text{ф треб}}} \to 1 \\ r \in R, r = \text{const}, r \leq r_{треб}. \end{array} \right. \quad (2)$$

Таким образом, обобщая выражения (1) и (2) функциональная устойчивость системы будет определяться отношением количества выполненных функций к требуемому количеству функций, которые система должна выполнить, исходя из потребностей вышестоящей системы, объектов, органов управления (лиц, принимающих решение):

$$\forall F_{\text{ф}} \forall t_{\text{ф}} \forall F_{\text{ф треб}} \exists A, \lim_{t_{\phi}\to\infty} \lim_{r\to\infty} \lim_{F_{\text{ф}}\to\infty} f(x) = A \left| \begin{array}{c} x = \dfrac{F_{\text{ф}}(r,t)}{F_{\text{ф треб}}} \\ \dfrac{t_{\text{ф}}}{t_{\text{ф треб}}} \to 1 \\ r \in R \end{array} \right. . \quad (3)$$

Для обеспечения устойчивого процесса функционирования системы предлагается, в отличие от известных подходов [6, 7, 10, 11], формализовать систему в виде совокупности взаимосвязанных структурной и функциональной характеристик. Структура системы характеризуется построением графа системы, вершины которого являются элементами системы, а дуги связями между элементами. Функциональная характеристика определяется графом выполнения целевого предназначения за счет выполнения целей, функций и задач системы и требований, предъявляемых к ним, за счет ресурсов системы. Связь структурной и функциональных характеристик системы осуществляется через ресурс системы. Ресурс рассматривается как ресурс первой и второй степени. К первому ресурсу относятся технические средства, находящиеся на элементах системы, обслуживающий и иной персонал системы. Ко второму типу ресурса отнесем производные качественные характеристики системы, появляющиеся вследствие функционирования ресурсов первого типа, самой системы, появления в ней новых связей, к нему, например, можно отнести пропускную способность линий связи.

Для реализации целевого предназначения системы, которое может меняться и зависит от потребностей вышестоящей системы, лиц, принимающих решение, а также для обеспечения ее устойчивого функционирования в условиях изменяющейся обстановки, формируется множество сценариев задействования элементов системы для выполнения различных задач, функций, целей системы. Совокупность таких состояний образуют множество состояний системы $S_1 = \{s_1, s_2, \ldots, s_i\}$, где i – количество состояний системы связи. Каждое состояние системы связи s_i характеризуется двумя составляющими структурной $s_с$ и функциональной $s_ф$, $s_i = \{s_с, s_ф\}$. Множеством функциональных характеристик элементов системы $s_ф = \{s_1, s_2, \ldots, s_ф\}$, где Ф – количество функциональных характеристик системы (задач, функций, целей системы), позволяющих за счет разнесенных в пространстве и времени ресурсов (элементов) системы, характеризующих ее структуру, $s_с = \{s_1, s_2, \ldots, s_с\}$, где c – количество совокупностей (набор) элементов системы, позволяющих выполнить каждую требуемую задачу, функцию, цель системы.

Совокупность состояний, характеризующих качество выполнения состояний S_1, образуют множество $S_2 = \{w_i\}$. Любое состояние определяется множеством показателей требований к функционированию системы и ее элементов $T^{(i)} = \left\{T_1^{(i)}, T_2^{(i)}, \ldots T_L^{(i)}\right\}$, где L – количество показателей требований.

Функционально устойчивое состояние системы называется такое состояние системы $S_{фу}$, в котором она способна гарантированно выполнить требуемый набор s_i, характеризуемый выполнением задач, функций и целей системы с требуемым качеством и в установленные сроки, тогда такое состояние будет иметь следующий вид:

$$W_{фу} = \left\{ s_i, w_i \middle| \forall i, \forall j : T_1^{(i)} \in T_1^{(\text{треб})}, T_2^{(i)} \in T_2^{(\text{треб})}, ..., T_L^{(i)} \in T_L^{(\text{треб})} \middle| t = t_\text{ф} \right\}.$$

Формирование сценариев действий представляет собой множество управляющих воздействий системы управления системой и ее органов управления, лиц, принимающих решение, которые можно представить, как

$$V = \{V_{11}, V_{21}, \ldots, V_{N1}, V_{12}, V_{22}, \ldots, V_{Ni}\},$$

где V_{Ni} – управляющее воздействие для i-го состояния системы, N – количество управляющих воздействий, позволяющих перевести систему в функционально устойчивое состояние.

Проблема обеспечение функциональной устойчивости сложных технических систем в современных условиях только возрастает [12], это связано с увеличением возможностей таких систем, возросшей нагрузкой на них, что определяет ее актуальность. Это же определяет их критичность для общества, других систем, промышленности, регионов, страны. В статье предлагается вариант декомпозиции функциональной устойчивости на непрерывность и автономность системы, характеризуемых выполнением системой функций за счет ресурсов. Кроме этого, в работе предлагается подход формирования сценариев выполнения функциональных характеристик системы (функций, задач, целей), выполнение которых позволит выполнить целевое предназначение системы, независимо от условий ее функционирования и воздействия на нее различных дестабилизирующих факторов.

Список используемых источников

1. Остроумов О. А., Савищенко Н. В., Лепешкин О. М. Выполнение регламента процесса управления — критерий определения критичности системы // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей III Всероссийской научно-технической конференции. Анапа, 2021. С. 625–634.

2. Сагдеев А. К., Лепешкин Е. О., Лепешкин О. М. Методологический подход оценки функциональной безопасности критической социотехнической информационной системы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. научн. ст. в 3-х т. СПб. : СПбГУТ, 2016. С. 294–299.

3. Петренко С. А. Концепция поддержания работоспособности киберсистем в условиях информационно-технических воздействий // Труды ИСА РАН. Т. 41. 2009. С. 175–193.

4. Бурлов В. Г., Лепешкин О. М., Кирилова Т. В. Моделирование процесса управления социальными и экономическими системами региона на основе потенциально активных элементов пространства и времени // Проблемы экономики и управления в торговле и промышленности. 2013. N 3 (3). С. 82–85.

5. Остроумов О. А. Методика обеспечения функциональной устойчивости системы связи // Вопросы радиоэлектроники. Сер. Техника телевидения. 2022. Вып. 1. С. 30–38.

6. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. N 4. С. 69–79.

7. Kotenko I., Saenko I., Lauta O. et al. An approach to modeling of the security system of intelligent transport systems based on the use of flat graphs // Lecture Notes in Networks and Systems (LNNS). 2021. Vol. 330. P. 440-451.

8. Кондрашов Ю. В., Сатдинов А. И., Синюк А. Д., Остроумов О. А. Концептуальная модель контроля функций системы связи для выявления конфликтных ситуаций // T-Comm: Телекоммуникации и транспорт. 2022. Т. 16. N 5. С. 21–27.

9. Лепешкин О. М., Остроумов О. А., Синюк А. Д. Систематизация основ методологии синтеза критической информационной инфраструктуры Российской Федерации // Военная мысль. 2021. N 8. С. 109–114.

10. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи : монография. СПб. : ПОЛИТЕХ-ПРЕСС, 2018. 214 с.

11. Одоевский С. М., Лебедев П. В. Методика оценки устойчивости функционирования системы технологического управления инфокоммуникационной сетью специального назначения с заданной топологической и функциональной структурой // Системы управления, связи и безопасности. 2021. N 1. С. 152–189. DOI: 10.24411/2410-9916-2021-10107.

12. Карпов М. А, Коцыняк М. А., Перов Р. А., Нечепуренко А.П. Методы обеспечения устойчивости системы защиты информационно-телекоммуникационной сети как динамической управляемой системы // Состояние и перспективы развития современной науки: сборник статей III Всерос. науч.-техн. конф. Военный инновационный технополис «ЭРА», Анапа, 2021. С. 690–696.

УДК 004.056
ГРНТИ 81.93.29

РАССМОТРЕНИЕ КОМПОНЕНТОВ ТЕХНОЛОГИИ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ FREEIPA, А ТАКЖЕ ВОПРОС О ЦЕЛЕСООБРАЗНОСТИ ПЕРЕХОДА НА ДАННОЕ РЕШЕНИЕ

А. Д. Макарова, Д. Н. Смирнов, А. Ю. Цветков, И. В. Чумаков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

На сегодняшний день тема централизованной системы управления и идентификации пользователей, а также создания набора групповых политик и контроля доступа к сетевым устройствам является важным аспектом обеспечения безопасности сети. На данный момент в мире не существует идеального решения, которое бы включала в себя работу всех операционных систем под одной технологией построения доверительных отношений в сети. Благодаря рассмотрению данного вопроса можно будет создать систему с поддержкой всех операционных систем, включая работу групповых

политик в сети и контроля доступа к сетевым ресурсам, что позволит повысить уровень защищенности в организациях, использующих в своем производстве различные варианты ОС.

доверительные отношения, FreeIpa, Windows AD, информационная безопасность.

Целью данного исследование является рассмотрение вопроса о необходимости перехода на технологию FreeIpa для построения доверительных отношений, создание централизированной системы управления, включающей в себя работу с идентификацией пользователей и создания групповых политик с возможностью контроля доступа к сетевым ресурсам.

Пару слов о FreeIpa. FreeIpa – это технология доверительных отношений созданная для централизованной системы управление и идентификации пользователей создания набора групповых политик и контроля доступа сети [1].

Основными преимуществами данной технологии является наличие открытого кода и возможность модифицировать технологию под требования компании, применяющие данную технологию. Наличие исходного кода позволяет без ограничения получать доступ к продукции.

Рассмотрим альтернативные варианты работы с доверительными отношения на подобии ALD Windows AD, Samba. В связи с тем, что ALD не поддерживает работы с семейством операционных системах Windows и технологией доверительных отношений Windows AD, применение данного решения не подходит для задач нашего времени. Технология Samba ориентированная на семейство операционных систем Windows, имея множество ограничений, а также отсутствие групповых политик для систем реализованных на Linux ОС вынуждает отказаться от данного решения. Однако Windows AD никак не уступает FreeIpa и возникает вопрос о необходимости перехода на данную технологию. Для этого рассмотрим преимущества и компоненты FreeIpa [2].

Первым преимуществом является удобство установки данного программного обеспечения, которая проходит без особых трудностей, имеет в наличии высокий уровень масштабируемости системы. Помимо удобного Web-интерфейса позволяющего управлять доверительными отношения в системе имеет дополнительное простое решение в виде утилиты командной строки с теми же функциями что и в Web-интерфейсе.

Включает в себя сетевой протокол, выполняющий синхронизацию внутренних часов компьютера с использованием сети – NTP.

Применяет для прохождения аутентификации сетевой протокол Kerberos.

Данный протокол предназначен для проведения надежной аутентификации для клиент-серверных приложений использующий криптографию с секретным ключом.

Для прохождения безопасной аутентификации в нескольких сайтах и приложениях одновременно используется один набор учетных данных при помощи метода SSO.

389 Directory Server применяется для централизованного управления доступом к ресурсам сетевых устройств и является службой каталогов уровня предприятия с открытым исходным кодом.

FreeIpa включается в себя настройку собственного DNS сервера. Задачей которого является получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене [3].

В данное решение для обеспечения доверительных отношений, как и в решение от Windows включен менеджер сертификатов, целью которого управление сертификатами, а также списками доверия сертификатов и списками отзыва сертификатов CTL и CRL.

Для реализации различных пространств и имен применяется технология SSSD (*System Security Services Daemon*), информацию о пользователях для данной технологии предоставляет база данных являющиеся доменом, который может служить источником данных для удаленной аутентификации. Имеется возможность применения нескольких механизмов получения информации для предоставления данных используется стандартным интерфейс PAM и NSS [4].

На основе данного перечня делаем вывод о том, что Windows AD ничем не уступает FreeIpa за исключением свободно открытого исходного кода, а также функционал поддержки в качестве всех операционных систем в мире, не включая Apple Macintosh на данный момент. Однако данная поддержка развивается в настоящее время, а также ChromeOS которая только сейчас начала набирать обороты.

Благодаря данной поддержки переход от Windows AD может быть максимально безболезненным для большинства организаций. Данный переход может потребоваться компаниям, которым важна безопасность и открытость исходного программного обеспечения, а также удобное централизированное управление пользователями и контроль доступа к сетевым ресурсам.

Список используемых источников

1. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства GNU Linux // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. С. 50–56.

2. Кантер Л. Построение корпоративной системы управления идентификационной информацией на базе FreeIPA // Пятнадцатая конференция разработчиков свободных программ. Тезисы докладов. Ответственный редактор В. Л. Черный. 2018. С. 21–25.

3. Lapko A. N., Ivko V. I., Nevrov A. A. The samba DC configuring for networking in heterogeneous networks // В сборнике: Modern informatization problems in the technological and

telecommunication systems analysis and synthesis (MIP-2020'AS). Proceedings of the XXV-th International Open Science Conference. 2020. PP. 243–247.

4. Даньшина А. В., Докшин А. Д., Ковцур М. М. Разработка сервера аутентификации на базе операционной системы Astra Linux // Региональная информатика и информационная безопасность. Сборник трудов конференций: Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2020. С. 262–265.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 621.391
ГРНТИ 49.33.01

ВЫЯВЛЕНИЕ ТРЕБОВАНИЙ, ПРЕДЪЯВЛЯЕМЫХ ГОЛОГРАФИЧЕСКИМ ТРАФИКОМ К СЕТЯМ СВЯЗИ

М. А. Маколкина, Б. О. Паньков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Стратегия развития телекоммуникаций текущего десятилетия включает в себя направление по глобальному и повсеместному внедрению услуг телеприсутствия, основывающихся на технологии голографии и её способностях построения трехмерных копий человека, задействовании роботов-аватаров и манипулирующих устройств с возможностью их объединения в логические группы и сообщества. Несомненно, в силу малой изученности физических принципов и недостатка технологических решений в области воспроизводящих голографических устройств, поставленные задачи будут реализованы не одномоментно, вследствие этого необходимо уже сейчас приступать к формированию списка сетевых требований для услуг телеприсутствия, предъявляемых в дальнейшем к параметрам линий связи РФ, функциональным возможностям телекоммуникационного оборудования и характеристикам трафика трехмерных изображений. Актуальность направления исследования обусловлена потребностью в обретении представления о требуемой эффективности сетевых интерфейсов, протоколов, а также топологии и принципах организации управляющих, коммутирующих и маршрутизирующих компонентов с практическими пояснениями по необходимым уровням качества обслуживания и восприятия при массовом внедрении голографических услуг телеприсутствия.

телеприсутствие, голография, передача трехмерных изображений, дополненная реальность, роботы-аватары, сети 2030, 6G, 3D, НТС.

Введение

В настоящее время наблюдается стремительное развитие сферы информационных технологий, сопровождающееся разработкой и тестированием принципиально новых и высокоперспективных методов и систем коммуникации, функциональные требования которых во много раз превосходят установленные на сегодняшний день пределы производительности и быстродействия сетей передачи данных [1].

Однако на первоначальном этапе формирования технологии, процесс стандартизации сдерживается недостатком исследовательских сведений, а также нередко возникающими концептуальными уязвимостями. Кроме того, составить представление последующих тенденций научной работы для организаций, участвующих в разработке рекомендаций и порядков функционирования новых технологий, помогают наработки и материалы, полученные в ходе испытаний и вмещающие в себя первоочередной список задач, требований и функциональных особенностей для той или иной эксплуатируемой системы.

Примером подобного рода сервиса, состоящего в ранней стадии развития, считается технология Голографического типа коммуникации (HTC – Holographic Type Communication), подразумевающая организацию аудиовизуального, со значительным эффектом реализма контакта между удаленными точками с привлечением инструментов идентификации и регистрации на стороне отправителя и методов последующего воспроизведения на получающем сегменте 3D объектов – голографии [2].

HTC предусматривает создание впечатления присутствия на основе голографических моделей коммуницирующих персон, или, иными словами, объемных 3D копий, обладающих возможностями передачи жестикуляции, эмоций человека, а также наделенными способностями идентификации взгляда и языка тела, перемещения в пространстве в зависимости от позиции наблюдения и масштабирования изображения в натуральный размер [3].

В соответствии с этим можно предположить, что размер данных, требуемый в перспективе на повсеместное развертывание голографической коммуникации, многократно умножится, и, как следствие, это приведет к необходимости резкого наращивания пропускной способности каналов связи, повышению качеств обслуживания и восприятия, а также сокращению показателей RTT (*Round Trip Time*), снижению колебаний задержки (джиттера) и уменьшению коэффициента потери пакетов.

Цель данной работы состоит в разработке структуры лабораторного стенда, служащего для тестирования прохождения голографического трафика через модельный сетевой сегмент с последующим выявлением требований, выдвигаемых технологией HTC к сети передачи данных, а также немаловажной задачей исследования является анализ влияния затухания

и пропускной способности канала связи на основные сетевые характеристики трехмерного потока.

Структура лабораторного стенда

В процессе выполнения исследования требуется осуществить захват и последующий анализ голографического трафика смоделированной услуги НТС с целью установления пороговых величин параметров, непосредственно влияющих на уровни качеств обслуживания (QoS) и восприятия (QoE), а также на конечный субъективный показатель, который, в рамках клиента, безусловно, занимает приоритетное место.

На базе технического оснащения лаборатории кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, посредством модельной сети, было развернуто локальное подключение между RGB-D (*Red Green Blue-Depth*) камерой – Kinect v2 и проектором с поддержкой 3D – LG CineBeam HF85LSR.

Лабораторный стенд (рис. 1) организован с использованием оборудования плотного спектрального уплотнения «Волга», в котором мультиплексор DWDM V6 выполняет функцию объединения информационных каналов в одно волокно, а демультиплексор (DWDM V10), в свою очередь, на приемной стороне выводит из основного потока и распределяет оптические сигналы по индивидуальным приемникам.

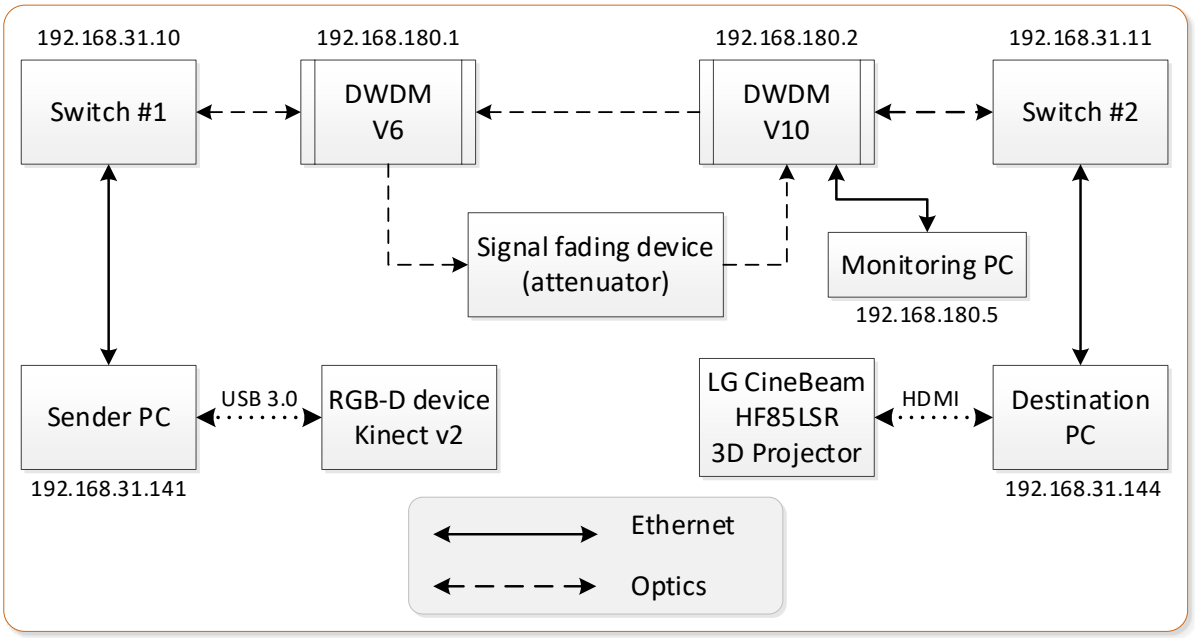


Рис. 1. Схема лабораторного стенда по обмену голографическими данными

В целях имитации различного километража оптоволоконной линии и приближения лабораторных условий к наиболее реальным, в разрыв магистральной линии внедрен оптический аттенюатор Grandway FHA2S01 с возможностью выбора затухания в диапазоне от 0 до 80 дБ.

Кроме того, тестируемая сеть включает два управляемых коммутатора 2 уровня Fast Ethernet D-Link xStack DES-3526, применяемых для принудительного ограничения пропускной способности портов 100Base-TX и последующей оценке влияния этих действий на итоговое качество восприятия голографического изображения.

Потоковая передача голографического контента в режиме реального времени функционирует на базе программного инструмента OBS Studio (*Open Broadcaster Software*) модификации 27.2.3 и утилиты NDI (*Network Device Interface*) – плагина приема-передачи видеопотока в наилучшем качестве с незначительной латентностью [4].

В исследовании применен способ форсирования скорости доставки трехмерного изображения, организованный при помощи метода разложения кадра на части, остающиеся недвижимыми, и участки, в которых наблюдаются пиксельные изменения. Другими словами, ПО в режиме реального времени актуализирует области кадра только с идентифицированной трансформацией и тем самым значительно сокращает объем данных, требуемых для пересылки.

Оценка влияния параметров канала связи
на характеристики голографического потока

Первостепенным шагом исследования является тест воздействия затухания сигнала (dB) оптической линии, последовательно устанавливаемого на аттенюаторе в пределах от 0 до 27 дБ (рис. 2, см. ниже), на частоту битовых ошибок BER (*Bit Error Rate*) и качество транслируемой голографической визуализации. Анализ проводился с целью выявления максимального радиуса
действия услуги голографической коммуникации, в масштабе которого требования по QoS и QoE могут быть полностью удовлетворены без задействования систем регенерации сигнала и дополнительных устройств обнаружения и исправления ошибок.

Исходя из полученных результатов, можно сделать вывод, что до предела затухания сигнала в 18 дБ, величины битовых ошибок и потерь пакетов не преодолевают нулевой границы, что обуславливается задействованием системой DWDM аппаратного алгоритма прямой коррекции ошибок FEC (*Forward Error Correction*) [5]. Последующее ослабление уровня сигнала приводит к истощению производительности коррекции, и, как следствие, возникновению битовых ошибок в сопровождении с ухудшением субъективной оценки качества восприятия.

Рис. 2. Воздействие затухания сигнала на величины RTT и BER

Затухание сигнала равное 27 дБ (эквивалентная длина оптической линии – 135 км) представляется критическим (при отсутствии систем регенерации) для голографического трафика услуг НТС в исследуемой модельной сети в силу того, что число ошибок в битах в момент времени достигает максимально возможного для исправления значения и влечет за собой переход системы DWDM в режим «Авария» (трафик прекращен) [6].

Из результатов, представленных на рис. 2 следует, что показатели RTT изменяются в диапазоне от 0,097 мс до 1,124 мс и обуславливаются взаимным воздействием задержек, образующихся вследствие ограничений физического уровня, быстродействия сетевого оборудования и ПО, а также функциональных возможностей протоколов, применяющихся для формирования и передачи трехмерного потока данных.

В течение опытных испытаний голографическая видеотрансляция отвечала допустимому значению субъективного качества восприятия до предела затухания сигнала в 18 дБ (90 км). Наряду с этим отмечалось наилучшее качество изображения, высокие индексы цветопередачи и кадровой частоты, плавность движения полностью детализированных объектов, полное отсутствие паразитных шумов и запаздываний аудиопотока, а также регистрировалась едва ли заметная задержка между движениями, захваченными RGB-D камерой, и их экранизацией 3D проектором на удаленной стороне модельной сети. При дальнейшем увеличении затухания сигнала

в канале связи, наблюдалось экспоненциальное снижение и ухудшение приведенных выше показателей, что также проявлялось при достижении минимального для НТС порогового значения полосы пропускания интерфейса коммутатора в 16 Мбит/с.

Заключение

В целях обеспечения и достижения приемлемых для услуг голографической коммуникации сетевых условий, требуется привлечение модернизированных и быстродействующих алгоритмов кодирования и обработки данных, задействование производительных и надежных протоколов транспортного уровня, а также улучшение и реорганизация систем построения, сжатия и преобразования голографических трехмерных кадров перед их отправкой в канал связи.

Для повсеместного распространения технологии голографических звонков важным условием также является вовлечение и использование в качестве фундамента новых, высокоперспективных поколений сетей связи, способных удовлетворить предъявляемые услугой требования по ультрамалым значениям задержек и сверхвысокой надежности передачи.

Список используемых источников

1. Кучерявый А. Е., Киричек Р. В., Маколкина М. А., Парамонов А. И., Дунайцев Р. А. Новые перспективы научных исследований в области сетей связи на 2021–2024 годы // Информационные технологии и телекоммуникации. 2020. Том 8. N 3. С. 1–19. DOI 10.31854/2307-1303-2020-8-3-1-19.

2. Kiran Makhijani. Holographic Type Communication / Delivering the Promise of Future Media by 2030. 15 Oct 2021, Geneva. 24 p.

3. Голограммы в повседневной жизни [Электронный ресурс] // VC.ru. URL: https://clck.ru/FyV3L (дата обращения 15.12.2022).

4. NDI – Технология передачи данных по локальным сетям [Электронный ресурс] // Stream Park. URL: https://clck.ru/33JxH9 (дата обращения 18.12.2022).

5. Прямая коррекция ошибок (FEC) при передаче данных [Электронный ресурс] // FS Community. URL: https://clck.ru/33Jwu9 (дата обращения 22.12.2022).

6. Мультисервисная DWDM-платформа «Волга» [Электронный ресурс] // T8 Community. URL: https://clck.ru/33JxSs (дата обращения 12.01.2023).

УДК 004.94
ГРНТИ 49.03.09

ОЦЕНКА ЗАДЕРЖЕК В СЕТЯХ МНОЖЕСТВЕННОГО ДОСТУПА МЕТОДОМ ИММИТАЦИОННОГО МОДЕЛИРОВАНИЯ

М. А. Маркелова, А. А. Шелехов

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

*Настоящее исследование посвящено разработке математической модели инфокоммуникационных сетей с различными топологиями с возможностью учета корреляционных связей между узлами. На первом этапе проведено имитационное моделирование при помощи сетевого симулятора NS-3. Для введения связи между узлами предложен метод создания дополнительной связи со случайным законом ее активации, такой подход позволяет ввести корреляции между информационными потоками, которые идут от узлов к центральному хабу. В результате моделирования получены файлы с дампами данных сетевого трафика в формате *.pcap, которые могут быть использованы для дальнейшего статистического анализа. Таким образом, предлагается инструмент для генерации реализаций данных трафика в инфокоммуникационной сети топологии звезда с зависимыми узлами.*

имитационное моделирование, инфокоммуникационные сети, трафик, дамп.

В современном мире сетевые симуляторы поддерживают самые востребованные сегодня технологии, такие как 5G, Интернет вещей (IoT), беспроводные локальные сети, мобильные одноранговые сети, беспроводные сенсорные сети, специальные автомобильные сети, когнитивные радиосети, LTE и т. д.

Симуляторы имеют множество преимуществ: простоту реализации, низкую стоимость, анализ в реальном времени результатов, а также других параметров, влияющих на всю сеть. Помимо явной экономии подход с использованием симуляторов позволяет проводить эксперименты без построения реальной сети, что есть достаточно трудоёмкий и требовательный ко времени процесс. При этом в программных решениях можно использовать лишь определённые модули оборудования, что лишний раз доказывает выигрыш от использования симуляторов. Большинство из них используют моделирование дискретных событий, в котором сохраняется список ожидающих «событий», которые обрабатываются по порядку, при этом некоторые из них запускают будущие события. Например, событие прибытия пакета

на одном узле, инициирующий событие прибытия этого пакета на нисходящий узел.

При моделировании сетей разработчики сталкиваются со следующими проблемами: задержкой трафика – часто возникают ситуации, когда данные не могут быть своевременно собраны и обработаны, а также ситуации, когда требуемые данные не могут быть получены; увеличением энергопотребления – из-за мобильности устройства потребляют больше энергии, при этом их ресурсы остаются прежними; проблемы, связанные с безопасностью передачи данных – при динамическом изменении сетевой структуры появляются новые возможности для атак.

Моделирование взаимодействия в инфокоммуникационных сетях крайне затруднительно без знаний о характере взаимосвязей между узлами сети и/или пользователями [1]. Цель исследования – построение аналитического инструмента и программной реализации для оценки мгновенной пропускной способности канала сети, её отказоустойчивости, в том числе в интересах динамической маршрутизации сетей.

В данной работе в качестве системы для создания и проведения моделирования был выбран симулятор NS-3. Он позволяет задавать топологию системы, вводить в модель концентраторы и устанавливать соединения между ними.

Рассмотрим термины, которые являются в теории сетей базовыми с точки зрения среды моделирования NS-3. Для обозначения вычислительного устройства используется базовая абстракция, которую называют узлом. Этой абстракции соответствует класс Node. Класс Node предоставляет методы, которые позволяют управлять вычислительными устройствами в процессе моделирования.

В среде NS-3 узлы должны восприниматься в качестве компьютеров, которым добавляется функциональность. К узлам привязываются стеки протоколов, *это* иерархически организованный набор сетевых протоколов, достаточный для организации взаимодействия узлов в сети, а также сетевые устройства и приложения. В симуляторе сети NS-3 приложения на узлах запускаются по аналогии с тем, как работают программные пользовательские приложения на компьютере в реальном мире. Абстракция приложений реализована классом Application. Он включает методы для создания и контроля приложений в процессе моделирования.

В NS-3 каждый узел подключается к каналам связи. Базовая абстракция каналов связи разработана в виде класса Channel, который содержит методы контроля объектов каналов связи. Абстракция сетевого устройства в NS-3 включает аппаратное средство и драйвер программного обеспечения. Сетевое устройство привязывается к узлу, что предоставляет возможность наладить соединение с другими устройствами, которые привязаны к другим узлам, соединенным через каналы связи.

Модель сетевого устройства разработана в виде класса NetDevice. Класс NetDevice предоставляет методы контроля узлов и каналов связи.

При реализации сетевого устройства может потребоваться выполнение большого количества типовых операций: добавить IP-адрес, привязать сетевое устройство к узлу, добавить стек протоколов и затем подключить сетевое устройство к каналу. В NS-3 реализованы классы, называемые Topology Helpers, которые объединяют множество стандартных операций в удобную модель. Topology Helpers предоставляют набор классов и методов, способствующих облегчению выполнения стандартных операций.

Первым этапом моделирования стала реализация модели инфокоммуникационной сети с топологией «звезда». В ней периферийные узлы подключены к единому хабу, который управляет движением трафика (рис. 1).

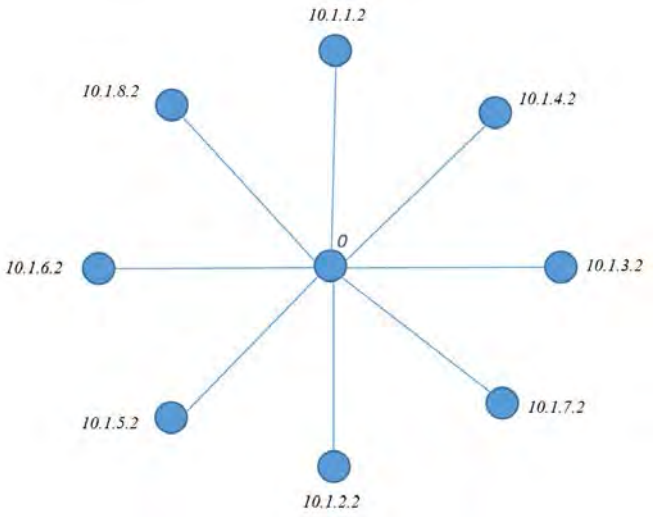


Рис. 1. Граф модели сети с топологией звезда с указанием IP адресом

На текущем этапе исследований в имитационной модели используется HTTP трафик, в дальнейшем планируется обогащение и другими типами, в частности моделирование различных видео/аудио потоков.

На транспортном уровне используется протокол TCP, с пропускной способность канала (DataRate) в 5 Мбитс/с и задержкой (Delay) в 2 мс (рис. 2).

```
66
67  PointToPointHelper pointToPoint;
68  pointToPoint.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
69  pointToPoint.SetChannelAttribute ("Delay", StringValue ("2ms"));
70  PointToPointStarHelper star (nSpokes, pointToPoint);
71  InternetStackHelper internet;
72  star.InstallStack (internet);
73  star.AssignIpv4Addresses (Ipv4AddressHelper ("10.1.1.0", "255.255.255.0"));
74
```

Рис. 2. Присвоение IP адресов узлам сети и настройка параметров протокола TCP

В результате моделирования были получены файлы с дампами данных сетевого трафика в формате *.pcap (рис. 3), которые могут быть подвергнуты дальнейшему анализу.

```
In [3]: pkt.summary()
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 S
PPP / IP / TCP 10.1.1.1:50000 > 10.1.1.2:49153 SA
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.1:50000 > 10.1.1.2:49153 A
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.1:50000 > 10.1.1.2:49153 A
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.1:50000 > 10.1.1.2:49153 A
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.1:50000 > 10.1.1.2:49153 A
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.2:49153 > 10.1.1.1:50000 A / Raw
PPP / IP / TCP 10.1.1.1:50000 > 10.1.1.2:49153 A
```

Рис. 3. Пример содержания файла с дампами передаваемых пакетов

Следующим этапом моделирования было обеспечение возможности создания и параметризации корреляционных связей между узлами. Алгоритм такой связи состоит в том, что среди узлов в сети выбирается пара, между которыми вводится дополнительная взаимосвязь (рис. 4).

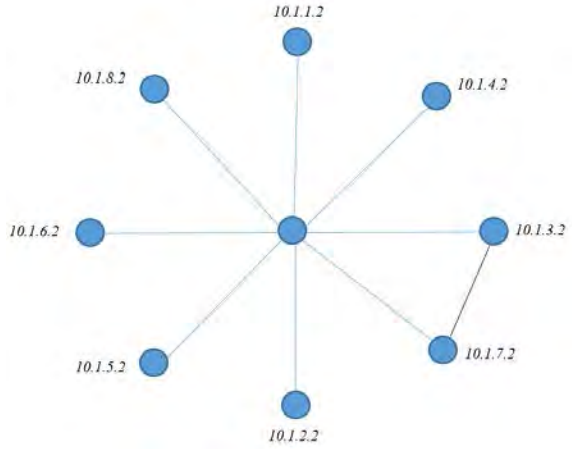


Рис. 4. Создание дополнительной связи между двумя узлами сети

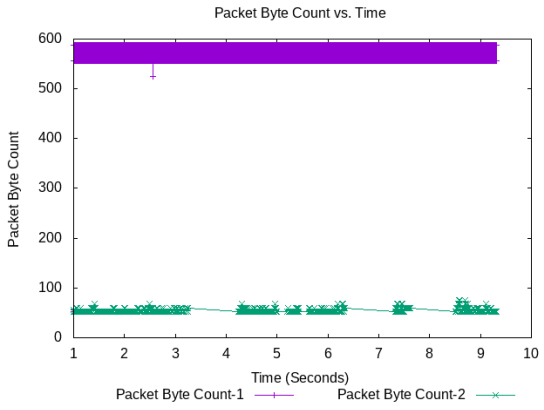


Рис. 5. Режим пропадания трафика в узле 2

В такой конфигурации один из узлов становится управляющим и с момента его активации (начала обмена трафиком с хабом), запускается функция, содержащая в себе таймер со случайным числом, при достижении которого во втором (зависимом) узле прекращается обмен трафиком с хабом.

После прекращения обмена трафиком в узле 2, запускается новый таймер со случайным значением, который отсчитывает промежуток времени для повторного запуска обмена трафиком. Таким образом реализован механизм периодического прерывания (задержек) в обмене трафиком зависимого узла. Характеристики трафика в узлах 1 и 2 в режиме пропадания представлены на рис. 5 (см. выше).

Заметим, что количеством задержек в процессе моделирования, их длиной и диапазоном изменения случайной величины можно управлять, эти параметры и позволяют параметризировать корреляционное взаимодействие между узлами.

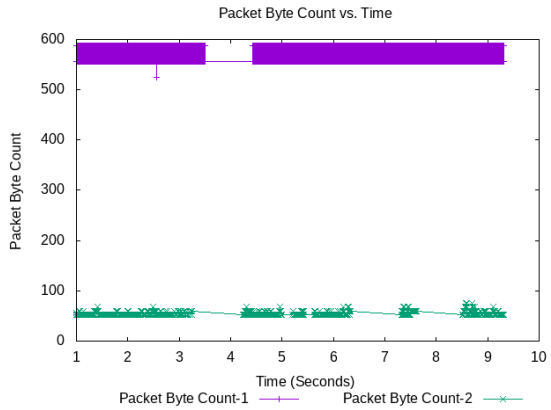


Рис. 6. «Пропадание» пакетов в узле 1, инициированное отсутствием трафика в узле 2

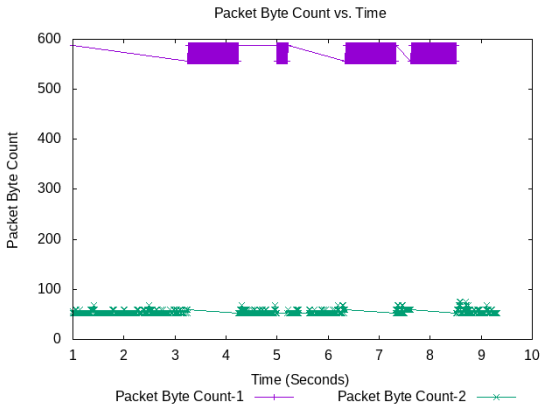


Рис. 7. Обмен трафиком узлами 1 и 2 в режиме инверсии

Далее в рассмотренной модели было добавлено следующее изменение. В момент прекращения обмена трафиком в ведомом узле для ведущего узла тоже включался механизм задержки, по истечении которой этот узел прекращал обмен с хабом (рис. 6). Данный эффект моделирует режим пропадания пакетов в узле 1, инициированный отсутствием трафика в узле 2.

Следующим способом задания корреляционного взаимодействия стала модель инверсионного обмена трафиком узлов с хабом. В данном случае обмен трафиком происходит таким образом. В моменты отсутствия обмена трафика в одном канале трафик перенаправляется в другой. Текущая реализация в модели базируется на представленных выше абстракциях задержек и потому имеет не идеальные результаты при небольшой их величине в силу инертности. Данный недостаток будет устранен при использовании другого базиса управляющей функции в следующей реализации данной модели.

Описанные выше механизмы могут быть скомбинированы, а так же их влияние может быть расширено и на остальные узлы сети, что позволит моделировать более сложные корреляционные механизмы в плотных топологиях. Так же ведущие и зависимые узлы могут быть объединены в группы и подсети, что позволит реализовывать сценарии корреляции между группами устройств, что актуально, например, в системах массового обслуживания [2].

Список используемых источников

1. Nguyen V. D., Markelov O. A., Serdyuk A. D., Vasenev A. N., & Bogachev M. I. Universal rank-size statistics in network traffic: Modeling collective access patterns by Zipf's law with long-term correlations // Europhysics Letters. N 123 (5). 50001. PP. 1–5.
2. Дык В., Маркелов О. А., Богачев М. И. Моделирование агрегированного сетевого трафика узла инфокоммуникационной сети на основе суперстатистического подхода с учетом эффектов долговременной зависимости и нестационарного характера пользовательской активности // Известия высших учебных заведений России. Радиоэлектроника. 2017. N 5. С. 47–53.

Статья представлена научным консультантом,
профессором кафедры РС СПбГЭТУ «ЛЭТИ»,
доктором технических наук, доцентом М. И. Богачевым.

УДК 004; 519
ГРНТИ 20.01; 81.93.29

КИБЕРПОЛИГОНЫ И ИСПЫТАТЕЛЬНЫЕ ПОЛИГОНЫ: ЗАРУБЕЖНЫЙ ОПЫТ ЗАЩИТЫ ИНФОРМАЦИИ И СИСТЕМ ОТ КИБЕРУГРОЗ

А. Н. Метельков, А. В. Шестаков

Санкт-Петербургский университет ГПС МЧС России

В статье рассмотрен зарубежный опыт использования технологии киберполигонов и испытательных стендов в защите информации и систем от киберугроз. Опыт США и других стран в применении киберполигонов для обучения в условиях цифровой трансформации, гибридных войн в киберпространстве требует глубокого осмысления и учета в развитии аналогичных систем в Российской Федерации, государственных органах и высших образовательных учреждениях. По результатам исследования на основе программно-целевых подходов к проблематике киберполигонов, реализуемых Минцифры России, и с учетом прецедентов в мировой практике возможно развитие ведомственных технологий, например, в МЧС России.

киберполигон, угрозы, компьютерные атаки, устойчивость, меры безопасности

Информационная сфера играет важную роль в обеспечении реализации конституционных положений и стратегических национальных приоритетов, направленных на формирование безопасной информационной среды и устойчивой информационной инфраструктуры.

В развитии информационной безопасности произошли серьезные изменения. Кибератаки становятся все более изощренными. Традиционный многоуровневый подход к кибербезопасности может обнаруживать и предотвращать только сравнительно несложные угрозы. В современных кибератаках реализуются тщательно разработанные способы обхода обычных мер безопасности путем изучения правил обнаружения. Традиционные средства контроля могут неадекватно противостоять внутренним угрозам в случае атак со стороны лиц, имеющих правомерный доступ. Проблемой для реагирующих групп стало управление уязвимостями, из-за постоянного увеличения их числа, сложность оценки реальных рисков, определения приоритетов и автоматизации исправлений.

События кибербезопасности могут существенно повлиять не только на деятельность государственных служб и бизнес-операции, но и разрушить технологические процессы с остановкой производства. Среди возможных вариантов воздействий – нарушение интернет-соединения, отключение электроэнергии и другие. В связи с цифровой трансформацией и изменениями в российском образовании становится востребованным метод ситуационного анализа (кейс-метод) [1]. Все это предопределяет важность обнаружения и реагирования на киберугрозы.

Современная проблематика киберполигонов

На национальном мероприятии ИНФОФОРУМ-2023 (7–8 февраля с. г.) отмечено существование дефицита квалифицированных кадров в сфере информационной безопасности и выявлен ряд ключевых аспектов.

Во-первых, повышению уровня подготовки способствуют образовательные программы с закреплением знаний при отработке практических навыков отражения кибератак на Национальном киберполигоне ПАО «Ростелеком», который становится ядром научно-образовательных центров. Компания «Ростелеком-Солар» создала несколько сегментов киберполигона, представляющих цифровые копии типовых IT-инфраструктур в ключевых отраслях экономики. Проект Минцифры России и ПАО «Ростелеком» положил начало практико-ориентированной подготовке будущих специалистов. Системные тренировки по отражению кибератак позволяют существенно повысить киберустойчивость организаций и отраслей экономики страны в целом.

Во-вторых, с целью повышения устойчивости информационных систем, для реализации требований Указа Президента Российской Федерации от 01.05.2022 № 250, актуальным является обеспечение готовности к своевременному обнаружению, предупреждению и ликвидации последствий

компьютерных атак и реагированию на инциденты. Поставленные задачи требуют незамедлительной реализации и в образовательной сфере.

В-третьих, трансформация деструктивных вызовов, качественное изменение внутренних и внешних угроз отражены в Стратегии национальной безопасности РФ и Доктрине информационной безопасности РФ. В Доктрине отмечено, что состояние информационной безопасности в области технологий и образования характеризуется низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением. Мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и средств зачастую не имеют комплексной основы. Ликвидация возникшего несоответствия между усложнившимися условиями функционирования информационных систем и снижением информационной безопасности возможна путем совершенствования научной и экспериментальной базы. Одной из проверенных за рубежом и в России технологий в этой сфере является технология киберполигона.

Достаточно актуальна потребность в глубоком понимании методологии атак для того, чтобы знать, как эффективно смягчить их. Киберполигон – это именно та виртуальная, замкнутая учебно-тренировочная программная среда, которая предназначена для углубления такого понимания. В основе киберполигона – способность моделировать и интегрировать системы для создания сложных сетей [2, с. 3].

Программно-аппаратный комплекс киберполигона обладает ядром для инициализации в автоматическом режиме атак, база сценариев которых может пополняться. Базовая инфраструктурная технология полигонов производителями не раскрывается. Киберполигон открывает возможности для проверки различных моделей, изучения и осмысления процессов и технологий обеспечения информационной безопасности. Киберполигоны поддерживают практическое (экспериментальное) обучение с помощью непосредственного обучения [3, 4, 5] или киберупражнений [6, 7].

Методы обучения с использованием технологий кибер- (CR) и испытательных (TB) полигонов разнообразны: геймификация; имитация нападения; ролевое обучение; соревновательные упражнения; учения по киберзащите (CDX) и др. Моделируемые среды являются одним из путей к созданию реалистичных сценариев целевых систем, облегчая обучение с помощью убедительных иллюстраций реальных инцидентов безопасности и динамики угроз. Киберполигон позволяет: имитировать виртуальные сетевые IT инфраструктуры, компьютерные атаки, организовать виртуальные рабочие места, проводить киберучения и тренировки.

Понятие «киберполигон» (CR) в США [8] определено Национальным институтом стандартов и технологий (NIST) как «интерактивные и смоделированные представления, относящиеся к локальной сети, системе, инструментам и приложениям организации», а испытательные стенды (ТВ), как «настраиваемый и расширяемый киберполигон с имитацией промышленных процессов». Киберполигоны и испытательные полигоны дополняют друг друга, поскольку сети операционных технологий и ICT переплетаются с достижениями в области связи, внедрением Интернета вещей (IoT) и промышленного IoT (IIoT) в различных секторах экономики.

Преимущества использования систем симуляции атак на организации достоверны, так как они масштабно и регулярно применяются уже полтора десятилетия. В апреле 2022 года НАТО провело в Эстонии масштабные ежегодные учения Locked Shields с целью повышения квалификации специалистов по кибербезопасности. Задачами злоумышленников были стирание веб-страниц и размещение собственных сообщений на сайте противника. Отрабатывались атаки на элементы энерго и водообеспечения.

Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Как и прототип Интернета в военном ведомстве США в 2002 г. зародились технологии киберполигонов.

В феврале 2006 г. Управление национальной кибербезопасности Министерства внутренней безопасности США провели национальное кибер-учение Cyber Storm. В 2021 г. Министерство внутренней безопасности объявило о завершении полугодовых учений по моделированию кибератак для подготовки США и их союзников к реальным атакам на критически важные системы. Национальная стратегия безопасности киберпространства США является координационным центром федерального правительства, обеспечивающим взаимодействие государственных и местных органов власти, частного сектора и международного сообщества относительно объединения усилий по снижению уязвимости киберпространства в соответствии с полномочиями и обязанностями Национального плана реагирования DHS (NRP). Американская национальная система реагирования описывает обеспечение готовности путем разработки приложений по инцидентам для каждой опасности. В приложениях по инцидентам отражаются координирующие структуры, используемые для предоставления основных возможностей и поддержки миссий реагирования, уникальных для конкретного типа инцидента, а также описываются специализированные группы реагирования, ресурсы, роли, обязанности и другие особенности сценария. Кроме Cyber Storm Правительством США совместно с частным сектором для проверки

готовности к реагированию, координации и восстановлению по отношению к вектору смоделированных кибер-событий на международном, федеральном и государственном уровнях проведены и другие киберучения, такие как Cyber Annex.

Технологии киберполигона –
один из путей обеспечения устойчивости информационных систем

Тренинги играют ключевую роль в формировании и проверке организационной и технической готовности, которая необходима для своевременного обнаружения и реагирования при проведении реальных кибератак. Центральное место в обучении посредством упражнений, имитирующих наступательные и оборонительные операции, занимает формирование команд (красная, синяя, белая, фиолетовая, зеленая, серая, желтая). Групповое обучение с участием нескольких команд, повышает осведомленность организации о киберситуации и сокращает время реагирования для выявления и пресечения кибератаки.

Для доставки целевого вредоносного кода за рубежом на учениях используются сложные сети управления несанкционированным доступом. В атаках применялись программы-вымогатели, распределенный отказ в обслуживании, компрометация реестров службы доменных имен, утечки данных, а в некоторых случаях в сочетании с внутренними угрозами.

Обучение кибербезопасности может иметь две формы. Первая предназначена для специалистов по безопасности и направлена на улучшение понимания последних угроз и повышение уровня навыков защиты от них и смягчения их последствий. Вторая направлена на повышение осведомленности о кибербезопасности среди специалистов, не связанных с безопасностью, и широкой общественностью.

Для проведения учебных программ требуются специальные испытательные стенды и инфраструктура, которые помогают реализовать и выполнять учебные сценарии и предоставляют обучаемым игровую площадку. Сценарии могут воспроизводить спектр кибератак, что повышает эффективность обучения. Обучение в эмулируемой среде ускоряет эффективное изучение опыта, а динамическое взаимодействие способствует более глубокому пониманию последствий любого деструктивного действия.

Изучение зарубежного опыта показывает, что в развитых странах заметное внимание уделяется национальным планам или стратегиям по обеспечению безопасности киберпространства. Зарубежный опыт применения киберполигона целесообразно учитывать при разработке отечественных образцов и при выборе вариантов внедрения технологии в процесс подготовки кадров для органов государственной власти.

Статья подготовлена в рамках выполнения в 2023 году прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, регистрационный номер ЕГИСУ НИОКТР № 123030100017-2 и № 123030100009-7 от 01.03.2023.

Список используемых источников

1. Трапезникова Т. Н. Новейшие педагогические технологии: кейс-метод (метод ситуационного анализа) // Территория науки. 2015. N 5. С. 52–59.

2. Leitner M.et al. AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research // in Proceedings of the European Interdisciplinary Cybersecurity Conference, New York, NY, USA, Nov. 2020. PP. 1–6. https://doi.org/10.1145/3424954.3424959.

3. Frank M., Leitner M., and Pahi T. Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education // In 2017 IEEE 3rd Intl Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress. IEEE, Orlando, FL, USA. 2017. PP. 38–46. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23.

4. Pham C., Tang D., Chinen Ken-ichi, and Beuran R. CyRIS: a cyber range instantiation system for facilitating security training // In Proceedings of the Seventh Symposium on Information and Communication Technology (SoICT'16). ACM, Ho Chi Minh City, Vietnam. 2016. PP. 251–258.

5. Kucek S. and Leitner M. Training the Human-in-the-Loop in Industrial Cyber Ranges // In Digital Transformation in Semiconductor Manufacturing (Lecture Notes in Electrical Engineering), Sophia Keil, Rainer Lasch, Fabian Lindner, and Jacob Lohmer (Eds.). Springer International Publishing, Cham. 2020. PP. 107–118. https://doi.org/10.1007/978-3-030-48602-0_10/

6. Ferguson B., Tall A., and Olsen D. National Cyber Range Overview. In 2014 IEEE Military Communications Conference (MILCOM). IEEE, Baltimore, MD. 2014. PP. 123–128.

7. Vykopal J., Vizvary M., Oslejsek R., Celeda P., and Tovarnak Dl. Lessons learned from complex hands-on defence exercises in a cyber range // In 2017 IEEE Frontiers in Education Conference (FIE). IEEE Computer Society, Indianapolis, IN, USA. 2017. PP. 1–8. https://doi.org/10.1109/FIE.2017.8190713.

8. Метельков А. Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. 2022. N 1. С. 51–60.

УДК 621.396.4
ГРНТИ 50.37.03

ВАРИАНТ ФОРМУЛИРОВКИ ВЕРОЯТНОСТНЫХ ЧАСТНЫХ И КОМПЛЕКСНОГО ПОКАЗАТЕЛЕЙ ТЕХНИЧЕСКОЙ НАДЕЖНОСТИ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

А. В. Михайличенко[1], И. Б. Паращук[1], О. И. Пантюхин[2]

[1]Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрен возможный подход к формулировке вероятностного комплексного показателя технической надежности мобильных центров обработки данных на основе совместной условной вероятности выполнения требований к отклонениям его частных показателей надежности, характеризующих параметры безотказности, долговечности, ремонтопригодности и сохраняемости объекта такого класса. Проведен анализ потенциальных вариантов формулировки частных показателей и перспектив применения данного подхода для решения задач достоверного и оперативного оценивания и прогнозирования надежности современных мобильных дата-центров.

показатель технической надежности, мобильный центр обработки данных, требования, отклонения, условная вероятность, безотказность, ремонтопригодность.

Анализ исследований в области контроля и управления современными мобильными центрами обработки данных (МЦОД) показывает, что сравнительная вероятностно-временная и многокритериальная оценка технической надежности таких сложных информационно-технических объектов непосредственно по частным показателям не только мало информативна, почти не применима в реальной практике, но и, зачастую, противоречива, поскольку по одним показателям более надежным может оказаться один МЦОД, а по другим – совсем другой мобильный дата-центр, с другим или даже с таким же набором элементов – средств и комплексов связи, хранения и обработки данных [1, 2, 3].

Этот объективный факт, затрудняющий оценку и связанный с многообразием и разноплановостью анализируемых и подлежащих текущему и проактивному контролю аспектов и показателей надежности технических (аппаратно-программных) систем, присутствует, несмотря на то, что существует целый ряд международных и национальных стандартов, определяющих не только методологические подходы к анализу надежности систем такого класса, но и примерный перечень параметров, по которым она

могут быть оценена в целом, либо могут быть отдельно оценены такие аспекты технической надежности, как безотказность, долговечность, ремонтопригодность и сохраняемость [4, 5].

Помимо этого, приходится также учитывать субъективизм формулировки некоторых частных показателей технической надежности (ЧПТН), вносящий известную долю неопределенности в решение задач управления и вероятностно-временного оценивания безотказности, долговечности, ремонтопригодности и сохраняемости современных МЦОД [6, 7].

Выход из этой ситуации нам видится в формулировке и последующей текущей либо прогностической оценке вероятностного комплексного показателя технической надежности (КПТН) МЦОД, который бы функционально связывал все многообразие ЧПТН и требований к ним. Анализ различных методов формирования комплексных (обобщенных) показателей качества, надежности либо эффективности сложных систем показал, что наиболее полный учет особенностей решения задачи оценивания технической надежности МЦОД, а также естественное решение проблем нормализации и свертки систем показателей технической надежности (ПТН) достигается при применении метода вероятностной скаляризации [8, 9].

Сущность данного метода состоит в использовании в качестве КПТН совокупной (совместной) вероятности выполнения требований $p_{\text{вып птн}}(k)$, предъявляемых пользователем к технической надежности мобильного датацентра на k-м шаге его эксплуатации по безотказности, долговечности, ремонтопригодности и сохраняемости:

$$p_{\text{вып птн}}(k) = p(\Delta\vec{A}_{\text{птн}}(k) \le \Delta\vec{A}^{\text{тр}}_{\text{птн}}), \quad (1)$$

где $\Delta\vec{A}_{\text{птн}}(k)$ – вектор отклонений ПТН от требований на k-м шаге эксплуатации МЦОД, а $\Delta\vec{A}^{\text{тр}}_{\text{птн}}$ – вектор требований к этим отклонениям.

Предпочтение, отданное данному методу, обусловлено учетом в нем случайного характера изменений основной массы ПТН МЦОД, а также практической возможностью автоматического решения основных проблем многокритериальной вероятностно-временной оценки качества, надежности и эффективности функционирования сложных технических систем (т. е., в нашем случае, возможностью нормализации компонент векторных ПТН МЦОД и их свертки) в рамках выбранного вероятностного подхода к анализу технической надежности [9].

Фундамент данного метода зиждется на пошаговом (поэтапном) расчете ЧПТН на любом k-м шаге оценивания и их математически корректной «свертке» в КПТН МЦОД на этом же шаге. Математически метод может быть осуществлен на основе аппарата условных вероятностей, а также классических теорем функциональной и параметрической декомпозиции [9].

При этом вероятностный комплексный ПТН формируется из условных вероятностей выполнения требований к отклонениям ЧПТН МЦОД.

Иными словами, для методики, учитывающей вероятностно-временную физическую сущность трансформации ПТН МЦОД на *k*-м шаге его эксплуатации и, учитывая тот факт, что ПТН представляют собой отклонения параметров надежности от требуемых значений, КПТН $p_{\text{вып птн}}(k)$, опираясь на выражение (1), может быть аналитически записан как совместная условная вероятность выполнения требований к значениям отклонений показателей безотказности, долговечности, ремонтопригодности и сохраняемости МЦОД:

$$\begin{aligned} p_{\text{вып птн}}(k) = p_{\text{б}}(k)[(\Delta\vec{A}_{\text{б}}(k) \le \Delta A_{\text{б}}^{\text{тр}})/(\Delta\vec{A}_{\text{д}}(k) \le \Delta\vec{A}_{\text{д}}^{\text{тр}}) \bigcap (\Delta\vec{A}_{\text{р}}(k) \le \Delta\vec{A}_{\text{р}}^{\text{тр}}) \bigcap \\ \bigcap (\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}_{\text{с}}^{\text{тр}})] \times p_{\text{д}}(k)[(\Delta\vec{A}_{\text{д}}(k) \le \Delta\vec{A}_{\text{д}}^{\text{тр}}) / (\Delta\vec{A}_{\text{р}}(k) \le \Delta\vec{A}_{\text{р}}^{\text{тр}}) \bigcap \\ \bigcap (\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}_{\text{с}}^{\text{тр}})] \times p_{\text{р}}(k)[(\Delta\vec{A}_{\text{р}}(k) \le \Delta\vec{A}_{\text{р}}^{\text{тр}}) / \\ /(\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}_{\text{с}}^{\text{тр}})] \times p_{\text{с}}(k)[(\Delta\vec{A}_{\text{с}}(k) \le \Delta\vec{A}_{\text{с}}^{\text{тр}})], \end{aligned} \quad (2)$$

где $\Delta\vec{A}_{\text{б}}(k), \Delta\vec{A}_{\text{р}}(k), \Delta\vec{A}_{\text{д}}(k), \Delta\vec{A}_{\text{с}}(k), \Delta\vec{A}_{\text{б}}^{\text{тр}}, \Delta\vec{A}_{\text{р}}^{\text{тр}}, \Delta\vec{A}_{\text{д}}^{\text{тр}}$ и $\Delta\vec{A}_{\text{с}}^{\text{тр}}$ – вектора показателей безотказности, долговечности, ремонтопригодности и сохраняемости соответственно (в виде их отклонений от требований) на *k*-м шаге эксплуатации МЦОД и вектора соответствующих требований; $p_{\text{б}}(k)$, $p_{\text{р}}(k)$, $p_{\text{д}}(k)$ – условные вероятностей выполнения требований к отклонениям показателей безотказности, долговечности и ремонтопригодности на *k*-ом шаге эксплуатации МЦОД, определяемые с учетом (при условии) выполнения требований к отклонениям показателей сохраняемости; $p_{\text{с}}(k)$ – безусловная вероятность выполнения требований к отклонениям показателей сохраняемости на *k*-м шаге эксплуатации МЦОД.

При этом вариант формулировки отдельного вероятностного частного ПТН, характеризующего, например, такой аспект (грань) надежности МЦОД, как безотказность, может быть представлен в виде условной вероятности выполнения требований на *k*-м шаге эксплуатации МЦОД к отклонениям значений вероятности безотказной работы $\Delta p_{\text{бр}}(k)$, средней наработки до отказа $\Delta T_{\text{ср}}(k)$, средней наработки на отказ $\Delta T_{\text{о}}(k)$ и интенсивности потока отказов $\Delta\lambda_{\text{по}}(k)$, рассчитываемой при условии выполнения требований, например, к отклонениям одного из ключевых параметров безотказности – средней доли безотказной наработки $\Delta I(k)$:

$$p_{\text{б}}(k) = p(\Delta\vec{A}_{\text{б}}(k) \le \Delta\vec{A}_{\text{б}}^{\text{тр}}) =$$
$$p_{\text{б/сд}}(k)[(p_{\text{бр}}(\Delta p_{\text{бр}}(k) \le \Delta p_{\text{бр}}^{\text{тр}}) \bigcap p_{\text{ср}}(\Delta T_{\text{ср}}(k) \le \Delta T_{\text{ср}}^{\text{тр}}) \bigcap$$
$$p_{\text{о}}(\Delta T_{\text{о}}(k) \le \Delta T_{\text{о}}^{\text{тр}}) \bigcap p_{\text{ипо}}(\Delta\lambda_{\text{по}}(k) \le \Delta\lambda_{\text{по}}^{\text{тр}}) / (\Delta I(k) \le \Delta I^{\text{тр}})] \times \quad (3)$$
$$\times p_{\text{сдбн}}(k)[(\Delta I(k) \le \Delta I^{\text{тр}})],$$

где $p_{\text{б/сд}}(k)$ – совместная (по вероятности безотказной работы $p_{\text{бр}}(\Delta p_{\text{бр}}(k) \le \Delta p_{\text{бр}}^{\text{тр}})$ и вероятностям выполнения требований к отклонениям средней наработки до отказа $p_{\text{ср}}(\Delta T_{\text{ср}}(k) \le \Delta T_{\text{ср}}^{\text{тр}})$, средней наработки на отказ $p_{\text{о}}(\Delta T_{\text{о}}(k) \le \Delta T_{\text{о}}^{\text{тр}})$ и интенсивности потока отказов $p_{\text{ипо}}(\Delta\lambda_{\text{по}}(k) \le \Delta\lambda_{\text{по}}^{\text{тр}}))$ условная вероятность выполнения требований к отклонениям показателей безотказности (без учета средней доли безотказной наработки) на *k*-м шаге эксплуатации МЦОД, определяемая при условии выполнения требований к отклонениям значений средней доли безотказной наработки; $p_{\text{сдбн}}(k)[(\Delta I(k) \le \Delta I^{\text{тр}})]$ – безусловная вероятность выполнения требований к отклонениям средней доли безотказной наработки МЦОД.

Таким образом, можно с большой долей уверенности утверждать, что, с учетом оговоренных ограничений на множество ПТН, формулировка вероятностного комплексного ПТН может быть осуществлена на основе условных вероятностей выполнения требований к отклонениям частных показателей надежности МЦОД, характеризующих параметры его безотказности, долговечности, ремонтопригодности и сохраняемости. Предложен вариант формулировки ЧПТН, включающий условную вероятностную меру выполнения требований к отклонениям частных параметров безотказности. Предложенный подход обладают высокой универсальностью, а сочетание применения метода вероятностной скаляризации и математического аппарата условных вероятностей обуславливает обещающие перспективы в вопросах достоверного и оперативного оценивания и прогнозирования надежности современных мобильных центров такого класса.

Список используемых источников

1. Андреев А. В., Яковлев В. В., Короткая Т. Ю. Теоретические основы надежности технических систем. Учебное пособие. СПб. : Изд. Полит. ун-та, 2018. 164 с.

2. Изергина А. Р. Обзор статистических методов оценки надежности // Математические модели современных экономических процессов, методы анализа и синтеза экономических механизмов. Актуальные проблемы и перспективы менеджмента организаций в России: сб. ст. XII Всерос. науч.-практ. конф. Самара: Изд-во СамНЦ РАН, 2018. С. 45–50.

3. Паращук И. Б., Михайличенко Н. В., Михайличенко А. В. Нейро-нечеткие сети и алгоритмы гранулярных вычислений в задачах интеллектуальной обработки данных

для оценки надежности мобильных дата-центров // Применение искусственного интеллекта в информационно-телекоммуникационных системах. Сборник материалов научно-практической конференции. СПб. : ВАС, 2021. С. 110–115.

4. Межгосударственный стандарт ГОСТ 27.002-2015 Надежность в технике. Термины и определения. М. : Стандартинформ., 2016. 30 с.

5. Национальный стандарт РФ ГОСТ Р 51901.5-2005 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности. М.: Стандартинформ., 2005. 44 с.

6. Паращук И. Б., Михайличенко А. В., Крюкова Е. С. Анализ зашумленных и неоднородных данных о значениях параметров надежности дата-центров // Современные технологии: актуальные вопросы теории и практики: сборник статей Международной НПК. Пенза: МЦНС «Наука и Просвещение», 2021. С. 74–77.

7. Паращук И. Б., Башкирцев А. С., Михайличенко Н. В. Анализ уровней и видов неопределенности, влияющей на принятие решений по управлению информационными системами // Информация и космос. 2017. N 1. С. 112–120.

8. Надежность и эффективность в технике. Том 3. Эффективность технических систем / Под ред. В. Ф. Уткина и Ю. В. Крючкова. М. : Машиностроение, 1988. 328 с.

9. Терентьев В. М., Санин Ю. В. Анализ эффективности функционирования автоматизированных сетей многоканальной радиосвязи. СПб. : ВАС, 1992. 80 с.

UDCC 629.12
SCSTI 20.53.01

PROCEDURES FOR GRANULAR SELECTION OF ANALYZED PARAMETERS OF TECHNICAL RELIABILITY OF MODERN DISK STORAGE SYSTEMS

A. Mikhaylichenko, I. Parashchuk

Military Communications Academy named after Marshal of the Soviet Union S.M. Budyonny

The issues of reasonable, reliable choice of analyzed parameters of technical reliability of disk storage systems used, for example, in modern mobile data centers are considered. A formal description of the approach to the granular selection of filling sets of such parameters is implemented, the composition of which must be formed taking into account inaccurate, "noisy" indistinctly specified initial data. The proposed approach is intended to act as a decision support system in the interests of formulating an impossible, but complete and reasonable system of controlled parameters, which, in turn, is designed to increase the accuracy and efficiency of solving the problem of analyzing the technical reliability of systems of this class.

analyzed parameters, disk storage systems, technical reliability, inaccurate, "noisy" indistinctly specified initial data, fuzziness.

A reasonable choice of the optimal set of analyzed parameters of technical reliability of any complex system, both in domestic and foreign practice, is the initial and one of the main stages of assessing the reliability of systems of this class, including disk storage systems [1, 2].

Modern disk storage systems (DSS) are a complex of interconnected specialized equipment and software. They are designed for storing and transmitting large amounts of information, and they allow organizing the content (preservation) of this information on separate disk platforms with optimal distribution of storage resources [3, 4].

Disk data storage systems are not only hardware and software complexes for storing and processing large amounts of information, but also rightfully belong to the class of complex engineering systems, since they have a large number of interrelated elements, can be divided into subsystems, are difficult to operate, have control subsystems, and their interaction with the external the environment is multifaceted and not always predictable. At the same time, DSS are able to store various information – files, including media, structured (database management system – DBMS) and unstructured data (Big Data), archives and backups. As a rule, modern technical solutions are used in disk storage systems as data carriers – hard drives, mainly SSD (All Flash Array systems), as well as hybrid solutions combining SSD- and HDD-drives in one DSS, which, of course, should have a high level of technical reliability [5, 6].

That is why the choice of the optimal set of analyzed parameters in the interests of assessing the technical reliability of the DSS is an urgent and paramount task. Tasks of this kind become particularly relevant in conditions when there is various kinds of uncertainty as to the specification (formulation) of the technical reliability parameters (TRP) themselves of the DSS, and the uncertainty of the observation (measurement) data for the values of these TRP in the dynamics of the life cycle of systems of this class. In these cases, such problems are usually solved using methods of fuzzy set theory, the theory of artificial neural networks or neuro-fuzzy computing [7].

However, the mentioned methods are not always able to help in solving the problem of choosing the optimal set of analyzed TRP of the DSS, since both the data (often expert) for the formulation of the set of TRP and the observation and measurement data, in addition to their inherent vagueness, are either redundant or inaccurate, obtained (formulated) with errors – "noisy".

The analysis of modern research in this field shows that in these cases modern mathematical approaches from the field of data mining can be applied, for example, methods and algorithms of granular computing [8].

The physical and analytical meaning of granular computing (GC) consists in the correct mathematical unification of sets of indistinctly specified inaccurate, "noisy" data into subsets called information granules (IG). In our case, the IG is a set of controlled TRP of the DSS, the composition of which must be formed

taking into account inaccurate, "noisy" vaguely specified initial data – opinions, preferences of experts and decision makers about the number and nomenclature of these analyzed TRP. The inaccuracy and "noise" of these fuzzy data is most often associated with the uncertainty of information about the design features of the DSS, about the environment, the nature, degree and frequency of destructive effects on the DSS, significantly affecting the technical reliability of the controlled disk storage system.

Indicators of technical reliability of DSS numerically characterize the degree of those specific properties inherent in this system that determine its technical reliability. The existence of TRP of the DSS having dimensionality (for example, such as the technical resource and service life of the elements of the DSS), as well as dimensionless TRP (for example, the availability coefficient or the probability of failure-free operation), aggravates the problem of choosing the analyzed parameters, makes it non-trivial.

The complexity is also added by the variety of existing reliability parameters of complex systems tested in practice, since modern regulatory documents provide for the presence of both single and complex TRP. At the same time, single reliability parameters is usually grouped into four groups: maintainability, durability and persistence parameters [1, 2].

If, for example, it is necessary to make an optimal choice of the analyzed maintainability parameters – to form the optimal number and nomenclature of a subset of the maintainability parameters of the DSS, as one of the facets of its technical reliability, the GC predetermines a number of sequential information and computing procedures.

The maintainability parameters of the DSS can be: the average recovery time of the functional state of the element (device) DSS or DSS as a whole; the coefficient of restoration of the functional state for the allotted period of time; the intensity of the flow of restoration of the functional state, as well as the average labor intensity of restoring the functional state of the element (device) DSS or DSS in general. The initial data is a subset of fuzzy data – expert opinions on the optimal composition of the vector of maintainability parameters. At the same time, all elements of this fuzzy subset (according to the number of experts and the TRP recommended by them for inclusion in the optimal system of maintainability parameters) have corresponding membership functions [8]. The problem of the optimal choice of the analyzed parameters is that experts have formulated several (in the worst case, many) different opinions about the inclusion or non–inclusion of a particular TRP in the optimal subsystem of the maintainability parameters of the DSS.

The first procedure in the framework of GC – is information granulation. The initial data for this procedure are inaccurate, "noisy" opinions and preferences of experts in the form of fuzzy sets that characterize the possible optimal number and nomenclature of the subsystem of maintainability parameters.

In essence, these are vaguely formulated expert opinions about whether or not a particular TRP should belong to the optimal set of controlled parameters of the maintainability of the DSS. Inaccurate, "noisy" fuzzy data – opinions and preferences of experts are grouped in the IG according to the principle of similarity (proximity of values) of membership functions. At the same time, one IG includes fuzzy data (opinions) with a minimum numerical distance between the values of their membership functions.

The second procedure in the framework of GC – is granular summation. During this procedure, a mathematically correct combination of several expert opinions on the optimal number and nomenclature of TRP of the DSS takes place. This procedure is carried out by defuzzification and fuzzy-granular mathematical unification, for example, of two inaccurately specified ("noisy") fuzzy sets, the components of which characterize, for example, the average recovery time and the intensity of the recovery flow.

The third procedure in the framework of the GC – is the calculation of the trace function of the granular sum, which allows you to determine the trend of experts' preferences when choosing, for example, from four components. In other words, when choosing from four different expert opinions on the desirability (preferably) of including a specific parameter of technical reliability, for example, the average recovery time in the composition of the optimal, non-redundant subsystem of the maintainability parameters of the DSS.

The fourth procedure in the framework of the GC is the search for a minimum in the IG, and a minimum that characterizes not fuzzy data (opinions), but the values of their membership functions. This procedure allows us to obtain a subset of TRP, the elements of which mathematically correctly, taking into account fuzzy data and their membership functions, determine the total, generalized (with the help of GC), expert opinions on the importance (significance) of a particular TRP for the analysis of the technical reliability of the DSS as a whole.

These GC procedures make it possible to level out, neutralize various types of uncertainty of the initial data, and the result of solving problems of this class is reduced to suboptimal subsets of reliability parameters in need of control. At the same time, the number and nomenclature of TRP included in these subsets must meet the requirements for completeness, operationality, but, at the same time, be non-redundant, measurable and have a minimum dimension.

Thus, procedures (applications of granular calculations) are proposed to improve the methodology for the synthesis of an optimal system of reliability parameters. The procedures are aimed at finding the optimal number and nomenclature of controlled parameters of the technical reliability of the DSS in the presence of vaguely specified inaccurate, noisy source data.

The practical application of the proposed sequence of GC procedures will increase the reliability of determining the composition of the set of TRP of real technical systems, improve the quality of analysis and reliability management

of disk storage systems. All this, in turn, will contribute to the timely and reliable management of the elements of the DSS, which means an increase in the technical reliability of information support systems and complexes.

References

1. Kolowrocki K. Relability of Large and Complex System. Amsterdam: Elsevier, 2014. 460 p.

2. Kotenko I. V., Parashchuk I. B. Formation of Indicators for Assessing Technical Reliability of Information Security Systems // 2018 International Russian Automation Conference (RusAutoCon) / IEEE Xplore Digital Library. 2018. Vol. 8501650. PP. 1–6.

3. Somasundaram G., Srivastava A. From data storage to information management. 2nd ed. St. Petersburg: Peter, 2016. 544 p. [in Russian].

4. Savyak V. N. Modern technologies of disk data storage systems // Networks & Business. 2003. No. 2. [Electronic resource]. URL: https://www.ixbt.com/storage/modern-storagesys.shtml (access date: 15.11.2022). [in Russian].

5. Parfenov Yu. P. Postrelational data warehouses: textbook. manual. Yekaterinburg: Ural Publishing House, 2016. 120 p. [in Russian].

6. Parashchuk I. B., Kryukova E. S., Mikhaylichenko N. V. Multiparametric data storage systems, data centers and electronic libraries: a method for monitoring technical condition parameters and quality analysis // XVII St. Petersburg International Conference "Regional Informatics (RI-2020)": Conference proceedings. Part 1 \ SPOISU. St. Petersburg: 2020. PP. 102–104. [in Russian].

7. Parashchuk I. B., Bashkirtsev A. S., Mikhaylichenko N. V. Analysis of levels and types of uncertainty affecting decision-making on the management of information systems // Information and Space. 2017. No. 1. PP. 112–120. [in Russian].

8. Butakova M. A., Guda A. N., Ivanchenko O. V., Karpenko E. V. Elements of the theory of granular computing with fuzzy approximate information granules // Bulletin of the Rostov State University of Railways. 2015. No. 4 (60). PP. 27–33. [in Russian].

УДК 004.04
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ НА ОСНОВЕ ВИРТУАЛИЗАЦИИ И ЖИВОЙ МИГРАЦИИ ДЛЯ СЕТЕЙ СВЯЗИ БУДУЩЕГО ПОКОЛЕНИЯ

П. П. Михайлов, А. С. А. Мутханна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Одна из основных реализаций сетей связи следующего поколения основываются на низких задержках, что позволит получить быстрый доступ к разным сервисам. И для достижения минимального времени обращения к приложению или сервису

от устройств Internet of Thing. Для обработки данных потребуется размещение серверов для туманных вычислений, но тогда мы сталкиваемся с вопросом как размещать\мигрировать требуемые приложения по требованию, так как приложения изначальна в облаке. В данном материале попробуем рассмотреть, как может происходить миграция сервисов между облаками.

интернет вещей, туманные вычисления, миграция сервисов.

Рассматривая беспроводную связь следующего поколения и всё больше проявляющиеся средства полностью или полуавтоматизированные, то прослеживается связь взаимодействие данных сетей связи и разных отраслей промышленностей. Т. к. автоматизированные средства имеющие множества сенсоров, которые получают обширные данные, и на основе полученных данных улучшают точность, надежность для расчета принятых решений. И, следовательно, имея обширные блоки гетерогенных данных от различных устройств мы имеем возможность на их основе создать различные приложения/сервисы, которые помогут «пользователю» получать, управлять и/или реагировать на события.

Понимая, что беспроводную связь следующего поколения больше рассчитаны на использования бизнес-клиентов, которые получают доступ к сетям с широкими возможностями настройки, адаптированным к их конкретным требованиям, экономичным, своевременным и эффективным способом, который может регулироваться соглашением об уровне обслуживания.

Возьмем для примера автомобильный сектор, и для современного «подключенного» автомобиля требуется чрезвычайно универсальная сеть, которая может одновременно обеспечивать высокую пропускную способность, сверхнадежность и низкую задержку для вспомогательного / автономного вождения, сбора и анализа данных с датчиков телеметрии, связи между устройствами. Непрерывность обслуживания при перемещении между сетями разных операторов является важной функцией, которую необходимо обеспечить.

И теперь мы получаем ряд предположительных сервисов для данного сектора и это такие как удаленная телеметрия, отслеживание безопасного и эффективного движения, сцепка, удаленный водитель и многие другие сервисы [1].

Как было написано ранее, что для многих сервисов потребуется работать в режиме с низками задержками, т.к. дорожная обстановка может измениться в любой момент и реакция на событие должно быть реализована с требуемым качеством. И для уменьшения задержек при обращению к требуемым сервисам оптимально будет их перенести в инфраструктуру туманных вычислений, что и поможет реализовать непрерывность обслуживания с минимальными задержками.

В данной статье мы опустим тот факт, что еще потребуется рассчитать, где же реализовать данную инфраструктуру и в каком количестве, что бы можно было обеспечить качество работы сервиса с надлежащим качеством. Можем предположить, что узлы туманных вычислений будут построены на базовых станциях в сотовых сетях, что достаточно логично для нашего примера (рис. 1).

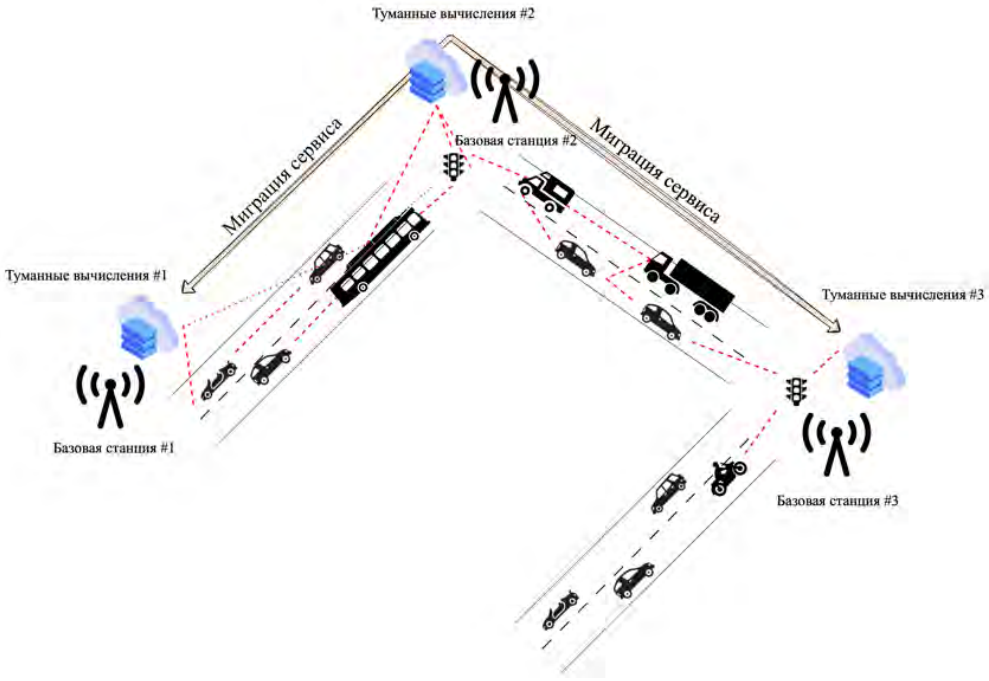


Рис. 3. Миграция услуг [2]

В первой части мы описали зачем и для чего нам нужна миграция сервисов. А теперь попробуем описать возможные способы и инструменты для миграции сервисов между туманными вычисленьями.

Для начало нужно понимать, что мы переносим приложение для выполнения тех или иных запросов «пользователя». Приложение может быть как полное так и декомпозированное, т. е. переноситься только часть или микросервис. В контексте туманных вычисление такие сервисы инкапсулируются в виртуальные машины или контейнеры (рис. 2).

Виртуализация - это классический подход, когда приложение упаковывается в образ виртуальной машины, который развертывается в инфраструктуре гипервизора. Этот образ содержит операционную систему, необходимые библиотеки и саму программу, реализующую сервис.

Контейнеризация – это экземпляр исполняемого приложения, который объединяется вместе со всеми связанными файлами конфигурации, библиотеками, зависимостями и средой выполнения. Контейнеры – небольшие, быстрые и портативные, потому что могут не включать в себя гостевую операционную систему, а используют функции и ресурсы основной операционной системы.

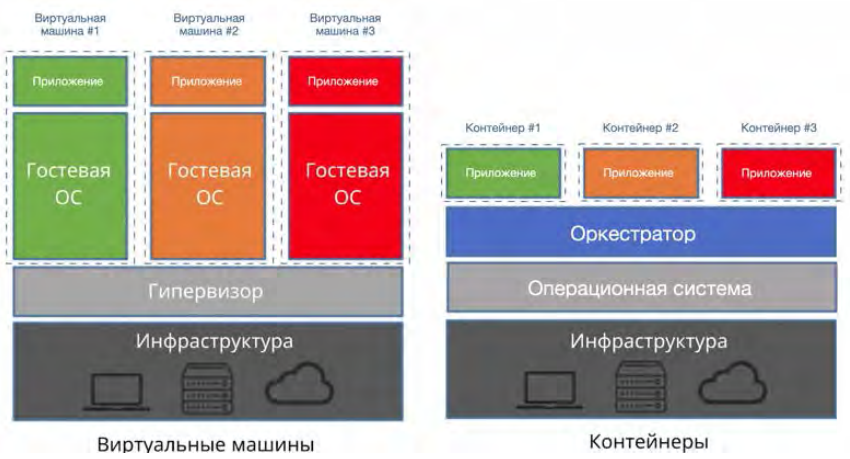


Рис. 4. Сравнение виртуализации и контейнеризации [3]

Из выше описанных способов, видим, что контейнерная технология дает ряд преимуществ по сравнению с обычной виртуализацией серверов:

- Приложение «собранное» на одном компьютере, можно развернуть на другом.
- Контейнеры совместно используют одну операционную систему, не требуется запускать отдельные экземпляры операционной систему.
- Контейнеризация намного меньше занимает место, т.к. не содержит образ операционной системы.

Если после кратного обзора способа миграции можно сделать предположительный выбор в сторону контейнеризация, по причинам универсальности, простаты развертывания. То, вот вид миграции можем представить в виде нескольких вариантов реализации. И, как их использовать, возможно, что-то гибридное, это будет зависеть от таких факторов, как причина миграции. Она может быть инициирована, как подвижным устройством между базовыми станциями, причем нужно учитывать скорость перемещения, так и объем переносимого сервиса. Так же причины переноса могут быть для балансировки рабочей нагрузки на сервера туманных вычислений, так и перенаправление ресурсов из-за недоступности или отключения узла вычислений.

Первый вид миграции (рис. 3), можем описать, как без миграции во время движения, в нашем примере транспортное средство. То есть приложение, развернутое у одной базовой станции, а транспортное средство при перемежение между базовыми станциями получает услугу через транспортную сеть.

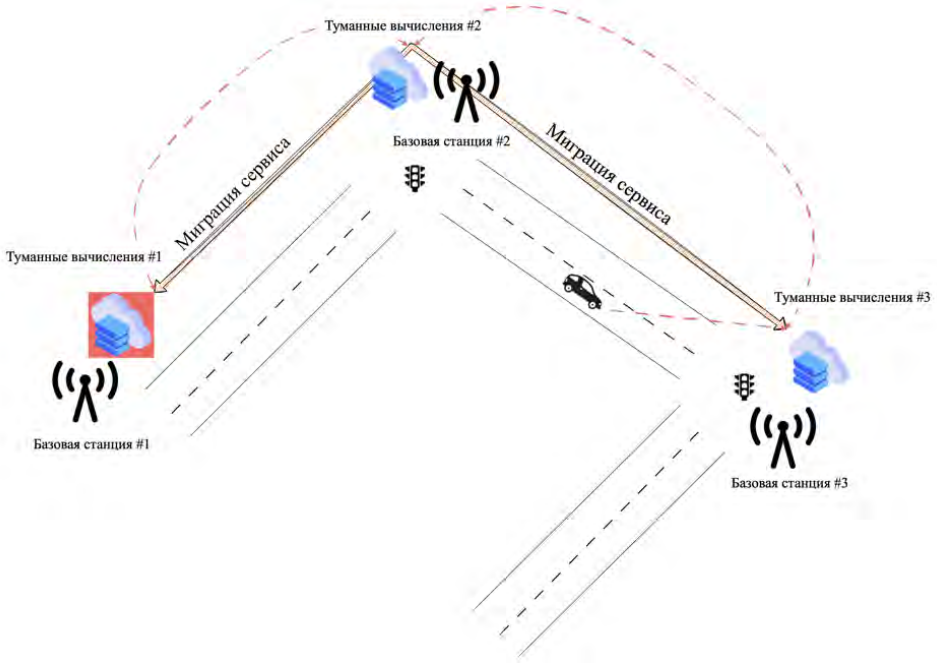


Рис. 5. Первый вид миграции [4]

Второй тип можем представить (рис. 4), как вид обслуживания абонента при передвижении от одной базовой станции к другой, так и сервис будет мигрировать, т.е. миграция будет выполняться в сочетании с передачей обслуживания.

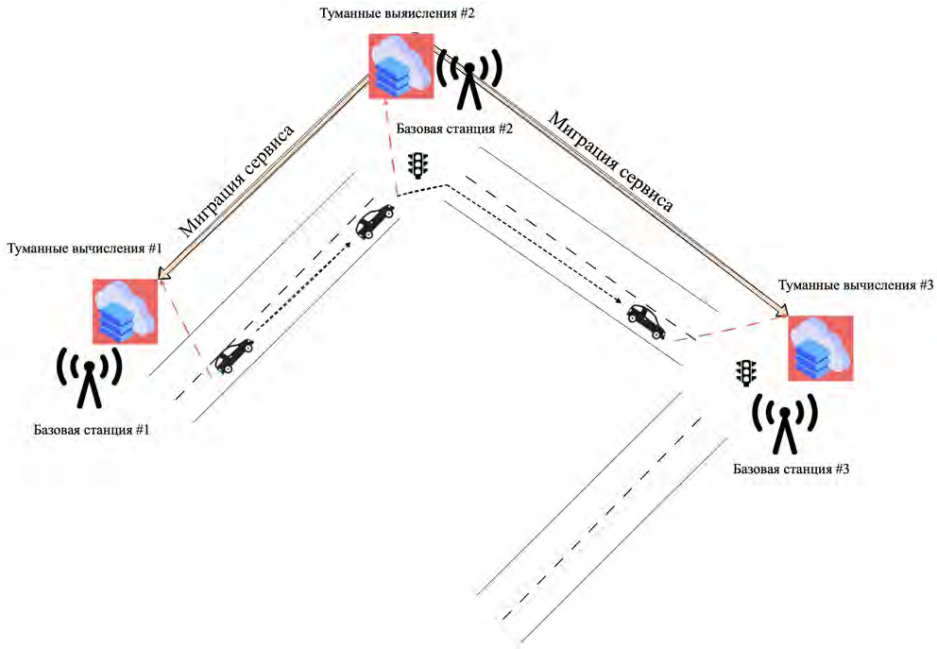


Рис. 6. Второй вид миграции [4]

И можем представить еще один вид миграции (рис. 5), который будет основан на первом и втором типе. Основой реализации данной схемы это требования приложения/сервиса к задержкам. Очевидным фактом является

то, что чем дальше от источника сигнала, тем дольше распространяется сигнал, и следовательно и наши приложения могут иметь трудности при взаимодействии с транспортным средством.

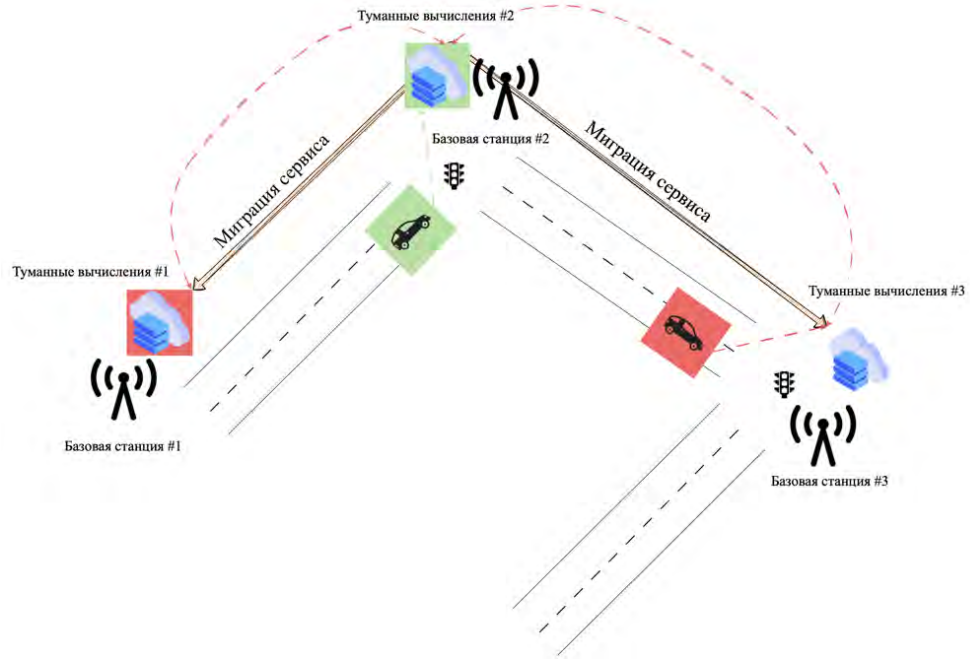


Рис. 7. Третий вид миграции [4]

В данном кратком обзоре были указаны основные точки для дальнейшего исследования миграции сервисов. И, как видно, что при первом приближении какой-либо реализации, возникают вопросы для детального рассмотрения и дискуссии.

Список используемых источников

1. Михайлов П. П. Исследование возможностей «сетевой нарезки» (network slicing) : бакалаврская работа : 17.06.21 / Михайлов Павел Павлович. СПб., 2021. 65 с.

2. Stypsanelli I., Medjiah S., Prabhu B. Reducing Service Migrations in Fog In- frastructures by Optimizing Node Location // 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC). Apr 2020, Paris, France. PP. 13–19.

3. Doug Jones. Virtual Machine – VM vs. Container [Электронный ресурс] // NetApp URL: https://www.netapp.com/blog/containers-vs-vms/ (дата обращения 15.02.2023).

4. Li J, Shen X, Chen L, Pham D, Ou J, Wosinska L, et al. Service migration in fog computing enabled cellular networks to support real-time vehicular communications // IEEE Access. 2019. N 7. PP. 13704–13714.

УДК 004
ГРНТИ 20.15.05

МЕТОДОЛОГИЯ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ ДЛЯ РАЗВЕРТЫВАНИЯ ПРОГРАММНОГО ПОДАВИТЕЛЯ WI-FI

О. А. Михалев, М. М. Рябов

Военная орденов Жукова и Ленина краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Некоторые известные примеры были сосредоточены на радиоэлектронной борьбе. Например, американские военные вложили значительные средства в автоматизацию с помощью программ беспилотных летательных аппаратов только для того, чтобы конкуренты, такие как иранцы, создавали стратегии вмешательства в эти системы. Ирану удалось захватить сверхсекретный американский разведывательный беспилотник, обманув его, заставив спуститься в неправильном месте, заглушив его управляющие сигналы и предоставив ему поддельные данные GPS. Эта статья сосредоточена на подходе к радиоэлектронной борьбе для развертывания программного подавителя помех Wi-Fi. Программный глушитель Wi-Fi помех может отключать цели, используя режим DoS pursuit. В статье описывается методология того, как программное обеспечение также может быть использовано для подавления беспроводных сигналов.

Wi-Fi, Беспроводная связь, Помехи Wi-Fi, радиоэлектронная борьба, беспроводные атаки.

Понятие радиоэлектронной борьбы появилось совсем недавно. Очень сложные процедуры, такие как GPS и Wi-Fi, возможны благодаря коммуникациям и нашему образу жизни. Беспилотные летательные аппараты (БПЛА) и сетевые камеры наблюдения могут быть атакованы различными способами, но их передача данных часто является наиболее уязвимой. Вместо того чтобы напрямую атаковать эти системы, средства радиоэлектронной борьбы предпочитают прерывать и влиять на соединения для передачи данных, на которые полагаются эти автоматизированные устройства. Такие устройства часто перестают работать или возвращаются к ожидаемому и уязвимому поведению по умолчанию, когда у них нет согласованного соединения. Ряд громких происшествий включал в себя радиоэлектронную борьбу. Например, американские военные [1] вложили значительные средства в автоматизацию с помощью программ беспилотных летательных аппаратов только для того, чтобы такие противники, как иранцы, разработали стратегии саботажа этих технологий. Иран [2] был способен захватить

сверхсекретный американский разведывательный беспилотник, заглушив его командный сигнал и предоставив ему поддельные данные GPS, в результате чего он потерпел крушение в неправильном месте. Чтобы сделать американские гаджеты неэффективными, российские военные [3] вложили значительные средства в технологии создания помех и радиоэлектронной борьбы. Во время полета Россия [4] даже продемонстрировала способность вывести из строя американский линкор, отключив энергию корабля.

Большая часть этих изощренных атак основана на аппаратном обеспечении и требует владения гаджетами, которые либо запрещены, либо непомерно дороги. Однако, не все методы полагаются на аппаратное обеспечение. Даная работа сосредоточена на использовании стратегии радиоэлектронной борьбы для установки программного подавителя помех Wi-Fi.

В этой статье [5] рассматривается методология атаки с деаутентификацией Wi-Fi DoS для создания помех в беспроводных сетях. Такие атаки, как отказ в обслуживании, методы деаутентификации, «Человек посередине», несанкционированный корневой доступ и атака олицетворения пакетов, исследуются в отношении систем связи.

Проблемы, связанные с безопасностью беспроводной сети, являются предметом данной статьи [6]. Существует несколько методов поиска текущих недостатков безопасности, включая операционную систему Kali Linux. Существуют различные процессы, участвующие в общем процессе растрескивания для беспроводных сетей. Эффективность процесса зависит от скорости, с которой можно взломать ключ, и точности, с которой можно определить пароль. Преимуществом [7] этой операционной системы, несомненно, является широкий выбор различных инструментов для оценки уязвимостей и тестирования на проникновение, которые специально созданы для этичного взлома.

Стохастические, основанные на зондировании и адаптивные помехи уменьшаются с помощью DeepWiFi [8]. Автоэнкодер на основе глубокого обучения используется в радиочастотной интерфейсной обработке для извлечения характеристик полосы частот. После этого глубокая нейронная сеть обучается точно идентифицировать сигналы как Wi-Fi, помехи или бездействие. С помощью меток каналов пользователи могут эффективно получать доступ к занятым или перегруженным каналам, не мешая легальным трансляциям Wi-Fi, которые проверяются с помощью радиочастотного отпечатка пальца на основе машинного обучения, что приводит к повышению пропускной способности. Пошаговый процесс показан на рис. 1.

Настройка лаборатории – на этом этапе происходит настройка виртуальной машины Kali Linux и установка инструмента Airgeddon. Данный этап представляет собой установку всех необходимых пакетов через терминал.

Рис. 1. Методология

Выбор сетевого адаптера – понадобится адаптер Wi-Fi для создания помех Wi-Fi в любой сети, но только в том случае, если используется kali на виртуальной машине. Адаптер Wi-Fi в этом случае используется для включения режима монитора в kali.

Сетевой интерфейс в системе является начальной и конечной точками сетевого соединения между двумя или несколькими устройствами. Так, eth0 означает подключение по локальной сети, а wlan0 - беспроводную локальную сеть или Wi-Fi.

Включить режим монитора – режим монитора позволяет перехватывать пакеты, которые не предназначены для третьей стороны, и вводить поддельные пакеты в целевую сеть. Для подавления помех Wi-Fi будет использоваться инструмент Airgeddon. Это скрипт bash, который используется для выполнения аудита в сети. Чтобы загрузить инструмент Airgeddon на нашу машину kali, происходит процесс его клонирования из репозитория git, используя команду git clone в терминале. Чтобы запустить Airgeddon, текущий рабочий каталог меняется на каталог, в котором присутствует Airgeddon. Запуск Airgeddon происходит, запустив Airgeddon скрипт «airgedddon.sh».

Главное меню Airgeddon содержит разныее опции для различных меню атаки. По умолчанию выбранный сетевой интерфейс находится в управляемом режиме, он разрешает получать только те пакеты, которые предназначены для используемого устройства. Чтобы вводить пакеты, требуется изменить режим на «режим мониторинга», который позволяет перехватывать вводить поддельные пакеты, а также перехватывать те, что не предназначены для используемого устройства. Включение режима мониторинга позволяет проводить беспроводные атаки. Перевод сетевого интерфейса в режим мониторинга производится через главное меню.

Определить точку доступа – теперь Airgeddon проверяет наличие всех необходимых репозиториев и обновлений. Далее предлагается новый интерфейс Airgeddon, где необходимо выбрать сетевой интерфейс, который wlan0, в данном случае является беспроводной локальной сетью или Wi-Fi. Сетевой адаптер переводится в режим мониторинга, который позволяет перехватывать пакеты или вводить поддельные пакеты из целевой сети.

После нескольких минут сканирования пользователь получает список всех точек доступа, находящихся в диапазоне работы сетевого адаптера. Список содержит в себе такие параметры, как mac-адрес, тип шифрования, занимаемый канал и уровень сигнала.

Выбрать опцию атаки – чтобы перейти к следующему шагу, выбирается режим DoS-атаки, который предоставит наибольшее количество возможностей для DoS-атаки. Началу атаки предшествует исследование всех точек доступа, присутствующих в диапазоне адаптера Wi-Fi. Адаптер Wi-Fi должен находиться в режиме монитора. В ходе проверки программа выдает список всех точек доступа в пределах диапазона имеющегося адаптера Wi-Fi, остается выбрать целевую точку доступа вместе с типом атаки, которую нужно выполнить. Хорошим вариантом будет DoS-атака, которая позволяет отключать все устройства, подключенные к Wi-Fi.

Выполнить атаку – затем будет предложено перейти к новому интерфейсу, в котором предстоит выбрать, нужно ли включать режим преследования DoS (его включение позволяет непрерывно выполнять атаку, даже если целевая точка доступа пытается защититься от атаки, переключая каналы). В данный момент начинается атака на целевую точку доступа, которая постоянно отклоняет любой запрос на подключение от различных устройств, подключенных к конкретно выбранной точке доступа.

В данной статье представлен подход к радиоэлектронной борьбе для реализации программного подавителя помех Wi-Fi на основе Wi-Fi адаптера. В зависимости от способа использования данной технологии, выполнение вышеописанных действий в нелегальном порядке может являться уголовным преступлением, как и любое другое DoS-нападение. В любом случае, маршрутизатор сохраняет журналы атаки, к которым можно получить доступ, чтобы узнать дату и место атаки, соответствующий MAC-адрес и другие детали, которые могут быть использованы для легкой идентификации вас по соседним камерам безопасности или данным вышки сотовой связи. Рассмотрев все факты, в данной статье показывается, как можно осуществить подавление Wi-Fi помех, используя виртуальную машину на основе ОС Kali Linux и инструментарий библиотеки Airgeddon. Данная DoS-атака должна отключить все устройства, подключенные к Wi-Fi и предотвратить их повторное подключение.

Список используемых источников

1. На видео видно, как истребители запускают рой крошечных дронов | Fox News // foxnews. URL: https://www.foxnews.com/tech/video-shows-fighter-jets-launch-swarm-of-tiny-drones (дата обращения 01.10.2023).

2. Эксклюзив: Иран захватил американский беспилотник, говорит иранский инженер // CSMonitor.com URL: www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone- says-Iranian-engineer (дата обращения 01.10.2023).

3. US Dim Mak пункт 2: Уязвимость к кибер / радиоэлектронной войне // The Manila Times URL: https://www.manilatimes.net/2017/01/12/opinion/an alysis/us-dim-mak-point-2-vulnerability-cyberelectronic-warfare/306502 (дата обращения 01.10.2023).

4. Россия способна «нейтрализовать военные корабли США», утверждается в отчете // Daily Mail Online URL: https://www.dailymail.co.uk/news/article-4424320/Russia-able-neutralise-warships-report- claims.html (дата обращения 01.10.2023).

5. Как взломать Wi-Fi: автоматизация взлома Wi-Fi с помощью Besside-ng // WonderHowTo URL: https://null-byte.wonderhowto.com/how-to/hack-wi- fi-automating-wi-fi-hacking-with-besside-ng 0176170/ (дата обращения 01.10.2023).

6. Цисар П., Цисар С. М. Этический взлом беспроводных сетей в среде Kali Linux // Международный инженерный журнал. 2018. N 16.

7. Каушик К., Танвар Р., Авастхи А. К. Инструменты безопасности // Информационная безопасность и оптимизация. 2020. С. 181–188.

УДК 004
ГРНТИ 49.33.29

СОЗДАНИЕ БЛОКЧЕЙН-АЛГОРИТМА КОНСЕНСУСА НА БАЗЕ МОБИЛЬНЫХ УСТРОЙСТВ

Н. А. Мурашкин, А. В. Помогалова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М..А. Бонч-Бруевича

В последнее время технология Blockchain стала неотъемлемой частью жизни обычного человека во всем мире. Проблемы финансовых переводов, безопасности и конфиденциальности данных, как никогда стоят остро. Блокчейн перестал быть загадочным и далеким, пробравшись в мобильные криптокошельки и аккаунты цифровых бирж, доступные по касанию пальца в любой точке планеты. Мощность мобильных вычислительных устройств стала превышать мощность компьютеров десятилетней давности, что дает понять: технический прогресс не стоит на месте. Тогда почему блокчейн – это что-то мощное и доступное в полном объеме лишь владельцам сверхпроизводительных устройств? Данная работа представляет собой анализ предпосылок и возможностей создания блокчейн-алгоритма консенсуса на базе современных мобильных устройств.

Блокчейн, Ethereum, мобильное приложение, смартфон, алгоритм консенсуса, Proof-of-Work, Proof-of-Stake.

Технология блокчейн представляет собой децентрализованную, распределенную и открытую базу данных, которая обеспечивает безопасность и прозрачность записи всех транзакций. Одним из ключевых аспектов блокчейна является алгоритм консенсуса, который обеспечивает согласование всех участников сети. Основываясь на распространенности и производительности нынешних мобильных устройств, разработка такого алгоритма становится возможной, а практическая польза данного алгоритма играет огромную роль в повышения уровня децентрализации и гибкости сетей [1].

Существуют определенные проблемы и вызовы, которые необходимо учесть при разработке алгоритма консенсуса для мобильных устройств:

- Мобильные устройства имеют ограниченные ресурсы, такие как мощность процессора, оперативная память и заряд аккумулятора. Алгоритмы консенсуса, такие как Proof-of-Work (PoW), используемый в Bitcoin, требуют больших вычислительных мощностей и энергии, что делает их непригодными для использования на мобильных устройствах. В связи с этим, необходимо разработать алгоритм консенсуса, который будет эффективно использовать ограниченные ресурсы мобильных устройств [2].
- Мобильные устройства могут иметь переменное качество сетевой связи, особенно в случае перехода между различными сетями или зонами покрытия. Это может привести к задержкам в передаче данных и рассинхронизации состояния блокчейна. Алгоритм консенсуса должен быть устойчив к таким изменениям в качестве связи и обеспечивать корректное функционирование сети блокчейн.
- В отличие от стационарных компьютеров, мобильные устройства часто используются для хранения и передачи персональной и конфиденциальной информации. Это делает вопросы безопасности и приватности особенно актуальными при разработке алгоритма консенсуса для мобильных устройств. Алгоритм должен соответствовать высоким стандартам безопасности и приватности, чтобы защитить данные пользователей и их активы.

Для корректной работы распределенной вычислительной среды, где все устройства являются равноправными участниками, главным вопросом, поставленным перед разработчиком, является алгоритм принятия решения. Для разрешения данного вопроса разрабатываются алгоритмы консенсуса – алгоритмы, которые позволяют в равноправной среде без доверия к определенной информации принять общее одинаковое решение. Самыми популярными алгоритмами консенсуса на данный момент являются Proof-of-Work и Proof-of-Stake.

Proof-of-work – алгоритм защиты распределенных систем от злоупотреблений, принцип работы которого сводится к двум основным пунктам: необходимости выполнения определенной достаточно сложной и длительной задачи и возможности быстрой и легкой проверки результата [3].

Proof-of-stake – альтернативный алгоритм консенсуса, идея которого состоит в использовании «доли» в качестве ресурса, который определяет, какая именно нода (узел) получает право добычи следующего блока. Сложность в данном случае распределяется пропорционально в соответствии с балансом данного узла, то есть большим шансом сгенерировать следующий блок обладает узел с большим балансом [4].

К сожалению, данные алгоритмы не подходят задаче, решаемой в этой работе, поскольку время использования и количество вычислительных мощностей играют огромную роль в стабильности всей целостности системы. В связи с этим, необходимо разработать собственный алгоритм консенсуса, опирающийся на базовые принципы блокчейна.

Помимо самого алгоритма консенсуса, в данном вопросе, архитектура системы, а также конструкция сети играют огромную роль, поэтому эту проблему необходимо разобрать тщательным образом.

Серверная часть и блокчейн-часть системы должны отвечать за надежность и постоянство передаваемой информации, что будет реализовано в коде программы на языке Python. Помимо модулей передачи и использования данных в сети, на языке Python будут написаны модули вычисления хэшей транзакций, использующиеся для получения мощности мобильных устройств [5].

Что касается пользовательской части системы, то для оптимальной работы сети необходима разработка приложения для ОС Android, осуществляющего функцию майнинга и связи с сервером. Для такой разработки оптимальным решением будет использование языка программирования Kotlin, поскольку аппаратные средства данного языка могут решить необходимые задачи.

В целом, система должна содержать передовые разработки в области блокчейна и связи, однако ввиду ее особенностей необходимо также использовать и опыт предыдущих реализаций P2P-сетей. Для чего же он нужен? Поскольку мобильные устройства не обладают особой надежностью, в начале разработки необходима дополнительная вычислительная мощность, запрашиваемая с серверов.

Как и реализация общеизвестной Peer-to-Peer системы Gnutella, данная разработка будет основываться на принципе запроса id пользователя, подключенного к сети, с сервера, что хранит информацию об адресе в блокчейне, а также о вычислительной информации, что он передает, конечно же, в зашифрованном формате. Данный подход обусловлен тем, что при подключении одного мобильного устройства к серверу позволяет другим мобильным устройствам узнать о нахождении только что подключившегося пользователя с помощью серверов передачи (рис. 1).

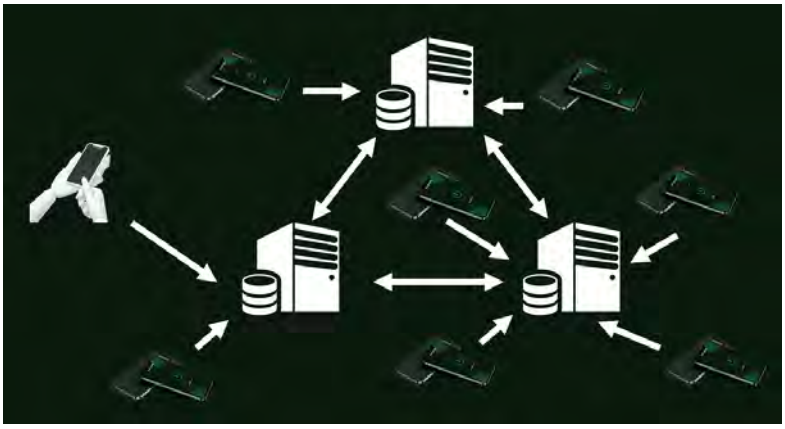


Рис. 1. Архитектура сети в первоначальном состоянии

Однако при выключении серверов все пользователи, что останутся в сети на момент отключения, будут знать друг о друге без поддержки информации с серверов, соответственно смогут общаться и передавать данные между собой (рис. 2).

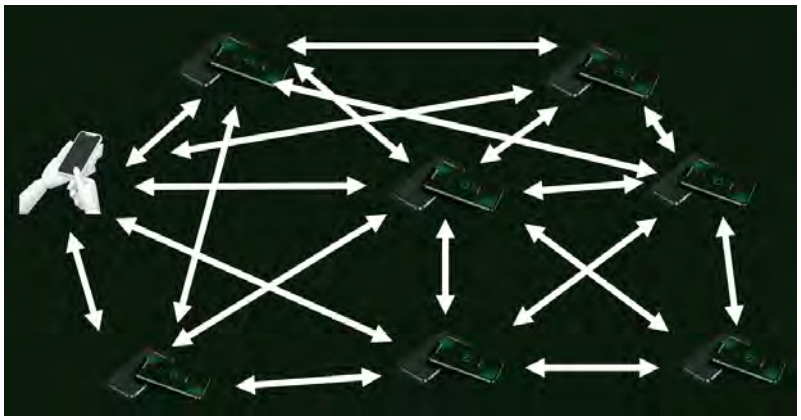


Рис. 2. Архитектура сети после отключения серверов перенаправления

Для подключения к общей сети блокчейна и передачи данных пользователю необходимо запустить приложение Verdatore (рис. 3), а также нажать на кнопку подключения к общей сети внутри интерфейса приложения.

Рис. 3. Приложение Verdatore в выключенном и включенном состоянии

Нажатие на данную кнопку запускает службу Android, что подключает телефон к сети, а после этого работает в фоновом режиме и использует процессор смартфона для вычисления хэшей транзакций, передавая вычислительную мощность созданной блокчейн сети [6].

В любой момент пользователь может отключить майнинг на его мобильном устройстве, просто нажав клавишу в приложении. Как и говорилось ранее, поскольку мощность устройства и заряд аккумулятора – важные

проблемы при постоянной работе, код программы будет ограничивать производительность вычисления хэшей для наибольшей продолжительности работы аккумуляторы и работоспособности устройства [7].

Таким образом, в данной работе были выделены проблемы реализации блокчейн-алгоритма консенсуса на базе мобильных устройств, а также предложены способы их разрешения. Помимо этого, был предложен вариант полноценной разработанной P2P-сети мобильных устройств с серверами перенаправления для реализации алгоритма, а также прототип приложения на базе Android для пользовательского взаимодействия с этим блокчейном.

Список используемых источников

1. Iansiti M., Lakhani K. R. The Truth About Blockchain. 2017. URL: https://hbr.org/2017/01/the-truth-about-blockchain

2. Ethereum Development Documentation. URL: https://ethereum.org/en/developers/docs/

3. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf

4. Max Wright. Delegated Proof of stake (DPoS) vs Proof of Work (PoW). 2015. URL: http://bytemaster.github.io/bitshares/2015/01/04/Delegated-Proof-of-Stake-vs-Proof-of-Work/

5. Skidanov A. The authoritative guide to Blockchain Sharding. 2018. URL: https://medium.com/nearprotocol/the-authoritative-guide-to-blockchain-sharding-part-1-1b53ed31e060

6. What is EOSIO URL:https://developers.eos.io/welcome/latest/index

7. Dai P., Mahi N., Earls J., Norta A. Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform. URL: https://qtum.org/user/pages/01.home/Qtum%20whitepaper_en%20v0.7.pdf

Статья представлена научным руководителем, доцентом кафедры ИКС СПбГУТ, кандидатом технических наук, доцентом В. С. Елагиным.

УДК 654.927.2
ГРНТИ 49.46.01

ОПТИЧЕСКИЕ СВОЙСТВА ВОДЫ И ЗАВИСИМОСТЬ ИХ ОТ ТИПА ВОДНОЙ СРЕДЫ

И. И. Павлов
Сибирский государственный университет телекоммуникаций и информатики

Развитие подводной оптической связи обеспечит изучение морского дна, наблюдение за глубоководными и океаническими нефтепроводами, подводной зоологической жизнью, обеспечение связи с подводными лодками и беспилотными системами и т. д.

На обеспечение оптической связи сильно влияет характеристика водного канала, также как мутность и соленость воды, которые могут снизить производительность. Кроме мутности и солености влияние оказывают примеси и молекулы воды, поэтому подводную среду необходимо рассматривать как сложную и динамическую среду. Чтобы получить более глубокие понимания подводной среды и характеристик канала, требуются обширные полевые исследования. В данной статье представлены оптические свойства воды, а также обсуждаются оптические свойства для разных типов воды.

оптические свойства воды, внутренние оптические свойства, внешние оптические свойства, тип воды, чистая морская вода, чистая океаническая вода, прибрежная океаническая вода, мутная вода гавани.

Молекулы воды и примеси, такие как взвешенные и растворенные частицы, органические и неорганические элементы, составляют подводную среду, поэтому ее можно рассматривать как сложную и динамичную среду. Взаимодействия между этими частицами и светом имеют место и классифицируются в соответствии с оптическими свойствами воды, которые различаются по нескольким соображениям, таким как местоположение, время суток, содержание органических и неорганических веществ и временные различия. Оптические свойства воды можно разделить на две части: внутренние и внешние [1].

Внутренние оптические свойства

Внутренние оптические свойства (ВОС) зависят исключительно от воды (компонентов и электромагнитных свойств воды) и твердых частиц, которые присутствуют в воде (взвешенные и растворенные частицы). Геометрия поля рассеянного света внутри среды не влияет на оптические свойства, присущие воде, то есть на ВОС не влияет способ освещения образца. Первичными ВОС являются коэффициент поглощения $\alpha(\lambda)$, коэффициент рассеяния $b(\lambda)$, функция объемного рассеяния (ФОР), коэффициент ослабления $c(\lambda)$, альбедо одиночного рассеяния ω_0 и показатель преломления [2].

Предположим, что проба воды имеет небольшой объем ΔV и толщину Δd, где коллимированный луч с мощностью излучения $P_I(\lambda)$ направляется на пробу воды. Часть этой мощности луча поглощается $P_A(\lambda)$, часть рассеивается $P_S(\lambda)$ на угол Ф, а остаточная мощность переносится через воду $P_T(\lambda)$. Отношение поглощенной мощности к общей падающей мощности обозначается как спектральная поглощающая способность $A(\lambda)$.

$$A(\lambda) = \frac{P_A(\lambda)}{P_I(\lambda)}.$$

Таким же образом, спектральное рассеяние, $B(\lambda)$ может быть найдено по отношению рассеянной мощности к падающей мощности.

$$B(\lambda)=\frac{P_S(\lambda)}{P_I(\lambda)}.$$

Коэффициент спектрального поглощения α(λ) можно найти, взяв предел, когда толщина приближается к нулю, для отношения спектрального поглощения $A(\lambda)$ к толщине Δd следующим образом:

$$\alpha(\lambda)=\lim_{\Delta d\to 0}\frac{A(\lambda)}{\Delta d}\left(m^{-1}\right).$$

И коэффициент спектрального рассеяния $b(\lambda)$ можно найти, взяв предел, когда толщина приближается к нулю для отношения спектрального рассеяния $B(\lambda)$ к толщине Δd следующим образом:

$$b(\lambda)=\lim_{\Delta d\to 0}\frac{B(\lambda)}{\Delta d}\left(m^{-1}\right).$$

Коэффициент ослабления спектрального луча $c(\lambda)$ может быть получен путем комбинирования коэффициента спектрального поглощения и коэффициента спектрального рассеяния как:

$$c(\lambda)=\alpha(\lambda)+b(\lambda),$$

где $\alpha(\lambda)$ и $b(\lambda)$ являются коэффициентами поглощения и рассеяния соответственно. Также единицы измерения коэффициентов $c(\lambda)$, α(λ) и $b(\lambda)$ измеряются в m^{-1} и λ является вакуумной длиной волны света в нм[3].

Угловое рассеяние на единицу расстояния и единичный телесный угол, β(Ф, λ) определяется как:

$$\beta(\Phi,\lambda)=\lim_{\Delta d\to 0}\lim_{\Delta\Omega\to 0}\frac{\beta(\Phi,\lambda)}{\Delta\Omega\Delta d}=\lim_{\Delta r\to 0}\lim_{\Delta\Omega\to 0}\frac{P_S(\Phi,\lambda)}{P_I\Delta\Omega\Delta d}\left(m^{-1}sr^{-1}\right),$$

где β(Ф, λ) представляет собой долю мощности, которая рассеивается из луча под углом Ф в телесный угол ΔΩ с центром на Ф.

$P_S(\lambda)$ является ли спектральная мощность, рассеянная на телесный угол, вычисляется как:

$$P_S(\Phi,\lambda)=I_S(\Phi,\lambda)\Delta\Omega.$$

Интенсивность падающего излучения вычисляется следующим образом:

$$E_I=\frac{P_I}{\Delta A}.$$

Подставив $\Delta V=\Delta d\ \Delta A$ который представляет собой объем воды, приводит к:

$$\beta(\Phi,\lambda)=\lim_{\Delta V\to 0}\frac{I_S(\Phi,\lambda)}{E_I(\lambda)\Delta(\Phi,\lambda)}.$$

Это уравнение обозначало функцию объемного рассеяния (ФОР) и ее можно объяснить, как интенсивность рассеяния на единицу падающего излучения на единицу объема воды. Путем интеграции β(Ф, λ) по всем направлениям можно рассчитать общую рассеянную мощность на единицу падающего излучения и единицу объема воды, этот параметр известен как коэффициент рассеяния.

$$b(\lambda)=\int\beta(\Phi,\lambda)d\Omega=2\pi\int_0^{\pi}\beta(\Phi,\lambda)\sin\Phi d\Omega.$$

Коэффициенты прямого (b_f) и обратного (b_b) рассеяния могут быть рассчитаны с помощью:

$$b_f(\lambda)=2\pi\int_0^{\pi/2}\beta(\Phi,\lambda)\sin\Phi d\Omega,$$

$$b_b(\lambda)=2\pi\int_{\pi/2}^{\pi}\beta(\Phi,\lambda)\sin\Phi d\Omega.$$

Путем нормализации ФОР с коэффициентом рассеяния может быть достигнута функция фазы рассеяния $\tilde{\beta}(\Phi,\lambda)$:

$$\tilde{\beta}(\Phi,\lambda)=\frac{\beta(\Phi,\lambda)}{b(\lambda)}\left(sr^{-1}\right),$$

$\tilde{\beta}(\Phi,\lambda)$ может быть выражена как вероятность события рассеяния фотона в угловом направлении Ф.

Альбедо одиночного рассеяния ω_0 может быть определено как отношение коэффициента рассеяния к коэффициенту ослабления, где коэффициент ослабления равен поглощению и рассеянию, поэтому результат закона альбедо одиночного рассеяния дает возможность рассеяния фотона, а не поглощения:

$$\omega_0=\frac{b(\lambda)}{c(\lambda)}.$$

Если значение коэффициента рассеяния больше значения коэффициента поглощения, то значение альбедо одиночного рассеяния равно 1, а если значение коэффициента поглощения больше значения коэффициента рассеяния, то значение альбедо одиночного рассеяния равно нулю [3].

Внешние оптические свойства

Внешние оптические свойства (ВнОС) основаны на двух основных факторах: среде и геометрической структуре освещения, т.е. является ли это коллимированным или рассеянным лучом [1]. Очевидные свойства обладают многими преимуществами, наиболее заметными из которых являются следующие. Во-первых, видимые свойства определяют направленность оптического луча. Во-вторых, они используются для оценки количества окружающего света для связи вблизи поверхности воды [2]. В-третьих, когда дело доходит до проникновения лучистой энергии в глубины океан, ВнОС очень важны [3]. Сияние, лучезарность и отражательная способность являются наиболее распространенными видимыми качествами. Видимая особенность может быть получена при использовании обычных и стабильных источников освещения. Таким образом, нисходящая интенсивность солнечного излучения не рассматривается как явное свойство из-за его изменения в зависимости от времени суток и состояния погоды [1]. Коэффициент диффузного ослабления – это оптическое свойство, которое зависит от геометрии светового поля [2]. В этих случаях либо соотношение свойств, на которые в равной степени влияет окружающая среда, является учитывается или нормализованная производная, как указано в следующем уравнении [4]:

$$k(z,\lambda) = -\frac{1}{E(0,\lambda)}\frac{dE(0,\lambda)}{dz},$$

где E определяется как исходное видимое свойство, такое как нисходящее излучение от Солнца.

Более подробную информацию об ВнОС, как их определения и измерения, можно найти [1, 5]. Каждый тип оптических свойств имеет особенности, которые способствуют реализации из ПОБС системы, где ВнОС используются для вычисления яркости окружающей среды вблизи поверхности воды, в то время как ВОС используются для определения бюджетов каналов связи.

Типы воды

Как географические, так и вертикальные различия приводят к различию океанских вод. Географические различия варьируются от прозрачности океанов до прибрежных районов, а вертикальная разница зависит от количества света, получаемого от солнца в дополнение к меньшему фоновому излучению. Несмотря на множество различных типов вод, его можно разделить на океанические и прибрежные районы в зависимости от нисходящей интенсивности солнечного света. Океаническая группа делится на четыре основных типа вод, которые обычно принимаются во внимание в литературе [6].

Чистая морская вода, рассеяние низкое, поэтому луч распространяется почти по прямой линии, но поглощение остается преобладающим, что приводит к большей потере сигнала, чем рассеяние в этих областях.

Чистая океанская вода, рассеяние является доминирующим фактором из-за обильной концентрации растворенных частиц и, следовательно, рассеяние оказывает большое влияние на общее затухание.

В прибрежной океанской воде поглощение, обусловленное фитопланктоном, является основным ограничивающим фактором, и, следовательно, идеальные длины волн склоняются к зеленому цвету.

Мутная вода гавани: она демонстрирует сильное поглощение в синем диапазоне длин волн из-за наличия как взвешенных веществ, так и цветных растворенных органических веществ, таких как фульвокислоты и гуминовые кислоты.

Из-за солености, которая влияет на скопления и скорость оседания взвешенных твердых частиц океаны и эстуарии имеют более низкую среднюю мутность, чем пресная вода в озерах и реках. Соленость влияет на скопление взвешенных частиц и прикрепляет их, что приводит к их стабильности на дне, и здесь показана взаимосвязь между соленостью, взвешенные твердые частицы и прозрачностью воды [7]. Значение коэффициента ослабления c(λ) зависит от типа и глубины воды. В таблице 1 показаны коэффициенты рассеяния, поглощения и экстинкции для различных типов вод [8].

ТАБЛИЦА 1. Оптические свойства типов океанической воды

Тип воды	a (m^{-1})	b (m^{-1})	c (m^{-1})	-10 дБ расстояние (м)
Пресная вода	0,04	0,02	0,042	53,55
Морская вода	0,114	0,036	0,15	15,25
Прибрежные воды	0,178	0,22	0,398	5,77
Вода в гавани	0,366	1,828	2,194	1,05

Список используемых источников

1. Mobley C. Light and Water: Radiative Transfer in Natural Waters'. Academic Press. New York, 1994, Vol. 565.

2. Buiteveld H., Hakvoort J. H. M., Donze M. Optical properties of pure water // Ocean Optics XII. SPIE, 1994. Vol. 2258. PP. 174–183.

3. Gordon H. R. Can the Lambert-Beer law be applied to the diffuse attenuation coefficient of ocean water? // Limnology and Oceanography. 1989. Vol. 34. N 8. PP. 1389–1409. doi: 10.4319/lo.1989.34.8.1389.

4. Gordon H. R., Brown O. B., Jacobs M. M. Computed relationships between the inherent and apparent optical properties of a flat homogeneous ocean // Applied optics. 1975. Vol. 14. N 2. PP. 417–427. doi: 10.1364/AO.14.000417.

5. Cochenour B. M., Mullen L. J., Laux A. E. Characterization of the beam-spread function for underwater wireless optical communications links // IEEE Journal of Oceanic Engineering. 2008. Vol. 33. N 4. PP. 513–521. doi: 10.1109/JOE.2008.2005341.

6. Håkanson L. The relationship between salinity, suspended particulate matter and water clarity in aquatic systems // Ecological Research. 2006. Vol. 21. PP. 75–90. doi: 10.1007/s11284-005-0098-x.

7. Mehedi S. A. H. M. M., Hasan A. M., Sadiq M. A., Akhtar H., Islam L.S.R.. (IJACSA, 2020).

УДК 654.927.2
ГРНТИ 49.46.01

КРАТКИЙ ОБЗОР ИСПОЛЬЗОВАНИЯ РАДИОЧАСТОТНОГО И ОПТИЧЕСКОГО СПЕКТРОВ В ПОДВОДНОЙ БЕСПРОВОДНОЙ СВЯЗИ

И. И. Павлов

Сибирский государственный университет телекоммуникаций и информатики

Технологии подводной связи прошли долгий путь с реализацией беспроводных технологий, которые используют акустические волны или электромагнитные волны. Последние могут быть реализованы в радиочастотном спектре или в оптическом спектре. Электромагнитные волны обеспечивают высокую скорость передачи данных и высокоскоростную связь. Более того, подводная радиочастотная связь обеспечивает плавный переход между водой и воздухом, и на нее не влияют свойства мутности воды. Беспроводная связь в оптическом спектре обладает высокой пропускной способностью и низкой стоимостью. По этой причине обзор в данной статье посвящен различным аспектам подводной беспроводной связи с использованием радиочастотного и оптического спектров.

электромагнитная волна, радиочастотная волна, скорость передачи данных, оптическая беспроводная связь, водная среда.

Подводная беспроводная связь с использованием радиочастотного спектра

Электромагнитные волны являются более быстрым средством связи. Электромагнитные волны в радиочастотном диапазоне могут достигать высокой скорости передачи данных на короткие расстояния, поэтому это хороший выбор для подводной беспроводной связи. Волны, имеющие частоту менее 300 ГГц известны как радиочастотные волны. По сравнению со скоростью распространения звука через воду скорость радиоволн намного выше (примерно в 2×10^5 раз), поскольку они распространяются в воде со скоростью $2{,}25\times10^8$ мс$^{-1}$ (при условии, что показатель преломления

воды = 1,3) в то время как радиоволны распространяются в вакууме со скоростью света ~3×10^8 мс$^{-1}$. На электромагнитные волны влияют несколько факторов, таких как температура, соленость и глубина, и это приводит к серьезному ослаблению всех электромагнитных волн и, таким образом, ограничивает расстояние прохождения сигнала через воду. Из-за высокой электропроводности воды на высокой частоте радиоволны распространяются в воде иначе, чем в воздухе. По этой причине линии связи на расстояниях, превышающих 10 м в океане, не так просто создать, как в очень высоких частотах, так и в ультравысоких частотах (ОВЧ и УВЧ, соответственно), и даже на высоких частотах. В диапазонах более низких частот, например, в диапазонах чрезвычайно низких частот и очень низких частот (ЧНЧ и ОНЧ, соответственно), ослабление электромагнитной волны может рассматриваться как достаточно низкое, чтобы обеспечить надежную связь на многие километры. Использовалась система подводной беспроводной связи, основанная на основе микроволн, эта система может осуществлять связь на горизонтальном расстоянии 85 м, используя большую мощность передачи около 100 Вт. Тем не менее, это требует использования усовершенствованных антенн и значительной мощности передачи. Был применен аналогичный метод, со скоростью передачи данных 500 кбит/с на горизонтальном расстоянии 90 м. Урибе и Гроте [1] достигли скорости передачи данных 10 Мбит/с на расстоянии 100 м за счет повышения пропускной способности подводных систем беспроводной связи на основе микроволн. Тем не менее, радиочастотные и микроволновые сигналы подвергаются серьезному ослаблению в воде. Например, радиоволны 2,4 ГГц имеют затухание около 1685 дБ/м в морской воде, которая имеет проводимость 4 S/м [2].

Ученый Льорет использовал двоичную фазовую манипуляцию (BPSK) и квадратурную фазовую манипуляцию (QPSK) модуляции при проведении многих экспериментов в области промышленности, науки и медицины с использованием 2,4 ГГц, поскольку он был способен охватывать диапазон 16–17 см под водой на частоте 2,4 ГГц [3]. Был установлен наилучший диапазон частот (3–100 МГц) для падающего луча на глубине менее 5 минут из воздуха в море [1].

В [4, 5], сообщалось, что при использовании дипольного излучения с высокой мощностью передачи, около 100 Вт, радиочастотные частоты в диапазоне МГц могут распространяться в морской воде до дальности действия 100 метров. Тем не менее, для этого требуется усовершенствованная конструкция антенн и высокая мощность передачи.

Сравнивая подводную радиочастотную связь с акустической волной и оптической волной, метод радиоволн демонстрирует два важных преимущества. Первым аспектом является относительно плавная передача с использованием интерфейса воздух/вода, который обеспечивает трансграничную связь путем объединения наземных и подводных систем

радиочастотной связи. Вторым свойством является его превосходная устойчивость к турбулентности и помутнению воды. Короткая дальность связи из-за слишком большого количества соли в воде, которая считается проводящей средой передачи и, таким образом, ограничивает распространение радиочастотных волн, которые распространяются на несколько метров на чрезвычайно низких частотах (30 – 300 Гц). И, сложные требования к конструкции для очень больших антенн, в зависимости от их расположения над или под водой.

Подводная беспроводная связь с использованием оптического спектра

Огромные антенны с высокой мощностью передатчика в пресной воде и значительным ослаблением в морской воде являются наиболее очевидными недостатками, которые ограничивают использование радиочастотных передач. Кроме того, подводная акустическая беспроводная связь страдает от низкой пропускной способности и ограничений на низкую скорость передачи данных. Все эти ограничения акустической и радиосвязи побудили исследователей рассмотреть вариант оптической беспроводной связи особенно видимый свет, для поддержки высокой скорости передачи данных при ограниченном диапазоне связи [6]. Подводная оптическая беспроводная связь способна достичь Гбит/с на расстоянии нескольких сотен метров из-за высокой частоты оптической несущей. Существенной причиной повышенного интереса к подводной оптической беспроводной связи является доступность готовой компонентов коммерческой электроники, которые снижают сложность устройства, стоимость и энергопотребление [7]. Оптическая беспроводная связь (ОБС) – это передача данных через оптический носитель, то есть ультрафиолетовый, видимый или инфракрасный, в неуправляемой среде распространения. Распространение оптических волн под водой часто демонстрирует отчетливые особенности в различных длинах волн l, как представлено на рис. 1. Дантли [8] определил, что меньшее количество длин волн ослабления находится в диапазоне длин волн 450–550 нм (синий и зеленый свет) по сравнению с другим диапазоном длин волн в 1963 году. Это связано с процессом фотосинтеза водорослей, особенно в прибрежных водах в теплое время года. Поэтому сенсорные системы подводной оптической связи и прибрежных приложений предназначены для работы в зеленом спектральном диапазоне. Такое поведение оптических волн было экспериментально подтверждено Гилбертом и др. [9]. В 1966 году, который лег в основу систем ПОБС.

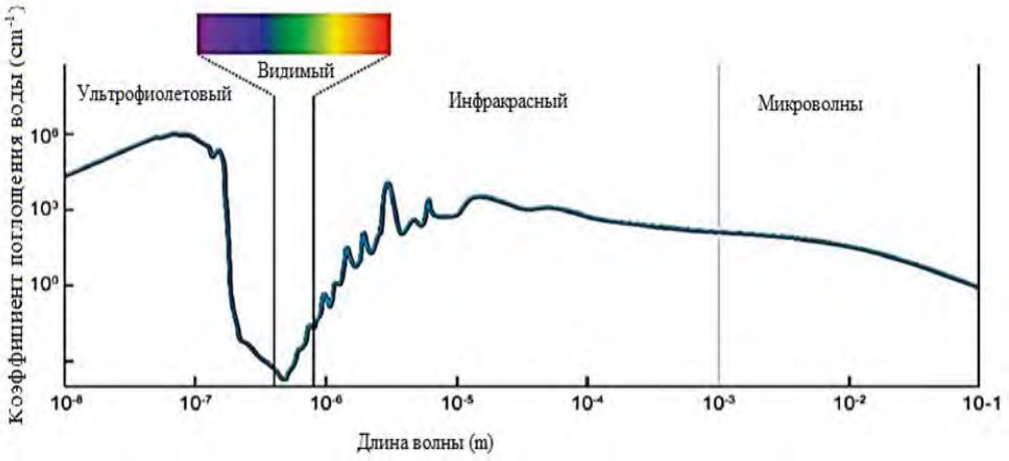


Рис. 1. Коэффициент поглощения чистой морской воды для различных длин волн пропускания

Первая в мире беспроводная телефонная система, позволяющая передавать речь, была создана в 1800 году Александр Грэм Белл и Чарльз Саммер Тейнтер, который был его помощником. Это изобретение получило название «фотофон», и оно было реализовано в соответствии с модифицированным солнечным лучом [10]. Новейшая эволюция высокоскоростных энергоэффективных оптоэлектронных устройств представила обещание скорости передачи данных ОБС до 100 Гбит/с при линиях передачи в несколько километров. Однако ОБС быстро развивалась по сравнению с подводной оптической беспроводной связи, и основной причиной этой задержки является сложность водной окружающей среды. Чтобы следить за поведением подводного света, исследователи провели несколько теоретических и экспериментальные исследования [11, 12, 13].

Системы подводной оптической беспроводной связи имеют много преимуществ по сравнению с радиочастотными и акустическими методами, но достижение подводной оптической беспроводной связи по-прежнему является задачей, перед которой стоит множество проблем. Тремя наиболее важными проблемами являются:

1) Как поглощение, так и рассеяние вызывают множество нежелательных эффектов распространения света. Чтобы ограничить эффект ослабления, вызванный взаимодействием фотонов с молекулами воды и другими частицами в воде, длина волны пропускающего света была специально выбрана в синем и зеленом спектре.

Наиболее важным из этих эффектов является интенсивное ослабление передаваемого светового сигнала, которое вызывает многолучевое замирание, низкая частота битовых ошибок (BER) на расстоянии связи в несколько сотен метров в условиях мутной воды.

2) Требуется точное условие выравнивания, чтобы гарантировать, что подводные оптические линии связи не будут временно отключены из-за несоосности между передатчиками и приемниками. Во многих исследованиях систем подводной оптической беспроводной связи использовались синие/зеленые лазеры или светодиоды, поскольку они отличаются преимуществом узкой расходимости луча. Несоосность связи может происходить часто, поскольку подводная среда является турбулентной на относительно небольших глубинах, особенно в системах ПОБС «поверхность-дно», основанных на вертикальных буях [12]. Серьезная проблема потери связи возникает из-за случайных движений морской поверхности [14].

3) Из-за сложности водной среды внедрение систем подводной оптической беспроводной связи требует надежных подводных устройств. На производительность и срок службы устройств подводной оптической беспроводной связи значительное влияние оказывает ряд природных явлений, таких как поток, температура, давление и соленость морской воды [15]. Батареи имеют ограниченное количество энергии, и их трудно подзарядить (солнечную энергию нельзя использовать под водой) [15].

Основным недостатком оптической связи является то, что дальность действия ограничена 1 – 100 метрами. Этот диапазон определяется водой и взвешенными частицами в воде, где свет ослабляется либо водой, либо рассеивается взвешенными частицами [16]. Другим недостатком является то, что оптическая связь обычно требует прямой видимости от передатчика к приемнику.

Список используемых источников

1. Uribe C., Grote W. Radio communication model for underwater WSN // 2009 3rd International Conference on New Technologies, Mobility and Security. IEEE, 2009. PP. 1–5. doi: 10.1109/NTMS.2009.5384789.

2. Schill F., Zimmer U.R., Trumpf J., paper presented at the Proceedings of ACRA, 2004, doi: 10.1.1.529.9671.

3. Кузнецов С., Огнев Б., Поляков С. Система оптической связи в водной среде // Первая миля. 2014. N 2. С. 46–51.

4. Al-Shamma'a A. I., Shaw A., Saman S. Propagation of electromagnetic waves at MHz frequencies through seawater // IEEE Transactions on antennas and propagation. 2004. Vol. 52. N 11. PP. 2843–2849. doi: 10.1109/TAP.2004.834449.

5. Абрамова Е. С., Павлова М. С., Абрамов С. С., Павлов И. И., Хан В. А. Принципы организации подводной оптической связи // Современные проблемы телекоммуникаций. Материалы Международной научно-технической конференции. Новосибирск, 2020. С. 445–448.

6. Truax B. Acoustic communication. Greenwood Publishing Group, 2001.

7. Gage C. P. Towards a Modular, Low-Power, Low-Cost, and High-Speed Underwater Optical Wireless Communication Transmitter / Electronic Theses and Dissertations. San Diego: UC, 2019. 63 p.

8. Duntley S. Q. Light in the sea // JOSA. 1963. Vol. 53. N 2. PP. 214–233. doi: 10.1364/JOSA.53.000214.

9. Gilbert G. D., Stoner T. R., Jernigan J. L. Underwater experiments on the polarization, coherence, and scattering properties of a pulsed blue-green laser // Underwater Photo Optics I. SPIE, 1966. Vol. 7. PP. 8–14. doi: 10.1117/12.971001.

10. Thompson S. P. The photophone // Nature. 1880. Vol. 22. N 569. P. 481. doi: 10.1038/022481a0.

11. Yi X., Li Z., Liu Z. Underwater optical communication performance for laser beam propagation through weak oceanic turbulence // Applied Optics. 2015. Vol. 54. N. 6. PP. 1273–1278. doi: 10.1364/AO.54.001273.

12. Tu B. et al. Acquisition probability analysis of ultra-wide FOV acquisition scheme in optical links under impact of atmospheric turbulence // Applied Optics. 2013. Vol. 52. N 14. PP. 3147–3155. doi: 10.1364/AO.52.003147.

13. Lu F., Lee S., Mounzer J., Schurgers C. Low-cost medium-range optical underwater modem: Short paper // Proceedings of the 4th International Workshop on Underwater Networks. 2009. PP. 1–4. doi: 10.1145/1654130.1654141.

14. Qasem Z. A. H., Leftah H. A., Sun H., Wang J., Qi, J., Esmaiel H. Deep learning-based code indexed modulation for autonomous underwater vehicles systems // Vehicular Communications. 2021. Vol. 28. P. 100314. doi: 10.1016/j.vehcom.2020.100314.

15. Hussein H., Esmaiel H., Jiang D. Fully generalised spatial modulation technique for underwater communication // Electronics Letters. 2018. Vol. 54. N. 14. PP. 907–909. doi: 10.1049/el.2018.0948.

16. Giles J. W., Bankman I. N. Underwater optical communications systems. Part 2: basic design considerations // MILCOM 2005-2005 IEEE Military Communications Conference. IEEE, 2005. PP. 1700–1705. doi: 10.1109/MILCOM.2005.1605919.

УДК 621.396.4
ГРНТИ 50.37.03

АНАЛИЗ И ОБЩАЯ КЛАССИФИКАЦИЯ РИСКОВ КИБЕРБЕЗОПАСНОСТИ ДЛЯ СИСТЕМ АВТОМАТИЗАЦИИ ДОКУМЕНТООБОРОТА НА БАЗЕ СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

И. Б. Паращук, В. А. Саяркин, А. В. Селезнев

Военная орденов Жукова и Ленина краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного

Проведен анализ и рассмотрены отличительные особенности угроз и грани возможного ущерба, вызванных основными рисками кибербезопасности для систем автоматизации документооборота на базе современных инфокоммуникационных сетей. Предполагается, что учет этих особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и технической реализации высококачественных подсистем кибербезопасности для систем

автоматизированной обработки электронных документов, использующих каналы и тракты современных инфокоммуникационных сетей.

инфокоммуникационная сеть, система автоматизации документооборота, электронный документ, риски, кибербезопасность.

Системы автоматизации документооборота, часто называемые также системами электронного документооборота, представляют собой совокупность территориально распределенных автоматизированных технических (аппаратно-программных и инфокоммуникационных) средств и комплексов для многопользовательского обмена электронными документами (ЭД). Они призваны сопровождать все или почти все процедуры управления функционированием организации (министерства, учреждения, департамента) с иерархической структурой, имея целью обеспечение качественного выполнения этой организацией своих задач [1, 2, 3, 4, 5].

При этом, являясь одним из базовых элементов типовой IT-инфраструктуры организации практически любого масштаба, классическая система автоматизации документооборота (САДО) обеспечивает не только и не столько обмен ЭД с использованием своей информационно-телекоммуникационной транспортной составляющей – современных инфокоммуникационных сетей (ИКС), но также предполагает и создание этих ЭД, управление доступом к ним пользователей, распространение этих ЭД по каналам и трактам ИКС между пользователями САДО, но главное – реализацию эффективного контроля над потоками ЭД в организации (министерстве, учреждении, департаменте) с иерархической структурой, создавая, тем самым, предпосылки для обеспечения высокого качества предоставляемых информационных услуг [6].

С точки зрения контента, предоставляемого САДО своим пользователям по каналам и трактам ИКС, принято различать ЭД в виде активных ЭД и архивов (различают протоколы и алгоритмы создания и управления актуальными и не актуальными ЭД, т. е., архивами), электронных материалов (данных), не попадающих под определение ЭД, протоколов (механизмов) реализации бизнес-процессов и обеспечения гарантии взаимосвязи между бизнес-процессами на основе потоков ЭД и протоколов (механизмов) коллективного сотрудничества – совместной, групповой работы над конкретными ЭД.

Не секрет, что весь этот контент, все эти ЭД и иные данные, создаваемые, хранимые и распространяемые в САДО по каналам и трактам ИКС, уязвимы, подвержены рискам модификации и уничтожения, нуждаются в дополнительных процедурах, обеспечивающих их кибербезопасность. Причем, особого внимания заслуживает контент САДО, распространяемый по открытым, не контролируемым каналам и трактам современных ИКС [7, 8].

В этой связи особую актуальность для понимания глубины проблемы, на наш взгляд, приобретают процедуры анализа и общей классификации возможных рисков (угроз) кибербезопасности ЭД и иных ресурсов, создаваемых, хранимых и распространяемых в рамках САДО по каналам и трактам современных ИКС [9].

При этом компонентами САДО, напрямую подверженными рискам кибербезопасности, являются не только и не столько данные (информация, ЭД) и их носители, но и процессы обработки этих данных в рамках систем такого класса, включая передачу ЭД по каналам и трактам современных ИКС.

С учетом того факта, что риски (угрозы) могут быть традиционно сгруппированы по нарушаемым аспектам кибербезопасности САДО, эти риски, как и для различных иных инфокоммуникационных систем, могут быть разделены на риски кибербезопасности с точки зрения нарушения конфиденциальности, нарушения целостности и нарушения доступности данных (ЭД), создаваемых, обрабатываемых и хранимых в рамках систем такого класса, а также передаваемых по каналам и трактам современных ИКС [10].

При этом считается, что наиболее серьезное значение имеют риски кибербезопасности САДО, связанные:

- с «утечкой» данных (ЭД) по техническим каналам взаимодействия между элементами САДО, а также по каналам и трактам транспортной (коммуникационной) базы таких систем – по каналам и трактам инфокоммуникационных сетей.
- с возможным несанкционированным доступом к данным (к ЭД), создаваемым, обрабатываемым и хранимым в рамках систем такого класса, а также передаваемым по каналам и трактам современных ИКС [9].

С точки зрения анализа и общей классификации, под кризисными событиями кибербезопасности для САДО с точки зрения нарушения конфиденциальности, могут пониматься такие явные риски, как:

- риски нарушения конфиденциальности автоматизированного рабочего места (АРМ) САДО – угроза непосредственного физического доступа к АРМ, когда потенциальный нарушитель заранее обладает данными идентификации (например, логин и пароль) легитимного пользователя или системного администратора САДО;
- риски воровства или перехвата данных (ЭД);
- риск нарушения конфиденциальности сервера операционной системы, на которой работает САДО – угроза загрузки на сервер вредоносного программного обеспечения, включая программы-шпионы, облегчающие потенциальный взлом САДО;
- риски нарушения конфиденциальности сервера САДО – угроза получения несанкционированного доступа напрямую к САДО, в обход сервера

операционной системы, т.е., минуя, обходя базовую систему кибербезопасности;

- риски нарушения конфиденциальности сервера базы данных САДО – угроза получения частичного или полного контроль над САДО и доступа к наиболее важным ЭД, хранимым в этой базе данных;
- риски для каналов взаимодействия между компонентами САДО – угроза перехвата пакетов между АРМ и базовыми серверами САДО;
- риски для каналов и трактов инфокоммуникационных сетей, действующих в интересах САДО – угроза преднамеренной подмены маршрутов доставки ЭД.

Под кризисными событиями кибербезопасности с точки зрения нарушения целостности, могут пониматься риски, ориентированные на основной объект САДО – электронный документ: риски нарушения целостности ЭД, циркулирующих в САДО (с точки зрения злоумышленной модификации заранее определенных системой вида и качества этих ЭД, хранящихся в базе данных САДО); риски нарушения целостности, т. е., вида и качества резервных копий ЭД.

И наконец, с точки зрения анализа и общей классификации, кризисными событиями и угрозами кибербезопасности с точки зрения нарушения доступности к коллекции ЭД, серверу операционной системы САДО, основному серверу САДО, серверу базы данных САДО, аппаратно-программным средствам САДО и каналам (каналам взаимодействия и каналам и трактам ИКС), выступать такие риски, как: риски нарушения доступности, связанные с халатным отношением при работе удаленного пользователя САДО; риски нарушения доступности, обусловленные непреднамеренными ошибками системных администраторов и иного персонала, обеспечивающих работу САДО.

Таким образом, проведен анализ и рассмотрены отличительные особенности угроз и грани возможного ущерба, вызванных основными рисками кибербезопасности для систем автоматизации документооборота на базе современных инфокоммуникационных сетей. Предполагается, что учет этих особенностей и классификационных признаков позволит повысить степень обоснованности принимаемых решений по разработке и технической реализации высококачественных подсистем кибербезопасности для систем автоматизированной обработки электронных документов, использующих каналы и тракты инфокоммуникационных сетей.

Список используемых источников

1. Национальный стандарт Российской Федерации ГОСТ Р ИСО 30300-2015 СИБИД. Информация и документация. Системы управления документами. Основные положения и словарь. М. : Стандартинформ, 2015. 18 с.

2. Тищенко А. А., Казаков Ю. М., Терехов М. В. и др. Автоматизация документооборота: учебное пособие. М. : Издательство Флинта. 2018. 108 с.

3. Коржук В. М., Попов И. Ю., Воробьева А. А. Защищенный документооборот. Часть 1: Учебно-методическое пособие. СПб. : Университет ИТМО, 2021. 67 с.

4. Паращук И. Б., Морозов И. В., Саяркин В. А. Подсистемы обеспечения безопасности электронного документооборота по каналам региональных телекоммуникационных сетей: требования и принципы построения // Региональная информатика (РИ-2022). Юбилейная XVIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2022)». Санкт-Петербург, 26–28 октября 2022 г.: Материалы конференции \ СПОИСУ. СПб, 2022. С. 114–116

5. Селезнев А. В., Паращук И. Б., Саяркин В. А. Современный электронный документооборот в автоматизированных системах диспетчерского управления движением поездов: вопросы защиты информации // Материалы V-й международной научно-практической конференции «Инновационная железная дорога. Новейшие и перспективные системы обеспечения движения поездов. Проблемы и решения». Сборник статей // Под общей редакцией М. Г. Яшина/ Санкт-Петербург, Петергоф: ВИ (ЖДВ и ВОСО), 2022. С. 405–413.

6. Стародубцев Ю. И., Бегаев А. Н., Давлятова М. А. Управление качеством информационных услуг / Под общ. ред. Ю. И. Стародубцева. СПб. : Изд-во Политехн. Ун-та, 2017. 454 с.

7. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства: научн. монография / Под общ. ред. В. А. Липатникова. СПб. : ВАС, 2020. 716 с.

8. Авраменко В. С., Беззубов О. В., Беляев С. В. и др. Технологии и средства построения инфокоммуникационных систем специального назначения: Часть II: Учебник / Под общ. ред. И. Б. Саенко. СПб. : ВАС, 2021. 416 с.

9. Ложников П. С., Жумажанова С. С. Об угрозах безопасности сведений ограниченного доступа в системах смешанного документооборота и правовом регулировании в области применения цифровых подписей с биометрической активацией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. N 4. С. 35–43.

10. Десницкий В. А., Паращук И. Б. Анализ и обеспечение защищенности данных пользователей беспроводных сенсорных сетей: показатели доступности, целостности и конфиденциальности // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. СПб. : 2019. С. 34–38.

УДК 621.396.4
ГРНТИ 50.37.03

ЭТАПЫ РАЗРАБОТКИ МОДЕЛЕЙ И МЕТОДОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ КАК ЭЛЕМЕНТОВ ПОЛИТИКИ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К РЕСУРСАМ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

И. Б. Паращук, В. А. Сундуков

Военная орденов Жукова и Ленина краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного

Рассмотрены, проанализированы и систематизированы физическая сущность и функциональное содержание этапов разработки современных моделей и методов многофакторной аутентификации пользователей в рамках реализации политики разграничения прав доступа этих пользователей к ресурсам инфокоммуникационных сетей. Проведен анализ возможных частных моделей и методов, позволяющих оценить качество аутентификации, оптимизировать и адаптировать процедуры данного многофакторного процесса проверки подлинности пользователей сети.

инфокоммуникационные сети, модели, методы, политика разграничения прав доступа, многофакторная аутентификация, пользователь, этап, ресурсы.

Политика разграничения прав доступа к ресурсам инфокоммуникационных сетей (ИКС) представляет собой набор правил и алгоритмов действий, с помощью которых администратор безопасности настраивает и управляет допуском к использованию этих ресурсов легальных пользователей всех автоматизированных рабочих мест ИКС, а также пользователей удаленных компьютеров, подключенных к общему серверу сети. При этом подразумевается, что настройка и управление правами доступа пользователей к ресурсам ИКС осуществляется комплексно и многогранно, начиная от процедур первичной и текущей авторизации, идентификации, первичной и текущей аутентификации пользователей (желательно – многофакторной) и заканчивая, например, динамическим, оперативным управлением правами в прикладных сетевых приложениях [1, 2, 3].

Авторизация рассматривается как процедура предоставления пользователю определенных прав доступа к ресурсам ИКС после прохождения им процедуры аутентификации, причем для каждого пользователя в рамках организации его беспрепятственного допуска к ресурсам сети заранее опре-

деляется диапазон прав, которыми он может воспользоваться при обращении к этим ресурсам. Под идентификацией легальных (авторизованных) пользователей ИКС, в том числи, и для предотвращения сетевых атак инсайдеров, понимается процедура их регистрации и последующего распознавания по оригинальному персональному идентификационному признаку [4, 5].

В области пересечения задач (целей, интересов) и процедур авторизации и идентификации как отдельных, значимых функций осуществления политики разграничения прав доступа, расположены функции, реализуемые в рамках аутентификации пользователей ИКС, под которыми понимается набор задач, решаемых в интересах проверки (верификации) подлинности субъекта доступа.

Иными словами, одним из важнейших элементов реальной политики разграничения прав доступа пользователей к ресурсам инфокоммуникационных сетей, является их аутентификация, позволяющая наверняка, однозначно убедиться в том, что пользователь сети, предъявивший персональный идентификатор (или подтвердивший факт обладания некой информацией, известной системе контроля доступа и доступной ему одному: логин, пароль, ключ и т. п.), в самом деле – именно тот пользователь ИКС (субъект доступа к ресурсам ИКС), чей идентификатор он предъявил [6, 7].

Многофакторная аутентификация – такая процедура, в процессе которой используется несколько типов аутентификационных факторов (атрибутов), которые может и должен предъявить (объявить) пользователь при доступе к ресурсам ИКС. Фактор (атрибут) аутентификации – определенный вид, объем либо носитель информации, предоставляемый пользователем ИКС при своей аутентификации.

Эти факторы (атрибуты) представляют собой знания, средства или объекты хранения одной из информационных компонентов, позволяющих осуществить легитимную процедуру аутентификации. Многофакторная аутентификация возникла вследствие того, что для обеспечения реализации реальной политики разграничения прав доступа пользователей к ресурсам инфокоммуникационных сетей уже явно недостаточно однофакторной (чаще всего, парольной) аутентификации.

Наборы факторов (атрибутов) определяют различные типы (механизмы) МФА, причем их обоснованный выбор и должен стать предметом разработки современных моделей и методов многофакторной аутентификации пользователей в рамках реализации политики разграничения прав доступа к ресурсам ИКС.

Анализ современного состояния и перспектив развития МФА позволил говорить о том, что этапами разработки современных моделей и методов

такой аутентификации в рамках реализации конкретной политики разграничения прав доступа к ресурсам ИКС, на наш взгляд, могут и должны быть:

1. Исследование и разработка моделей, методов и алгоритмов оценки качества МФА пользователей ИКС при их доступе к ресурсам сетей такого класса.

2. Исследование и разработка моделей и алгоритмов оптимизации процедур МФА пользователей ИКС на основе технологии искусственного интеллекта.

3. Исследование и разработка моделей и алгоритмов верификации и обеспечения непротиворечивости механизмов МФА пользователей ИКС.

4. Исследование и разработка моделей и алгоритмов выявления условий проведения и непосредственного выполнения адаптации механизмов МФА пользователей при реконфигурации политик разграничения доступа к ресурсам ИКС на основе технологии искусственного интеллекта.

В качестве исходных данных при разработке современных моделей и методов МФА выступают допустимая и суммирующая схемы разграничения прав доступа пользователей к ресурсам ИКС. Причем допустимая схема разграничения прав доступа к ресурсам ИКС, а значит, и соответствующие особенности МФА, задаются лицом, принимающим решения, а суммирующая схема и соответствующие ей свойства МФА возникают на основании базовых правил, присущих выбранной для конкретной ИКС политики (модели) разграничения прав доступа. Результатом решения задачи является значение обобщенного показателя, отражающего близость (сходство) между допустимой и суммирующей моделью и методами МФА.

Для решения задачи оценки качества МФА пользователей ИКС (в рамках первого этапа) могут быть предложены следующие подэтапы: выбор свойств и показателей качества МФА, создание универсальной модели описания процедур МФА, разработка метода и алгоритмов оценки качества МФА пользователей ИКС. В роли базовых особенностей и показателей, характеризующих МФА пользователей ИКС, предлагается принять точность аутентификации, целостность и доступность аутентификации такого типа для легитимного пользователя сети. Иными словами, точность покажет уровень организационно, физически, программно и лингвистически (семантически и синтаксически) правильного использования факторов (атрибутов) МФА. Целостность учитывает использование различных стандартов и протоколов безопасного распределения факторов (атрибутов) МФА между пользователями и подсистемами контроля доступа к ресурсам ИКС. Доступность гарантирует, что получение, хранение и обновление факторов (атрибутов) МФА обеспечивается своевременными действиями пользователя ИКС. Помимо этого, могут и должны быть учтены показатели качества средств и комплексов МФА, характеризующие их ремонтопригодность и отказоустойчивость.

Для решения задачи оптимизации процедур МФА пользователей ИКС на основе технологии искусственного интеллекта (второй этап) могут быть применены алгоритмы, основанные на глубоком обучении. Предлагается подход, позволяющий вывести правила формирования процедур МФА из существующих банков данных факторов (атрибутов) многофакторной аутентификации, где хранятся всевозможные знания, средства или объекты хранения различных информационных компонентов, позволяющих осуществить легитимную процедуру аутентификации конкретного пользователя. Для построения модели глубокого обучения на основе этих правил и хранимых факторов (атрибутов) МФА можно использовать нейронные сети.

Решение задачи верификации и обеспечения непротиворечивости механизмов МФА (в рамках третьего этапа) может быть реализовано с помощью известного подхода, основанного на методе «проверки на модели», который описывает множество состояний МФА, системы переходов между состояниями и индикаторную функцию, отмечающую каждое состояние МФА с набором свойств, истинных (верифицированных, непротиворечивых) для этого конкретного состояния.

И, наконец, решение задачи адаптации механизмов МФА пользователей при реконфигурации политик разграничения доступа к ресурсам ИКС (четвертый этап) предлагается организовать с использованием методов глубокого обучения и нечетких ситуационных алгоритмов (сетей). Причем, в модели глубокого обучения может быть применена составная искусственная нейронная сеть, основанная не только на многослойном персептроне, но включающая и нейросетевой автоэнкодер. На наш взгляд, подобный подход к интеллектуальной обработке данных МФА и адаптации ее механизмов позволит достаточно эффективно диагностировать коллизии в рамках процедур аутентификации и избегать их впредь, включая возможные сбои, связанные с реконфигурацией политик разграничения прав доступа.

Таким образом, рассмотрены, проанализированы и систематизированы физическая сущность и функциональное содержание этапов разработки современных моделей и методов МФА пользователей в рамках реализации политики разграничения прав их доступа к ресурсам ИКС. Проведен анализ возможных частных моделей и методов, позволяющих оценить качество, оптимизировать и адаптировать процедуры аутентификации.

Список используемых источников

1. Биячуев Т. А. Безопасность корпоративных сетей / под ред. Л. Г. Осовецкого. СПб. : СПб ГУ ИТМО, 2004. 161 с.

2. Мэйволд Э. Безопасность сетей. М. : НОУ «Интуит», 2016. 571 с.

3. Вострецова Е. В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.

4. Виткова Л. А., Паращук И. Б. Анализ современных инновационных решений по выявлению отклонений в эвристиках трафика сверхвысоких объемов для обнаружения

сетевых атак и защиты от них // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8 / СПОИСУ. СПб. : 2020. С. 99–102.

5. Андриянова Т. А., Саломатин С. Б. Комплексная оценка безопасности ведомственных сетей // Доклады Белорусского государственного университета информатики и радиоэлектроники. 2017, Том 109. N 7. С. 40–44.

6. Селезнев А. В., Сундуков В. А., Паращук И. Б. Многофакторная аутентификация пользователей информационных систем: особенности и проблемы // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конференции. Севастополь, 21–25 сентября 2021 г. / Севастопольский государственный университет, науч. ред. Б. В. Соколов. Севастополь : СевГУ, 2021. С. 51–52.

7. Паращук И. Б., Саенко И. Б. Оценка качества процесса реконфигурации политик разграничения доступа в облачных инфраструктурах критически важных информационных систем // Материалы конференции «Информационные технологии в управлении» (ИТУ-2020). СПб. : АО «Концерн «ЦНИИ «Электроприбор», 2020. С. 247–249.

УДК 004.056.5
ГРНТИ 81.93.29

НЕЙРО-НЕЧЕТКИЙ МЕТОД ДЕТЕКТИРОВАНИЯ УЯЗВИМОСТЕЙ ДЛЯ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ПРОЦЕССОВ И СРЕДСТВ ВЗАИМОДЕЙСТВИЯ ЧЕЛОВЕК – ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА В РАМКАХ КОНЦЕПЦИИ «SMART TRANSPORT»

И. Б. Паращук[1,2], А. А. Чечулин[1,3]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Военная орденов Жукова и Ленина краснознаменная академия связи
имени Маршала Советского Союза С. М. Буденного
3Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Предложен новый, нейро-нечеткий метод детектирования уязвимостей процессов и средств взаимодействия – интерфейсов взаимодействия– класса «человек – интеллектуальная система» в современных интеллектуальных транспортных системах, ориентированных на концепцию «Smart Transport». Данный метод эксплуатирует достоинства нейро-нечетких сетей, рассматривается как элемент политики безопасности и реализуется в рамках процедур повышения достоверности контроля защищенности подобных объектов. Практическое использование данного метода позволит устранить комплексную неопределенность (совместного типа: нечеткость и неполнота и противоречивость) исходных данных, имеющую место при решении задач поиска уязвимостей интеллектуальных интерфейсов подобного типа в реальных условиях реализации концепции «Smart Transport».

нейро-нечеткие сети, умный транспорт, интеллектуальная транспортная система, интерфейс, уязвимость, детектирование, метод.

Технические и программные решения в рамках концепции «Smart Transport» бурно развиваются в современном мире, в русскоязычной интерпретации их часто называют интеллектуальными транспортными системами (ИТС) [1, 2].

Это системы, так называемого, «умного» транспорта, использующие инновационные технологии, методы и средства, нацеленные на построение беспилотных транспортных комплексов, а также на оптимальную регулировку транспортных потоков, на «разгрузку» дорог и повышение безопасности дорожного движения. В идеале – для контроля и обеспечения бесперебойного движения не только наземного пассажирского транспорта, но и иных высокоскоростных (включая воздушные) транспортных потоков. По сути, это взаимоувязанная совокупность всех современных и перспективных «цифровых» и интеллектуальных инновационных решений в сфере транспорта и транспортной инфраструктуры. При этом контроль и обеспечение защищенности систем такого класса, является, по мнению отечественных и зарубежных исследователей, важнейшей задачей [3, 4].

Особого внимания в ИТС в рамках концепции «Smart Transport», на наш взгляд, заслуживает контроль защищенности процессов и средств взаимодействия (ПСВ) класса «человек – интеллектуальная система» (Ч-ИС). Данные ПСВ являются важным элементом ИТС, это интерфейсы, обеспечивающие обмен данными между оператором и интеллектуальной надстройкой ИТС в реальном времени и захват контроля над ними потенциальным нарушителем может привести к непоправимым последствиям.

Именно поэтому задачи выявления потенциальных угроз, задачи детектирования (выявления и идентификации) уязвимостей в ПСВ Ч-ИС для контроля их защищенности требуют особого внимания. Тем более, что задачи такого класса зачастую решаются в условиях различного рода неопределенности, связанной с неполнотой, нечеткостью, а зачастую, с противоречивостью исходных данных. При этом задачи детектирования «аномалий» в ПСВ Ч-ИС, квалифицирующих потенциальные угрозы их безопасности и наблюдаемых в условиях нечеткости исходных данных, часто предлагается решать на основе математики нечетких множеств [5].

Вместе с тем, учет иных классов неопределенности (помимо нечеткости) исходных данных для решения задач детектирования уязвимостей в ПСВ Ч-ИС, при данном методологическом и математическом подходе, невозможен. Задачи подобного класса предлагается решать с использованием методологии и математики современных нейро-нечетких сетей (ННС), которые позволяют, при работе с исходными данными, учитывать не только

их нечеткость, но и неполноту, и противоречивость этих данных, необходимых для достоверного детектирования уязвимостей в ПСВ Ч-ИС в интересах контроля их защищенности [6, 7, 8, 9].

Нейро-нечеткое детектирование (выявление и идентификация) уязвимостей в ПСВ такого типа в рамках ИТС в условиях нечеткости, неполноты и противоречивости исходных данных, имеет целью определение и категоризацию степени опасности конкретных уязвимостей для интерфейсов Ч-ИС. Метод детектирования уязвимостей в ПСВ Ч-ИС в интересах эффективного контроля их защищенности может быть применен на практике, например, для контроля безопасности интерфейса взаимодействия интеллектуальной системы подземных и наземных (и надземных) железнодорожных светофоров с человеком – дежурным машинистом поезда на линиях городских электричек Московского Центрального Кольца (МЦК).

В этом, как и в иных подобных случаях, нейро-нечеткий метод детектирования уязвимостей в ПСВ Ч-ИС, для примера контроля системы мониторинга машиниста поезда МЦК, будет объединять в себе две основные стадии: основная стадия – собственно последовательность детектирования уязвимостей с использованием обученной ННС и вспомогательная стадия.

В рамках предложенного нейро-нечеткого метода основная стадия – последовательность детектирования уязвимостей и обнаружения угроз с использованием обученной ННС, состоит из следующих этапов: фиксация (сбор нечетких, неполных и противоречивых исходных данных и их ввод в первый слой ННС); обработка (предварительная обработка в первом слое ННС); вычисление (вычисление параметров состояния с помощью ННС); анализ (определение состояния машиниста поезда).

На этапе сбора нечетких, неполных и противоречивых исходных данных определяется, какие исходные данные и как собираются (метод и элементы системы ИТС для сбора данных). Например, данные на основе электрокардиограммы машиниста поезда могут использоваться для записи частоты сердечных сокращений, а данные с камеры – для захвата изображений (видео) машиниста поезда МЦК. Данный этап осуществляется внутри кабины машиниста поезда МЦК. В зависимости от вычислительной сложности, степени неопределенности данных и типа уязвимости остальные три этапа могут проходить либо в транспортном средстве – поезде МЦК, либо в облачной вычислительной среде ИТС.

Вычисление параметров состояния с помощью ННС кроме традиционных нейро-нечетких механизмов, использует сравнение определенных числовых значений с некоторыми предопределенными или динамическими пороговыми значениями.

Предварительная обработка данных в первом слое ННС реализуется путем нейро-нечеткого преобразования исходных (собранных на первом этапе) данных в форму, которую можно непосредственно использовать для

расчета анализируемых параметров состояния защищенности интерфейсов типа Ч-ИС в рамках ИТС.

Определение состояния машиниста поезда – заключительный этап последовательности обнаружения уязвимостей. Здесь рассчитанные параметры сравниваются с соответствующими пороговыми значениями для определения наличия или отсутствия угрозы, соответствующей рассматриваемой уязвимости, возникающей в результате взаимодействия машиниста поезда МЦК как с самим транспортным средством – поездом, так и с интеллектуальной системой железнодорожных светофоров МЦК.

Вспомогательная стадия в рамках предложенного нейро-нечеткого метода предназначена для повышения качества основной стадии – последовательности обнаружения уязвимостей за счет обновления моделей обучения ННС, используемых на этапе предварительной обработки, и пороговых значений, используемых на этапе анализа.

При этом для создания моделей обучения ННС потребуются датасеты, которые содержат наборы данных в тех же форматах, что и на этапе сбора нечетких, неполных и противоречивых исходных данных о значениях параметров защищенности ПСВ в рамках ИТС типа «Smart Transport».

Таким образом, предложен новый, нейро-нечеткий метод детектирования уязвимостей процессов и средств взаимодействия (интерфейсов взаимодействия) класса «человек – интеллектуальная система» в современных интеллектуальных транспортных системах, ориентированных на концепцию «Smart Transport». Данный метод опирается на достоинства нейро-нечетких сетей, рассматривается как элемент политики безопасности и реализуется в рамках процедур повышения достоверности контроля защищенности подобных объектов. Практическое использование данного метода позволит устранить комплексную неопределенность (совместного типа: нечеткость и неполнота и противоречивость) исходных данных, имеющую место при решении задач поиска уязвимостей интеллектуальных интерфейсов подобного типа в реальных условиях реализации концепции «Smart Transport».

Работа выполнена при финансовой поддержке РФФИ (проект 19-29-06099) в СПб ФИЦ РАН (СПИИРАН).

Список используемых источников

1. Brown M. Smart Transport // Smart Cities in Application. Springer. 2020. PP. 69–83.

2. Sladkowski A., Pamula W. (Eds.) Intelligent transportation systems – problems and perspectives (Vol. 32). Springer International Publishing, 2016. 303 p.

3. Виткова Л. А., Израилов К. Е., Чечулин А. А. Классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020). IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2020. Т. 1. С. 253-258.

4. Elmaghraby A. S., Losavio M. M. Cyber security challenges in smart cities: Safety, security and privacy // Journal of Advanced Research. 2014. N 5. PP. 491–497.

5. Паращук И. Б., Чечулин А. А. Нечеткая идентификация уязвимостей в интерфейсах беспилотной транспортной среды «умного города» // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2022. Т. 1. С. 727–732.

6. Андриевская Н. В., Резников А. С., Черанев А. А. Особенности применения нейро-нечетких моделей для задач синтеза систем автоматического управления. // Фундаментальные исследования. Технические науки. 2014. N 11. С. 1445–1449.

7. Fuller R. Introduction to Neuro-Fuzzy Systems. Advances in Soft Computing Series. Springer – Verlag, Berlin, 1999. 289 p.

8. Паращук И. Б., Михайличенко Н. В. Особенности применения нейро-нечетких моделей для систем поддержки принятия решений в задачах оценки эффективности функционирования специализированных дата-центров // Информация и космос. 2019. N 1. С. 84–88.

9. Kotenko I. V., Parashchuk I. B., Omar T. K. Neuro-Fuzzy Models in Tasks of Intelligent Data Processing for Detection and Counteraction of Inappropriate, Dubious and Harmful Information // II International Scientific and Practical Conference «Fuzzy Technologies in the Industry» (FTI 2018), Ulyanovsk, Russia, October 23-25, 2018 / CEUR Workshop Proceedings (CEUR-WS). ISSN 1613-0073. 2018. Vol. 2258. PP. 116–125.

УДК 004.056
ГРНТИ 81.93.29

ОПИСАНИЕ УЯЗВИМОСТЕЙ ИНФОРМАЦИОННЫХ СИСТЕМ CVE-2022-1525, CVE-2022-1368, CVE-2022-1522, CVE-2022-38138 И МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ИМ

Д. И. Пекин, Е. С. Федорова,
В. А. Цыганов, Р. И. Шарапов, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье приведено описание ряда уязвимостей, связанных с работой информационных систем. В данной статье применялся анализ уязвимостей и атак, выполненный при помощи эксплуатации данных уязвимостей. Приведены примеры атак, выполненных с помощью эксплуатации данных уязвимостей. В статье так же описаны меры противодействия данным уязвимостям. На основании описанного в данной статье можно сделать вывод, что к наиболее распространенным причинам возникновения уязвимостей, как правило, относят: ошибки при проектировании и использовании программного обеспечения; несанкционированное внедрение и последующее использование ПО; внедрение вредоносного ПО; человеческий фактор. Своевременное реагирование на появление определенных уязвимостей и следование рекомендациям по их устранению

способствуют поддержанию общего уровня информационной безопасности на должном уровне.

информационная безопасность; уязвимость, кибератака, информационная система, мониторинг.

Повсеместное распространение информационных систем и неоправданно высокий коэффициент доверия к ним со стороны пользователей заставляют задумываться о рисках, которые связаны с таким обширным использованием информационных систем. Немаловажным аспектом является сетевое взаимодействие узлов, распределенных информационных систем, а также разрозненных Информационных систем. В рамках такого взаимодействия по сети передаются данные, идентификационные атрибуты и управляющие команды [1].

Потенциальная возможность взаимодействия с ИС, хранящими и обрабатывающими данные, в том числе стратегические и конфиденциальные, появилась у множества пользователей, среди которых неизбежно найдутся и злоумышленники [2]. Как правило для взаимодействия с информационными системами злоумышленники эксплуатируют уязвимости системы или – это присущие объекту информатизации свойства, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные особенностями процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, а также условиями эксплуатации [3]. Своевременный мониторинг сведений о появлении новых уязвимостей, может существенно повысить общий уровень информационной безопасности информационной системы [4].

В результате мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках 8 сентября 2022 года была опубликована информация об обнаруженных новых уязвимостях [5].

Первыми в списке стоят уязвимости:

- CVE-2022-1525 (BDU:2022-05592);
- CVE-2022-1368 (BDU:2022-05593);
- CVE-2022-1522 (BDU:2022-05594).

Данная группа уязвимостей относятся к уязвимостям микропрограммного обеспечения системы объемного измерения Cognex 3D-A1000 Dimensioning System и связаны с реализацией функций безопасности на стороне клиента с отсутствием проверки подлинности для функции изменения пароля с неправильной обработкой выходных данных для журналов регистрации [6]. Эксплуатация данной группы уязвимостей может позволить

нарушителю, который действует удалённо, повысить свои привилегии и в результате чего создавать произвольные лог-файлы, текстовые файлы о событиях, произошедших на сайте: информация о параметрах посещений сайта и ошибках, которые возникали на нем. Информация, хранящаяся в лог-файлах, служит основой для диагностики работы различных системных служб, а также для разнообразной аналитики, например, о посещаемости сайта или о попытках нарушения целостности системы [7].

Так же в списке была приведена уязвимость CVE-2022-38138 (BDU:2022-05595). Данная уязвимость относится к библиотеке TMW IEC 61850 Software Library и TMW IEC 60870-6 (ICCP/TASE.2) Software Library и связана с доступом к неинициализированному указателю. Эксплуатация данной уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании (DoS-атака) – это кибератака, в ходе которой злоумышленник стремится сделать компьютер или сетевой ресурс недоступными для предполагаемых пользователей путем временного или бессрочного нарушения работы хоста, подключенного к сети. Отказ в обслуживании обычно достигается путем заполнения целевой машины или ресурса избыточными запросами в попытке перегрузить системы и предотвратить выполнение некоторых или всех законных запросов [8, 9].

С помощью описанных выше уязвимостей был проведен ряд известных и официально задокументированных атак. В Telegram-канале (*https://t.me/cybersecs*) опубликована информация об атаке на инфраструктуру телекоммуникационного оператора «Крымтелеком» (*https://www.ktkru.ru*). Сообщается, что сайт компании недоступен и наблюдаются перебои мобильной связи и интернет-сети оператора. В ходе анализа установлено, что официальный сайт оператора в настоящее время недоступен [10].

В Telegram-канале (*https://t.me/onefistua*) опубликована информация об атаке на инфраструктуру компании ООО «ЧИСТОЗОР» (г. Москва), занимающейся производством оборудования для пищевой промышленности [11]. Сообщается, что злоумышленники получили полный доступ к CRM-системе управления фирмой на базе программного обеспечения 1С Enterprise 8.3. В качестве подтверждения приводятся скриншоты интерфейса управления CRM-системы компании [11].

В Telegram-канале (*https://t.me/itarmyofukraine2022*) с 8 сентября 2022 года продолжается координация DDoS-атак на различные сайты и ресурсы России. В качестве основной цели обозначены сайты и Интернет-ресурсы ПАО «Московский кредитный банк» (*https://mkb.ru/*). В качестве дополнительных целей приводятся следующие Интернет-ресурсы [12]:

- https://markirovka.crpt.ru/;
- https://1c-edo.ru;
- https://www.interfax.ru;

- https://auth.kontur.ru;
- https://api.taxcom.ru/v1.3/;
- https://service.ediweb.ru;
- https://diadoc-roaming.kontur.ru;
- https://edi.kontur.ru;
- https://diadoc-api.kontur.ru;
- https://e-vo.ru.

В Telegram-канале (*https://t.me/CyberSquattingChannel*) опубликованы URI-адреса, используемые в атаках с применением социальной инженерии, схожие с адресами интернет-ресурсов крупных российских компаний (такие, как: sbermarketref.ru; gazprom-energy.com; gazprom.za.com; avito-ii.online; okapay.ru; ostrovok.id8571.ru; ozon.id3819.ru; ozon.id7260.ru; ozon.id9114.ru) [13].

Эксплуатирования данных уязвимостей может привести к нарушению конфиденциальности информации, расположенной в различных информационных ресурсах. К примеру, в Telegram-канале (*https://t.me/cybersecs*), курируемом Владиславов Хорохориным, опубликована информация о наличии в открытом доступе исходных кодов сервиса по защите от DDoS-атак DDoS-Guard [14].

В результате анализа информации выяснилось, что объявление о продаже вышеуказанных данных опубликовано на Интернет-форуме Breach Forums (*https://breached.to*). Продавец сообщает, данные датируются маем 2021 года и содержат следующую информацию:

- запросы клиентов и ответы (имена, номера телефонов, сообщения, электронные письма, IP-адреса);
- все домены, использующие ddosguard;
- все dns-записи домена;
- ssl-сертификаты домена, открытые и закрытые ключи;
- имена загруженных файлов/скриншотов;
- серверные ip-адреса веб-сайта;
- журналы отправленных sms;
- все 42 000 пользователей (имена пользователей, bcrypt и хешированные (MD5) пароли, адреса электронной почты, полные имена, названия компаний, адреса, номера телефонов, ip-адреса, секретные ключи аутентификации);
- счета [15].

В качестве мер противодействия эксплуатации уязвимостей CVE-2022-1525 (BDU:2022-05592), CVE-2022-1368 (BDU:2022-05593), CVE-2022-1522 (BDU:2022-05594) и уязвимости можно привести установки обновлений из доверенных источников. В связи со сложившейся обстановкой и введен-

ными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков [16, 17].

В виде компенсирующих меры можно выделить:

- ограничение доступа к оборудованию из общедоступных сетей (Интернет);
- использование средств межсетевого экранирования;
- сегментирование сети с целью ограничения доступа к оборудованию из других подсетей;
- использование виртуальных частных сетей для организации удаленного доступа (VPN).

Важно отметить, что сами по себе уязвимости информационной безопасности не опасны. Они лишь открывают возможности для осуществления угроз ИБ. К наиболее распространенным причинам возникновения уязвимостей, как правило, относят: ошибки при проектировании и использовании программного обеспечения; несанкционированное внедрение и последующее использование ПО; внедрение вредоносного ПО; человеческий фактор. Своевременное реагирование на появление определенных уязвимостей и следование рекомендациям по их устранению способствуют поддержанию общего уровня информационной безопасности на должном уровне [18].

Список используемых источников

1. Красов А. В., Штеренберг С. И., Фахрутдинов Р. М., Рыжаков Д. В., Пестов И. Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // T-Comm: Телекоммуникации и транспорт. 2018. Т. 12. N 10. С. 36–40

2. Щеглов А. Ю., Щеглов К. А. Математические модели и методы формального проектирования системы защиты информационных систем: учеб. пособие. СПб. : Университет ИТМО, 2015. 93 с.

3. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика "РИ-2018". Материалы конференции. Санкт-Петербург, 2018. С. 570–571.

4. Волкогонов В. Н., Гельфанд А. М., Пестов И. Е., Поляничева А. В. Программное обеспечение мониторинга сети организации на основе системы zabbix. Свидетельство о регистрации программы для ЭВМ № 2020617706 Российская Федерация / В. Н. Волкогонов, А. М. Гельфанд, И. Е. Пестов, А. В. Поляничева ; заявитель и правообладатель СПбГУТ. – № 2020616735 ; заявл. 29.06.2020 ; опубл. 10.07.2020.

5. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г.А. Защита для распределенных отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. С. 329–334.

6. Красов А. В., Штеренберг С. И., Москальчук А. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. N 3 (88). С. 38–46.

7. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации. 2021. Т. 9. N 1. С. 47–58.

8. Красов А. В., Левин М. В., Фостач Е. С. Проблемы обеспечения безопасности облачных вычислений // Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 520–522.

9. Миняев А. А., Красов А. В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 3. С. 26–32.

10. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. N 1. С. 70–76.

11. Красов А. В., Штеренберг С. И., Голузина Д. Р. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. N 11. С. 39-47.

12. Виткова Л. А., Иванов А. И., Сергеева И. Ю. Исследование и разработка методик оценки рисков облачных ресурсов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 1. С. 152–155.

13. Виткова Л. А., Глущенко А. А., Сахаров Д. В., Чмутов М. В. Выбор оптимального метода оценки эффективности перехода к облачной архитектуре // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 168–171.

14. Виткова Л. А., Иванов А. И. Обзор актуальных угроз и методов защиты в сфере облачных вычислений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 179–182.

15. Пестов И. Е., Качуровский Ю. О. Использование брандмауэра для защиты информации // Инновационные технологии, экономика и менеджмент в промышленности. сборник научных статей по итогам XII международной научной конференции. НПП Медпромдеталь. Волгоград, 2021. С. 203–204.

16. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 1. С. 29-33

17. Пестов И.Е., Кошелева С.А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества. Сборник научных статей по итогам круглого стола со всероссийским и международным участием. Москва, 2021. С. 113–115.

18. Пестов И. Е., Алехин Р. В., Руденко С. А., Федоров П. О. Исследование воздействия ddos-атаки на виртуальную машину при наличии и отсутствии технологии

firewall // Теория и практика обеспечения информационной безопасности. Сборник научных трудов по материалам всероссийской научно-теоретической конференции. 2021. С. 263–269.

19. Пестов И. Е. Методика противодействия угрозам нарушения информационной безопасности инстансов и облачной инфраструктуры, основан на описании атак и методов противодействия им, используя теории графов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2022. С. 742–746.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ БЕЗОПАСНОСТИ АРХИТЕКТУР МОБИЛЬНЫХ ОС НА БАЗЕ LINUX (SAILFISH OS, UBUNTU TOUCH, HARMONYOS)

И. Е. Пестов, У. С. Юрова

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Современное общество стремительно развивается в направлении полностью подключенного интеллектуального мира, и такие тенденции выдвигают беспрецедентные требования к надежности и безопасности потребительских товаров. Новые смартфоны выходят на рынок технологий каждый день. Разработка портативных устройств с оперативной системой Linux, с сенсорным управлением, за последние несколько лет значительно продвинулась вперед. Планируя купить мобильный телефон, будь то новый или подержанный, люди учитывают определенные параметры, такие как цвет, размер, характеристики, качество камеры, процессора и памяти. Но самая игнорируемая часть - это операционная система. В статье проводится сравнительный анализ представленных на рынке современных мобильных операционных систем на базе Linux, таких как Sailfish OS, Ubuntu Touch, HarmonyOS, а также вопросы их конфиденциальности и безопасности.

*операционная система (ОС), мобильная платформа, микроядро, Linux, Sailfish OS, Ubuntu Touch, HarmonyOS, безопасность***.**

Аспекты безопасности мобильных платформ невозможно рассматривать отдельно друг от друга. Безопасность – это комплексное решение, охватывающее все стороны использования устройства от коммуникаций и изоляции приложений до низкоуровневой защиты и шифрования данных [1]. В данной работе будут тезисно описаны основные достоинства и проблемы современных мобильных ОС на основании таких важных критериев как:

- Исходный код.

Любой открытый код доступен для просмотра, изучения или изменения. Это дает преимущество перед закрытым программным обеспечением за счет возможности быстро выявлять проблемы и устранять их в кратчайшие сроки. Проприетарное ПО вынуждает пользователя принять тот уровень безопасности, который поставщик ПО готов предоставить. Поэтому в закрытом ПО могут быть скрыты различные уязвимости. Но стоит учитывать тот факт, что открытый исходный год также не является 100 % гарантией того, что все недостатки безопасности будут обнаружены и исправлены [2].

- Использование официального или стороннего репозитория.

Данные из сторонних репозиториев потенциально небезопасно использовать, так как злоумышленники могут получать доступ к вредоносным программам и помещать их в пакеты в открытых внешних репозиториях.

- Использование алгоритмов шифрования.

Шифрование данных позволяет сводить к минимуму угрозы утечки конфиденциальной информации через третьих лиц, даже в случае получения ими доступа к зашифрованным файлам.

Архитектура, рассматриваемых мобильных ОС

Одной из ключевых особенностей, рассматриваемых ОС, является использования микроядра, при котором архитектура системы построена на модульных блоках, функционирующих в виде процессов [3]. По сравнению с монолитным ядром, используемым в системе Android, микроядро дает много новых преимуществ:

- Высокий уровень безопасности. Объем кода в микроядре значительно сокращается, что приводит к упрощению анализа его безопасность, так как позволяет реализовать формальное математическое доказательство.
- Высокая надежность. Многие системные службы выполняются на модулях пользовательского режима, что не влияет на стабильность системы.
- Высокая масштабируемость. Модули можно удобно адаптировать и добавлять в соответствии с потребностями терминала, обеспечивая высокую масштабируемость [4].
- Независимость модулей. Модули пользовательского режима можно запускать, останавливать, удалять и обновлять независимо друг от друга.
- Поддержка распределенных вычислений. Все сервисные модули пользовательского режима являются независимыми управляемые и естественно поддерживающие распределенные вычисления.

Sailfish OS – это операционная система на базе Linux, основанная на проектах с открытым исходным кодом, таких как Mer, и включающая

пользовательский интерфейс с закрытым исходным кодом. Проект разрабатывает финская компания Jolla.

Sailfish OS в настоящее время использует трехуровневую архитектуру безопасности.

- Сторонние приложения, тщательно проверяются на наличие признаков злонамеренного поведения.
- Каждое приложение, независимо от его происхождения, запускается в изолированной программной среде Sailjail с явно назначенным набором разрешений для приложения, чтобы ограничить масштаб вредоносной активности, достижимой за счет использования возможной уязвимости в приложении.
- Кроме того, доступ к определенным конфиденциальным данным пользователя, доступен только для ограниченного набора привилегированных приложений и/или служб. Группы пользователей Linux используются для отделения привилегированных процессов от непривилегированных, а управление доступом к файловой системе обеспечивается ядром Linux [5].

Шифрование Sailfish основано на LUKS. LUKS – это стандарт шифрования жесткого диска Linux. Предоставляя стандартный формат на диске, он не только облегчает совместимость между дистрибутивами, но и обеспечивает безопасное управление несколькими пользовательскими паролями. Служба шифрования по умолчанию присутствует на каждом устройстве с ОС Sailfish. Она работает в фоновом режиме, даже если не активирована явно. Данные шифруются с помощью 256-битного алгоритма шифрования AES. Шифрование Sailfish распространяется на весь домашний каталог (т. е. /home).

Ubuntu Touch – это мобильная версия Ubuntu, созданная UBports. Проект с открытым исходным кодом, основанный на ядре Linux.

Безопасность Ubuntu Touch:

- Особое преимущество Ubuntu Touch поддержке функции AppArmor – это функция безопасности, которая позволяет приложениям получать доступ только к своим файлам с ограниченным доступом и не может работать в фоновом режиме. При каждом обращении программы к приватным данным отправляется запрос подтверждения.
- Модель доверия основана на доверенных и ненадежных приложениях. Большинство приложений, доступных в Ubuntu Touch OpenStore, работают в изолированной программной среде с ограниченным доступом. Проверка приложений может быть неполной, но по умолчанию они классифицируются как «Ненадежные». Важно отметить, что разрешение для приложений OpenStore на доступ к конфиденциальным данным обычно предоставляется или запрещается во время первого использования (кэширование результата для последующего использования по мере необходимости) [6].

- Система Content Hub, через которую приложения могут получить доступ к нужным файлам. Эта система действует как посредник, передавая только те данные, к которым был разрешён доступ приложению. Таким образом, конфиденциальность данных находится в зоне ответственности самого пользователя.
- Чтобы освободить пользователей от использования проприетарных мессенджеров, Ubuntu Touch продвигает использование любых открытых или размещение собственных репозиториев, что вызывает дополнительные риски безопасности.
- Полной поддержки шифрования диска (домашней папки) пока нет.

HarmonyOS – это операционная система от компании Huawei, которая может работать в большинстве современных интеллектуальных устройств. Она полностью совместима с программным обеспечением, разработанным под Android, Linux/Unix-системы и веб-приложения. Эта ОС использует особую технологию коммуникаций для интеграции отдельных устройств в виртуальное супер-устройство, что позволяет одному устройству управлять другими и обмениваться между собой данными.

Безопасность HarmonyOS основана на следующих моделях:

- В качестве модели разграничения доступа к защищаемой информации в HarmonyOS применяется классическая модель Белла – ЛаПадулы. Она основанна на мандатной модели управления доступом, при которой передача защищаемых данных от устройств с более высоким уровнем доступа к устройствам с более низким уровнем возможна только с согласия пользователя, а устройства с более низким уровнем доступа не могут получить данные с более высоким уровнем безопасности.
- Для обеспечения целостности данных применяется модель Биба (Biba), при которой приложения, программное обеспечение и пакеты с обновлениями из недоверенных источников не могут быть установлены на устройства с высоким уровнем безопасности. В ОС может быть загружено только подписанное цифровым сертификатом программное обеспечение, официально признанное HarmonyOS.
- HarmonyOS использует структурированную модель безопасности и присваивает метки безопасности пользователям, устройствам и данным, чтобы «разрешить доверенным пользователям получать санкционированный доступ к нужным» [7].
- Также устройства с HarmonyOS 2.0 предоставляют аппаратные механизмы для шифрования/дешифрования данных, получения ключей и поддерживают следующие алгоритмы:
  - симметричные алгоритмы типа AES-256;
  - алгоритмы хэширования типа SHA2 256, HMAC-SHA 512;
  - алгоритмы с открытым ключом типа RSA 4096.

Результат сравнительного анализа данных мобильных ОС на базе Linux представлен в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ мобильных ОС на базе Linux

Особенность	Sailfish OS	Ubuntu Touch	HarmonyOS
Разработан	Участники сообщества Sailfish Alliance , Mer , Jolla и Sailfish	Участники сообщества Ubports и Ubuntu (ранее Canonical Ltd)	Huawei
Лицензия	Бесплатная и с открытым исходным кодом, но пользовательский интерфейс и SDK являются проприетарными и имеют закрытый исходный код	Бесплатная и с открытым исходным кодом	Запатентовано, за исключением компонентов с открытым исходным кодом
Репозиторий	Разрешено использовать внешний репозиторий	Разрешено использовать внешний репозиторий	Только официальный
Ядро	Microkernel Android	Microkernel Android	Microkernel Android
Поддержка обновления системы	Да	Да	Да
Доступ к пользовательским данным для каждого приложения	Нет	Да	Начиная с версии 3.0+
Прокси сервер	Да	Нет	Только сторонние приложения и браузер
Шифрование на устройстве	Начиная с версии 3.3.0+ механизм AES-256	Нет	AES-256; SHA2 256, HMAC-SHA 512; RSA 4096
SSH-клиент	Да	Да	Да
VPN	Да	Да	Да
OpenVPN	Да	Да	Нет, но возможно со сторонними приложениями

В данной работе был проведен анализ мобильных операционных систем на базе Linux, основанных на микроядерной архитектуре. Программные и аппаратные проекты с открытым исходным кодом, такие как Ubuntu Touch, HarmonyOS и Sailfish стимулируют разработку мобильных устройств

на базе Linux. Большинство этих проектов в настоящее время находятся в разработке, но они развиваются достаточно быстро, и в будущем мы можем увидеть альтернативные операционные системы для ориентированных на конфиденциальность мобильных устройств, открытый исходный код которых дает широкие возможности для экспериментов. А ведь именно такие эксперименты двигают индустрию вперед.

Список используемых источников

1. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 657–662.

2. Теплюк П. А., Пономарьков С. М., Шарлаев Е. В. Методы эксплуатации уязвимостей уровня ядра операционных систем семейства LINUX // Программно-техническое обеспечение автоматизированных систем. 2019. С. 131–133.

3. Теплюк П. А., Пономарьков С. М., Шарлаев Е. В. Методы эксплуатации уязвимостей уровня ядра операционных систем семейства LINUX // Программно-техническое обеспечение автоматизированных систем : материалы всероссийской молодежной научно-практической конференции, Барнаул, 22 ноября 2019 года / Под редакцией А. Г. Якунина. Барнаул: Алтайский государственный технический университет им. И. И. Ползунова, 2019. С. 131–133.

4. Фёдорова О. В., Цветков А. Ю. Модули ядра linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 675–679.

1. Катасонов А. И., Красов А. В., Цветков А. Ю. Разработка универсального алгоритма по созданию простейших модулей ядра для различных версий ядра linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 438–442.

2. Татарникова Т. М. Ограничения утечки информации посредством неочевидных функций смартфона Android 5 // Информационно-управляющие системы. 2019. N 5 (102). С. 24–29.

3. Вострых А. В., Матвеев, А. В., Перлин, А. М., & Попивчак, И. И. и др. Специализированные мобильные приложения в сфере безопасности: сравнительный анализ решений и возможности развития // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2022. N 3. С. 128-137.

4. Яковлев И. А. Основы информационной безопасности // Научный Лидер. 2023. С. 13.

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.056.53
ГРНТИ 49.33.35

ПСЕВДОСЛУЧАЙНЫЕ ЧИСЛА И ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

И. И. Петров, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной работе показан метод получения псевдослучайной последовательности с помощью пользователя, два основных требования к последовательности случайных чисел, основные свойства любой периодической двоичной последовательности, тесты, применяемые для проверки качества генераторов и основные требования, которым должны удовлетворять криптографически стойкие генераторы псевдослучайных последовательностей и получаемые с их помощью гаммы.

генератор псевдослучайной последовательности, случайные числа, цикличность, сбалансированность, корреляция, графические тесты, статистические тесты, криптографически стойкие генераторы псевдослучайных последовательностей.

С приходом в мир компьютеров и их создателей, у человечества усилилась потребность в случайности и непредсказуемости.

Простые игральные кости и урны с карточками не удовлетворяли новым потребностям, ведь результатов броска может быть шесть, девять, двадцать четыре. А урна может переполниться и тогда карточки не перемешать. К тому же результат можно подтасовать. К тому же, бывает так, что нужно выбрать одно число из миллиона или же нужна случайная последовательность из миллиона и миллиона знаков.

Первые в мире программисты остро нуждались в случайных числах, поскольку полностью предсказуемый компьютер, который всё делает строго по заданный алгоритмам, полностью подчиняется поставленным задачам и следует инструкциям, нуждается в элементе случайности. Например, для защиты от взлома.

Так получилось, что в нашем мире существуют поистине случайные вещи. Люди научились использовать естественные явление, такие как ядерный распад, для того чтобы генерировать поистине случайные числа. Но в компьютерах нет радиоактивного тритя.

Вполне может быть, что именно поэтому система генерации случайных чисел в обычном компьютере работает плохо, поскольку используются псевдослучайные числа.

Используется двухуровневая система. Сначала выбирают зерно (сид). Небольшое случайное число, которое получают с помощью пользователя.

Пользователь нажимает клавиши в какие-то моменты времени.

Допустим, он нажал две клавиши, значит можно посчитать чётное число миллисекунд прошло между нажатиями или нечётное. Есть надежда, что это число будет случайное, непредсказуемое. Соответственно если пользователь нажал 8 клавиш, то мы может из этого извлечь 7 бит информации. А это мало, но всё же сколько-то. Поэтому на их основе производятся различные сложные преобразования, которые называются псевдослучайными генераторами. Иногда на их основе генерируются пароли, для удобства пользователей пароли могут храниться в веб-браузерах, но это понижает степень защиты таких паролей [1].

Есть разная степень надёжности псевдослучайных генераторов, бывают простые, которые на самом деле легко взломать, считается, что их никому не нужно взламывать. В задачах криптографии такие генераторы использовать не надо. Один из таких генераторов – это линейный конгруэнтный генератор.

Псевдослучайные числа генерируют с помощью сугубо математического алгоритма.

Псевдослучайная последовательность обязательно когда-нибудь начнёт повторяться. Это произойдёт, когда некое число встретится и используется в качестве начального значения во второй раз, и цикл пойдёт заново. Длина такого цикла до его повторения называется: период. Период строго ограничен размером сид. Если сид двухзначный, то алгоритм выдаст максимум 100 чисел, после чего какое-то начальное значение обязательно встретиться повторно. Из трёхзначного сид нельзя получить больше тысячи чисел, дальше алгоритм зациклится. Но если взять достаточно большое значение, то алгоритм может выдать поистине большое количество знаков до того как возникнет повтор.

Цикличность, корреляция и сбалансированность – это три основных свойства любой периодической двоичной последовательности.

Сбалансированность. Для каждого интервала последовательности количество двоичных единиц должно отличаться от числа двоичных нулей не больше чем на один элемент.

Корреляция. Если часть последовательности и её циклично сдвинутая копия поэлементно сравниваются, желательно, чтобы число совпадений отличалось от числа несовпадений не более чем на единицу.

Чтобы псевдослучайная последовательность была неотличима от действительно случайной, нужно чтобы компьютер не смог перебрать все возможные значения и не смог найти совпадения.

Очень важное различие между тем, что возможно сделать теоритически и тем, что возможно сделать за разумное время. Поэтому во многих ситуациях достаточно положится на достаточно секретный шифр вместо совер-

шенно секретного. Так же можно использовать облачные вычисления, которые обеспечивают доступ к вычислительным ресурсам, но такой метод имеет свои нюансы, связанные с безопасностью [2].

Псевдослучайные алгоритмы избавляют пользователей от необходимости предавать друг другу длинные случайные цепочки. Вместо этого они могут обменяться достаточно коротким случайным начальным значением и получить одну и ту же почти случайную последовательность.

Ранние шифрсистемы изначально разрабатывались как генераторы псевдослучайных чисел, но впоследствии стали генераторами шифрующей последовательности, но на данный момент ценность подобных последовательностей часто ставится под сомнение.

Непредсказуемость и случайность – это два основных требования к последовательности случайных чисел.

Непредсказуемость: каждое число в последовательности статистически не зависит от остальных чисел, то есть является непредсказуемым, невозможно узнать следующий элемент последовательности, зная предыдущий.

Если несколько раз запустить генератор по-настоящему случайных последовательностей и подать на его вход одни и те же числа, то на его выходе получатся разные случайные последовательности, другими словами последовательность нельзя воспроизвести – такая последовательность называется по-настоящему случайной. Случайность на постоянной основе используется в криптографических целях, где по-настоящему случайные последовательности просто необходимы.

Случайность, при создании последовательности псевдослучайных чисел в большинстве случаев предполагается, что данная последовательность псевдослучайных чисел является случайной в некотором определённом статистическом смысле.

Для доказательства того, что некая последовательность чисел является случайной, используются два критерия:

1. Однородное распределение, то есть частота появления каждого числа должна быть приблизительно одинаковой.

2. Независимость: ни одно значение в последовательности не должно зависеть от других.

Однако можно подобрать такой набор тестов, при использовании которого будут появляться доказательство того, что последовательность является зависимой. Рекомендуется применять набор тестов до тех пор, пока не будет уверенности, что независимость существует.

Для проверки качества генераторов применяются различные тесты. На данный момент не существует единого набора таких критериев, которые бы оценивали данные на случайность и их применимость для конкретной области. Существуют множество различных тестов оценки последовательности на действительную случайность.

На сегодняшний день методы оценки качества генераторов случайных и псевдослучайных последовательностей можно разделить на две группы:

1. Графические тесты. Выводы о свойствах исследуемой последовательности делают на основе графических зависимостей, в которых отражены последовательность.

2. Статистические тесты. Статистические свойства последовательностей определяются числовыми характеристиками.

Три основных общепринятых требования к криптографически устойчивым генераторам псевдослучайной последовательности и полученной с помощью гаммы [3]:

1. Период гаммы должен быть достаточно большим, чтобы его можно было применять для шифрования сообщений различной длины.

2. Гамма должна быть трудно предсказуемой или же, в идеальном случае, непредсказуемой вовсе. То есть если известны часть гаммы и генератор, то невозможно предсказать следующую или же предшествующую часть гаммы.

3. Генерирование гаммы должно быть простым, как в техническом плане, так и в организационном.

С развитием технологий большинство тестов можно автоматизировать и провести с помощью нейронных сетей [4].

На сегодняшний день большое количество людей активно вступают в дебаты по поводу того, какой генератор случайных чисел стоит использовать в той или иной системе, ядре операционной системы, языке программирования. Существует множество вариантов алгоритмов, заточенных на скорость, экономию памяти или же безопасность, и с каждым годом на них совершаются атаки, и вследствие чего они постоянно улучшаются и модернизируются, иногда даже появляются новые.

Подавляющее большинство программистов для повседневных задач, которые не связанны с безопасностью, полагаются на такие функции как rand(), эта функция более чем достаточна для большой и случайной последовательность данных.

Список используемых источников

1. Косов Н. А., Павлоцкий И. П. Анализ уязвимости систем хранения паролей в веб-браузерах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2021. Т. 1. С. 522–526.

2. Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А. Защита для распределённых отказов в обслуживании в облачных вычислениях // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII международной научно-технической и научно-методической конференции: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2019. Т. 1. С. 329–334.

3 Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. СПб. : ИЦ Интермедия, 2016. С. 100–112.

4. Косов Н. А., Мазепин П. С., Гришин Н. А. Применение нейронных сетей для автоматизации тестирования программного обеспечения // Наукосфера. 2020. N 6. С. 152–156.

УДК 004.056.53
ГРНТИ 49.33.35

ИССЛЕДОВАНИЕ ОСНОВНЫХ АСПЕКТОВ ASTRA LINUX, ПЕРВОЕ ЗНАКОМСТВО С ОПЕРАЦИОННОЙ СИСТЕМОЙ И ЕЁ УСТАНОВЩИКОМ, ПОЧЕМУ ГОССТРУКТУРЫ ПЕРЕХОДЯТ НА ASTRA LINUX, СТОИТ ЛИ ПЕРЕХОДИТЬ ОБЫЧНЫМ ПОЛЬЗОВАТЕЛЯМ

И. И. Петров, С. Н. Шемякин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье предоставлена информация содержащая: что такое операционная система Astra Linux в целом и операционная система общего назначения Astra Linux «Орел» Common Edition в частности, особенности установщика Astra Linux, информация о репозитории и его защищённости, удобство пользователя при использовании Astra Linux, почему госструктуры и коммерческий сектор переходят на неё, и почему она является основной отечественной операционной системой.

Astra Linux, Astra Linux «Орел» Common Edition, операционная система, установщик Astra Linux, репозиторий, безопасность Astra Linux.

Astra – это российская компьютерная операционная система (ОС) на базе ядра Linux, она была создана в рамках российской инициативы перехода на свободное программное обеспечение, то есть инициативы замены собственнического программного обеспечения на свободные аналоги с целью повышения безопасности и снижения зависимости от производителя-разработчика, к тому же она обеспечивает защиту данных до уровня «совершенно секретно» в российской классификации секретной информации за счёт обязательного контроля доступа.

Astra Linux до начала специальной военный операции и до того, как американская компания Microsoft объявила о сворачивании бизнеса в России, работала на предприятиях Минобороны, МЧС, ФСБ и других организаций, поскольку изначально была создана и развита для удовлетворения потребностей российской армии и спецслужб, однако всегда была лишь

дополнительным инструментом, более того, в течение 2010-х годов российские власти и промышленность предприняли первую попытку снижения зависимости от западных продуктов («индустриализация импортозамещения»). Сейчас отечественная операционная система становится основной, заменив собой Windows и получив поддержку и одобрение государства.

В январе 2018 года было объявлено, что Astra Linux будет развёрнута на всех компьютерах российской армии, а Microsoft Windows будет удалена. Через четыре года, 1 мая 2022 года, президент Российской Федерации Владимир Путин подписал указ о дополнительных мерах по обеспечению информационной безопасности госструктур. Согласно указу, 1 января 2025 года госорганам и госкомпаниям будет запрещено использовать средства защиты информации большинства зарубежных вендоров.

Компания «Русбитех-Астра» пять лет подряд занимает лидирующую позицию по проценту выручки среди конкурентов, например, по данным «СПАРК-Интерфакс», по итогам 2021 года чистая прибыль «Русбитех-Астра» составила 1,3 млрд рублей, доля выручки составила 69 %, показатель за 2022 год в компания не раскрыла.

Существует две доступные версии операционной системы: основная называется «Special Edition», а другая называется «Common Edition». Основными различиями между ними является тот факт, что первая является платной, в то время как вторая является бесплатной; первая доступна для архитектуры x86-64, архитектуры ARM и архитектуры Elbrus, в то время как последнее доступно только для архитектуры x86-64; первая имеет сертификат безопасности и обеспечивает 3 уровня безопасности операционной системы (которые названы в честь российских городов и которые от самого низкого до самого высокого: Орел, Воронеж и Смоленск), в то время как вторая не имеет сертификата безопасности и обеспечивает только самый низкий уровень безопасности операционной системы (Орел).

Таким образом, Русбитех-Астра предлагает несколько версий Astra Linux, одна из которых предназначена для общего использования: Astra Linux Common Edition Релиз «Орел» – операционная система общего назначения, которую можно скачать бесплатно, за защищённые решения придётся заплатить, например, за версию Special Edition, которая используется во многих российских государственных организациях. В частности, она используется в «Национальный центр управления обороной Российской Федерации».

В Astra Linux активно используется модуль обеспечения безопасности PARSEC [1].

Простой, быстрый и удобный установщик Astra Linux сразу добавляет в систему две раскладки клавиатуры, а также предлагает назначать клавиши для смены раскладки.

К тому же, при установке можно изменить состав системы во время инсталляции, в том числе и версию ядра, и получить в итоге, либо готовую к использованию операционную систему, или же заготовку, предназначенную для дальнейшей настройки.

Современная среда приятна глазу и не вызывает отторжения, выглядит весьма элегантно и будет по нраву большинству пользователей, при этом она демонстрирует отличную скорость работы, которая больше свойственна для простых оконных менеджеров или, например, облегчённых сред, типа OpenBox или JWM.

В режиме простоя система потребляет невероятно мало оперативной памяти в сравнении с более распространёнными системами, поэтому Astra Linux можно не боясь использовать даже для реанимации устаревших компьютеров и ноутбуков, мобильного решения у Astra Linux на момент 2023 года нет.

Стандартные приложения работают стабильно и открываются без каких бы то ни было проблем или же задержек, в том числе и веб-браузер Firefox, но все Astra не может похвастаться возможностями персонализации, к сожалению, малые возможности кастомизации среды могут раздражать пользователей, к тому же нет никаких расширений и виджетов как в более популярных операционных системах. Пользователь может лишь изменить положение панели задач, поменять обои рабочего стола (можно также изменить наложение логотипа), сменить основную тему и внешний вид курсора, после пары минут настройки можно получить приятное глазу оформление, но все стандартные обои сдержанные и нет никаких пёстрых картинок.

Операционную систему с помощью соответствующей опции можно установить с богатым набором программного обеспечения, если же нужно что-то иное, то в Astra Linux присутствует распространённый менеджер пакетов Synaptic, через который пользователь может установить всё необходимое.

Astra использует свои собственные репозитории хотя и связана с Debian, таким образом если по какой-то ни было причине нужно выйти за рамки, установленные разработчиком, пользователь столкнётся с нехваткой программ и компонентов, поскольку изначально ему будет доступен лишь базовый набор программ и компонентов, которые давно не обновлялись, к тому же нет графической утилиты для установки видеодрайвера.

Собственные репозитории, в которых находится только элементарный, самый базовый набор программ и компонентов, и несвежесть пакетов, обусловлены тем, что Astra Linux заточена под госслужбы и ведомства. У неё множество сертификатов по безопасности. Всё, что есть в Astra Linux, сначала кропотливо и досконально проверяется на закладки и прочее, что гарантирует очень хорошую защиту от вирусов [2].

К сожалению, Astra Linux не рассчитана на домашнее использование и слабо подготовленных пользователей, в том числе и её бесплатная версия Astra Linux «Орёл» Common Edition.

Пока, отечественные производители не могут предложить что-то дружелюбное, как Linux Mint или POP!_OS, чистая Ubuntu будет удобнее для использования обычному пользователю.

Astra Linux «Орёл» Common Edition работает стабильно, не зависает и не фризит, удобна в использовании и приятный внешний вид больше похож на Windows XP, чем на Linux, так же она проста и удобна в установке, имеет низкие требования к аппаратной части и её можно смело использовать даже на устаревших компьютерах и ноутбуках, большой набор дополнительных утилит, высокая степень защиты данных, есть практически весь спектр инфраструктурного ПО для импортозамещения и ряд уникальных особенностей безопасности. Присутствует хорошая защита от атак с использованием rootkit [3]. Фишкой же является мандатный контроль доступа и целостности.

Вместе с этим в Astra Linux есть ряд существенных недостатков, такие как: версии пакетов старее, чем у последних версий Ubuntu, свой репозиторий меньше, чем у Ubuntu и Debian.

Astra – это отличная система на базе Linux. Она лёгкая, быстрая и удобная, приятна глазу и проста в использовании, но только до тех пор, пока пользователю не захочется использовать все предлагаемые ею возможности, поскольку тогда придётся читать инструкции и вникать в саму суть операционной системы, что большинству пользователей делать совершенно не хочется, что в свою очередь отбивает всё желание, поэтому намного легче скачать что-то, уже полностью готовое к использованию.

Astra Linux отлично себя показывает в коммерческом секторе, на серверах и в отраслях с повышенными требованиями к безопасности.

В данной исследовательской работе были рассмотрены основные особенности установщика Astra Linux, удобство пользователя при использовании Astra Linux «Орел» Common Edition, коммерческая направленность Astra Linux, почему госорганы и коммерческий сектор переходит на отечественную операционную систему, защищённость репозиториев и две главные их особенности, так же было обращено внимание на указ президента Российской Федерации Владимира Владимировича Путина от 1 мая 2022 года, согласно которому 1 января 2025 года госорганам и госкомпаниям будет запрещено использовать средства защиты информации большинства зарубежных вендоров.

Список используемых источников

1. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа

в операционных системах семейства GNU Linux // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 2. С. 50–56. doi 10.46418/2079-8199_2020_2_8.

2. Штеренберг С. И., Красов А. В., Цветков А. Ю. Компьютерные вирусы. Ч. 1. СПб. : СПбГУТ, 2015. 62 с.

3. Попов А. А., Федорова О. В., Цветков А. Ю. Исследование современных механизмов обеспечения защиты конечных устройств под управлением ОС семейства Linux от атак с использованием rootkit // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. N 3. С. 36–43.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ СОВРЕМЕННЫХ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ, ВЛИЯЮЩИХ НА ЗАЩИЩЕННОСТЬ ИНФОРМАЦИИ

Т. С. Петрова, Д. В. Сахаров, А. А. Тасюк

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Безопасность информации в современных распределенных вычислительных сетях представляет собой сложную проблему, на которую влияют различные функции, такие как сегментация сети, контроль доступа, решения по управлению идентификацией и доступом, безопасность конечных точек и системы обнаружения вторжений. Эти функции играют решающую роль в защите конфиденциальной информации от несанкционированного доступа и других угроз безопасности.

информационная безопасность, распределенная вычислительная сеть, информационное противоборства, кибер-конфликт, киберугрозы.

Распределенные вычислительные сети (РВС) являются ключевым инфраструктурным компонентом в федеральных государственных органах. Они используются для обмена информацией, обработки и хранения данных, а также для управления различными процессами [1]. Однако такая высокая интеграция РВС в деятельность федеральных государственных органов также делает их уязвимыми к кибернетическим атакам.

Кибернетическое противоборство – это одна из самых серьезных угроз безопасности для РВС федеральных государственных органов. Кибернети-

ческие атаки могут быть направлены на критические информационные системы и сети, а также на конфиденциальную информацию и государственную тайну. Эти атаки могут быть нанесены с использованием различных технологий, таких как сетевая эксплуатация, фишинг, вредоносное ПО и социальная инженерия [2].

Одним из ключевых принципов защиты РВС является многоуровневая защита, которая включает в себя технологические, организационные и юридические меры. Технологические меры защиты включают в себя использование файрволлов, антивирусных программ и систем мониторинга [3]. Организационные меры защиты включают в себя разработку и соблюдение политик и процедур безопасности, а также обучение и информирование персонала. Юридические меры защиты включают в себя создание законодательных актов, положений и рекомендаций, которые регулируют и контролируют использование РВС в федеральных государственных органах.

Анализ угроз безопасности распределенной вычислительной сети федерального государственного органа в условиях кибернетического противоборства является важным и необходимым процессом для обеспечения безопасности информации и систем в этих органах. Этот анализ должен включать оценку рисков и угроз, а также принятие мер по их минимизации и управлению. Аудит должен включать в себя технологические, организационные и юридические меры защиты. Важность обеспечения безопасности распределенной вычислительной сети федерального государственного органа не может быть переоценена, поскольку это необходимо для защиты критической информации и систем, которые обеспечивают нормальную работу федерального государственного органа и поддерживают национальную безопасность [4].

Чтобы обеспечить безопасность распределенной вычислительной сети, федеральный государственный орган должен принимать меры по усилению защиты своих сетей и информации. Это использование современных технологий защиты, таких как шифрование, учетные записи и аутентификация, межсетевое экранирование и мониторинг сети. Такие меры позволяет обеспечить конфиденциальность, целостность и доступность информации, которая хранится и обрабатывается в распределенной вычислительной сети.

Также необходимо разработать и соблюдать правила и процедуры безопасности, которые будут регулировать доступ к сети и информации. Это может включать в себя ограничения доступа к определенным ресурсам сети, обязательное прохождение обучения по безопасности и проверку идентификации для доступа к конфиденциальной информации.

Важно заметить, что надежность и безопасность распределенной вычислительной сети зависит не только от технологических мер, но и от пове-

дения пользователей. Поэтому необходимо обеспечить обучение и информирование пользователей о способах защиты от киберугроз и принятия надлежащих мер в случае обнаружения угрозы [5].

Кроме того, необходимо проводить регулярные аудиты и оценку рисков, чтобы обнаруживать и исправлять уязвимости в сети [6]. Включающие в себя тестирование на проникновение, сканирование сети и анализ журналов системы.

В кибернетическом противоборстве критическое значение имеет способность оперативно обнаруживать и реагировать на киберугрозы [7]. Для этого необходимо использование инструментов анализа сети, а именно создание системы обнаружения вторжений, которая будет оперативно обнаруживать и анализировать аномальное поведение в сети. Это позволяет идентифицировать слабые места в системе и принимать меры для их устранения.

В заключении, распределенная вычислительная сеть федерального государственного органа подвержена различным угрозам безопасности в условиях кибернетического противоборства. Чтобы защитить сеть от этих угроз, необходимо применять меры безопасности на различных уровнях, от обеспечения защиты информации до мониторинга и реагирования на киберугрозы.

В целом, анализ угроз безопасности распределенной вычислительной сети федерального государственного органа в условиях кибернетического противоборства является критически важным для обеспечения безопасности информации и предотвращения кибератак. Потому как требует использования комплексного подхода, включающего технологические, организационные и поведенческие меры защиты. Необходимо регулярно проводить анализ угроз и проверять систему на уязвимости, а также создавать системы мониторинга и реагирования на киберугрозы.

Список используемых источников

1. Пешков А. И., Сахаров Д. В. Нормативно-правовые проблемы безопасности территориально распределенных информационных систем в офтальмологии // Офтальмохирургия. 2022. N S4. С. 132–137.

2. Бударный Г. С., Казанцев А. А., Красов А. В., Поляничева А. В. Разновидности нарушений безопасности и типовые атаки на операционную систему // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х ст. СПб. : СПбГУТ, 2022. Т. 1. С. 406–411.

3. Тасюк А. А. Принцип действий администратора безопасности для настройки защищенного режима в организации при помощи dlp // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2018. N 1. С. 107–110.

4. Бабков И. Н., Казаков Н. И., Карельский П. В., Миняев А. А. Определение показателей эффективности систем мониторинга и корреляции событий информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании

(АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х ст. СПб. : СПбГУТ, 2022. Т. 1. С. 125–129.

5. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. N 1. С. 70–76.

6. Чесноков А. Д. Информационная безопасность // StudNet. 2022. Т. 5. N 1. С. 478–489.

7. Dombrowski P., Demchak Ch. C. Cyber war, cybered conflict, and the maritime domain // Naval War College Review. Vol. 67. N 2. PP. 70–96.

УДК 004.71
ГРНТИ 49.27

ОБЗОР ПОДХОДОВ К ИЗМЕРЕНИЮ КАЧЕСТВА ОБСЛУЖИВАНИЯ И ВОСПРИЯТИЯ В СИСТЕМАХ ТАКТИЛЬНОГО ИНТЕРНЕТА

Е. С. Понамаренко

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

С развитием сотовой связи и достижением мобильных сетей пятого поколения технологиям Тактильного Интернета уделяется значительное внимание. В любой системе важно учитывать параметры и характеристики для измерения качества обслуживания и восприятия пользователей. Предметом исследования является обзор подходов к измерению качества обслуживания и восприятия в системах Тактильного Интернета. Метод исследования: сбор и анализ имеющихся исследований по теме измерения качества обслуживания и восприятия в системах Тактильного Интернета. Основные результаты. Приведено описание различных методов и подходов к измерению качества обслуживания и восприятия. Практическая значимость. На основе предложенных подходов представляется возможность для разработки новых методов и/или улучшения существующих.

Тактильный Интернет, хаптик-взаимодействия, кинестетическая информация, тактильный кодек, качество обслуживания, качество восприятия.

Введение

Для оценки хаптик-взаимодействий для Тактильного Интернета (ТИ), необходимо определить показатели оценки, отражающие качество восприятия (*Quality of Experience*, QoE) конечных пользователей. Кроме того, процесс оценки должен учитывать двунаправленный характер хаптик-взаимодействий: пользователи не только ощущают тактильную обратную связь,

аналогичную аудио/видео, но и физически воздействуют на окружающую среду [1].

Показатели QoE

QoE определяется как многоуровневая парадигма восприятия и поведения пользователей, представляющая эмоциональные, когнитивные и поведенческие реакции, которые являются как субъективными, так и объективными при работе с услугами, продуктами или приложениями [2, 3]. Соответственно, QoE для тактильных интернет-приложений должна включать: технические показатели, т. е. качество обслуживания (Quality of Service – QoS) и нетехнические показатели, т. е. пользовательский опыт (User eXperience – UX). Категория UX включает в себя три части: показатели восприятия (перцептивные), физиологические и психологические показатели. Эта организация более высокого уровня, как показано на рис. 1 (см. ниже), повторяет очевидную таксономию для оценки приложений Тактильного Интернета, и все вместе более настраиваемо в зависимости от параметров, необходимых для оценки. Например, поставщики услуг, желающие оценить только QoS приложения, могут пренебречь параметрами UX.

Параметры QoS для тактильных устройств обычно включают технические факторы, такие как задержка, джиттер, синхронизация и потеря пакетов и т. д. (табл. 1, см. ниже). Качество рендеринга относится к качеству основных модальностей в приложениях Тактильного Интернета. Сначала каждая модальность рассматривается отдельно, и в конечном итоге рассматриваются смешанные модальности. Соответствующие параметры UX были классифицированы как: параметры, связанные с восприятием, психологические и физиологические параметры. Измерения восприятия отражают то, как пользователи объективно воспринимают приложение, основанное на тактильных ощущениях. Психологические и физиологические параметры отражают субъективные состояния пользователя. Примерами параметров, представляющих эти категории [4], являются синхронизация медиа (параметр QoS), усталость и интуитивность пользователя (связанные с восприятием), хаптик рендеринг (параметр качества рендеринга) и степень погружения (психологическая).

Рис. 1. Организация более высокого уровня модели для приложений ТИ

ТАБЛИЦА 1. Параметры QoS

Время отклика	Время, затрачиваемое системой на реагирование на действие, измеряемое в миллисекундах или микросекундах
Задержка	Время, необходимое пакету, чтобы добраться от источника до места назначения, измеряется в миллисекундах или микросекундах.
Конфиденциальность	Речь идет о том, какой личной информацией можно делиться с кем и можно ли обмениваться сообщениями так, чтобы никто их не видел.
Защищенность	Уровень защиты информации, которой обмениваются с помощью мультимедийных технологий.
Пропускная способность	Объем данных, переданных от источника к получателю или обработанных за заданный промежуток времени. Измеряется обычно в битах в секунду или байтах в секунду

Субъективное качество обслуживания в системах ТИ

До сих пор QoE в хаптик системах оценивалось в основном с помощью субъективных тестов с участием пользователя [5]. Классически испытуемые оценивают системные артефакты по шкале оценки абсолютной категории, которая использует оценку качества по пятибальной шкале [6]:

1) Оценка 5 баллов – незаметный: задержка отсутствует, высокая точность передачи информации

2) Оценка 4 балла – ощутимый, но не беспокоящий: присутствует небольшая задержка, высокая точность передачи информации

3) Оценка 3 балла – слегка беспокоящий: присутствует небольшая задержка, средняя точность передачи информации

4) Оценка 2 балла – беспокоящий: высокая задержка, средняя точность передачи информации

5) Оценка 1 балл – сильно беспокоящий: высокая задержка, низкая точность передачи информации

Для оценки качества параметров можно использовать разработанный на кафедре Сетей связи и передачи данных в СПбГУТ программно-аппаратный комплекс для сбора, передачи и воспроизведения кинестетической информации в рамках концепции Тактильного Интернета [7]. Рекомендации по разработке экспериментов с участием людей можно найти, например, в [4].

Объективное качество обслуживания в системах ТИ

Субъективное тестирование QoE в хаптик системах обычно занимает много времени и стоит дорого [8], поскольку специализированное хаптик оборудование затрудняет распараллеливание тестов. Кроме того, поскольку испытуемые, как правило, новички в хаптик технологиях, необходим тщательный мониторинг (контроль) экспериментатора. Для решения этих проблем желательно объективное тестирование QoE. Оценка QoE посредством объективного тестирования основана на алгоритмических моделях человеческого восприятия и/или измерении нескольких параметров, связанных с предоставлением услуг. На данный момент в литературе доступно очень мало исследований по оценке качества хаптик-взаимодействий. Их можно разделить на две группы в зависимости от того, как прогнозируется качество.

1) Прогнозирование качества на уровне сигнала: Первая работа в этом направлении исследований была представлена в [9]. В этой работе для учета перцептивной значимости ухудшения хаптик сигнала с помощью просто заметной разницы (JND) было получено взвешенное по восприятию пиковое отношение сигнал/шум (HPW-PSNR).

В другой работе [8] предложена система прогнозирования качества для сжатия кинестетических сигналов для телеоперации. Однако предложенный

подход способен лишь качественно предсказать оценки пользователей. В [4] вводится метрика среднеквадратичной ошибки восприятия (MSE).

Вышеперечисленные объективные показатели качества сосредоточены на измерении точности сигнала путем вычисления «расстояния» между двумя сигналами перцептивным способом. Однако все они оценивают качество сигнала на основе показателей погрешности, которые работают исключительно на основе выборки за выборкой, так что вариации, зависящие от содержания, не учитываются. Чтобы восполнить этот пробел, в [10] была введена мера оценки качества хаптик ощущений – haptic SSIM (*structure similarity* – индекс структурного сходства). Основная предпосылка заключается в том, что качество сигнала оценивается с учетом зависимостей соседних выборок и что «штрафуются» только воспринимаемые искажения после учета чувствительности человека.

2) Прогнозирование качества на системном уровне: Работа в [11] предоставляет математическую модель системного уровня для приложений хаптик аудиовизуальной среды HAVE (*haptic audio visual environment*), основанную на взвешенной линейной комбинации между QoS и параметрами UX.

Модель авторов была оценена эмпирически с использованием субъективных тестовых площадок на 30 участниках, которые использовали HAVE игру под названием «Balance ball» (балансировочный мяч).

Заключение

Прогнозирование QoE на системном уровне для тактильных систем может быть выполнено тремя подходами. Первый подход основан на субъективных тестах, в которых пользователи явно высказывают свое мнение о хаптик-взаимодействиях, которые они использовали. Затем результаты проходят через регрессионный анализ, чтобы получить оптимизированные технические факторы, которые улучшают общее впечатление. Этот подход очень дорогой, требует много времени и не обладает повторяемостью. Кроме того, он не может быть применен в режиме реального времени.

Второй метод основан на алгоритмических и/или математических выводах. При таком подходе QoE увеличивает QoS, но не заменяет его полностью. Такой подход страдает от проблем с осуществимостью и точностью, поскольку не существует всеобъемлющей модели, которая могла бы количественно оценить многомерность и большую индивидуальную изменчивость.

Третий метод основан на подходе, основанном на машинном обучении. В области оценки визуального качества было предложено множество универсальных моделей машинного обучения [12, 13]. Основная проблема подхода к машинному обучению заключается в том, как сформировать точные

правила из человеческого семантического описания того, что они испытывают. Например, люди могут описать свои ощущения «очень хорошие», «удовлетворительные» или «ужасные». Непосредственное сопоставление человеческих лингвистических описаний со значимыми характеристиками, которые хорошо отражают качество стимулов, является решающим для создания подобных систем.

Список используемых источников

1. El Saddik A., Orozco M., Eid M., and Cha J. Haptics: General principles // in Haptics Technologies. 2011. PP. 1–20

2. Möller S. and Raake A., Quality of Experience. New York, NY, USA: Springer, 2014.

3. Wu W., Arefi A., Rivas R., Nahrstedt K., Sheppard R., and Yang Z. Quality of experience in distributed interactive multimedia environments: Toward a theoretical framework // In Proc. 17th ACM Int. Conf. Multimedia, 2009. PP. 481–490.

4. Hamam A., El Saddik A., and Alja'am J. A quality of experience model for haptic virtual environments // ACM Trans. Multimedia Comput., Commun., Appl. 2014. Vol. 10, No. 3. P. 28.

5. Steinbach E. Haptic communications // Proc. IEEE. Apr. 2012. Vol. 100. No. 4. PP. 937–956.

6. Streijl R. C., Winkler S., and Hands D. Mean opinion score (MOS) revisited: Methods and applications, limitations and alternatives // Multimedia Syst. Mar. 2016. Vol. 22, No. 2, PP. 213–227,

7. Сапунова Е. С. Разработка программно-аппаратного комплекса для сбора и воспроизведения кинестетической информации при помощи акселерометра // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей; Сборник лучших докладов конф. СПб. : СПбГУТ, 2022. С. 274–277

8. Chaudhari R., Steinbach E., and Hirche S. Towards an objective quality evaluation framework for haptic data reduction // in Proc. IEEE World Haptics Conf. Jun. 2011. PP. 539–544.

9. Sakr N., Georganas N. D., and Zhao J. A perceptual quality metric for haptic signals // in Proc. IEEE Int. Workshop Audio Vis. Environ. Games. Oct. 2007. PP. 27–32.

10. Hassen R. and Steinbach E., HSSIM: An objective haptic quality assessment measure for force-feedback signals // in Proc. IEEE Int. Conf. Quality Multimedia Exper. 2018.

11. Hamam A. and El Saddik A., Toward a mathematical model for quality of experience evaluation of haptic applications // IEEE Trans. Instrum. Meas. Dec. 2013. Vol. 62, No. 12. PP. 3315–3322,

12. Saad M. A., Bovik A. C., and Charrier C. Blind image quality assessment: A natural scene statistics approach in the DCT domain // IEEE Trans. Image Process. Aug. 2012. Vol. 21, No. 8. PP. 3339–3352.

13. Moorthy A. K. and Bovik A. C. Blind image quality assessment: From natural scene statistics to perceptual quality // IEEE Trans. Image Process. Dec. 2011. Vol. 20, No. 12. PP. 3350–3364,

Статья представлена научным руководителем, доцентом кафедры ССиПД СПбГУТ, кандидатом технических наук А. И. Выборновой.

УДК 004.056
ГРНРТИ 28.23

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ СИСТЕМ ОБЪЕКТОВ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ В КОНТЕКСТЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

В. О. Попова[1], А. А. Чечулин [1,2]

[1]Национальный исследовательский университет ИТМО
[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Сектор ядерных объектов критически важной инфраструктуры обладает уникальными характеристиками и требует особого подхода к обеспечению кибербезопасности объектов. Потенциальная реализуемость киберугрозы для систем управления промышленных объектов критически важной инфраструктуры, подтверждена как в ходе экспериментов, проводимых различными структурами, ответственными за безопасность данных систем, так и уже случившимися инцидентами по кибербезопасности. В данном исследовании проанализированы и систематизированы отличительные особенности объектов критически важной инфраструктуры по предложенным критериям, что в итоге позволит определить типы возможных кибератак и эффективно им противодействовать.

объекты критически важной инфраструктуры; анализ уязвимостей; открытые базы данных.

Потенциальная реализуемость киберугрозы для систем управления промышленных объектов, в частности для АЭС, подтверждена как в ходе экспериментов, проводимых различными структурами, ответственными за безопасность данных систем, так и уже случившимися инцидентами по кибербезопасности. Кибербезопасность АСУ ТП АЭС можно определить, как составную часть информационной безопасности АЭС, которая заключается в поддержании значений рисков для АЭС (экономических, экологических, социальных), связанных с возможным нарушением (умышленным и не умышленным) доступности, целостности или конфиденциальности информации (программ, данных и их потоков) в АСУ ТП АЭС, в заданных пределах.

Общая модель взаимодействия информационной и кибербезопасности для атомной промышленности разработана МАГАТЭ и показана на рис. 1 [1, 2].

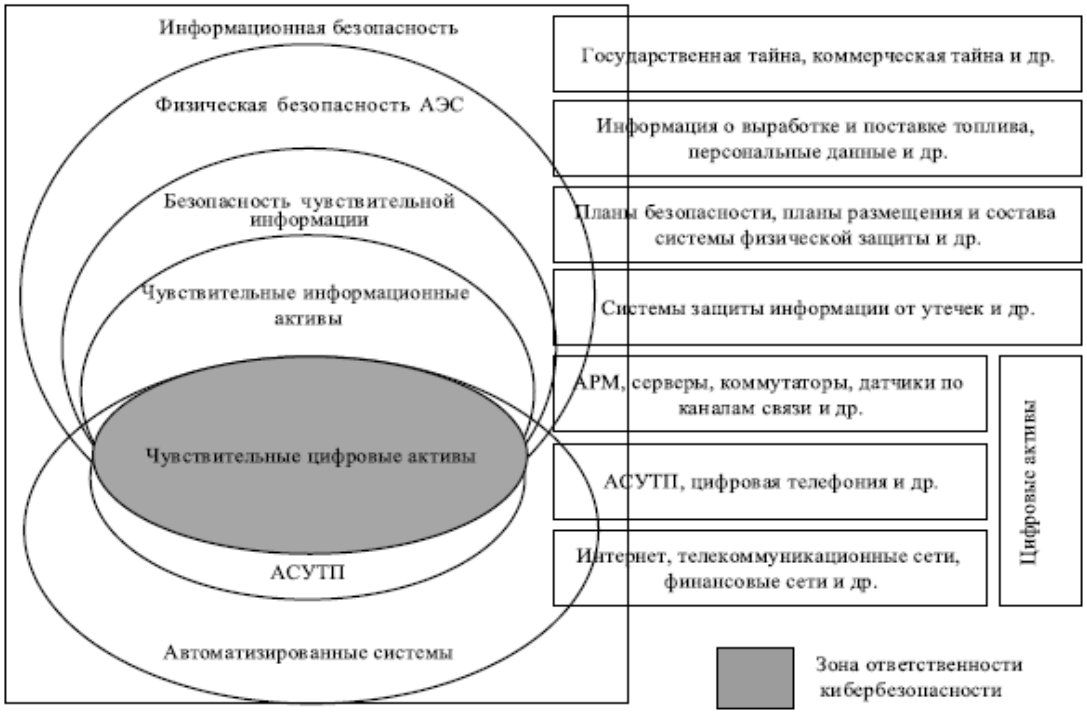


Рис. 1. Общая модель взаимодействия информационной и кибербезопасности для атомной промышленности

Сектор ядерных объектов критически важной инфраструктуры обладает уникальными характеристиками и требует особого подхода к обеспечению кибербезопасности объектов. С одной стороны, такие объекты, как например АЭС, практически повсюду защищаются глубоко проработанными и всеобъемлющими системами норм и правил физической ядерной безопасности (ФЯБ), которые позволяют принципиально устранить некоторые вопросы, связанные с кибербезопасностью. С другой стороны, уникальность сектора создает проблемные точки и барьеры для эффективного противодействия киберугрозам. К таким особенностям относятся, в частности, уникальная инфраструктурная сложность ядерных объектов критически важной инфраструктуры.

Объекты критически важной инфраструктуры разнообразны и включают, например, малые исследовательские реакторы на базе университетов. Но в большинстве случаев, в частности, когда в анализ включаются АЭС, речь идет об исключительно сложных, масштабных и опасных объектах. Соответственно, для поддержки функционирования АЭС требуется исключительно сложная ИТ-система [3, 4, 5]. Такая сложность порождает ряд последствий и проблем, которые требуют продуманного решения:

Во-первых, для ядерных объектов критически важной инфраструктуры не существует универсальных стандартных решений по интеграции ИТ-подсистем объекта. Так, каждая АЭС с точки зрения своей ИТ-инфраструктуры, ее архитектуры и топологии является уникальным объектом,

на котором реализованы оригинальные решения по ИТ-интеграции. Соответственно, в каждом случае сетям и ИТ-системам такого объекта присущ уникальный набор уязвимостей кибербезопасности и брешей в защите сетевого периметра. Это серьезно ограничивает возможности и практический смысл применения операторами гражданских ядерных объектов накопленного опыта и лучших практик.

Во-вторых, проблема доверия к ИТ-поставщикам и необходимость обеспечения целостности цепочек поставок ИТ-продукции, особенно для АСУ ТП. Операторы не располагают возможностями провести доскональную проверку тысяч контроллеров, дистанционных терминалов, маршрутизаторов, программных комплексов по управлению производственными процессами и т. д. на скрытый функционал, вредоносное ПО или ошибки. Это серьезная проблема, поскольку, как уже говорилось выше, каждый оператор АЭС вынужден зависеть от многих десятков и даже сотен поставщиков, а многие из них – транснациональные компании.

В-третьих, сложность внутренней ИТ-инфраструктуры гражданских ядерных объектов и интенсивность потоков данных в этой инфраструктуре требуют комплексного и всеобъемлющего подхода к кибербезопасности, который принципиально выходит за рамки только лишь реагирования на инциденты.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 19-29-06099 мк).

Список используемых источников

1. Международное агентство по атомной энергии, Безопасность атомных электростанций: проектирование. Серия норм МАГАТЭ по безопасности № NS-R-1, МАГАТЭ, Вена (2003).

2. Международное агентство по атомной энергии, Компьютерная безопасность на ядерных установках. Серия изданий МАГАТЭ по физической ядерной безопасности, № 17, МАГАТЭ, Вена (2012).

3. Ганчев Б. Г., Калишевский Л. Л., Демешев Р. С. Ядерные энергетические установки. М. : Энергоатомиздат, 1990. 629 с.

4. Иванов В. А. Эксплуатация АЭС: Учебник для вузов. СПб. : Энергоатомиздат. Санкт-Петербургское отделение. 1994. 384 с.

5. Острейковский В. А. Эксплуатация атомных станций : учебник для вузов. М. : Энергоатомиздат, 1999. 928 с.

УДК 004.715
ГРНТИ 81.93.29

РЕАЛИЗАЦИЯ ФУНКЦИЙ БЕЗОПАСНОСТИ НА МАРШРУТЗАТОРАХ ESR Eltex

В. Д. Проничев, И. А. Ушаков, В. С. Филёва

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Многоуровневый подход к безопасности маршрутизации позволяет создать надежную защиту от основных сетевых угроз. Особое внимание уделяется многофункциональности маршрутизаторов серии ESR, позволяющей соединить в себе различные средства для обеспечения защищенности сети по всему контуру. В рамках статьи рассматриваются функции маршрутизаторов ESR, обеспечивающие безопасность от потенциальных атак, а также обосновывается конкурентоспособность отечественных маршрутизаторов на рынке в условиях импортозамещения.

маршрутизаторы, функции безопасности, импортозамещение, сравнительный анализ.

Введение

В современном мире информационная безопасность – это жизненно необходимое условие обеспечение интересов человека, общества и государства [1]. В условиях постоянно развивающихся технологий обеспечение безопасности сетей должно совершенствоваться для реализации полной и надежной защиты от сетевых угроз. В связи с этим возникает вопрос о необходимости использования современного и многофункционального оборудования, которое сможет обеспечить требуемый уровень безопасности сети.

Импортозамещение

В условиях текущей геополитической ситуации импортозамещение является основным вектором развития информационных технологий в стране.

Такое направление было определено еще в 2014 году. Так, в Постановлении Правительства Российской Федерации от 15 апреля 2014 года № 313 [2] говорится о создании государственной программы «Информационное общество», основными направлениями реализации которой является: внедрение в промышленную эксплуатацию отечественных технологий защиты информации; создание российской среды разработки программного обеспечения; создание отечественных инновационных технических изделий в сфере информационных технологий и т. д.

А уже в Постановлении Правительства Совета Федерации РФ от 20 апреля 2016 года № 154 [3] говорится о том, что необходимо разработать комплекс мер, направленных на повышение информационной безопасности в связи с изменившейся геополитической ситуацией и введением санкций, направленных на ослабление российской экономики; принять меры, направленные на стимулирование использование хозяйствующими субъектами российского программного обеспечения и оборудование и т. д.

И наконец, в Указе Президента РФ от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [4] говорится о том, что с 1 января 2025 года органам (организациям) запрещается использовать средства защиты информации, происходящие из недружественных государств, либо производителями которых являются организации, находящиеся под их юрисдикцией, прямо или косвенно подконтрольные им либо аффилированные с ними.

В связи с вышеизложенными тема импортозамещения является не только актуальной, но и критически важной для поддержания необходимого уровня безопасности сети.

Функции безопасности,
реализуемые на отечественных маршрутизаторах

Маршрутизаторы серии ESR имеют ряд функций безопасности, которые обеспечивают защиту сети от различных угроз, такие как вредоносные программы, атаки на сеть и т. д. Ниже приведены некоторые из этих функций [5]:

1. Система обнаружения/предотвращения вторжений (IDS/IPS).

Система обнаружения/предотвращения вторжений анализирует передаваемые внутренние потоки данных, находя в них те последовательности битов, которые могут представлять собой вредоносные действия и события [6].

В случае, если в сети используется система обнаружения вторжений, то при регистрации подозрительной активности система отправляет уведомление инженеру по информационной безопасности, если же используется система предотвращения вторжений, то в случае обнаружения подозрительных действий, она блокирует нежелательный трафик.

Из особенностей реализации системы обнаружения/предотвращения вторжений на отечественных маршрутизаторах можно выделить следующее:

а) возможна автоматизированная загрузка правил из открытых источников, таких как SSL Blacklist, базы данных сигнатур известных атак и т. п.;

б) существует сервис EDM (*Eltex Distribution Manager*), который реализует механизм передачи лицензируемого контента на устройства производства Eltex;

в) возможность создания пользовательских правил, в том числе, используя формат SNORT/SURICATA.

2. Межсетевой экран с поддержкой зон безопасности

Данный межсетевой экран защищает локальную сеть от неавторизованного доступа из внешних не доверенных сетей, он блокирует весь нежелательный трафик, как на вход, так и на выход на основе специальных правил, которые называются списками контроля доступа.

3. Поддержка протоколов NetFlow и SFlow

Данные протоколы предназначены для отправки статистики принятых и отправленных маршрутизатором данных. Данная статистика содержит в себе информацию об источнике и назначении данных (IP), URL-адреса (в случае http), объем переданной/принятой информации, использованные протоколы.

4. Зеркалирование (SPAN, RSPAN)

Это технологии, позволяющие настроить сетевое устройство так, чтобы все пакеты, приходящие на один порт или группу портов, дублировались на другом с целью их дальнейшего анализа и мониторинга.

5. Протоколы AAA (Authentication, Authorization, Accounting)

Данный класс протоколов отвечает за аутентификацию, авторизацию учет, на маршрутизаторах серии ESR поддерживается реализация данного класса протоколов с помощью локальной базы данных, протоколов RADIUS, TACACS+ или LDAP.

6. Виртуальные частные сети (VPN)

Также маршрутизаторы поддерживают технологии построения частной сети поверх другой, зачастую общедоступной, то есть Интернет.

Маршрутизаторы поддерживают L3-туннели (IP4IP4, IP over GRE и IPsec), L2-туннели (L2TPv3, Ethernet over GRE), а также есть возможность строить динамические туннели типа “точка-многоточие” (DMVPN), которые используются в топологиях hub and spoke.

Сравнительная характеристика двух маршрутизаторов

Рассмотрев основные функции безопасности, реализуемые на отечественных маршрутизаторах серии ESR, проведем сравнительный анализ характеристик двух маршрутизаторов (Eltex ESR 1500 FSTEC [7] и CISCO ASR1002-X [8]). Оба маршрутизатора используются в средних и крупных предприятиях и имеют примерно одну и ту же стоимость. В таблице 1 (см. ниже) указаны некоторые характеристики обоих устройств.

Как видно из таблицы, отечественный маршрутизатор не уступает по характеристикам своему зарубежному аналогу, что позволяет сделать вывод о том, что подобные маршрутизаторы можно интегрировать в российских компаниях в рамках импортозамещения, не беспокоясь об ухудшении производительности существующей сети. Также стоит отметить, что отечественный маршрутизатор сертифицирован Федеральной Службой

по Техническому и Экспортному Контролю (ФСТЭК), что позволяет использовать данные маршрутизаторы в государственных организациях, ведомственных структурах и др.

ТАБЛИЦА 1. Сравнительная характеристика маршрутизатора ESR 1500 FSTEC и Cisco ASR-1002-x

Характеристика	ESR-1500 FSTEC	Cisco ASR1002-X
Firewall/NAT/маршрутизация (кадры 1518 байт)	12,83 Гбит/с	10 Гбит/с
Firewall/NAT/маршрутизация (кадры 70 байт)	606 Мбит/с	–
Firewall/NAT/маршрутизация (IMIX)	5,93 Гбит/с	–
IPsec VPN (кадры 1456 байт)	5,12 Гбит/с	4 Гбит/с
IPsec VPN (IMIX)	2,38 Гбит/с	–
Оперативная память	4 Гб	4 Гб
Постоянная память	1 Гб	8 Гб
Количество одновременно поддерживаемых VLAN	4 тыс.	4 тыс.

Заключение

Рассмотренная линейка отечественных маршрутизаторов предоставляют обширный набор функций безопасности, которые помогут защитить инфраструктуру сети предприятия от различных угроз.

Дальнейшее развитие отечественной отрасли телекоммуникационного оборудования позволит осуществить полный переход на отечественные программно-аппаратные комплексы, что снизит зависимость от зарубежных технологий, а также повысит надежность и безопасность используемого оборудования. Кроме того, развитие отечественной отрасли может привести к улучшению качества конечного продукта и снизить его стоимость, что делает отечественное телекоммуникационное оборудование более конкурентоспособным на рынке. Поэтому, развитие отечественной отрасли телекоммуникационного оборудования является важным этапом в жизни страны, но требует комплексного подхода и грамотной стратегии.

Список используемых источников

1. Титова Е. Р., Егшатян М. И. Информационная безопасность в современном мире [Электронный ресурс] // Евразийский Научный Журнал: электрон. научн. журн. 2020. N 12. URL: https://journalpro.ru/articles/informatsionnaya-bezopasnost-v-sovremennom-mire/ (дата обращения 15.03.2023).

2. Постановление Правительства РФ от 15 апреля 2014 г. N 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”».

3. Постановление Совета Федерации Федерального Собрания РФ от 20 апреля 2016 года N 154 «О развитии информационных технологий в Российской Федерации и мерах поддержки отечественной ИТ-отрасли».

4. Указ Президента РФ от 1 мая 2022 года N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

5. Управление безопасностью. URL: https://docs.eltex-co.ru/pages/viewpage.action?pageId=219939065 (дата обращения 15.03.2023).

6. Общие понятия о системах обнаружения и предотвращения вторжений. URL: https://habr.com/ru/company/otus/blog/479584/ (дата обращения 15.03.2023).

7. Сервисный маршрутизатор ESR-1500. URL: https://eltex-co.ru/catalog/service_gateways/esr-1500/ (дата обращения 16.03.2023).

8. Сравнение сервисных маршрутизаторов Eltex ESR-1700 и Cisco ASR1002-X. URL: https://www.newnets.ru/knowledge/26012/ (дата обращения 16.03.2023).

УДК 519.2
ГРНТИ 49.03.05

ПОВЫШЕНИЕ СКОРОСТИ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ КОДОВ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Н. С. Пщелко, Ю. В. Санин

АО НИИ «Рубин»

В настоящее время при решении задач цифровой обработки сигналов, связанных с их обработкой и сжатием сигналов, находят применение дискретные вейвлет-преобразования и, в частности, способ обработки сигналов с применением дискретного вейвлет-преобразования в конечных полях Галуа. Показано, что данные преобразования проводятся на основе вейвлетов и обеспечивают более высокую точность преобразований по сравнению с традиционными подходами, однако требуют подбора значений используемых оснований системы остаточных классов. Разработка алгоритма нахождения оснований системы остаточных классов позволяет оперативно проводить вычисления заданного количества оснований для различных видов вейвлетов в целях вычисления дискретного вейвлет-преобразования.

цифровая обработки сигналов, дискретное вейвлет-преобразование, система остаточных классов.

Анализ подходов, приведенных в [1], позволил выявить проблему цифровой обработки сигналов (ЦОС), заключающуюся в том, что особенность вейвлетов и обрабатываемых сигналов требует подбора значений используемых оснований системы остаточных классов (СОК). Данная процедура требует значительных временных затрат.

Кроме того, в ряде источников [2, 3], говорится, что модулярные структуры обработки изображений обеспечивают высокую степень отказоустойчивости за счет перераспределения вычислительных ресурсов при изменении структуры набора оснований. Таким образом, изменение типа обрабатываемых сигналов потребует оперативного измения состава набора оснований СОК, а, следовательно, возникает задача разработки алгоритма определения набора оснований СОК с заданными диапазоном и временем определения.

При преобразованиях изображений с помощью вейвлетов коэффициенты передаточной функции цифрового фильтра выражаются в виде дробей, содержащих иррациональные числа, что затрудняет их представление в виде целочисленных значений.

В [3] рассмотрены вейвлеты Добеши, койфлеты, биортогональные вейвлеты и мультивейвлеты, которые могут быть применены при выполнении операций ЦОС и сжатия изображений.

Для интерпретации коэффициентов передаточной функции вейвлетов, представленных в виде дробных чисел в модулярном базисе, и проведения вычислений ДВП в конечных полях Галуа, был реализован алгоритм.

Предложенный алгоритм реализован программно и позволяет проводить вычисление оснований для выбранного типа вейвлета.

В таблице 1 приведены сравнительные вычисличельные затраты (количество итераций), необходимые для определения оснований СОК.

ТАБЛИЦА 1. Вычислительные затраты для определения оснований СОК

Тип вейвлета	Количество искомых модулей						
	3	5	10	15	20	30	50
	Макс. итер. = 200			Макс. итер. = 500			Макс. итер. = 1000
Haar, TS, CDF22, CDF24, MIT97, BCW3	1995	3791	8405	32063	41678	69381	230358
Db4	6769	11581	29394	108214	154027	221456	807103
Coif6	6766	15737	34600	100715	141158	201010	672066
Multi-wavelet CL3	35384	45084	82496	289113	396150	645605	2068224

Как следует из таблицы 1, увеличение количества определяемых оснований СОК требует увеличения количества итераций, затрачиваемых на обработку каждого числа.

Очевидно, что сложность вычисления оснований СОК зависит от количества иррациональных чисел, в которых представлен исследуемый тип вейвлета. Так, при определении 50 возможных оснований для вейвлета Хаара требуется примерно в 8,97 раза меньше вычислений, чем для мультивейвлета CL3.

Следует отметить, что не все найденные основания по предложенному алгоритму являются взаимнопростыми числами. Следовательно, алгоритм требует внесения модуля проверки чисел на их взаимную простоту.

Результаты анализа вычислительных затрат показали, что менее сложный вейвлет Хаара для реализации вычислений в МК может быть задан меньшим диапазоном оснований, по сравнению с более сложным мультивейвлетом CL3, который может быть представлен диапазоном с бóльшими значениями разрядности.

Исходя, из полученных результатов можно сделать следующие выводы:

– разработанный алгоритм определения оснований СОК, для выполнения вычислений ДВП в конечных полях Галуа позволяет определять заданное количество модулей для различных видов вейвлетов, которые представлены в виде дробей с иррациональными числами;

– вычислительные затраты, требующиеся на определение оснований, зависят от сложности представления коэффициентов передаточных функций вейвлетов в иррациональных числах;

– разрядность вычислений для реализации ДВП в конечных полях Галуа зависит от сложности вейвлетов и представления их коэффициентов передаточных функций.

Таким образом, рассмотренная реализация алгоритма нахождения оснований СОК, в целях выполнения ДВП в конечных полях Галуа, позволяет оперативно проводить вычисления заданного количества оснований СОК для различных видов вейвлетов.

Данная реализация может быть использована для повышения отказоустойчивости вычислительных средств, работа которых основана на выполнении операций в СОК.

В дальнейших иследованиях возможна модификация алгоритма для исключения из вычислений оснований СОК, которые не являются взаимнопростыми к ранее определенным.

В статье модификация алгоритма не проводилась с целью показать весь набор применимых оснований СОК для интерпретации коэффициентов вейвлетов различной сложности в целых числах.

Список используемых источников

1. Гиш Т. А., Калмыков И. А. и др. Выполнение дискретного вейвлет-преобразования Добеши в модулярном коде // Современные наукоемкие технологии. 2018. N 2. С. 27–31.

2. Воробьев В. И., Грибунин В. Г. Теория и практика вейвлет-преобразования // ВУС. 1999. С. 181–182.

3. Keinert F. Wavelets and multiwavelets. Boca Raton, to CRC Press LLC, 2004. PP. 240–243.

УДК 004.056(075.8)
ГРНТИ 81.96

ОЦЕНКА СЛОЖНОСТИ МЕТОДА ПРОВЕРКИ КОРРЕКТНОСТИ ЗАПОЛНЕНИЯ ИЗБИРАТЕЛЕМ БЮЛЛЕТЕНЯ В СИСТЕМЕ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

В. Д. Салман

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Исследуется способ, позволяющий контролирующему органу убедиться, что избиратель проголосовал правильно за каждого кандидата. Особенность решения этой задачи заключается в том, что проверка выполняется по зашифрованному бюллетеню и контролирующий орган не знает, как проголосовал избиратель. Для решения задачи используется методы доказательства с нулевым разглашением секрета и свойства гомоморфного шифрования. Проведена оценка сложности реализации данного способа.

система дистанционного электронного голосования, проверка доказательства корректности заполнения бюллетеня, доказательство с нулевым разглашением секрета.

Электронная система голосования – это удаленная система, использующая интернет, мобильные компьютеры, смартфоны для того, чтобы дать возможность избирателям голосовать на выборах.

Известны следующие системы ДЭГ: на основе микс-сетей, на основе слепой подписи и на основе гомоморфного шифрования [1]. В этих системах решаются две главные задачи: обеспечение тайны голосования и обеспечение анонимности голосования, в том числе и для избирательной комиссии.

Для всех систем голосования существует достаточно много угроз, связанных с действиями нарушителя и неправомерными действиями участни-

ков протокола голосования. В последнее время большое внимание при построении систем электронного голосования уделяется защите от угрозы преднамеренного ли непреднамеренного неправильного заполнения бюллетеня голосования избирателем. Эта задача не является тривиальной, так как контроль правильности заполнения бюллетеня должен осуществляться в зашифрованном виде, без раскрытия того, как проголосовал избиратель.

В [2] рассматривается протокол электронного голосования с проверкой корректности заполнения бюллетеней. Протокол работает следующим образом: сначала, избиратель шифрует свой бюллетень и получает криптограмму B_i. Далее, он должен доказать, что в криптограмме зашифрованы значения $\{0,1\}$. Для этого формируется доказательство корректности заполнения своего бюллетеня. Криптограмма и доказательство отправляется в избирательную комиссию. ИК проверяет доказательства для (B_i), если проверка прошла успешно, то голос избирателя принимается. Далее ИК расшифровывает и подсчитывает голоса.

В [3] доказательство и проверка доказательства корректности заполнения бюллетеня избирательной комиссией разработаны для более общего случая, когда вариант выбора избирателя принадлежит заданному диапазону возможных значений. Сложность такого доказательства сильно зависит от количества возможных вариантов голосования на выборах.

Целью работы является оценка сложности метода проверки доказательство корректности заполнения бюллетеня в системе ДЭГ, основанный на сравнении дискретных логарифмов.

Модель системы ДЭГ на основе гомоморфного шифрования

Рассматриваемая в работе система ДЭГ, включает в себя: избирателей, сервер, блокчейн (БЧ) и избирательную комиссию (ИК) (рис. 1, см. ниже).

Будем далее рассматривать систему ДЭГ, построенную на основе гомоморфной системы шифрования Эль-Гамаля. Под гомоморфным шифрованием понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких – либо алгебраических операций над открытыми сообщениями. Свойство гомоморфного шифрования позволяет агрегировать голоса в зашифрованном виде и после расшифровать одну криптограмм, получив сразу результат голосования.

Основными этапами функционирования системы являются: инициализация системы; аутентификация избирателей; голосование; подсчет голосов и объявление результатов голосования.

Каждый избиратель выбирает кандидата (кандидатов) из списка кандидатов, шифрует свой голос с помощью открытого ключа и отправляет его в БЧ. После завершения голосования в БЧ осуществляется агрегирование голосов, результаты отправляются в избирательную комиссию. Сервер,

на котором генерировались открытый и закрытый ключи передает закрытый ключ избирательной комиссии, а если было разделение ключа, доверенные лица передают свои доли ключа избирательной комиссии, ИК восстанавливает закрытый ключ. Далее избирательная комиссия расшифровывает результаты голосования с помощью закрытого ключа и объявляет итог голосования.

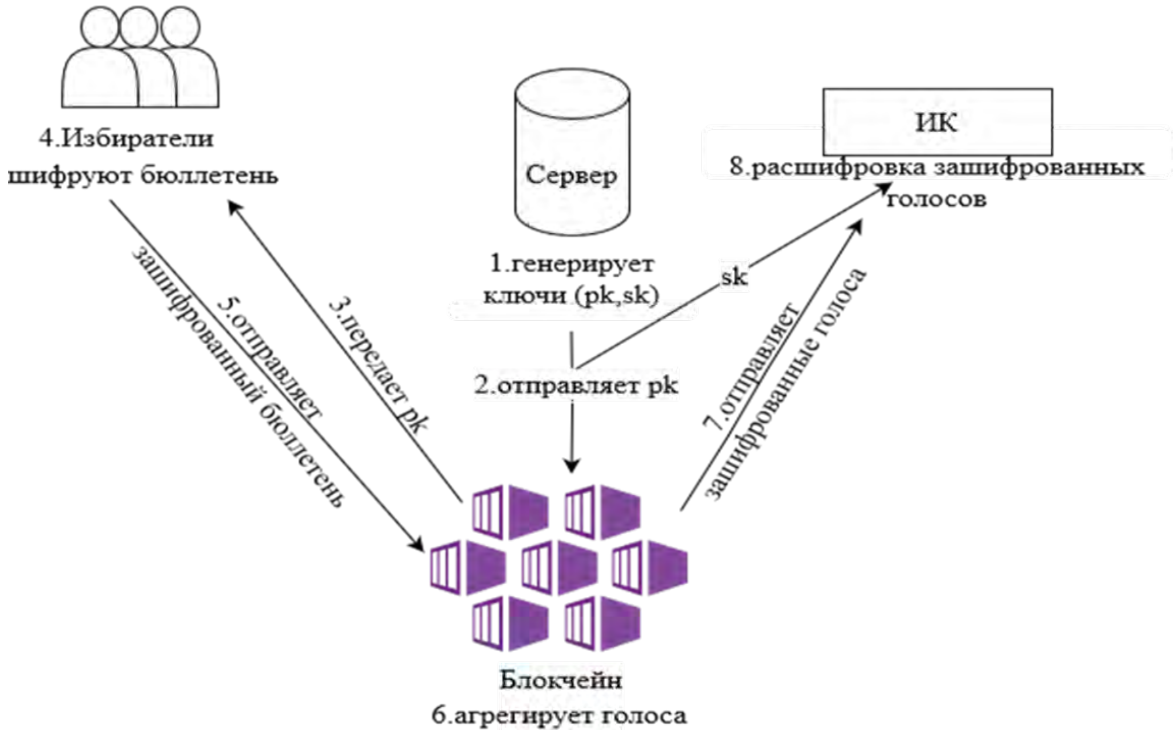


Рис. 1. Модель системы ДЭГ

Одна из угроз в данной системе ДЭГ заключается в том, что избиратель может неправильно (умышленно или случайно) заполнить свой бюллетень и это повлияет на результаты голосования. Чтобы предотвратить эту угрозу, применяются различные методы проверки корректности заполнения бюллетеня, основанные на методах доказательство с нулевым разглашением секрета. Одним из таких методов является метод, основанный на сравнении дискретных логарифмов.

Рассмотрим далее модель системы ДЭГ на основе схемы гомоморфного шифрования Эль-Гамаля [4].

Генерация ключей

– Выбираем закрытый ключ случайным образом:

$$1 \leq s \leq p - 1.$$

– Генерируем открытый ключ

$$h = g^s \, mod \, \text{p} \tag{1}$$

Шифрования бюллетеня

$$C_i = (x_i, y_i) = (g^r, h^r \cdot G^{v_i}) \, mod \, p, \tag{2}$$

где (x_i, y_i) – две части криптограммы C_i, $v_i \in \{0,1\}$ – выбор избирателя, r – случайное число, $1 \leq r \leq p-1$.

Дешифрования бюллетеня

$$Dec(C_i) = \frac{y_i}{x_i^s} \, mod \, p, \tag{3}$$

где *Dec()* – функция дешифрования.

Заполнение бюллетеня

Бюллетень в электронном виде представляет собой строку символов (1,0), где 1 – голос «за» и (0) – голос «против», поданные за каждого кандидата. Пример правильного заполнения бюллетеня показан в таблице 1.

ТАБЛИЦА 1. Формирование правильного заполнения бюллетеня

Кандидаты	D1	D2	D3	D4	……..	Dk
Выбор избирателя	1	0	0	1	……..	0

Как видно из таблицы 1, избиратель подал голос «ЗА» за первого и четвертого кандидатов, и голос «ПРОТИВ» за остальных кандидатов. Таким образом, бюллетень должен содержать только значения $\{0,1\}$. Для того, чтобы подтвердить, что он действительно заполнил свой бюллетень корректно, необходимо использовать схему доказательства корректности заполнения бюллетеня.

Метод проверки корректности заполнения бюллетеня для каждого шифртекста

В целом алгоритм голосования и формирования доказательства корректности голосования включает следующие шаги: избиратель загружает открытый ключ из БЧ; выбирает своего кандидата; шифрует бюллетень по схеме Эль-Гамаля и формирует доказательство того, что он зашифровал свой бюллетень из значений $\{0,1\}$. Алгоритм шифрования и формирования доказательства для двух вариантов правильного голосования приведен в таблице 2.

ТАБЛИЦА 2. Формирование доказательства корректности заполнения бюллетеня

Избиратель: голосование и формирование доказательства		Оценки сложности (при выборе v_i = 1)
проголосовал «за» кандидата: $v_i = 1.$	«против» кандидата: $v_i = -1.$	
избиратель случайным образом выбирает числа:		
$\alpha, w, r_1, d_1 \in \mathbb{Z}_q$	$\alpha, w, r_2, d_2 \in \mathbb{Z}_q$	$O(l)$
Осуществляет шифрование бюллетеня по каждому кандидату		
вычисляет: $x = (g^{\alpha}) \bmod p$ $y = h^{\alpha} G^{vi} \bmod p$	$x = (g^{\alpha}) \bmod p$ $y = h^{\alpha} / G^{vi} \bmod p$	1M 2M
Формирует доказательства корректности шифрования, вычисляя:		
вычисляет: $a_1 = g^{r_1} x^{d_1} \bmod p$ $b_1 = h^{r_1} \left(yG^{vi}\right)^{d_1} \bmod p$ $a_2 = g^{w} \bmod p$ $b_2 = h^{w} \bmod p$	$a_1 = g^{w} \bmod p$ $b_1 = h^{w} \bmod p$ $a_2 = g^{r_2} x^{d_2} \bmod p$ $b_2 = h^{r_2} (y/G^{vi})^{d_2} \bmod p$	2M 3M 1M 1M
хэш-функцию $c = H(x, y, a_1, b_1, a_2, b_2) \bmod q$		
вычисляет доказательство: $d_2 = c - d_1 \bmod q$ $r_2 = w - \alpha d_2 \bmod q$	$d_1 = c - d_2 \bmod q$ $r_1 = w - \alpha d_1 \bmod q$	*O(k)* *O(k)*
Всего		10M

Последняя колонка в этой и следующей таблицах содержит оценки сложности выполнения соответствующих операций. *M* обозначит операцию умножения. Далее избиратель отправляет значения $(A, B, a_1, b_1, a_2, b_2, u_1, u_2, t_1, t_2)$ проверяющему (в БЧ). БЧ проверяет, что избиратель правильно заполнил свой бюллетень согласно таблице 3.

ТАБЛИЦА 3. Алгоритм проверки корректности голосования за кандидата

Проверяющий (БЧ)	*Оценки сложности*
$c = d_1 + d_2 \bmod q$	*O(k)*
$a_1 = g^{r_1} x^{d_1} \bmod p$	2M
$b_1 = h^{r_1} (yG)^{d_1} \bmod p$	2M
$a_2 = g^{r_2} x^{d_2} \bmod p$	2M
$b_2 = h^{r_2} (y/G)^{d_2} \bmod p$	2M
Всего	8M

Можно сделать такие выводы. Сложность доказательства корректности заполнения бюллетеня требует во много раз большего количества операций по сравнению с операциями шифрования и расшифрования голоса избира-

теля, которые принципиально необходимы для обеспечения тайны голосования. Поэтому сложность всех операций по проверке корректности заполнения бюллетеня является определяющей в процедуре голосования. По сложности вычислений, которые выполняются избирателем и блокчейном они примерно одинаковые, однако при большом числе избирателей (сотни тысяч), нагрузка на блокчейн будет существенной. В этой связи актуальным является разработка алгоритмов проверки корректности заполнения бюллетеня, имеющих не высокую сложность именно на стороне блокчейна.

Список используемых источников

1. Okediran O. O., Omidiora E. O., Olabiyisi S. G. A Review of the Underlying Concepts of Electronic Voting // Inf. Knowl. Manag. 2012. Vol. 2, N 1. PP. 14.

2. Seol S., Kim H., Park J. H. An Efficient Open Vote Network for Multiple Candidates // IEEE Access. IEEE, 2022. Vol. 10. November. PP. 124291–124304.

3. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1997. Vol. 1233. PP. 103–118.

4. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // Springer- Verlag. 1998. PP. 10–18.

Статья представлена научным руководителем, профессором кафедры ЗСС СПбГУТ, доктором технических наук, профессором В. А. Яковлевым.

УДК 004.056(075.8)
ГРНТИ 81.96

МЕТОД ПРОВЕРКИ КОРРЕКТНОСТИ ЗАПОЛНЕНИЯ ИЗБИРАТЕЛЬНОГО БЮЛЛЕТЕНЯ В СИСТЕМЕ ДИСТАНЦИОННОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

В. Д. Салман, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Разработан метод для проверки корректности заполнения бюллетеня в целом, который имеет низкую сложность на стороне блокчейна. Получены оценки сложности вычислений при формировании доказательства корректности заполнения бюллетеня избирателем и оценки сложности проверки доказательства контролирующей стороной. Описание метода сопровождается числовым примером правильного заполнения избирательного бюллетеня.

система дистанционного электронного голосования, проверка доказательства корректности заполнения бюллетеня, доказательство с нулевым разглашением секрета, КС Эль-Гамаля.

Системы дистанционного электронного голосования (ДЭГ) все шире входят в жизнь современного общества. Получили распространение системы электронного голосования на основе микс-сетей, на основе слепой подписи и на основе гомоморфного шифрования [1]. Одной из практических систем ДЭГ, основанных на гомоморфном шифровании является ДЭГ России [2]. В этой системе Организатор (Комиссия ДЭГ) и Учетчик (БЧ) генерируют ключевые пары (ключи шифрования и расшифрования бюллетеней). На блокчейне формируется итоговый открытый ключ шифрования, который передается Регистратору и избирателю. Избиратель генерирует ключевую пару (открытый и закрытый ключи) электронной подписи. Избиратель и Регистратор выполняют протокол формирования подписи вслепую для ключа проверки ЭП избирателя. Избиратель заполняет бюллетень из значений {1- «За», 0- «против» кандидата и шифрует их с помощью ключа шифрования бюллетеней, формирует доказательство корректности содержимого бюллетеня, состоящее в том, что его выбор соответствует либо 0, либо 1. Также формируется доказательство корректности заполнения бюллетеня в целом. Избирательная комиссия расшифровывает бюллетени и осуществляет подсчет голосов.

Для всех систем голосования существует достаточно много угроз, связанных с действиями нарушителя и неправомерными действиями участников протокола голосования [3]. В последнее время большое внимание при построении систем электронного голосования уделяется защите от угрозы преднамеренного ли непреднамеренного неправильного заполнения бюллетеня голосования избирателем. Эта задача не является тривиальной, так как контроль правильности заполнения бюллетеня должен осуществляться в зашифрованном виде, без раскрытия того, как проголосовал избиратель.

Целью работы является разработка метода проверки заполнения избирательного бюллетеня в целом для системы ДЭГ, построенной на основе криптосистемы Эль-Гамаля

Рассматриваемая система ДЭГ, включает в себя: избирателей, сервер, блокчейн (БЧ) и избирательную комиссию (ИК) (рис. 1).

Каждый избиратель выбирает кандидата (кандидатов) из списка кандидатов, шифрует свой голос с помощью открытого ключа и отправляет его в БЧ. После завершения голосования в БЧ осуществляется агрегирование голосов, результаты отправляются в избирательную комиссию. Сервер, на котором генерировались открытый и закрытый ключи передает закрытый ключ избирательной комиссии. Далее избирательная комиссия расшифровывает результаты голосования с помощью закрытого ключа и объявляет итог голосования.

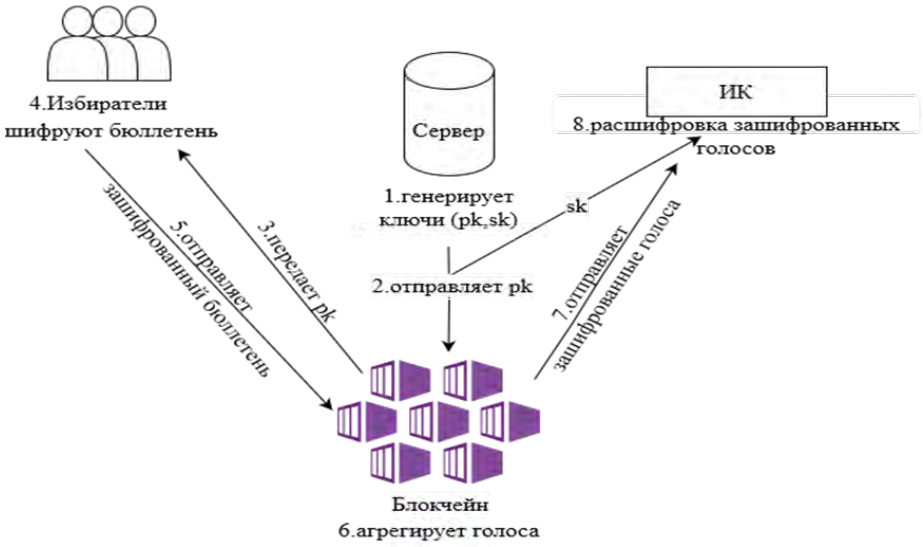


Рис. 1. Модель системы ДЭГ

Одна из угроз в данной системе ДЭГ заключается в том, что избиратель может нарушить правила голосования. То есть, например, избиратель может выбрать трех кандидатов, хотя разрешено выбрать только одного или двух.

Рассмотрим далее модель системы ДЭГ на основе схемы гомоморфного шифрования Эль-Гамаля [4].

Генерация ключей на сервере

– Выбирается закрытый ключ s случайным образом:

$$1 \leq s \leq p - 1,$$

где p – простое число. Закрытый ключ передается в избирательную комиссию.

– Генерируется открытый ключ, который доступен всем избирателям

$$h = g^s \ mod \ p, \tag{1}$$

Шифрования бюллетеня

Криптограмма $C_i = (A_i, B_i)$, состоит из двух частей

$$(A_i, B_i) = \left(g^{ri}, h^{ri} \cdot G^{v_{ij}}\right) mod \ p, \tag{2}$$

где $v_{ij} \in \{0,1\}$ – выбор избирателя, r_i – случайное число, $1 \leq r_i \leq p - 1$. $i = 1,2 \dots k$, k – число кандидатов.

Дешифрования бюллетеня

$$Dec(C_i) = \frac{B_i}{A_i^s} \ mod \ p = g^{vij}, \tag{3}$$

где *Dec()* – функция дешифрования.

Заполнение бюллетеня

Бюллетень в электронном виде представляет собой строку символов (1,0), где 1 – голос «за» и (0) – голос «против», поданные за каждого кандидата. Номер кандидата соответствует его позиции в строке – бюллетене. После голосования избиратель формирует доказательство корректности голосования за каждого кандидата proof Ci, например, используя схему CGS [5] и отправляет зашифрованный бюллетень и доказательство в блокчейн.

Подсчет голосов

Блокчейн проверяет корректность голосования, агрегирует голоса и отправляет результат в избирательную комиссию, которая с помощью секретного к и осуществляет подсчет голосов.

В рассмотренном выше случае, контролирующий орган может убедиться, что избиратель правильно проголосовал за каждого кандидата (ЗА или ПРОТИВ). Но он не может проверить, выполнены ли правила голосования по заданному варианту голосования. В данной работе предлагается метод проверки корректности заполнения бюллетеня в целом, имеющий меньшую сложность вычислений по сравнению с другими методами [2].

Будем считать, что ключи (открытый закрытый) сгенерированы. Избиратель V_j выполняет следующие действия:

– Голосует за каждого кандидата $v_{ij} \in \{0,1\}\ i = 1,2,..,k; j = 1,2 \dots, n$ – число избирателей.

– Выбирает случайным образом числа $r_i \in \{1, \dots, q-1\}$;

– Шифрует свой бюллетеня с помощью открытого ключа h

$$(A_i, B_i) = (g^{r_i}, h^{r_i} \cdot g^{v_{ij}})\ mod\ p, \quad (4)$$

где $v_{ij} = \{0,1\}$.

– Формирует доказательство корректности голосования для каждой криптограммы C_i- proof (C_i) и посылает C_i и proof (C_i) в БЧ. БЧ проверяет доказательство корректности каждой криптограммы. Для проверки правильности голосования в целом избиратель и блокчейн выполняют следующие протокол:

– БЧ генерирует величину $A_{k+1} = g^{r_{k+1}}$, $r_{k+1} \in Z_p$, генерирует число $c \in Z_p$ и посылает $(g^{r_{k+1}}, c)$ избирателю.

– Далее, избиратель и БЧ генерируют числа:

$$y_1 = \frac{1}{A_2 \cdot A_3 \dots A_{k+1}};\ y_2 = \frac{A_2}{A_3 \cdot A_4 \dots A_{k+1}};\ \dots\ y_i = \frac{\prod_{j<i} A_j}{\prod_{j>i} A_j};\ \dots\ y_{k+1} = A_1, A_2, .., A_k, \quad (5)$$

– Вычисляет для каждого кандидата D_i величины:

$$U_{D1} = y_1^{r_1} g^{v_{1j}},\ \ U_{D2} = y_2^{r_2} g^{v_{2j}},\ \dots, U_{Dk} = y_k^{r_k} g^{v_k}. \quad (6)$$

– Находит произведение:

$$\prod_{i=1}^{k} U_{Di} = \prod_{i=1}^{k} y_i^{r_i} g^{v_i j}, \quad (7)$$

и посылает его в БЧ.

– Далее, вычисляет:

$$T = h^t \text{ и } w = t + \sum_{i=1}^{k} r_i \cdot c, \quad (8)$$

где $t \in Z_p$ и тоже посылает их в БЧ.

– БЧ вычисляет:

$$U_{Dk+1} = y_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}}, \quad (9)$$

$U_\Sigma = \prod_{i=1}^{k} U_{Di} \cdot g_{k+1}^{r_{k+1}} \cdot g^{v_{k+1}} = \prod_{i=1}^{k+1} U_{Di} = \prod_{i=1}^{k+1} \frac{\prod_{j<i} g^{r_j \cdot g^{v_{ij}}}}{\prod_{j>i} g^{r_j}} = \prod_{i}^{k+1} g^{\sum_{j<i} r_j r_i - \sum_{i>j} r_j r_i} \cdot g^{v_{ij}},$

Можно показать, что

$$\sum_{i=1}^{k+1} (\sum_{j<i} r_j r_i - \sum_{i>j} r_j r_i) = 0, \quad (10)$$

тогда:

$$U_\Sigma = \prod g^{v_{ij}} = g^{\sum v_{ij}} = g^{\sum_{i=1}^{k} v_i j + v_{k+1}} \quad (11)$$

Пусть $v_{k+1} = -m$, где m-максимальное количество голосов для данного варианта голосования. Тогда $U_\Sigma = g^{\sum_{i=1}^{k} v_i - m}$. Если избиратель проголосовал правильно, то

$$\sum v_i = m, \text{ и } U_\Sigma = 1, \quad (12)$$

что свидетельствует о корректности заполнения бюллетеня при правильном голосовании избирателя.

Однако, избиратель при формировании U_{Di} может изменить значение g^{v_i}, так чтобы при неправильном голосования условие (12) выполнялось. Поэтому БЧ выполняет проверку сравнения:

$$h^w =^? T \cdot V, \quad (13)$$

$h^w = h^{t + \sum_{i=1}^{k} r_i \cdot c}$, где $V = (\prod_{i=1}^{k} B_i \Big/ U_\Sigma \cdot g^{-v_{k+1}})^c = (h^{\sum r_i} \cdot g^{\sum_{i=1}^{k} v_i} \cdot g^{-\sum_{i=1}^{k+1} v_i} \cdot g^{+v_{k+1}})^c.$

Если избиратель проголосовал правильно, то $\sum_{i=1}^{k} v_i - \left(\sum_{i=1}^{k+1} v_i\right) + v_{k+1} = 0$, тогда $V = h^{(\sum r_i)c}$ и $T \cdot V = h^t \cdot h^{(\sum r_i)c} = h^w$. Сравнения выполнено. Следовательно, избиратель проголосовал правильно.

Сложность данного алгоритма формирования и проверки доказательства корректности заполнения бюллетеня в целом может оценить на основе выше приведенных соотношений так:

- количество возведений в степень на стороне избирателя – 6M+k(3M);
- количество возведений в степень в БЧ – 7M + k(2M).

Рассмотрим пример проверки корректности заполнения бюллетеня в целом. Будем использовать схему Эль Гамаля с параметрами $p = 11,\ g =$

$6, s = 3, h = 7$, где *s* – закрытый ключ, *h* – открытый ключ. Пусть в голосовании участвуют четыре кандидата: D1, D2, D3, D4. Избиратель голосует ЗА за кандидата D1 и против остальных кандидатов, то $m = 1$.

Избиратель случайным образом выбирает числа r_i и вычисляет A_i соответствие (4): $r_1 = 10,\ A_1 = 1;\ r_2 = 9,\ A_2 = 2;\ r_3 = 8,\ A_3 = 4$ и $r_4 = 6,\ A_4 = 5$. Далее, вычисляет вторую части криптограммы B_i соответствие (4), то $B_1 = 6; B_2 = 8; B_3 = 9; B_4 = 4$.

Далее, БЧ случайным образом выбирает числа $r_5 = 7$ и $c = 2$, вычисляет $A_5 = g^{r_5}\ mod\ p = 8$ и посылает $(A_5 = 8, c = 2)$ избирателю.

Далее, избиратель и БЧ генерируют в соответствии с (5) числа: $y_1 = 6;\ y_2 = 9;\ y_3 = 1;\ y_4 = 2;\ y_5 = 3$. Избиратель вычисляет для каждой криптограммы величины: $U_{D1} = 3; U_{D2} = 4\ ; U_{D3} = 1;\ U_{D4} = 10$ и также БЧ вычисляет $U_{D5} = 5$.

Далее, избиратель вычисляет произведение соответствие (7):

$\prod_{i=1}^{k} U_{Di} = 10$, выбирает случайном образом число *t* = 2, вычисляет: $T = 5$ и $w = 2$ в соответствии с (8) и посылает их в БЧ.

БЧ вычисляет: $U_{D5} = 5$ в соответствии с (9): $v_{k+1} = -m$, то $v_5 = -1$. Далее БЧ вычисляет: $U_{\sum} = g^{\sum_{i=1}^{k} v_i - m} = 6^{1-1}\ mod\ 11 = 6^0\ mod\ 11 = 1$,

БЧ выполняет проверку сравнения (13): $h^w mod\ p = 5; T \cdot V\ mod\ p = 5$, то $h^w = T \cdot V$. Сравнения выполнены.

В результате исследования разработан алгоритм для проверки правильности заполнения бюллетеня в целом, который имеет низкую сложность на стороне блокчейна. Данной алгоритм проверки позволяет убедиться в том, что избиратель правильно выбрал количество кандидатов из диапазона возможных значений.

Список используемых источников

1. Del Blanco D. Y. M., Alonso L. P., Alonso J. A. H. Review of Cryptographic Schemes applied to Remote Electronic Voting systems: Remaining challenges and the upcoming post-quantum paradigm // Open Mathematics. 2018. Vol. 16, N 1. PP. 95–112.

2. Russia C.E.C. Описание протокола ДЭГ к выборам, голосование на которых состоится 17, 18 и 19 сентября 2021 г. С. 13.

3. Jefferson B. D. et al. Analyzing internet voting security // Commun. ACM. 2004. Vol. 47, № 10. PP. 59–64.

4. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms // Springer- Verlag. 1998. PP. 10–18.

5. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 1997. Vol. 1233. PP. 103–118.

УДК 004.7
ГРНТИ 49.33.29

ОБЗОР ВЫСОКОСКОРОСТНЫХ СИСТЕМ 50G-PON

А. Р. Салтыков, А. Ю. Слепогин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Системы 50G-PON являют собой новый набор стандартов ITU-T и значительно превосходят в скорости сети G-PON и XG-PON. Достижение такого скачка в производительности требует эволюции в основе самой технологии доступа. 50G-PON использует фундаментальные достижения в области оптических приемопередатчиков, работающих в сочетании с улучшенной процедурой коррекцией ошибок и кодированием. Это также вводит ключевые нововведения в процедуры активации, работу на основе конкуренции и расширенные криптографические особенности. Благодаря этим улучшенным возможностям системы 50G-PON готовы к повышенным требованиям для предоставления новых высококачественных услуг.

50-GPON, contention-based operation, приемопередатчик, кодирование.

Введение

В апреле 2021 года МСЭ-Т достиг важной вехи, согласившись на первый три рекомендации, определяющие систему 50G-PON [1]:

1. Общие требования (G.9804.1): Унаследованные функции, связанные с развернутой инфраструктурой оптоволокна, дополняются поддержкой новых сервисов, требующих высокой пропускной способности, эффективности, низкой задержки и безопасности. Сосуществование с установленными PON-системами и миграция с них имеют важное значение.

2. Общий уровень конвергенции передачи (ComTC) спецификация (G.9804.2): Определена независимо от скорости передачи данных и, таким образом, применима к будущим одноволновым мультиплексирующим системам с временным разделением (TDM) и многоволновым мультиплексирующим системам с разделением по времени и длинам волн (WDM) PON.

3. PMD с одной длиной волны 50G-PON (G.9804.3) спецификация, являющаяся первой в семействе HS-PON PMD.

Обзор PON ITU-T

50G-PON продолжает использовать TDM/TDMA и в настоящее время поддерживает скорость передачи данных по нисходящей линии 50 Гбит/с и два варианта скорости передачи данных по восходящей линии (25 Гбит/с и 12,5 Гбит/с). Основные параметры приведены в таблице 1 [2].

ТАБЛИЦА 1. Основные параметры оптических интерфейсов

Параметры оптического интерфейса в нисходящем потоке 49,7664 Гбит/с.			
Название	Единица измерения	Значение	
OLT передатчик			
Номинальная линейная скорость	Гбит/с	49.7664	
Рабочая длина волны	nm	1340–1344	
Линейный код		NRZ	
Минимальные оптические возвратные потери	дБ	32	
Параметры оптического интерфейса в восходящем направлении 12,4416 Гбит/с			
ONU приемник			
Номинальная линейная скорость	Гбит/с	12.4416	
Рабочая длина волны	nm	1	2
		1260~1280	1290~1310
Линейный код		NRZ	
Минимальные оптические возвратные потери	дБ	32	
Параметры оптического интерфейса в восходящем направлении 24,8832 Гбит/с			
ONU приемник			
Номинальная линейная скорость	Гбит/с	12.4416	
Рабочая длина волны	nm	1	2
		1260~1280	1290~1310
Линейный код		NRZ	
Минимальные оптические возвратные потери	дБ	32	

Он может работать поверх развернутых ODNS, одновременно сосуществуя с системами PON, уже находящимися в эксплуатации. Это стало возможным благодаря плану длины волны, который облегчает мультиплексирование с разделением по длине волны различных поколений PON на одном и том же ODN, как показано в спектре расширение на рис. 1. Примечательно, что план длины волны 50G-PON допускает сосуществование с G-PON или XG(S)-PON для обеспечения плавного пути обновления системы за счет использования соответствующего параметра длины волны выше по потоку, то есть спектральных опций (1) или (2) [2].

На сетевом уровне спектральное сосуществование могло бы также позволить предоставлять новые услуги в качестве дополнения к устаревшим системам PON; например, устаревший FTTH, совмещенный с новым беспроводным транспортом. Пятикратное увеличение скорости нисходящей линии на длину волны по сравнению с предыдущими поколениями PON

в сочетании с новыми функциями ТС способствуют дальнейшему увеличению пропускной способности, низкой задержке, более высокую эффективность и улучшенную безопасность, требуемые на уровне услуг. Нисходящий канал передачи данных 50G-PON показан в функциональном расширении на рис. 1, где синие и розовые блоки представляют, соответственно, подуровень адаптации физического интерфейса (PHY) уровня ТС и сам PHY.

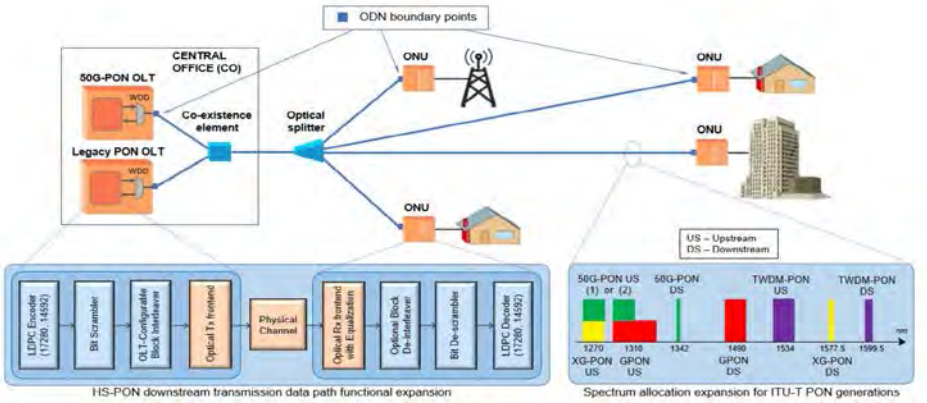


Рис. 1. Архитектура системы PON со сценариями развертывания, нижестоящим каналом передачи данных и распределением спектра PON

Для 50G-PON в OLT можно использовать компактный передатчик с оптическим усилением (Tx). Такой передатчик может быть реализован в виде монолитно интегрированного лазера с модуляцией электропоглощения (EML) и полупроводникового оптического усилителя (SOA). Такой EML + SOA Tx может передавать более 10 дБм в оптоволокно на OLT при модуляции со скоростью 50 Гбит/с [4]. Накопленная волоконная хроматическая дисперсия (CD) в нисходящем канале должно допускаться до 77,1 пс/нм (при 1342 ± 2 нм).

Для того, чтобы ограничить штраф, вызванный межсимвольной интерференцией (ISI), вызванной CD-индуцированием, необходимо минимизировать чирп длины волны EML+SOA Tx. В ONU предполагается, что номинальный класс 25 Гбит/с будет использоваться Rx. Это обусловлено наличием подходящих устройств на лавинных фотодиодах (APD) и целью сохранить низкую стоимость ONU. Ключевые элементы в полной нисходящей линии связи показаны на рис. 2 [3].

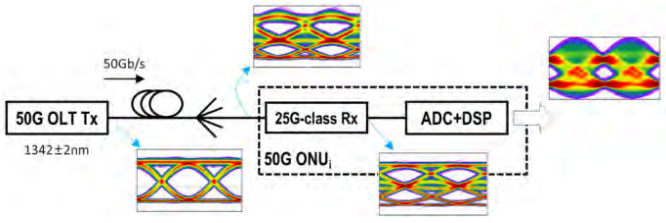


Рис. 2. Пример нисходящей линии передачи 50G-PON с экономичным эффективным приемником класса 25 Гбит/с. Вставки: Качественные глазковые диаграммы в ключевых точках

В настоящее время устройства APD класса 25 Гбит/с (25G-APD) являются зрелыми, коммерчески доступными компонентами, но устройства APD класса 50 Гбит / с все еще только появляются в исследовательских лабораториях. Кроме того, 25G-APDS, как правило, обеспечивают лучшую производительность в отношении ключевых параметров, таких как лавинообразный прирост и отзывчивость. В ходе исследования ITU-T было подтверждено, что экономичный 25G-APD Rx с последующим выравниванием может обеспечить высокую чувствительность на скорости 50 Гбит/с. Необходимое выравнивание может быть реализовано с использованием DSP в интегральных схемах, которые выигрывают от масштабирования затрат / размеров / скорости благодаря закону Мура.

The contention-based operation

В системах TDM/TDMA PON, как только ONU активированы, пакеты передачи от разных ONU следуют друг за другом с интервалом в защитное время. Обычно, в любой данный момент, только несколько ONU имеют данные для отправки; однако, чтобы идентифицировать активные ONU, OLT должен выделить пакет для каждого ONU. Предоставление такого направленного распределения для нагрузки без восходящего трафика в типичном случае может привести к потере от 15 до 25 процентов восходящей полосы пропускания. Чтобы улучшить использование полосы пропускания, спецификация ComTC вводит операцию, основанную на конкуренции [2]. Новый класс введены явно назначаемые широковещательные идентификаторы распределения. Вместо того, чтобы быть связанными с конкретным ONU, такие идентификаторы распределения связаны с конкретной функцией, основанной на конкуренции, такой как поддержка бездействия, защита длины волны в TWDM PON и режим бдительного сна. Как только OLT назначает широковещательный идентификатор распределения для функции, основанной на конкуренции, он может отозвать направленные распределения для ONUs. Если OLT обнаруживает коллизию в интервале времени, связанном с распределением широковещательной передачи, он временно восстанавливает направленные распределения, чтобы определить те, которые действительно требуют пропускную способность восходящей передачи для удовлетворения их потребностей. Как показано на рис. 3, операция, основанная

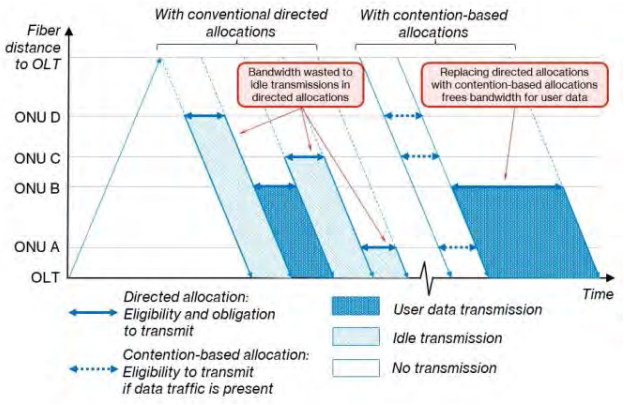


Рис. 3. Contention-based operation

на конкуренции, использует одно широковещательное распределение для замены нескольких направленных распределений.

Заключение

Проект HS-PON расширяет возможности ITU-T PON по сравнению с предыдущими поколениями за счет увеличения пропускной способности линии, а также повышения ее надежности и эффективности, при этом критически важно поддерживать сосуществование с установленными развертываниями. Являясь первым результатом проекта, 50G-PON знаменует собой начало нового поколения высокоскоростных PON-систем ITU-T.

Пандемия COVID-19 привела к усилению внимания к сетям доступа из-за значительного изменения приоритетных вариантов использования.

Например, видеоконференции, дистанционное здравоохранение и дистанционное образование стали насущной необходимостью в большинстве домашних хозяйств.

Так же в настоящее время, в определенных сферах деятельности требуется высокоскоростное взаимодействие между командными центрами управления.

Система 50G-PON, несомненно, станет ключом к удовлетворению этих будущих сетевых потребностей.

Список используемых источников

1. Higher speed passive optical networks. ITU-T G.9804 series of Recommendations. G.9804.1 (Requirements), approved in Nov. 2019. G.9804.2 (ComTC), consented in April 2021, G.9804.3 (50G-PON PMD), consented in Apr. 2021.

2. Geng D., Khotimsky D., Liu D., Liu X., Luo Y., Nesset D., Oksman V., Strobel R., Van Hoof W., Wey S. J. 50G-PON: The First ITU-T Higher Speed PON System René Bonk // IEEE communications magazine. 2022. Vol. 60. N 3. PP. 48–54.

3. Rosales R., Cano I., Nesset D., Zhicheng Y., Brenot R., Dubrovina N., Duran-Valdeiglesias E., Debregeas H., Carrara D., and Lelarge F. First Demonstration of an E2 Class Downstream Link for 50Gb/s PON at 1342nm // 2020 European Conference on Optical Communications (ECOC). IEEE, 2020. PP. 1–4.

4. Liu X., Shen A., Cheng N., Luo Y. and Effenberger F. Performance improvements in bandwidth-limited and digitally-equalized 50G-PON downstream transmission via block-interleaving over four LDPC codewords // Optical Fiber Communication Conference. Optica Publishing Group, 2021. P. M3G. 6.

5. Advanced encryption standard (AES) / NIST FIPS-197, Nov. 2001.

Статья представлена заведующей кафедрой ФиЛС СПбГУТ, кандидатом технических наук, доцентом М. С. Былиной.

УДК 654.739
ГРНТИ 45.47.35

МЕТОД ОЦЕНКИ ПРОПУСКНОЙ СПОСОБНОСТИ СИММЕТРИЧНОГО КАБЕЛЬНОГО ТРАКТА СТРУКТУРИРОВАННОЙ КАБЕЛЬНОЙ СИСТЕМЫ

А. Б. Семенов[1], Е. Г. Соколов[2]

[1]Национальный исследовательский Московский государственный строительный университет
[2]Московский технический университет связи и информатики

Рассмотрен метод оценки шенноновской пропускной способности симметричных кабельных трактов высокоскоростных информационных кабельных систем. Показана возможность определения этого параметра по характеристике PSNEXT линейного кабеля. Обосновано превалирующее влияние на пропускную способность кабельной системы перекрестных помех на ближнем конце. Установлен рост влияния разъемов на пропускную способность кабельного тракта по мере наращивания его класса, т. е. увеличения максимальных скоростей передачи информации, гарантированно поддерживаемых СКС.

симметричный кабельный тракт, переходная помеха, шенноновская пропускная способность, комбинирование классов, структурированные кабельные системы.

Физический уровень современной внутриобъектовой информационной системы в основной массе случаев реализуется на основе структурированной кабельной системы (СКС). Характеристики симметричных кабельных трактов СКС нормируются стандартами исходя из постулата применения для их построения элементной базы одинаковой категории, что далеко не всегда соблюдается на практике. Переход на «mix-and-match»-структуры неизбежно меняет пропускную способность тракта. В известных источниках степень такого влияние не рассматривается. Далее решается актуальная в этой связи задача быстрой оценки величины пропускной способности и влияния на нее параметров отдельных элементов, входящих в состав кабельного тракта.

Математическая модель

Одним из путей наращивания эффективности построения и эксплуатации симметричных кабельных трактов СКС является максимально полная утилизация их потенциальной пропускной способности, что достигается глубокой обработкой линейного сигнала на передающем и приемном концах [1]. Предельно достижимое значение этого параметра задается известной теоремой Шеннона.

С учетом превалирующего влияния переходных шумов различной природы, сильной частотной зависимости затухания и переходной помехи, а также 4-парной схемы организации связи, искомую пропускную способность можно определить в интегральной форме как:

$$W = 4 \cdot 0,6 \cdot \int_0^{\infty} log_2(1 + GPSACR(f))df ,$$

где – $GPSACR(f)$ – глобальная защищенность от суммарной переходной помехи. Коэффициент 0,6 учитывает рекомендованный IEEE эксплуатационный запас.

Величина $GPSACR(f)$ определяется $PSNEXT(f)$ – суммарным переходным затуханием на ближнем конце; $PSFEXT(f)$ – суммарным переходным затуханием на дальнем конце; и $IL(f)$ – затуханием кабельного тракта [2]. С учетом независимости источников, порождающих переходные помехи, далее считается, что переходная помеха ближнего и дальнего концов суммируются по мощности.

Частотная характеристика $PSNEXT(f)$ в пределах $f_0 < f < f_в$ описывается стандартами как:

$$PSNEXT(f) = -20lg\left(10^{\frac{PSNEXT_{кабеля} - k_{кабеля}lg(f)}{-20}} + 10^{\frac{PSNEXT_{разъема} - k_{разъема} \cdot lg(f)}{-20}}\right),$$

где f_0, $f_в$ – нижняя и верхняя граничная частоты, соответственно.

Ранее было установлено, что можно принять $f_0 = 0$ [3]. $f_в$ представляет собой решение уравнения $GPSACR(f) = 0$ [4].

Затухание кабельного тракта находится как:

$$IL = (L_э / 100) \cdot (a\sqrt{f} + b \cdot f + c / \sqrt{f}) + 4 \cdot e \cdot \sqrt{f} ,$$

где $L_э$ – электрическая длина тракта; a, b, c и e – постоянные коэффициенты, зависящие от категории элементной базы.

Защищенность от суммарной переходной помехи на дальнем конце, определяющая $PSFEXT(f)$, составляет

$$PSACRF(f) = -20lg\left(10^{\frac{PSACRF_{кабеля} - m_{кабеля}lg(f)}{-20}} + 4 \cdot 10^{\frac{PSACRF_{разъема} - m_{разъема}lg(f)}{-20}}\right).$$

Схема определения глобального переходного затухания

Непосредственное определение величины W – сложная процедура, которая мало пригодна для широкой инженерной практики. Для ее упрощения можно воспользоваться тем фактом, что физические основы формирования помехи ближнего и дальнего концов идентичны. Это позволяет выполнить вклад последней через корректирующую добавку к *NEXT*, т. е. принять

$$NEXT'_{кабеля} = NEXT_{кабеля} + \Delta FEXT_{\text{кабеля}},$$

$$NEXT'_{разъема} = NEXT_{разъема} + \Delta FEXT_{разъема}.$$

Параметр $GPSACR(f)$ зависит напрямую от $PSNEXT'_{\text{кабеля}}$ и $PSNEXT'_{\text{разъема}}$:

$$GPSACR(f) = \left(\begin{array}{l} 10^{\frac{PSNEXTкабеля(f)}{-20}} + 10^{\frac{PSNEXTразъема(f)}{-20}} + \\ +10^{\frac{PSFEXTкабеля(f)}{-20}} + 10^{\frac{PSNEXTразъема(f)}{-20}} \end{array} \right)^{-1}$$

В рабочем частотном диапазоне кабельных трактов СКС различных классов соотношения между $10^{\text{PSNEXTкабеля/-20}}$ и $10^{\text{PSFEXTкабеля/-20}}$ можно аппроксимировать линейной функцией. Аналогичное справедливо для слагаемых, описывающих влияние на W разъемных соединителей.

В верхней части рабочего частотного диапазона переходную помеху определяет преимущественно *PSNEXT*. Данную особенность, которая существенно упрощает расчет шумов, на примере техники класса *D* иллюстрирует рис. 1.

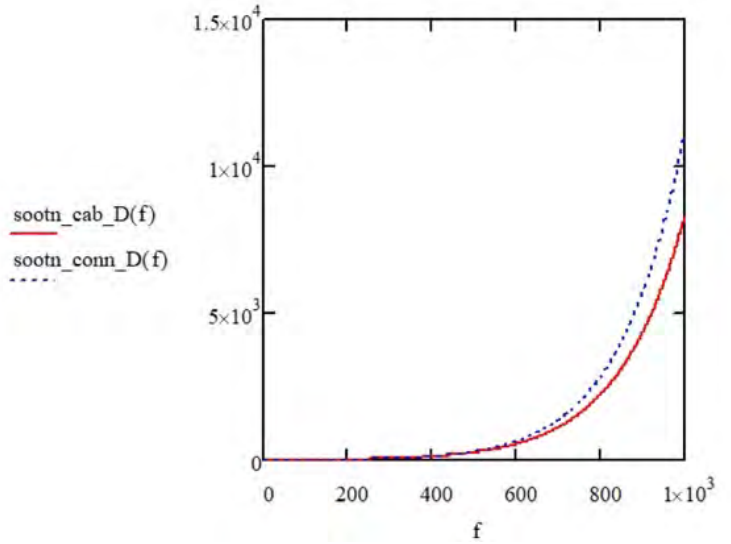


Рис. 1. Соотношения между влияющими слагаемыми, отвечающими за соотношения влияния *PSNEXT/PSFEXT* разъемов (пунктирная линия) и кабеля (сплошная линия) для техники класса D

Для задания поправочных коэффициентов обратимся к линейной аппроксимации, в результате чего приходим к выражениям вида:

$$10^{-PSNEXT_{кабеля}(f)/20} + 10^{-PSFEXT_{кабеля}(f)/20} = $$
$$= 10^{-PSNEXT_{кабеля}(f)/20} \cdot [1 + (p_{кабеля} + k_{кабеля} \cdot f)]$$
$$10^{-PSNEXT_{разъема}(f)/20} + 10^{-PSFEXT_{разъема}(f)/20} = $$
$$= 10^{-PSNEXT_{разъема}(f)/20} \cdot [1 + (p_{разъема} + k_{разъема} \cdot f)].$$

Конкретные значения коэффициентов p и k приведены в таблице 1.

ТАБЛИЦА 1. Поправочные коэффициенты для расчета W

Категория	$p_{\text{кабеля}}$	$k_{\text{кабеля}}$	$p_{\text{разъема}}$	$k_{\text{разъема}}$
D	0,64	$-5{,}2\times10^{-3}$	1,73	$-1{,}9\times10^{-2}$
E	-0,07	29×10^{-3}	1,90	$-1{,}1\times10^{-2}$
EA	-0,46	31×10^{-3}	1,93	$-1{,}1\times10^{-2}$
F	1,14	-4×10^{-3}	2,62	$-1{,}2\times10^{-2}$
FA	1,30	$-3{,}9\times10^{-3}$	2,24	-1×10^{-2}

В результате приходим к

$$\frac{P_{\text{сигнал}}(f)}{P_{\text{шум}}(f)} = \left(\begin{array}{l} 10^{\frac{PSNEXT_{кабеля}(f)}{-20}} \cdot \left(1 + p_{кабеля} + k_{кабеля} \cdot f\right) + \\ +10^{\frac{PSNEXT_{разъема}(f)}{-20}} \cdot \left(1 + p_{разъема} + k_{разъема} \cdot f\right) \end{array} \right)^{-1}$$

Далее находятся параметры глобальной переходной помехи и защищенности от нее:

$$GPSNEXT(f) = 20\lg\frac{P_{\text{сигнал}}(f)}{P_{\text{шум}}(f)},$$

$$GPSACR(f) = GPSNEXT(f) - IL(f).$$

Расчеты защищенности

Расчеты защищенности $GPSACR(f)$ выполнялись для наиболее неблагоприятного по стандартам случая 100-метровой физической протяженности кабельного тракта. Погрешность вычислений W не превышает 4 %.

ТАБЛИЦА 2. Теоретическая пропускная способность 4-коннекторного симметричного кабельного тракта 100-метровой физической длины

W, Мбит/с	Кабель				
Разъем	D	E	E_A	F	F_A
D	1324	1869	1647	2413	2502
E	1606	2560	2693	3975	4172
EA	1602	2547	2679	3940	4135
F	1813	3304	3496	8919	9866
FA	1831	3359	3552	9512	10520

Полученное соотношение с привлечением конкретных значений параметров затухания и влияния для кабеля и разъемов (указаны в стандарте или заимствуются из документации производящей компании) так же позволяет оценить пропускную способность симметричного кабельного тракта в случае комбинирования кабеля и разъемов различных категорий. Результаты соответствующих расчетов приведены в таблице 2.

Выводы

1. Превалирующее влияние на пропускную способность симметричного кабельного тракта оказывает переходная помеха ближнего конца.
2. Кабель по сравнению с разъемами оказывает заметно большее влияние на пропускную способность тракта.
3. По мере роста класса кабельного тракта вклад разъемов в общий объем шумов увеличивается.
4. При необходимости наращивания пропускной способности в процессе эксплуатации СКС следует реализовывать линейную часть на кабеле более высокой категории и выполнять замену разъема при модернизации.

Список используемых источников

1. Семёнов А. Б. 25G Ethernet и структурированная проводка // Журнал сетевых решений LAN. 2018. No 2. С. 44.

2. Гроднев И. И., Верник С. М. Линии связи. М. : Радио и связь. 1988. ISBN 5-256-00120-5.

3. Семенов А. Б., Кандзюба Е. В. Перспективы увеличения протяженности симметричного тракта систем цифрового видеонаблюдения // Перспективные технологии в средствах передачи информации – ПТСПИ-2017 : Материалы 12-й международной научно-технической конференции, в 2-х томах, Суздаль, 05–07 июля 2017 года. Суздаль: Владимирский государственный университет им. Александра Григорьевича и Николая Григорьевича Столетовых, 2017. Т. 1. С. 215–218.

4. Запорощенко Е. К., Семёнов А. Б. Перспективы техники категорий 7 и 7А в проектах построения информационных кабельных систем современных объектов недвижимости // Кабели и провода. 2022. N 4 (396). С. 31–36.

УДК 004.056
ГРНТИ 81.93.29

ИСПОЛЬЗОВАНИЕ JA3 ХЭШЕЙ В КАЧЕСТВЕ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

М. А. Скорых

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В работе рассмотрен подход к обнаружению компьютерных атак и инцидентов в шифрованном HTTPS-трафике. Актуальность темы обусловлена сложностью анализа шифрованного сетевого трафика современными системами обнаружения вторжений. В ходе работы подробно рассмотрен процесс формирования JA3 хэша. Продемонстрирован стенд с эмуляцией компьютерных атак на веб-ресурсы при помощи программного обеспечения Burp Suite, а также заражения узлов известными видами вредоносного программного обеспечения: Cobalt Strike, Merlin, Metasploit. Показана возможность обнаружения смоделированных компьютерных атак и инцидентов с использованием JA3 хэша в качестве индикатора компрометации, перечислены достоинства и недостатки указанного метода и дальнейшие направления исследований.

JA3 хэш, HTTPS, сетевой трафик, выявление аномалий, системы обнаружения вторжений, вредоносное программное обеспечение, Cobalt Strike, Metasploit, Burp Suite, Merlin.

В 2023 году в условиях большой информатизации всех сфер жизнедеятельности человека, все большую роль играет информационная безопасность. В открытых источниках можно найти множество информации об успешных компьютерных атаках, которые впоследствии становились причиной крупных компьютерных инцидентов. Для противодействия деструктивным воздействиям в информационном пространстве создаются различные средства защиты информации. Одним из классов таких систем являются сетевые IDS (*Intrusion Detection System*), обнаруживающие вредоносные воздействия в сетевом трафике. Слабой стороной IDS является сложность анализа шифрованного сетевого трафика, будь то распространенные сетевые протоколы, такие как HTTPS, RDP, SSH, или самостоятельно разработанные алгоритмы передачи данных (например, в случае работы различных APT-группировок). Особое внимание среди шифрованных протоколов можно уделить протоколу HTTPS, т. к. он является одним из наиболее распространенных протоколов, использующихся в сетях различных организаций. Под протоколом HTTPS могут происходить различные компьютерные атаки на веб-приложения, а также можно реализовать канал управления

зараженными устройствами в сети. В данной статье будет рассмотрен подход JA3 хэширования с целью обнаружения вредоносной активности в HTTPS-трафике.

Постановка задачи

Задачей исследования является построение стенда с эмуляцией типовых компьютерных атак (далее – КА) и инцидентов (далее – КИ), происходящих в шифрованном HTTPS-трафике, подробное описание алгоритма вычисления JA3 хэша, а также оценка возможности применения данного метода для детектирования КА и КИ.

JA3 хэш

Метод JA3 хэширования был рассмотрен в блоге Salesforce Engineering Джоном Альтхаусом в 2017 году [1]. JA3 хэш представляет собой отпечаток клиентского приложения в SSL/TLS-соединении. Данный подход обеспечивает идентификацию клиентского приложения в TLS-соединении.

Протокол TLS различных версий, а также протокол SSL, может использоваться как для шифрования различных данных пользователя при работе в сети Интернет, так и для шифрования каналов управления различных семейств вредоносного программного обеспечения (далее – ВПО).

Алгоритм вычисления JA3 хэша.

JA3 собирает десятичные значения байтов следующих полей: версия TLS/SSL (*TLSVersion*), набор шифров (*Cipher Suites*), список расширений (*List of Extensions*), эллиптические кривые (*Elliptic Curves*) и форматы эллиптических кривых (*Elliptic Curve Formats*). Затем полученные десятичные значения полей объединяются в порядки их встречи в сетевом пакете, используя символ «,» чтобы разграничить каждое поле, и «-», чтобы разграничить каждое значение в каждом поле.

С обновлением TLS 1.2 RFC4492 был изменен на RFC8422, а поле «эллиптические кривые» (*EllipticCurve*) стало называться «поддерживаемые группы» (*Extension: supported_groups*).

Порядок полей, следующий (с учетом RFC8422): версия TLS/SSL (*TLSVersion*), набор шифров (*Cipher Suites*), список расширений (*List of Extensions*), «поддерживаемые группы» (*Extension: supported_groups*) и форматы эллиптических кривых (*Elliptic Curve Formats*).

Для сообщения «Client Hello», изображенного на рис. 1, десятичные значения необходимых полей будут выглядеть следующим образом:

TLSVersion = 771
Cipher Suites = 49200-49172-4865-4866-4867
List of Extensions = 5-10-11-13-65281-16-18-43-51
Extension: supported_groups = 29-23-24-25
Elliptic Curve Formats = 0

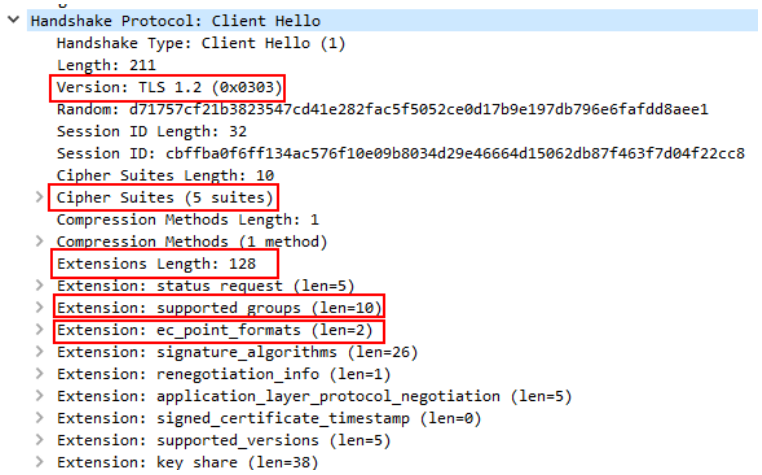


Рис. 1. Параметры сообщения «Client Hello», инициированного маячком Cobalt Strike

Десятичные значения конкатенируются в одну строку:

771,49200-49172-4865-4866-4867,5-10-11-13-65281-16-18-43-51,29-23-24-25,0

От полученной строки берется MD5-сумма и получается итоговый JA3 хэш:

4264590bacd8b2accb2021b7adb3b98e

Как можно увидеть, алгоритм получения JA3 хэша не требует больших вычислительных мощностей.

Использование JA3 хэшей в целях выявления компьютерных атак

JA3 хэширование позволяет идентифицировать клиентское приложение, инициирующее TLS-сессию. Рассмотрим несколько видов вредоносного программного обеспечения и утилит для пентеста, которые могут использовать протокол HTTPS при передаче данных.

Cobalt Strike это коммерческий фреймворк для эмуляции угроз от компании Fortra [2]. С помощью этой утилиты возможно проводить широкий спектр компьютерных атак, включающих разведку, эксплуатацию уязвимостей, постэксплуатацию, скрытую коммуникацию и другие возможности. Эксперты компании Cisco Talos заявили, что во втором квартале 2020 года Cobalt Strike использовался в 66% вымогательских атак.

Burp Suite – это распространенная интегрированная платформа для тестирования безопасности веб-приложений от компании PortSwigger [3]. В бесплатной версии Burp Suite поддерживается функционал HTTP(S)/WebSockets прокси, модули «Repeater», «Decoder», «Sequencer», и «Comparer». Burp Suite содержится в дистрибутиве Kali Linux и является одним из самых используемых фреймворков для тестирования безопасности веб-приложений.

Merlin – это кроссплатформенный фреймворк управления и взаимодействия постэксплуатации, написанный на языке программирования Go [4].

В функционал фреймворка входит создание канала управления по протоколу HTTP(S), создание агентов под различные платформы, функции управления зараженной системой

Metasploit вероятно наиболее распространенный фреймворк для тестирования на проникновение с открытым исходным кодом, разработанный сообществом информационной безопасности и компанией Rapid7 [5]. Входит в состав дистрибутива Kali Linux и содержит множество модулей эксплуатации уязвимостей, постэксплуатации, разведки, кодировки.

В целях получения JA3 хэшей от вышеуказанного программного обеспечения, был собран стенд, изображенный на рис. 2:

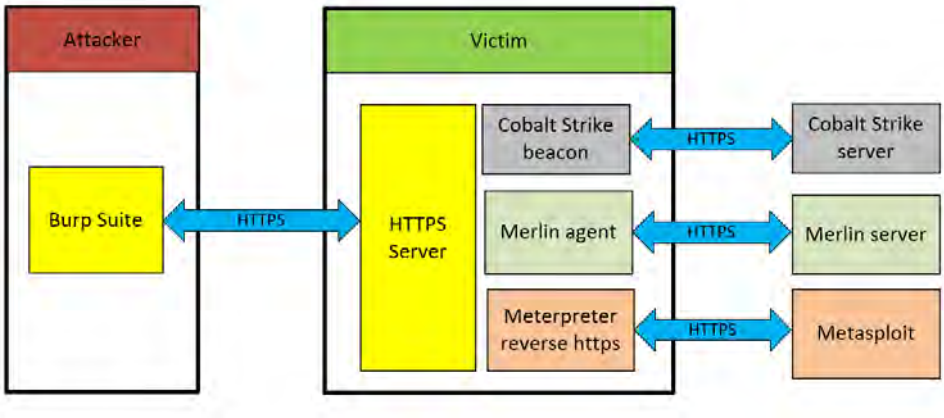


Рис. 2. Схема стенда с эмуляцией компьютерных атак и инцидентов

На виртуальном стенде машина жертвы была заражена 3-мя семействами ВПО (*Cobalt Strike, Merlin, Metasploit*). Каждый агент ВПО устанавливал соединение со своим сервером управления по протоколу HTTPS, а также в установленный промежуток времени, отправлял keepalive-сообщения (при каждом keepalive-сообщении устанавливалась новая HTTPS-сессия). В результате записи сетевого трафика с последующим вычислением JA3 хэша, удалось выяснить, что при каждом установлении TLS-сессии параметры сообщения “Client Hello” оставались неизменными для каждого семейства ВПО, JA3 хэша которых представлены в таблице 1:

ТАБЛИЦА 1. Значения JA3 хэшей для различных видов ПО

Вид ПО	JA3 хэш
Cobalt Strike	4264590bacd8b2accb2021b7adb3b98e
Merlin	72a589da586844d7f0818ce684948eea
Metasploit	5d65ea3fb1d4aa7d826733d2f2cbbb1d
BurpSuite	bac7558b8d784f94cf9f906114695744 dfd0bc4a6d8c21e500d6be9121fd44d7

Кроме того, на машине жертвы был установлен HTTPS-сервер. С атакующей машины проводились КА на веб-приложение при помощи фреймворка Burp Suite. В результате анализа сетевого трафика, удалось выяснить, что фреймворк Burp Suite генерирует 2 различных JA3 хэша, представленных в таблице 1.

Заключение

Таким образом имея базу репутации JA3 хэшей, появляется возможность детектировать активность различных семейств ВПО и утилит для пентеста в сетевом трафике.

Возможно несколько вариантов использования JA3 хэшей в целях обеспечения компьютерной безопасности: обнаружение HTTPS-каналов управления известных образцов ВПО, обнаружение в HTTPS-трафике вредоносной деятельности, генерируемой человеком, обнаружение эксфильтрации данных.

Преимуществом JA3 хэшей является возможность обнаружения утилит пентеста и различного ВПО в HTTPS-трафике без перечня стандартных для сетевого трафика индикаторов компрометации – IP-адресов и доменных имен. Кроме того, преимуществом JA3 хэшей является поддержка их вычисления в распространенных средствах анализа трафика [6].

Недостатками JA3 хэшей являются: отсутствие общей базы репутации, вероятность ложноположительного решения, наличие способов подделки JA3 хэша, необходимость учитывать JA3 хэш HTTPS-сервера (JA3S хэш), недостаточная изученность технологии.

Дальнейшим направлением исследований является поиск пути решения любого из вышеуказанных недостатков.

Список используемых источников

1. Open Sourcing JA3 [Электронный ресурс] // Salesforce Engineering Blog. URL: https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41/ (дата обращения 12.02.2023).

2. Cobalt Strike Features. URL: https://www.cobaltstrike.com/features/ (дата обращения 12.02.2023).

3. Burp Suite Community Edition. URL: https://portswigger.net/burp (дата обращения 12.02.2023).

4. Merlin. URL: https://GitHub.com/Ne0nd0g/merlin (дата обращения 12.02.2023).

5. Metasploit. URL: https://www.metasploit.com/ (дата обращения 12.02.2023).

6. Скорых М. А., Израилов К. Е., Башмаков А. В. Задачаориентированное сравнение средств анализа сетевого трафика // Теория и практика обеспечения информационной безопасности: сборник научных трудов по материалам Всероссийской научно-теоретической конференции (Москва, 03 декабря 2021 г.). 2021. С. 103–107.

Статья представлена научным руководителем, доцентом кафедры ЗСС СПбГУТ, кандидатом технических наук, К. Е. Израиловым.

УДК 004.056
ГРНТИ 81.96

РЕШЕНИЕ СИСТЕМЫ УРАВНЕНИЙ НА ОСНОВАНИИ КИТАЙСКОЙ ТЕОРЕМЫ ОБ ОСТАТКАХ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА МОНТГОМЕРИ

Е. В. Таров, С. Н. Шемякин, В. А. Яковлев

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Рассмотрен способ применения алгоритма Монтгомери для уменьшения вычислительных затрат модульных вычислений при решении системы уравнений на основе китайской теоремы об остатках. Программная реализация предложенного способа на языке Python показала, что применение алгоритма Монтгомери значительно увеличивает скорость решения системы для чисел большой разрядности в сравнении со стандартным алгоритмом.

информационная безопасность, криптография, модульная арифметика, алгоритм Монтгомери.

Китайская теорема об остатках (КТО) – это одна из важнейших математических теорем, которая позволяет решать системы уравнений с несколькими модулями. Она находит широкое применение в теории чисел и многих других областях математики и информатики [1, 2, 3, 4].

Одним из ключевых инструментов при решении систем уравнений, связанных с КТО, является алгоритм Монтгомери, который позволяет эффективно вычислять арифметические операции с использованием модульной арифметики и сокращать количество операций умножения и деления [5].

КТО широко применяется в криптографии, в частности, в схемах шифрования и аутентификации, таких как Rivest–Shamir–Adleman (RSA), Digital Signature Algorithm (DSA) и Elliptic-curve cryptography (ECC). Эти схемы используют арифметику больших чисел. Например:

– В алгоритме DSA используются числа с размерностью 1024 бит или более;

– В криптосистеме RSA криптограмма формируется с размером модуля 1024, 2048 и более бит;

– В ГОСТ 34.10-2018 используется модульное умножение для чисел разрядности 256 бит.

Цель данной работы – разработать способ применения алгоритма Монтгомери при решении систем уравнений, связанных с КТО, и показать,

что применение данного алгоритма может значительно ускорить модульные вычисления.

Рассмотрим более подробно алгоритм решения системы уравнений при помощи КТО. Пусть нам нужно вычислить такое значение *x*, которое бы удовлетворяла следующей системе уравнений:

$$\begin{cases} x = a_1 \bmod m_1 \\ x = a_2 \bmod m_2 \\ \dots \\ x = a_t \bmod m_t \end{cases}, \quad (1)$$

где $m_1, m_2, ..., m_t$ – это попарно простые натуральные числа, а $a_1, a_2, ..., a_t$ – остатки от деления искомого числа *x* на соответствующие простые модули.

В таком случае в соответствии с КТО для вычисления *x* необходимо для всех значений *i* (где *i* = 1, 2, …, *t*) провести следующие вычисления:

$$M_i = \frac{M}{m_i}, \quad (2)$$

$$M_i N_i = 1 \bmod m_i, \quad (3)$$

где $M = m_1 * m_2 * ... * m_t$. После этого вычислить искомое значение *x* по формуле:

$$x = \sum_{i=1}^{t} a_i M_i N_i \bmod M. \quad (4)$$

Из формулы (4) можно заметить, что при непосредственном вычислении по ней необходимо проводить большое число модульных умножений по большому модулю *M*, что сильно влияет на скорость вычисления *x*. Для повышения скорости можно воспользоваться алгоритмом Монтгомери.

Алгоритм Монтгомери — это метод ускорения операций над большими числами. Он применяется для ускорения операций умножения и возведения в степень по модулю. Основной принцип работы алгоритма Монтгомери заключается в том, что вместо операций умножения и деления используются операции сдвига и сложения, что позволяет существенно ускорить вычисления [6, 7].

Это реализуется посредством замены вычислений по изначальному модулю *M* на вычисления по более удобному модулю. Для этого выбирается разработчиком удобный модуль *R*, такой что *R* > *M* и gcd(*R*, *M*) = 1.

Также стоит сказать, что модуль *R* образует свое кольцо классов вычетов, которое называют кольцом Монтгомери.

Опишем подробнее принцип работы алгоритма Монтгомери [6, 7]. Пусть имеется модуль *M* и два числа *x* и *y*, при этом *x*,*y* < *M*. Требуется найти

$xy \bmod M$. Для этого необходимо провести следующие предварительные вычисления:

1. Вычислить модуль R по следующей формуле:

$$R = \beta^m,$$

где β – основание системы счисления, m – количество разрядов в записи модуля M в системе счисления β.

2. При помощи расширенного алгоритма Евклида найти линейное разложение:

$$Rr - Mn = 1, \quad (5)$$

где $r = R^{-1} \bmod M$, $n = (-M)^{-1} \bmod R$.

3. И вычислить значение $R^2 \bmod M$.

После предварительных вычислений нужно применить функцию Монтгомери:

$$z_R = \varphi_R(x, y) = xyr \bmod M$$

Программа вычисления функции $\varphi_R(x, y)$ принимает на вход два числа – известные множители x и y. После чего производит модульное умножение данных чисел эффективным способ, заменяя операции деления, умножения и взятия остатка на битовые сдвиги и возвращает результат вычислений z_R. При этом число r из формулы (5) добавляется на выходе $\varphi_R(x, y)$. Это свидетельствует об отображении произведения чисел x и y в кольцо Монтгомери.

Для обратного отображения в исходное кольцо, образованное классом вычетов по модулю M, нужно применить данную функцию повторно для результата прошлого шага z_R и предварительно вычисленного значения $R^2 \bmod M$. Это будет выглядеть следующим образом:

$$\varphi_R(z_R, R^2) = z_R R^2 r = xy \bmod M.$$

В результате будет получено искомое значение $xy \bmod M$.

Рассмотрим теперь применение алгоритма Монтгомери в КТО.

Пусть нам нужно вычислить такое значение x, которое бы удовлетворяла следующей системе уравнений (1).

Выполним все вычисления по формулам (2)-(3). После чего искомое значение x найдем с применением функции Монтгомери следующим образом:

$$xR = \sum_{i=1}^{t} \varphi_R(\varphi_R(a_i, M_i), N_i) \bmod M,$$

$$x = \varphi_R(xR, R^3 \bmod M),$$

где xR – результат модульного умножения формулы (4), отображенный в кольцо Монтгомери. При этом для обратного отображения применяется значение $R^3 \bmod M$ которое может быть вычислено предварительно вместо значения $R^2 \bmod M$.

В ходе исследования была разработана программная реализация предложенного способа решения системы уравнений на основе алгоритма Монтгомери и способа прямого вычисления по формуле (4) на языке Python. Программа применялась для решения системы из 8 уравнений. Результаты сравнения двух способов вычислений представлены в таблице 1.

ТАБЛИЦА 1. Результаты сравнения алгоритмов

Количество бит модуля M	Отношение времени работы обычного алгоритма к Монтгомери
128	1,34
256	1,78
512	2,68
1024	4,42
2048	8,08

Из таблицы видно, что применение алгоритма Монтгомери позволяет значительно ускорить модульные вычисления при решении систем уравнений на основе китайской теоремы об остатках. При этом ускорение становится более заметным при работе с числами большой разрядности.

Таким образом, результаты данной работы подтверждают эффективность алгоритма Монтгомери при решении систем уравнений с применением КТО и показывают, что его использование может значительно сократить время модульных вычислений в алгоритмах криптографических преобразований.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. СПб. : Интермедия, 2017. 312 с.

2. Коржик В. И., Просихин В. П. Основы криптографии: учебное пособие по специальности 210403 «Защищенные телекоммуникационные системы связи». СПб. : Линк, 2008.

3. Панкратова И. А. Теоретико-числовые методы криптографии: учебное пособие. Томский государственный университет. Томск : Национальный исследовательский Томский государственный университет, 2009. 120 с.

4. Кнут Д. Э. Искусство программирования. Том 1. Основные алгоритмы. М. : Мир, 1976. 735 с.

5. Montgomery P. L. Modular multiplication without trial division. // Mathematics of computation. 1985. Vol. 44, No. 170. PP. 519–521.

6. Лобес М. В., Червяков Н. И. Повышение скорости выполнения операции модульного возведения в степень многоразрядных чисел // Инфокоммуникационные технологии. 2009. N 7. С. 8–12.

7. Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теорико-числовые методы криптографии. М. : Лань, 2011. 400 с.

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ОСНОВЫХ ХАРАКТЕРИСТИК И ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ SIEM-СИСТЕМ

А. С. Учинин, А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В современном мире быстро развивающихся технологий механизмы защиты информационной структуры предприятия приобрели важную роль среди компьютерных технологий.

С развитием технологий развивались и методы получения несанкционированного доступа и атак на корпоративные сети. В связи с этим защита сетей внутри предприятий становилась более комплексной и составной, начинала включать в себя все большее количество различных систем, предотвращающих нанесение вреда инфраструктуре сети. Количество информационных событий в корпоративных сетях может быть слишком большим для анализа каждой системы отдельно. Задачу структурирования и корреляции информации, полученной от различных служб обеспечения безопасности сети, решили SIEM-системы, собирающие и анализирующие данную информацию в реальном времени.

SIEM, защита информации, информация, данные, системы обеспечения защиты информации, контроль, инцидент.

Введение

Крупные предприятия имеют большую развернутую инфраструктуру сети, иногда разные точки данной инфраструктуры могут быть разнесены географически далеко друг от друга. Разумеется, в современном информационном мире к сетям предприятий применяются определенные механизмы защиты такие как межсетевые экраны, IDS/IPS – системы предотвращения/обнаружения вторжений, DLP-системы, предназначенные для защиты предприятий от утечек конфиденциальной информации и так далее. Каждая из данных систем может быть подвержена атаке, уследить за атаками на все

эти системы сложно физически даже для группы системных и сетевых инженеров. SIEM-системы решают данную задачу в реальном времени.

Основная часть

Security Information and Event Management (SIEM) – это объединение двух механизмов: SEM, который отвечает за мониторинг событий безопасности в реальном времени и SIM, выполняющий функцию хранения и анализа данных с различных систем обеспечения безопасности инфраструктуры сети предприятия. В своей сущности SIEM-системы не способны предотвратить получение несанкционированного доступа к сети предприятия или нарушение целостности и конфиденциальности передаваемой информации. В задачи этих систем входит автоматизированное получение, хранение и анализ информации об инцидентах безопасности внутри сети предприятия. Решения SIEM сортируют данные безопасности, что упрощает работу администраторов безопасности внутри сети. Данные системы предоставляют возможность использовать заранее определенные правила мониторинга событий безопасности или создавать свои собственные, для которых можно задать приоритет оповещений.

Систем управления информацией и событиями безопасности (SIEM) выполняют три важные функции при их реализации:

1) **Обнаружение угроз** – SIEM-системы собирают и анализируют информацию, связанную с событиями безопасности и, в соответствии с правилами, выставляют инцидентам уровень опасности, в зависимости от критичности данных инцидентов.

2) **Расследование угроз** – на основе полученных данных об инцидентах безопасности SIEM-системы составляют отчёты, благодаря которым администратор информационной безопасности может провести расследование угроз.

3) **Реагирование на инцидент** – комплекс мероприятий, реализуемый SIEM-системами и направленный на прекращение кибератак или утечек данных из инфраструктуры предприятия. Сама система управления информацией и событиями безопасности, как говорилось ранее, не предотвращает атак, реагирование означает, что система оповещает администратора ИБ об угрозе, ее типе и уровне (высокий/низкий), на основе этого администратор принимает меры по нивелированию данной угрозы.

Принцип работы современных SIEM систем построен на следующих механизмах:

- **Агрегация данных** – процесс, при котором информация, связанная с работой всех устройств в сети таких как маршрутизаторы, межсетевые экраны, сервера и т. д., собирается в специальные журналы данных, управляемые SIEM-системами, данные нормализуются и приводятся к единообразному формату.

• **Таксономия** – классификация нормализованных данных, в зависимости от их содержания.

• **Корреляция** – механизм, обеспечивающий соотнесение между собой событий, удовлетворяющих определенным условиям, полученным от различных систем обеспечения ИБ (от устройств и сервисов) внутри сети предприятия. В SIEM системах правила корреляции представлены в формате Rule Based Reasoning, это означает, что они содержат набор условий, различных триггеров, счетчиков и сценариев действий. На рис. 1 приведены различные источники входных данных для процесса корреляции [5].

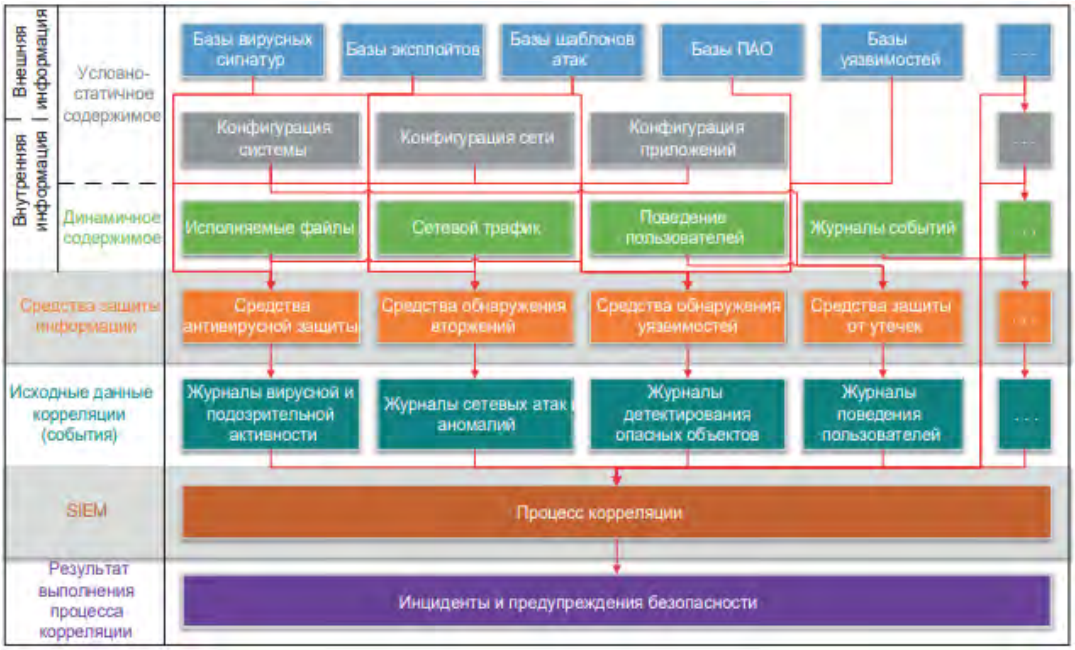


Рис. 1. Входные данные для корреляции

• Для удобства отслеживания администратором сети отчетности у SIEM систем присутствуют **панели мониторинга**, предоставляющие информацию о событиях в виде графиков и диаграмм.

SIEM системы собирают и формируют отчеты об инцидентах и основными источниками информации можно назвать следующие устройства/сервисы:

1. IDS/IPS системы – формируют логи об инцидентах, связанных с сетевыми атаками.
2. Сервисы контроля доступа и аутентификации (например, RADIUS)
3. Активное сетевое оборудование, такое как коммутаторы, маршрутизаторы и т. д.
4. Средства антивирусной защиты.
5. DLP системы.
6. Рабочие станции пользователей.
7. Межсетевые экраны.

8. Контроллеры домена и др.

На рис. 2 представлена упрощенная схема работы SIEM-системы внутри организации. Задача данной схемы показать взаимодействие сервисов и устройств с SIEM-сервером. Пунктирными линями показано, что каждое устройство и каждый сервис внутри сети взаимодействует с SIEM-сервером, передавая log-файлы инцидентов сети, стоить учесть, что оборудование и сервисы могут сами предоставлять файлы логов SIEM-системам, но также SIEM системы иногда сами запрашивают данные файлы.

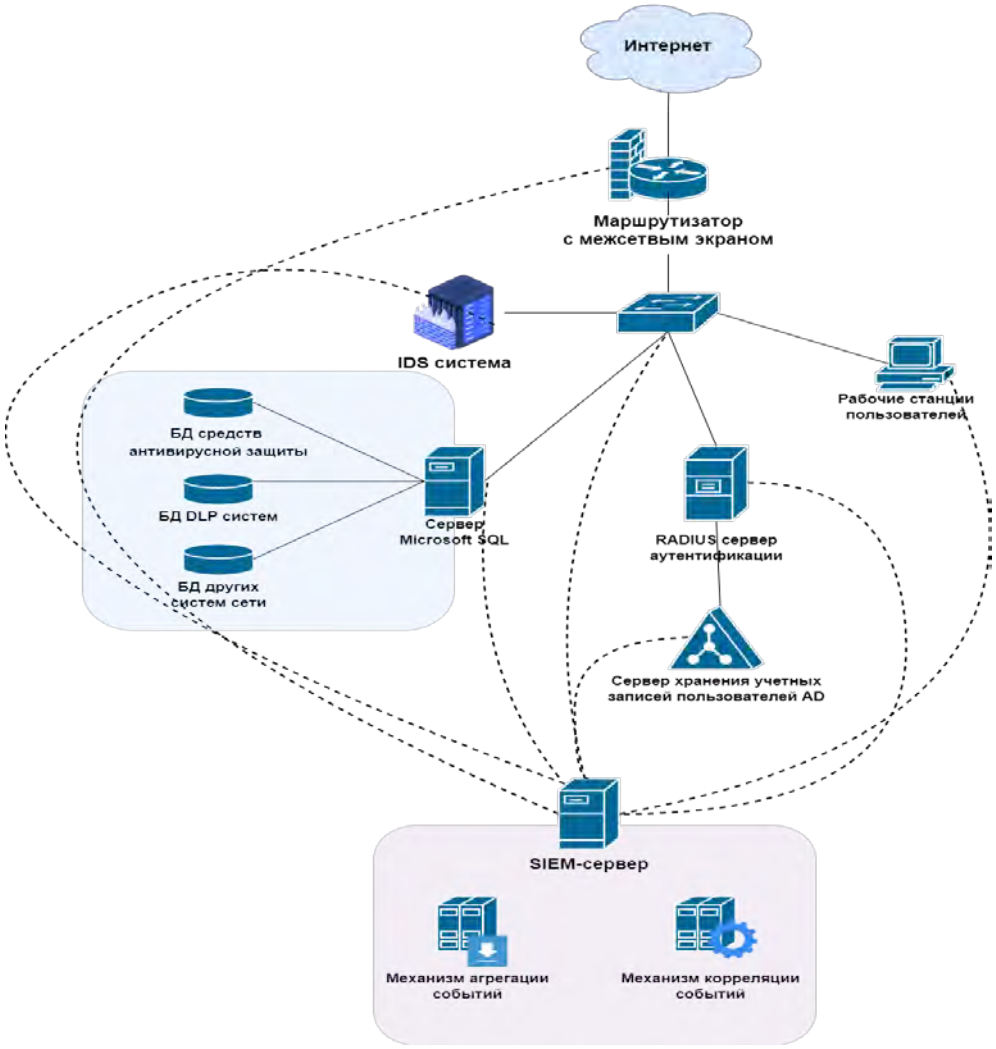


Рис. 2. Схема сети с реализованной SIEM-системой

Изначально SIEM-сервер собирает данные со всех источников, агрегирует их, приводит в единообразный формат. Затем необходимо дать классификацию данным для того, чтобы понять какие из событий несут угрозу инфраструктуре предприятия, а какие не оказывают влияния и не требуют особого изучения администраторами информационной безопасности. Например, две неудачные попытки входа пользователя на рабочую станцию

и срабатывание IDS-системы, эти два инцидента не могут быть классифицированы как одинаковые уровни угрозы безопасности сети. Таким образом происходит формирование цепочек событий с временной последовательностью наступления. На схеме рис. 2 не отражен процесс таксономии (классификации) данных, так как этот процесс является переходным между корреляцией и агрегацией. Следующим шагом SIEM-сервер коррелирует полученную информацию – соотносит между собой инциденты и события в соответствии с заданными условиями. Пример работы правила корреляции относительно рис. 2: непрерывные попытки подключения на сервер базы данных удаленно в течение 10 часов, которые, в конечном итоге, оказались успешными, после чего на сервере началось несанкционированное копирование данных на другой удаленный сервер, находящийся вне сети предприятия. В данном примере произошло два инцидента безопасности: неудачные попытки входа на протяжение долго времени, т. е. brute force атаки для подбора данных и несанкционированное копирование файлом баз данных на сервер, находящийся удаленно в другой сети. В данном случае механизм корреляции SIEM-системы сформирует инцидент информационной безопасности и предоставит отчет администраторам ИБ, которые, в свою очередь, должны будут должным образом среагировать на событие и принять необходимые меры.

Исходя из сказанного выше, можно выделить основные преимущества и недостатки SIEM-систем.

Решения SIEM имеют множество преимуществ для любой организации, заботящейся о безопасности, которая наняла квалифицированных специалистов по ИБ. Некоторые из этих преимуществ приведены ниже:

- Позволяет службам безопасности быстро выявлять сетевые угрозы и снижать последствия кибератак.
- Предоставляет аналитикам по безопасности централизованное представление о безопасности всей инфраструктуры предприятия. Все конечные точки, сетевые устройства и сервисы безопасности отправляют данные об инцидентах ИБ SIEM-серверу для хранения и обработки.
- Обеспечивает расширенное обнаружение вредоносных программ и активирует оповещения системы безопасности.
- Позволяет организациям легко собирать данные из требований соответствия
- SIEM-системы поддерживают большое количество источников событий, многие современные системы могут анализировать события от более чем 200 источников, список источников всегда пополняется.
- Большинство SIEM-систем имеют графический Web-интерфейс управления, что упрощают работу администраторов информационной безопасности.

• Существует большое количество бесплатных, open source SIEM-систем, многие из которых поддерживаются своими разработчиками, например, RuSiem free.

К сожалению, SIEM системы не идеальны и имеют также и существенные недостатки:

• Внедрение всех элементов управления решением SIEM в организации – комплексная задача, которая может занять немалое количество времени: от 3 до 6 месяцев.

• Коммерческие решения SIEM дорогие. Организации малого и среднего бизнеса могут быть не в состоянии позволить себе эти решения, поскольку их первоначальные инвестиции могут достигать сотен тысяч долларов.

• Понимание и анализ информации, генерируемой решениями SIEM – задача, требующая специальных знаний. Предприятия, внедряющие решения SIEM, также должны создать центр управления безопасностью, где будет обрабатываться вся информация, генерируемая системами SIEM.

• Решения SIEM генерируют как минимум более 10 000 событий в день. Если информация интерпретируется неправильно из-за неправильно настроенной SIEM-системы, преимущество решения SIEM может превратиться в недостаток.

• Некоторые open source решения SIEM-систем не поддерживаются и не обновляются своими разработчиками, соответственно ни о какой технической поддержке не может быть и речи. Явным пример является SIEM-система Wazuh, правила которой не обновляются на GitHub уже более четырех лет, хотя сама система и Web-интерфейс для ее управления работают.

Заключение

Системы SIEM имеют первостепенное значение, поскольку они значительно упрощают анализ событий безопасности, поступающих от огромного количества журналов, собранных сетевыми устройствами и сервисами безопасности. SIEM не только отфильтровывает ненужные данные журналов, но также позволяет администраторам ИБ расставлять приоритеты для определенных событий, создавая предупреждающие уведомления.

Без решения для управления информацией и событиями безопасности большинство подозрительных действий в инфраструктуре организации могут остаться незамеченными аналитиками безопасности. Решения SIEM также помогают организациям выполнять требования соответствия, поскольку они создают отчеты со всеми событиями безопасности и журналами. Без решений SIEM этот процесс пришлось бы выполнять вручную, что является весьма сложной задачей, требующей большого количества времени.

Быстрое реагирование на инциденты является обязательным требованием для любой организации, чувствительной к безопасности. Аналитикам безопасности нужны соответствующие данные, чтобы реагировать на инциденты безопасности. SIEM не только предоставляет эту информацию, но также предоставляет инструменты SIEM для автоматизации реагирования на эти инциденты.

Список используемых источников

1. Цветков А. Ю. Анализ существующих методов атак типа переполнения буфера на операционные системы семейства Microsoft // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференцияи: сб. науч. ст. в 4 т. СПб. : СПбГУТ, 2019. С. 751–756.

2. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства Linux // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2018. Т. 1. С. 657–662.

3. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. N 2. С. 50–56.

4. Катасонов А. И., Цветков А. Ю. Анализ механизмов разграничения доступа в системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2020. Т. 1. С. 563–568.

5. Федорченко А. В., Котенко И. В. Корреляция информации в SIEM-системах на основе графа связей типов событий // Информационно-управляющие системы. 2018. N 1. С. 58–67. doi:10.15217/issn1684-8853.2018.1.58

6. Сизов В. А., Киров А. Д. Проблемы внедрения SIEM-систем в практику управления информационной безопасностью субъектов экономической деятельности. Открытое образование. 2020. N 24 (1). С. 69–79.

7. Что такое SIEM? URL: https://thecyphere.com/blog/what-is-siem/

8. Сравнение SIEM-систем. Часть 1. URL: https://www.anti-malware.ru/ compare/SIEM-systems#part314

9. SIEM: ответы на часто задаваемые вопросы. URL: https://habr.com/ru/post/172389/

Статья представлена заведующим кафедрой ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым

УДК 004.7
ГРНТИ 49.33.29

ОБЗОР ТЕКУЩЕГО ПОЛОЖЕНИЯ ПРИМЕНЕНИЯ СЕТЕВОГО КОДИРОВАНИЯ В БЕСПРОВОДНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

А. И. Фомин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье выполнен краткий обзор актуальных исследований в области сетевого кодирования в беспроводных сетях передачи данных, которые были проведены в период за последние 10 лет, а также рассмотрены существующие протоколы, основанные на методе сетевого кодирования. Подчёркнуты особенности рассмотренных исследований и приведена их значимость. Изложение выполнено на основе группировки по годам исследований.

беспроводные сети, сетевое кодирование, протоколы.

Сетевое кодирование является перспективной технологией для повышения производительности и безопасности беспроводных сетей передачи данных. В данной статье представлен обзор текущего состояния сетевого кодирования в беспроводных сетях передачи данных. Для актуальности были изучены исследования за последние 10 лет обсуждаются теоретические основы и практическая реализация сетевого кодирования. Также в обзоре представлен ряд протоколов, которые используют сетевое кодирование. Цель данной статьи – предоставить всесторонний обзор текущего состояния сетевого кодирования в беспроводных сетях передачи данных.

В 2012 на кафедре Электротехники и вычислительной техника университета Торонто было проведено исследование использования методов сетевого кодирования для распространения контента и потоковой передачи мультимедиа в одноранговых сетях (P2P) [1]. Авторы обсуждали проблемы и ограничения традиционных методов P2P и объясняли, как сетевое кодирование может повысить эффективность и надежность таких сетей. Было представлено подробное описание предложенных алгоритмов сетевого кодирования и оценка их эффективность с помощью моделирования и экспериментов. Данное исследование подводит к выводам об эффективности использования сетевого кодирования, которое может значительно повысить пропускную способность, масштабируемость и надежность систем P2P-распространения контента и потоковой передачи мультимедиа [1].

В 2012 группа авторов из университета Нортуэстрен и политехнического университета Виргинии изучила производительность беспроводных широковещательных сетей с использованием сетевого кодирования и ретрансляционных узлов [2]. Авторы разработали структуру для анализа пропускной способности и стабильности сети при наличии случайного сетевого кодирования и ретрансляционных узлов. Они показывают, что сочетание сетевого кодирования и ретрансляционных узлов может улучшить пропускную способность и стабильность беспроводных широковещательных сетей. В исследовании также приводятся численные результаты, иллюстрирующие эффективность предложенной схемы в различных сетевых сценариях. В целом, данная статья вносит вклад в понимание преимуществ сетевого кодирования и узлов ретрансляции в беспроводных широковещательных сетях и дает представление о проектировании эффективных беспроводных сетей [2].

В 2013 была предложена концепция протокола оппортунистического сетевого кодирования под названием PlayNCool, который использует преимущества сетевого кодирования для повышения производительности беспроводных mesh-сетей [5]. Протокол направлен на оптимизацию локальной маршрутизации между узлами ячеистой сети путем динамической адаптации операций сетевого кодирования к условиям сети. Это достигается за счет использования сквозной передачи пакетов со случайным линейным сетевым кодированием, перекодированием на промежуточных узлах и определением дополнительных узлов для каждого отдельного канала связи. Результаты моделирования показали, что PlayNCool превосходит традиционные методы маршрутизации пакетов по пропускной способности, задержке и коэффициенту доставки пакетов.

В 2014 коллектив разработчиков из Хьюстонского университета и бразильского федерального университета Минас-Жерайс представили новый протокол распространения данных CodeDrip для беспроводных сенсорных сетей, использующий сетевое кодирование [3]. Протокол CodeDrip использует сетевое кодирование для объединения пакетов из разных источников в общую комбинацию этих пакетов с последующей передачей на соседние узлы, сокращая общее количество передач за счёт отсутствия необходимости в перезапросах во время декодирования и повторных передач. Оценка производительности CodeDrip, проведённая в исследовании с помощью моделирования показывает, что он позволил уменьшить число передаваемых по сети пакетов [3, 4].

Также с 2014 года рабочая группа NWCRG разрабатывает протокол Tetrys (протокол сетевого кодирования на лету), предназначенный для повышения надежности и эффективности передачи данных в беспроводных сетях передачи данных, чувствительных к задержкам и потерям [6]. Прото-

кол использует схему кодирования, которая позволяет кодировать и декодировать пакеты данных «на лету», уменьшая задержку и сложность процесса кодирования. Сами пакеты формируются в кодовом буфере переменной длины, а все пакеты, поступающие от источника, записываются в буфер кодирования и хранятся до прихода подтверждения о получении пакета.

В 2016 году на 7 международной конференции EUSPN была предложена энергоэффективная модель сетевого кодирования для беспроводных сенсорных сетей (WSNs) [7]. Целью авторов является повышение энергоэффективности беспроводных сенсорных сетей путем сокращения количества передач, необходимых для распространения данных, при сохранении качества обслуживания. Был предложен алгоритм для выбора линейных коэффициентов сетевого кодирования, а также решение для возможности декодирования информации получателем данных. Авторы оценивают производительность предложенной модели с помощью моделирования и показывают, что она превосходит как традиционные методы маршрутизации, так аналогичную схему сетевого кодирования и маршрутизации без предложенного алгоритма по энергоэффективности [7].

В 2018 годом коллектив из южнокорейского университета Сонгюнгван предложил схему распределенного систематического сетевого кодирования (DSNC) для надежной загрузки контента в беспроводных мультимедийных сенсорных сетях (WMSN) [8]. Цель авторов – повысить надежность загрузки контента в WMSNs за счет использования методов сетевого кодирования. Предложенная схема DSNC заключается в том, что закодированные в каждом узле пакеты передаются на головной узел, где происходит декодирование информации со всех узлов, а зачем кодирование в модифицированные пакеты систематического сетевого кодирования с последующей отправкой на узел получателя, тем самым снижая коммуникационные затраты и повышая надежность загрузки контента [8]. Проведённые тесты производительности показали высокие результаты с точки зрения вероятности декодирования, избыточности и измерения качества изображения по сравнению с другими схемами на основе сетевого кодирования [8].

Также в 2018 году был представлен предложен подход на основе сетевого кодирования, который может повысить производительность беспроводной связи в системах автоматизации [9]. Цель авторов является повышение надежности и уменьшение задержки беспроводной связи в системах промышленной автоматизации за счет использования методов сетевого кодирования. Предложенный подход использует метод сетевого кодирования, которая позволяет нескольким датчикам передавать свои данные одновременно, тем самым уменьшая задержку и повышая надежность беспроводной связи. Авторы оценивают эффективность предложенного подхода с помощью экспериментов и показывают, что он превосходит схемы без сетевого кодирования по надежности, задержке и пропускной способности.

В 2020 году коллектив сотрудников из Санкт-Петербургского университета телекоммуникаций и Института проблем управления провели ряд исследований, посвящённых использованию сетевого кодирования для сбора данных с наземных сенсорных сетей беспилотными летательными аппаратами (БПЛА) [11, 12, 13]. Был разобран концепт такой сети и способы его реализации и разработана модель. Предложенный подход использует сетевое кодирование для минимизации энергопотребления, времени полёта и обеспечения надежной передачи данных даже при наличии ошибок в канале [12]. Авторы оценивают границы применимости предложенной концепции с помощью моделирования. Данное исследование показало перспективность применения сетевого кодирования в беспроводных сенсорных сетях для сбора данных с помощью БПЛА [14].

В 2021 году в рамках научно-исследовательской работы на кафедре Сетей связи и передачи данных в СПбГУТ был разработан датаграммный протокол с сетевым кодированием NCDP [14]. Данная работа описывает концепцию нового протокола для многоадресной маршрутизации передачи данных в случае нескольких источников информации и нескольких потребителей информации. В статье предлагается использовать сетевое кодирование для обеспечения более эффективного использования доступной пропускной способности и повышения производительности беспроводных сетей. Были описаны структура и алгоритмы, а также результаты моделирования, демонстрирующие преимущества протокола по сравнению с существующими методами передачи данных без использования сетевого кодирования [14].

Сетевое кодирование — это перспективный метод, который показывает большой потенциал в повышении производительности беспроводных сетей передачи данных. Было показано, что использование сетевого кодирования в беспроводных сетях позволяет повысить пропускную способность, уменьшить задержки и повысить надежность. В рассмотренных исследованиях продемонстрированы различные применения сетевого кодирования в беспроводных сетях передачи данных, включая многоадресную передачу, mesh-сети, беспроводные сенсорные сети и сети автоматизации.

Список используемых источников

1. Feng Ch., Li B. Network Coding for Content Distribution and Multimedia Streaming in Peer-to-Peer Networks // IEEE. 2012. Ch. 1. PP. 1–22.

2. Yalin E. S., Randall A. B., and Dongning G. Throughput and stability for relay-assisted wireless broadcast with network coding // IEEE Journal on Selected Areas in Communications. 2013. Vol. 31. PP. 1506–1516.

3. Ribeiro Junior N., Vieira M. A., Vieira L. F., Gnawali O. CodeDrip: Data Dissemination Protocol with Network Coding for Wireless Sensor Networks // Proceedings of the 11th European Conference on Wireless Sensor Networks – Volume 8354 (EWSN 2014). 2014. PP. 34–49.

4. Ribeiro Junior N., Tavares R. C., Vieira M. A. M., Vieira L. F. M., Gnawali O. CodeDrip: Improving data dissemination for wireless sensor networks with network coding // Ad Hoc Networks. 2017. Vol. 54. PP. 42–52.

5. Pahlevani P., Lucani D. E., Pedersen M. V., Fitzek F. H. P. PlayNCool: Opportunistic network coding for local optimization of routing in wireless mesh networks // 2013 IEEE Globecom Workshops. Atlanta, GA, USA: IEEE, 2013. PP. 812–817.

6. Detchart J., Lochin E., Lacan J., Roca V. Tetrys, an On-the-Fly Network Coding protocol [Электронный ресурс] // IETF. URL: https://www.ietf.org/id/draft-irtf-nwcrg-tetrys-04.html/ (дата обращения 01.03.2023).

7. Khodabakhshi B., Khalily M. An Energy Efficient Network Coding Model for Wireless Sensor Networks [Электронный ресурс] // Sciencedirect. URL: https://www.sciencedirect.com/science/article/pii/S1877050916321548/ (дата обращения 01.03.2023).

8. Chau P., Shin J., Jeong J. Distributed Systematic Network Coding for Reliable Content Uploading in Wireless Multimedia Sensor Networks [Электронный ресурс] // MDPI. URL: https://www.mdpi.com/1424-8220/18/6/1824?type=check_update&version=1/ (дата обращения 01.03.2023).

9. Swamy V., Suri S., Rigge P., Weiner M., Ranade G., Sahai A., Nikolić B. Real-Time Cooperative Communication for Automation Over Wireless // IEEE Transactions on Wireless Communications. 2017. Vol. 16. PP. 7168–7183.

10. Vladimirov S., Vishnevsky V., Larionov A., Kiricher R. Concept of UFP based WBAN Data Acquisition Network // DCCN 2020. 2020. PP. 1-8.

11. Vladimirov S., Vishnevsky V., Larionov A., Kiricher R. The Model of WBAN Data Acquisition Network Based on UFP// Distributed Computer and Communication Networks. 2020. PP. 220–231.

12. Vladimirov S., Vishnevsky V., Kiricher R. Network Coding for the Interaction of Unmanned Flying Platforms in Data Acquisition Networks // ICFNDS '20: The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). 2020. PP. 1–7.

13. Владимиров С. С., Вишневский В. М., Мухтаров А. А., Киричек Р. В. Сбор данных с нательных сенсорных сетей на основе беспилотных летающих платформ с использованием метода сетевого кодирования // Труды НИИР. 2020. N 4. С. 57–64.

14. Владимиров С. С., Фомин А. И. Концепция протокола многоадресной передачи на основе метода сетевого кодирования // Информационные технологии и телекоммуникации. 2021. Т. 9. N 1. С. 26–36.

Статья представлена научным руководителем, доцентом кафедры ССПД СПбГУТ, доктором технических наук, доцентом С. С. Владимировым.

УДК 004.455.2
ГРНТИ 50.43.19

АНАЛИЗ МЕХАНИЗМОВ ПОДДЕРЖКИ СОСТОЯНИЯ ИНФРАСТРУКТУРЫ ОБЛАЧНОГО СЕРВИСА

С. П. Фомин, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В данной статье производится описание нескольких подходов к автоматизированному развертыванию сервисов, описываются общие проблемы при данном типе развертывания. В настоящее время всё чаще используются механизмы автоматизированного развертывания сервисов. Уже развернутые сервисы требуют отслеживания состояния в реальном времени. Целью данной работы является изучение требований к системе, которая будет поддерживать состояние сервисов, описание методов поддержки состояния. Будет произведён анализ различных механизмов для поддержания состояния инфраструктуры облачного сервиса, а также предоставление наиболее подходящего механизма для решения выделенных проблем.

развертывание, Ansible, Gitlab, Terraform.

В настоящее время чаще всего используются механизмы автоматизированного развертывания сервисов, они позволяют развернуть нужные приложения на большом количестве серверов заказчика, что позволяет уменьшить затраты по времени и исключить человеческий фактор.

Ansible – безагентный инструмент для управления конфигурациями, позволяющая выполнять операции по настройке ОС и установке различного ПО [1].

Преимущества Ansible (рис. 1):

- Использует для подключения SSH, вместо запроса агентов;
- Простой язык написания плейбуков YAML;
- Присутствует доступная и большая база документации;
- Работа простота использования: работе с Ansible можно научиться за короткое время Ansible осуществляется в режиме Push и Pull.

GitLab – это полноценная платформа DevOps с открытым исходным кодом, предоставляемая в виде единого приложения, коренным образом меняющая способ совместной работы и создания программного обеспечения командами разработчиков, безопасности и операционных систем.

GitLab Runner – это агент, который собственно и занимается выполнением инструкций из специального файла .gitlab-ci.yml. Для корректной работы Runner его нужно связать с нашим проектом в GitLab.

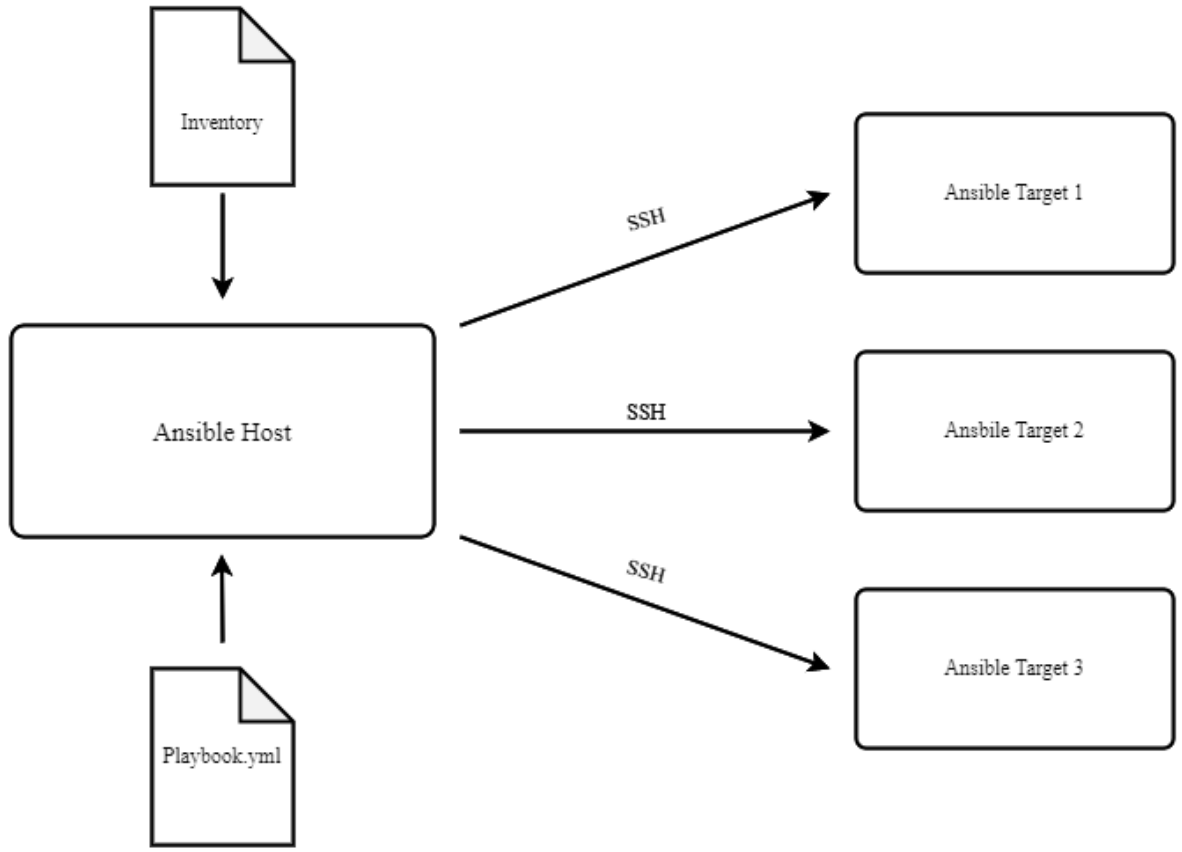


Рис. 1. Схема развертывания сервисов через Ansible

Приемущества GitLab:

- Встроенная функция CI / CD;
- Предлагает очень гибкие и универсальные функции;
- Выполняется проверка кода и улучшается совместная работа с помощью запросов на слияние;
- Происходит контроль версий (возможен откат на предыдущие стабильные версии).

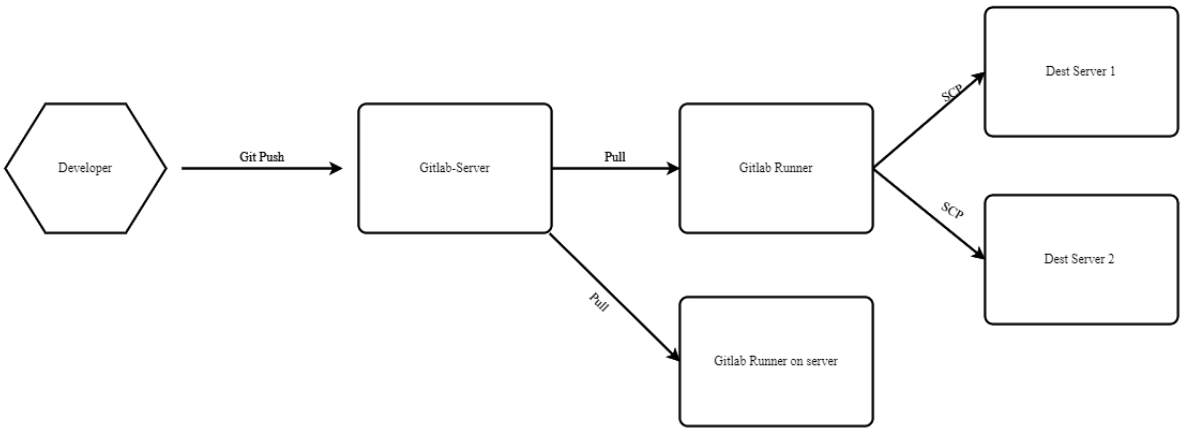


Рис. 1. Схема развертывания сервисов через GitLab CI

Но даже при таком автоматизированном подходе к развертыванию сервисов могут возникать различные проблемы [2].

- **Замена файлов**. Зачастую требуется обновление или замена конфигурационных файлов или перегенерация какого-то статичного контента. В этом случае пользователи могут получать ошибки, пока не произошло переключения трафика со старой версии ПО на новую. В случае же, когда развертывание закончилось неудачей, есть риск несовместимости файлов.
- **Изменение конфигурации.** Часто инфраструктурой могут пользоваться несколько специалистов, они также могут изменять конфигурацию этой инфраструктуры. Механизм отслеживания состояния должен оперативно оповещать об изменениях в инфраструктуре и предлагать различные методы по решению этих проблем.
- **Несовместимость различных версий.** При обновлении некоторых сервисов может произойти проблема несовместимости различных сервисов. Механизм должен иметь возможность откатить недавно обновленное приложение до версии, из-за которой не будет возникать конфликтов в работе инфраструктуры.

Требования к системе, которая будет поддерживать состояние инфрастуктуры:

1. Оперативное отслеживание изменений – механизм должен отслеживать изменения в инфраструктуре и сообщать об этих изменениях.
2. Возможность вернуть в исходное состояние – механизм должен предлагать вариант резервирования состояния, перед изменением инфраструктуры.
3. Реакция на изменение – механизм должен реагировать на изменение инфраструктуры, которые проводятся пользователями.

Методы поддержания состояния инфраструктуры

IaC (Инфраструктура как код) – это процесс управления и обеспечения инфраструктуры с помощью кода, которая исключает физическую конфигурацию оборудования. С помощью IaC, инфраструктура можно развернуть за считанные секунды, а масштабирование можно планировать исходя из нагрузок на инфраструктуру или отдельные ее части [3].

Существуют различные механизмы для поддержания состояние облачной инфраструктуры, рассмотрим такие как, Ansible, TerraForm, GitLab CI.

Ansible – безагентный инструмент для управления конфигурациями, позволяющая выполнять операции по настройке ОС и установке различного ПО. Ansible выполняет команды, описанные в файле конфигурации playbook.yml для списка серверов, указанных в файле inventory, данные сервера можно группировать по требованиям к установке. Ansible может работать в двух типах Push и Pull.

Terraform – это инструмент для безопасного и эффективного создания, изменения и управления версиями инфраструктуры. Желаемое состояния инфраструктуры описывается в конфигурационном файле, в нем же указывается провайдер, который будет выполнять работу.

Используются 3 команды:

1. Terraform init – инициализация провадйера;
2. Terraform plan – валидация конфигурационного файла;
3. Terraform apply – применение конфигурации.

GitLab Runner, это приложение запускает тесты и отправляет результаты в GitLab CI. GitLab CI – это сервер непрерывной интеграции с открытым исходным кодом, который координирует тестирование. Runner будет выполнять задания, поступающие из GitLab CI. GitLab определяет какому раннеру выдавать задания по тегам, которые выдаются этим раннерам.

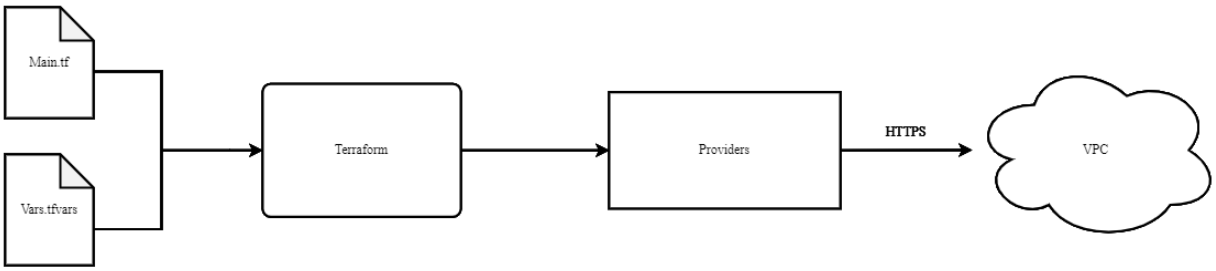


Рис. 3. Схема развертывания инфраструктуры через TerraForm

ТАБЛИЦА 1. Сравнение функциональных возможностей механизмов поддержания состояния инфраструктуры

Механизм поддержания инфраструктуры	Ansible	TerraForm	GitLab CI (GitLab Runner)
Язык описания инфраструктуры	Императивный и декларативный	Декларативный	Декларативный
Отслеживание изменений	В Ansible нет отслеживания изменений в инфраструктуре Изменения в инфраструктуре выполняются в ручном режиме	Все изменения в инфраструктуре, созданной Terraform, отслеживаются	Реагирует на изменение кода
Возможность вернуть исходное состояние	Не предусмотрена	Все объекты, созданные Terraform, будут воссозданы заново, если они будут удалены любым другим процессом	Возврат в исходное состояние возможен

Механизм поддержания инфраструктуры	Ansible	TerraForm	GitLab CI (GitLab Runner)
Реакция на изменения	Отсутствуют описательные сообщения об ошибках, когда дело доходит до отладки сложных сборников воспроизведения	Сообщает об изменениях в инфраструктуре	Реагирует на изменение кода
Поддержка различных оперативных систем	Плохая поддержка OS Windows	Нет проблем с поддержкой OS	Нет проблем с поддержкой OS
Шаблонизация	Обеспечивает полную поддержку создания шаблонов	Обеспечивает частичную поддержку создания шаблонов	Полагается на внешние способы шаблонизации
Изменчивость конфигурации	Позволяет изменять конфигурацию	Конфигурация не может быть изменена	Позволяет изменять конфигурацию

Вывод:

Анализируя возможности механизмов отслеживания состояния облачной инфраструктуры можно сделать вывод что Terraform подходит для отслеживания изменений инфрастуктуры, созданной Terraform, так как он уведомляет об изменениях, а также для отката изменений, которые были произведены неверно. В то время как Ansible подойдет для изменения конфигурационных файлов различных приложений без их удаления, а также для обновления приложений.

Список используемых источников

1. Ansible Documentation [Электронный ресурс]. URL:https://docs.ansible.com/ (дата обращения 20.02.2023)

2. Хамбл Джез, Фарли Дейвид. Непрерывное развертывание ПО: автоматизация процессов сборки, тестирования и внедрения новых версий программ : пер. с англ. М. : ООО «И.Д. Вильямс», 2011. 432 с.

3. Калашников А. О., Бугайский К. А. Инфраструктура как код: формируется новая реальность информационной безопасности. // Информация и безопасность. 2019. Т. 22. Вып. 4. С. 495–506.

Статья представлена научным руководителем, заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А.А. Зарубиным

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕХАНИЗМОВ ЗАЩИТЫ И АТАК В ОПЕРАЦИОННЫХ СИСТЕМАХ

А. Ю. Цветков

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Обеспечение безопасности в современной операционной системе в большей степени зависит от качества реализуемых механизмов, заложенных изначально при разработке. Такие ошибки могут нести, как непреднамеренный характер, так и преследовать определённые цели: не задокументированный сбор информации и статистике о системе, получение доступа к вычислительным ресурсам и др. В связи с тем, что вероятность существования в развернутой системе такого рода уязвимостей не равна нулю, необходимо провести анализ существующих базовых средств обеспечения информационной безопасности, а также противодействие неразрешенному поведению пользователей и процессов.

операционная система, контроль доступа, атака НСД, привилегии.

Существующие операционные системы (ОС) согласно принятым определениям [1, 2], представляет из себя собой комплекс программ, обеспечивающих управление и обработки входящих заданий. Как и прикладные программы, ОС разрабатывают множество программистов, которые могут допускать ошибки при проектировании и во время реализации функций системы. Такие недоработки могут быть использованы злоумышленниками различных целей: сбор информации о системе, получение несанкционированного доступа (НСД) и др. Для понимания рисков информационной безопасности необходимо провести анализ встроенных механизмов противодействия атакам основанных на ошибках при разработке ОС и соотнести с этими атаками.

Согласно [1, 2], взаимодействие с аппаратной частью, в ОС GNU\Linux представляется, как взаимодействие с файловой системой. Например, требуется передать последовательность байт через COM-порт, достаточно передать данные на поток ввода. Следовательно, обеспечение безопасности строиться на разграничение доступа к файлам и системным вызовам. Неограниченный доступ к ресурсам. Существует три основные модели разграничения доступа [5, 7]: дискреционная, мандатная модели и управление доступа на основе ролей. Дискреционная модель реализована в качестве базового механизма контроля доступа, две другие – расширенного. Рассмотрим оба варианта.

В качестве субъектов, к которым применяется разграничение доступа являются:

- владелец файла (UID);
- группа владельцев (GID);
- остальные пользователи.

Для всех субъектов определены три операции, совершаемые над файлами:

- чтение (R – Read);
- запись (W – Write);
- исполнение (X – eXecutable).

ТАБЛИЦА 1. Структура прав доступа файла

Владелец UID	Группа GID	Остальные Other
R (+/-)	R (+/-)	R (+/-)
W (+/-)	W (+/-)	W (+/-)
X (+/-)	X (+/-)	X (+/-)

Из выше сказанного следует, что доступ к файлу определяется по девяти атрибутам (табл. 1).

Разграничение доступа к системным вызовам построено на разделение все субъектов на две категории:

- привилегированные,
- непривилегированные.

К первой группе относиться только пользователь «root». Он имеет неограниченный доступ ко всем системным вызовам. Важно отметить, что некоторые системные вызовы, могут быть использованы только привилегированными пользователями. Если он непривилегированный, то ему доступен ограниченный список системных вызовов, вызов которых не приведет к нарушениям работы системы.

В ОС GNU\Linux существует два механизма повышения привилегий пользователя:

- запуск программы с битами SetUID (SetGID);
- использование привилегий Capability.

Обычная пользовательская программа работает при соблюдение следующего условия [5]:

$$\boldsymbol{EUID = RUID = UID} \quad (1)$$

Из выражения (1) следует, что запущенная программа имеет привилегии, которые есть пользователя, запустившего ее и имеющий присвоенный системой UID. Так же из выражения (1) следует, что рассмотренная выше команда «ping» не может быть выполнена, так как полномочий пользователя, определяемых идентификатором UID (UID > 0), будет недостаточно.

Для обхода этого ограничения в ОС GNU\Linux введена возможность запуска процесса с EUID, не равным RUID [5]. Следующей механизм может быть описан выражением:

$$\boldsymbol{RUID = UID\ user}; \quad (2)$$

$$\boldsymbol{EUID = UID\ owner\ file}, \quad (3)$$

где UID user – идентификатор пользователя, запустившего программу, а UID owner file – идентификатор владельца файла.

Для выполнения такого механизма, исполняемый файл должен обладать атрибутом SetUID. Обычно владельцем таких файлов является пользователь «root».

На смену ему пришел механизм разрешений POSIX (*Capability*). Он позволяет разбить привилегии суперпользователя на множество частей, которые можно разрешать и запрещать независимо друг от друга [5]. Разрешения делятся на две части:

- разрешения процессов;
- разрешения файлов.

Процесс ОС имеет три набора разрешений:

- доступные (*Permitted*);
- наследуемые (*Inheritable*);
- текущие (*Effective*).

Когда процесс порождает дочерние процессы, наборы разрешений дочерних процессов переноситься из родительского. Когда процесс порождает дочерний процесс, его новые наборы рассчитываются по определенным формулам (4), (5), (6).

$$pI' = pI; \tag{4}$$

$$pP' = fP \mid (fI \& pI); \tag{5}$$

$$pE' = pP' \& fE, \tag{6}$$

где (pI', pP', pE') – наборы разрешений дочернего процесса, (pI, pP, pE) – наборы разрешений родительского процесса, (fI, fP, fE) – наборы разрешений файла.

Хотя данные механизмы более гибкие, чем установка атрибута «SetUID», и позволяют ограничить возможности злоумышленника, но некорректное распределение разрешений является потенциальной угрозой безопасности системы.

Расширенные средства (*SELinux*), как и использование capability, позволяет более тонко настроить права доступа к ресурсам сети. Пользователям системы назначаются роли, таким образом, что они не смогут доступ к файлам или процессам, если не установлена специальная метка.

Для понимая, расширенных средства обеспечения безопасности, существует следящие термины:

- сущность (*identity*);
- домен (*domain*);
- тип (*type*);
- роль (*role*);
- контекст безопасности (*security context*);
- переход (*transition*);

• политика (*policy*).

Одним из важных компонентов являться контекст безопасности. Это набор атрибутов, которые связаны с объектами системы, такими как файлы, каталоги, процессы, сокеты и т. п.

$$identity{:}\,role{:}\,type(or\ domain). \quad (7)$$

Вторым важным компонентом – политика. Это наборы правил, управляющие списком ролей, к которым имеет право доступа пользователи, какие роли имеют доступ к каким домена, и какие домены имеют доступ к каким типам.

Из рассмотренного выше следует, что расширенная система управления доступом ОС GNU\Linux представляет из себя мощный механизм. Она позволяет более тонко решить задачи по обеспечению разграничения доступа к ресурсам ОС. Однако использование строгой политики в качестве основного, приведет к множеству проблем с приложениями, использующие нестандартные настройки.

Все существующие варианты атак НСД на вычислительные ресурсы можно разделить на три класса [6, 7, 8]:

• атаки, рассчитанные на использование ошибок в коде программы, вызывающем внешние команды;

• атаки, рассчитанные на организацию переполнения буфера;

• атаки, рассчитанные на перехват того или иного системного ресурса пользователя в некотором временном интервале.

В последствие такие программы были объединены в комплект утилит, получивший название «RootKits». Для дистанционного управления запускается нелегальный демон удаленного доступа, открывающий сетевой порт, который якобы «не замечают» модифицированные утилиты. При этом, чтобы сохранить максимальное приближение к оригинальному файлу, троянские утилиты имитируют дату создания файла и его размер [7, 8, 9, 10].

Однако по мере усложнения систем появлялись и более совершенные вредоносные программы. Был разработан новый класс руткитов, получивший название LKM-руткиты (*Loadable Kernel Module*, загружаемые модули ядра) [7, 8, 9, 10]. Это руктиты, поражающие ядро системы: они работают в режиме ядра, что позволяет им скрываться в системе намного искуснее руткитов пространства пользователя. В текущий момент именно такие руткиты в основном поражают системы на основе UNIX.

В большинстве случаем основной целью таких атак – повышение привилегий до уровня суперпользователя. А также главное проблемой является, что базовые механизмы ОС GNU\Linux не могут контролировать доступ при успешном проведение атаки. Расширенные механизмы могут решить эту проблему, благодаря тому реализованы отдельно от базовой. Но вредоносное программное обеспечение LKM Rootkit, может получить привилегии

уровня ядра системы. На таком уровне не базовые, не расширенные механизмы не работают. Поэтому важно сосредоточить внимание на LKM Rootkit, как самой опасной атаке типа НСД на операционную систему.

Список используемых источников

1. Вахалия Ю. UNIX изнутри: пер. с англ. СПб. : Питер, 2003. 843 с.
2. Максвелл С. Ядро Linux в комментариях: пер. с англ. К. : ДиаСофт, 2000. 488 с.
3. Хевиленд К., Грей Д., Салама Б. Системное программирование в Unix. Руководство программиста по разработке ПО: пер. с англ. М. : ДМК Пресс, 2000. 368 с.
4. Померанц О. Ядро Linux. Программирование модулей: пер. с англ. М. : КУДИЦ-ОБРАЗ, 2000. 112 с.
5. Манн С., Митчел Э., Крелл М. Безопасность Linux: Руководство администратора по системам защиты с открытым исходным кодом: пер. с англ. М. : Вильяме, 2003. 621 с.
6. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных // Региональная информатика «РИ-2018» : материалы конференции, Санкт-Петербург, 24–26 октября 2018 года. СПб. : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2018. С. 570–571.
7. Зимин А. Е., Косов Н. А. Обеспечение информационной безопасности в процессе создания и использования программ для ЭВМ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб. : СПбГУТ, 2017. Т. 1. С. 343–348.
8. Ковалев Д., Ковцур М. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 // Первая миля. 2014. N 3. С. 72–77.
9. Никитин В. Н., Ковцур М. М., Юркин Д. В. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи // Информационно-управляющие системы. 2014. N 1. С. 70–75.
10. Гераськина В. С., Сахаров Д. В., Пестов И. Е., Виткова Л. А. Методы и стратегии оповещения населения об угрозах возникновения кризисных ситуаций // Информационная безопасность регионов России (ИБРР-2017) : Материалы конференции, Санкт-Петербург, 01–03 ноября 2017 г. СПб. : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2017. С. 507–509.

Статья представлена научным руководителем, заведующим кафедры ЗСС СПбГУТ, кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.455.2
ГРНТИ 50.43.19

АНАЛИЗ МЕХАНИЗМОВ РАЗВЁРТЫВАНИЯ ОБЛАЧНЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ПОДХОДА ИНФРАСТРУКТУРА КАК КОД

А. В. Цурбелев, А. А. Швидкий

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Облачные системы в современном мире приобретают всё большую популярность в различных сферах инфокоммуникационных технологий. В данной статье рассмотрен подход развёртывания инфраструктуры, что позволяет решить проблемы конфигурирования, масштабируемости и взаимодействия различных её компонентов. Проведён сравнительный анализ существующих на данный момент инструментов развёртывания по различным критериям, их основные преимущества и недостатки.

инфокоммуникациооные технологии, облачный провайдер, Infrastracture as Code.

Влияние облачных вычислений на промышленность и конечных пользователей трудно переоценить: программное обеспечение, работающее в облачных сетях, изменило многие аспекты повседневной жизни. Используя облачные вычисления, стартапы и предприятия могут оптимизировать затраты и расширить свои предложения без самостоятельной покупки оборудования и программного обеспечения, и управления ими. Независимые разработчики имеют право запускать глобально доступные приложения и онлайн-сервисы.

Инфраструктура как код (IaC) – это подход к автоматизации развертывания инфраструктуры и её изменений путем определения желаемых состояний ресурсов и их взаимосвязей в виде кода. Код написан на специализированных, удобочитаемых языках IaC [1]. Фактические ресурсы в облаке создаются (или изменяются) при выполнении кода. Затем инструменту будет предложено взаимодействовать с поставщиком облачных услуг или системой развертывания от вашего имени, чтобы применить необходимые изменения, не используя веб-интерфейс поставщика облачных услуг. Код может быть изменен всякий раз, когда это необходимо – после выполнения инструмент IaC позаботится о поиске различий между желаемой инфраструктурой в коде и реальной инфраструктурой в облаке, предпринимая шаги для приведения фактического состояния в соответствие с желаемым.

Чтобы IaC работал на практике, созданные ресурсы не должны впоследствии изменяться вручную (неизменяемая инфраструктура), поскольку

это создает несоответствие между ожидаемой инфраструктурой в коде и фактическим состоянием в облаке. Кроме того, измененные вручную ресурсы могут быть воссозданы или удалены во время будущих выполнений кода, и все такие настройки будут потеряны. Решение этой проблемы заключается во включении изменений в код инфраструктуры.

Основными преимуществами IaC являются [2]:

- Развертывание: устранение ручного взаимодействия с облачными провайдерами означает более высокую скорость развертывания.
- Восстановление: выявление проблем в конфигурации может означать быстрое восстановление после сбоев.
- Согласованность: каждый раз ресурсы развертываются одинаково, что устраняет уязвимость инфраструктуры.
- Возможность повторного использования: повторное использование частей архитектуры инфраструктуры в будущих проектах.

Инструменты IaC можно разделить на три общих категорий:

- Средства управления конфигурацией;
- Средства шаблонизации серверов;
- Средства инициализации ресурсов.

В таблице 1 приведены критерии, по которым осуществлялось сравнение основных инструментов IaC.

ТАБЛИЦА 1. Сравнение способов использования популярных средств IaC

Инструмент	Тип	Исходный код	Язык/подход	Агент	Master-сервер
Chef	Управл. конфигурацией	Открытый	Процедурный	Нужен	Нужен
Puppet	Управл. конфигурацией	Открытый	Декларативный	Нужен	Нужен
Ansible	Управл. конфигурацией	Открытый	Процедурный	Нет	Нет
Cloud-Formation	Иниц. ресурсов	Закрытый	Декларативный	Нет	Нет
Terraform	Иниц. ресурсов	Открытый	Декларативный	Нет	Нет

Процедурный и декларативный языки [3]. Процедурный стиль – когда код пошагово описывает, как достичь желаемого конечного состояния. Декларативный подход: в коде описывается нужное нам конечное состояние. На первый взгляд подходы похожи, можно привести пример чтобы продемонстрировать различие. С помощью Ansible, в котором используется процедурный подход разворачивается 10 серверов. А потом повысилась нагрузка и необходимо увеличить количество серверов до 15. Теперь напи-

санный ранее процедурный код становится бесполезным; если просто запустить его снова, поменяв значение на 15, будет развернуто 15 новых серверов, что в сумме даст 25. В случае с декларативным кодом нужно лишь описать желаемое конечное состояние, а инструмент, например, Terraform разберется с тем, как этого достичь, учитывая любые изменения, сделанные в прошлом. Таким образом, чтобы развернуть еще пять серверов, Terraform поймет, что уже есть десять серверов и создаст еще пять.

Наличие или отсутствие центрального сервера. Для хранения состояния инфраструктуры и распространения обновлений требуется наличие так называемого master-сервера, который выкатывает обновления на все остальные серверы. Это даёт следующие преимущество: это единое централизованное место, где можно просматривать и администрировать состояние инфраструктуры. Однако из-за этого появляются серьёзные недостатки: дополнительная инфраструктура, необходимо разворачивать дополнительный сервер или даже кластер дополнительных серверов (для высокой доступности и масштабируемости), сделать так, чтобы клиент мог общаться с центральным сервером, а последний – со всеми остальными серверами. Это обычно требует открытия дополнительных портов и настройки дополнительных систем аутентификации.

Наличие или отсутствие агентов. Например, Chef, Puppet и SaltStack требуют установки своих агентов на каждый конфигурируемый сервер, вследствие чего требуется предварительная подготовка, требуется тщательно и регулярно обновлять программное обеспечение агента, обеспечить безопасность (открыть исходящие порты на каждом узле, настроить аутентификацию агента на сервере)

Совместное использование нескольких инструментов. В реальности при построении инфраструктуры, скорее всего, придется работать сразу с несколькими из них. Например, Terraform и Ansible при совместном использовании (рис. 1, см. ниже) позволяют быстро приступить к работе, поскольку не нужна никакая дополнительная инфраструктура (*Terraform* и *Ansible* – сугубо клиентские приложения). Средствами Terraform создаём не только серверы, но и базы данных, кэши, балансировщики нагрузки, правила маршрутизации, а с помощью Ansible устанавливаются и конфигурируются приложения которые будут взаимодействовать с инфраструктурой.

Подводя итоги, хочется сказать, что рассмотренный метод Infrastructure as Code для развёртывания IT-инфраструктуры имеет множество преимуществ. Он направлен на то, чтобы устранить путаницу в ручных процессах и сделать их более эффективными и продуктивными. Однако не стоит забывать и о трудностях, возникающих при его использовании.

Рис. 1. Совместное использование Terraform и Ansible

Список используемых источников

1. Брикман Евгений. Terraform: инфраструктура на уровне кода. СПб. : Питер, 2020. 368 с. ISBN 978-5-4461-1590-7.

2. Huttermann Michael. DevOps for Developers. Apress Berkeley, CA, 2012. 196 p. ISBN 978-1-4302-4569-8.

3. Morris Kief. Infrastructure as Code. O'Reilly Media, 2020. 430 p. ISBN 978-1-0981-1467-1.

Статья представлена научным руководителем, заведующим кафедрой ИКС СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным

УДК 004.056.57
ГРНТИ 81.93.29

МОДЕЛИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ МАШИННОГО И ГЛУБОКОГО ОБУЧЕНИЯ

С. И. Штеренберг

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Известно, что количество умных устройств в настоящее время неуклонно растет. Растет потребность их защищать, усложняются алгоритмы и методы атаки на системы, в которых заложены основополагающих элементы развития искусственного интеллекта. Имеется ввиду, что в ходе развития ИИ, становится нужной разработка единой методологии построения систем защиты информации, направленных на защиту любых интеллектуальных систем и устройств. Особое место в проектировании занимают «иммунные системы» кибербезопсности, в которые будут входит различные компоненты от «знания угроз» до обработки Больших данных. О моделировании таких систем и будет данная статья.

SIEM, IDS, искусственный интеллект, машинное обучение, глубокое обучение.

Начальное проектирование интеллектуальной системы обнаружения вторжений (далее – СОВ) планируется начать с внедрения «иммунных механизмов» кибербезопасности [1, с. 25]. Имеется ввиду, что будут использованы следующие компоненты:

1. Знание угроз (*X-Force IRIS*) – подробный анализ вредоносного программного обеспечения (далее – ПО);
2. Конечная точка (*BigFix*) – управляемое обнаружение и реагирование;
3. Программные агенты (далее – ПА) – управляемые компоненты проектируемых нейронных сетей (далее – НС);
4. Организационная ветвь защиты и аналитика, которая разделяется на:

a. Экосистема безопасности (App Exchange) – услуги безопасности для гибридного облака (облачные технологии, облачные системы);

b. Консалтинг в области безопасности (Командные центры X-Force IRIS);

5. Распределенная информационная система (далее – РИС), которая использует интеллектуальные технологии кибербезопасности (рис. 1).

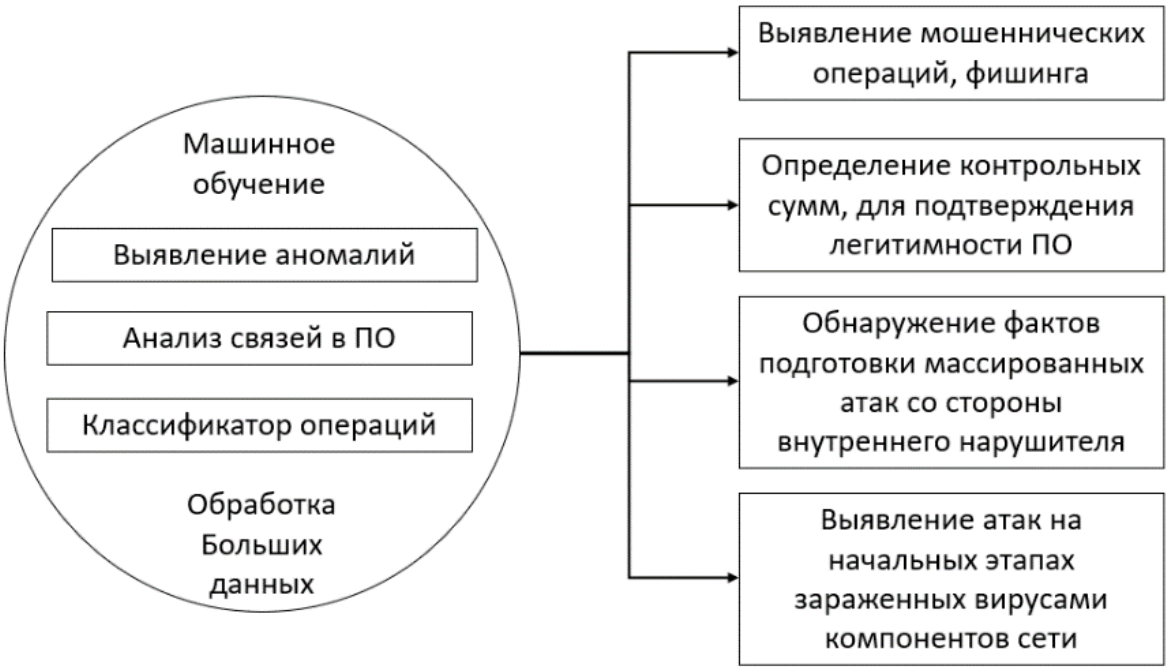


Рис. 1. Интеллектуальные технологии кибербезопасности

Стоит заметить, что для данного перечня технологий необходимо учитывать перспективные возможности ПО с сопровождающей его интеллектуальной СОВ. Для этого предлагается фрагмент перспективной системы обеспечения кибербезопасности (рис. 2) [1, с. 85].

Рис. 2. Фрагмент модели перспективной интеллектуальной СОВ на основе компонентов мошанного и глубокого обучения

Для фрагментарной модели характерны следующие стратагемы:

1) Мониторинг групповых массовых атак;
2) Накопление данных об иммунитете ПО в РИС;
3) Представление злоумышленников в типах воздействий;
4) Представление динамики возмущения и сценариев возврата поведения интеллектуальной СОВ;
5) Разработка схемы макро-восстановления НС в условиях постоянных кибератак;
6) Применение средств денотационной, аксиоматической и операционной семантики для всей НС;
7) Самовосстановление возмущенного поведения киберсистемы с НС при решении целевых задач по обеспечению кибербезопасности.

Одним из ключевых элементов в построении данной интеллектуальной СОВ, является представление самого ИИ как механизма. Имеется ввиду что понимается под ИИ и из чего будет состоять данное ПО для СЗИ. На рис. 3 представлена детализирующая концепция предлагаемых механизмов для ИИ [2, с.104]. Предлагаемое определение объектов РИС, может быть механически конструктивным для накопления данных в результате работы ассоциативной памяти для всего процесса ИИ в РИС.

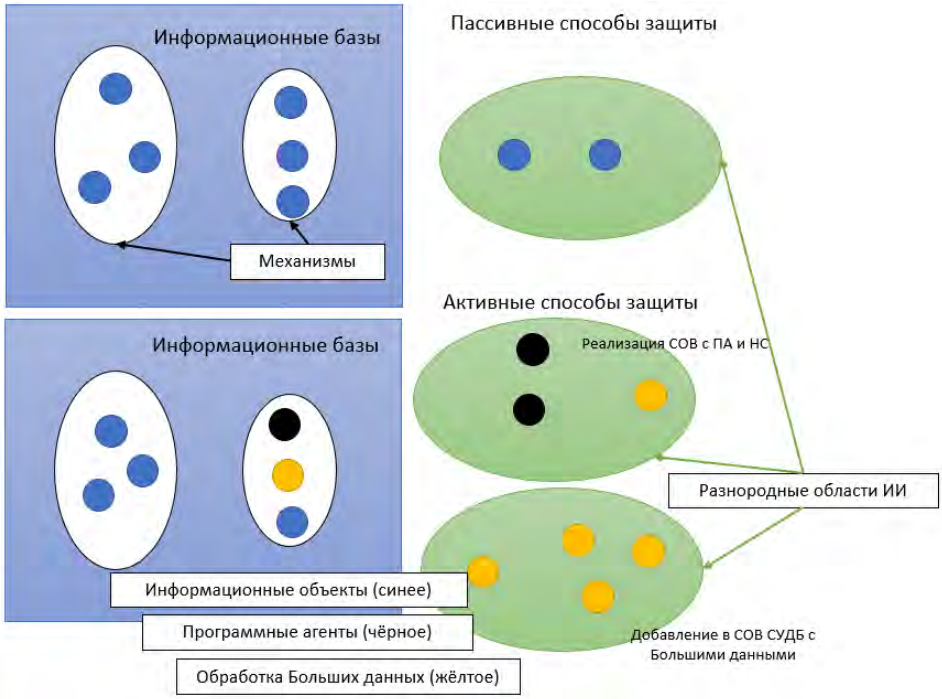


Рис. 3. Схемы взаимодействия элементов в модели интеллектуальной СОВ, формирование детализирующей концепции ИИ

В соответствии с представленной схемой для всей модели интеллектуальной СОВ выделяются:

1) Формы и классы представленных объектов;
2) Принципиальное описание механизмов;
3) Основные связи между механизмами и принципы согласования работы НС.

Благодаря схематичному и фрагментарному представлению модели интеллектуальной СОВ становится возможным представление данного концепта для вычисления свойств СЗИ в РИС. Для модели актуальными становятся характеристики: T – событие «положительного выполнения задач» СОВ, D – событие «отрицательного выполнения задач» СОВ. Под положительными эффектами будут являться успешно распознанные и устраненные угрозы, под отрицательными – менее успешно или не распознанные и не устраненные угрозы РИС. Строится для данной модели интеллектуальной СОВ примитивная задача по соответствующей формуле (1) [3, с. 105]:

$$P(D \mid T) = \frac{P(D \mid T)P(D)}{P(D \mid T)P(D) + P(T \mid \neg D)P(\neg D)} \quad (1)$$

Соответственно для всей СОВ будут формироваться особые альтернативные подходы к выбору граничных условий модели интеллектуальной СОВ в РИС. При наличии набора помеченных заранее данных и «предсказательной способности», в модели заработают механизмы определения ошибок I-го и II-го рода в целом для СОВ.

Для составления классификатора в модели интеллектуальной СОВ будет введено также понятие имплементации. Сам конструктор будет принимать входящие параметры – псевдосчетчика для использования при вычислении вероятности срабатывания корректного и некорректного обслуживания РИС при помощи СОВ. «Иммунные способы» [4, с. 107] необходимы для распространения принципов обнаружения вторжений по РИС. Предлагается в подобную модель внедрять такие элементы как:

1. Алгоритмы «с памятью», которые выполняют анализ события с учетом состояний СОВ;
2. Детерминированные алгоритмы для контроля поведения НС в РИС;
3. Нечеткие и нейронечеткие алгоритмы поведения НС для анализа последовательности событий в РИС для вычисления нужных пороговых значений для управления НС;
4. Корректирующие процессы, исключающие управление операторами.

В модели интеллектуальной СОВ важно понимать, что создание «абсолютно стойкой» СЗИ принципиально невозможно. В новой модели важно обозначить стоимостную составляющую [5]. Это достаточно подробно иллюстрирует формула (2), связывающая данные о рисках, процентную статистику по реализации мер защиты и издержки:

$$R = \sum_{i=1}^{n} (A_i B_i + C_i) < R_{\max}, \qquad (2)$$

где n – количество рисков (угроз); A – оценка риска; B – потери от риска; C – меры защиты; R_{max} – издержки.

Итого, имея базовые конструкты для сборки модели, вступит в силу инженерия машинного и глубокого обучения для интеллектуальной СОВ (рис. 4) [6]

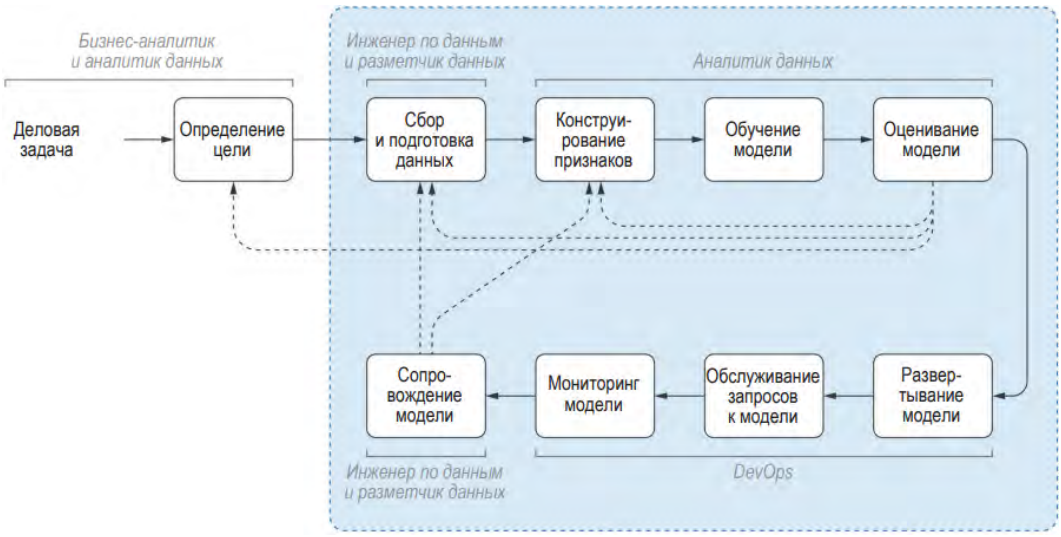


Рис. 4. Жизненный цикл СОВ с применением машинного и глубокого обучения в ней

Подведя итог, следует сказать, что разрабатываемая модель строится от принципов построения крупных РИС в рамках концепции Индустрии 4.0 [1, 3]. В данном моделировании будут присутствовать элементы:

1) Модель угроз для ИИ (Участие процессов глубокого и машинного обучения);
2) Модель ПО интеллектуального СОВ для синхронизации с компонентами систем ИИ (SIEM);
3) Классификация угроз для интеллектуального СОВ с компонентами ИИ.

Алгоритмы машинного и глубокого обучения будут принимать на входе специальные наборы обучающих параметров для интеллектуальной СОВ. Ориентироваться нужно будет на основе того, чтобы модель работала лучше, чем простой эвристический анализ для прочих СЗИ. Практически, механизмы ИИ (в виде машинного и глубокого обучения) будут реализованы в виде конвейеров, которые будут содержать последовательные этапы преобразования данных (в том числе и технологии Больших данных).

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, Соглашение №. 40469-05/2022-д от 30.06.2022 г.

Список используемых источников

1. Петренко С. А. Киберустойчивость Индустрии 4.0: научная монография. СПб. : «Издательский Дом «Афина», 2020. 256 с.

2. Рапопорт Г. Н., Герц А. Г. Биологический и искусственный разум. Ч.1. Сознание, мышление и эмоции. М. : Книжный дом «ЛИБРОКОМ», 2011. 182 с.

3. Грас Д., Data Science. Наука о данных с нуля: пер. с. Англ. 2-е изд., перераб. И доп. СПб. : БХВ-Петербург, 2022. 416 с.

4. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / под редакцией С.Ф. Боева. 2-е изд. Университет Иннополис. Иннополис: «Издательский Дом «Афина», 2018. 448 с.

5. Бондарев В. В., Введение в информационную безопасность автоматизированных систем: учебное пособие. М. : изд-во МГГУ им. Н. Э. Баумана, 2016. 250 с.

6. Бурков А. Инженерия машинного обучения / пер. с англ. А. А. Слинкина. М. : ДМК Пресс, 2022. 306 с.

A N N O T A T I O N S

PLENARY MEETING

Lobatsky I. Safe City – Practice and Innovative Solutions for the Benefit of Citizens. – PP. 5–12.
To ensure a safe environment for life in St. Petersburg, the state information system "Hardware and software complex "Safe City" was created, which included security systems and industry systems. Some of these systems are presented in this article.
Key words: "Safe city", automated systems, video surveillance, security, monitoring.

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Abramov S., Abramova E., Pavlov I., Pavlova M. A Brief Overview of Underwater Wireless Acoustic Communication. – PP. 13–17.
Based on the analysis and review of scientific works in the field of wireless underwater acoustic communication, the article presents a brief history of the formation of underwater acoustic communication and its development. The question of how the transmission speed and transmission distance changed in underwater acoustic communication is considered. Also, to solve the problem of the underwater acoustic channel, several modulation schemes were discussed and proposed.
Key words: underwater wireless communication, underwater acoustic communication, data transfer rate, underwater acoustic sensors.

Abramova E., Goryachkina A., Fedorov P., Fileva V., Shemyakin S. Methods to Counter the IControl REST API Vulnerability and Sophos Firewall Web Administration Console Vulnerabilities. – PP. 17–23.
This article describes a number of vulnerabilities related to the operation of information systems. In this article, the analysis of vulnerabilities and attacks performed by exploiting these vulnerabilities was applied. Examples of attacks performed by exploiting these vulnerabilities are given. The article also describes measures to counter these vulnerabilities. Based on what is described in this article, we can conclude that the most common causes of vulnerabilities, as a rule, include: errors in the design and use of software; unauthorized introduction and subsequent use of the software; the introduction of malware; human factor. Timely response to the

emergence of certain vulnerabilities and following the recommendations for their elimination contribute to maintaining the overall level of information security at the proper level.
Key words: Information Security, vulnerability, cyber attack, information system, monitoring.

Abramova E., Krasov A., Polaynicheva A. Trends in the Development and Security of IP Telephony. – PP. 23–28.
The digital age has created a culture where everything is available on demand. This is because businesses are experiencing a growing need for cost-effective communication solutions that can support enterprise mobility. This is where VoIP systems come in. This technology allows users to implement flexible communication systems. VoIP is based on IP and uses the Internet, which inherits all vulnerabilities. To do this, it is necessary to qualitatively protect every resource on the network. Considering specifically the telephone equipment, there are also a number of threats, namely interception of calls, representation by illegitimate users, number substitution and much more.
Key words: PBX, IP telephony, infrastructure, attack.

Avramenko V., Lukin I. Predicting the Delivery Time of Large-Volume Messages in a Data Transmission Network based On a Recurrent Neural Network. – PP. 29–32.
The article proposes an approach to the implementation of the function of predicting the delivery time of large-volume messages in transmission networks based on recurrent neural networks of long short-term memory. As a result of the work of an artificial neural network, predictive values of the message delivery time are formed. Based on the results of forecasting, if necessary, control actions are developed to ensure timely delivery of messages.
Key words: data transmission network, message, timeliness, neural networks, forecasting.

Agaev R., Tsvetkov A. Development of a Method to Counter NSD Attacks in the Application Memory. – PP. 32–35.
The topic of unauthorized access to application memory is one of the most relevant in the field of information security. Unauthorized access to memory can lead to leakage of confidential information, data modification, violation of system integrity and other dangerous consequences. To solve this problem, a method is presented to prevent unauthorized access to application memory using XOR encryption and obfuscation of program code.
Key words: *Application memory, exclusive OR, XOR, obfuscation, unauthorized access*.

Adam I., Kargina D., Kolesnik A., Nasedkin B. Exploring Polarization and Phase Fluctuations of Optical Radiation in Turbulent Atmosphere in CVQKD. – PP. 36–41.
Safe and secure information exchange between two parties is a main goal of quantum communication systems. In this aspect continuous variable quantum key distribution protocols are promising candidates of implementation in free-space communication scenario due to compact sizes, high key rates and low cost. As well these systems can be easily implemented in mobile devices, including self-driving cars and drones. In this work the influence of polarization and phase fluctuations on system parameters in turbulent atmosphere and methods of their compensation are investigated. Obtained results shows promising employment of continuous variables protocols in free-space quantum communication systems.
Key words: CVQKD, polarization fluctuation, phase fluctuation, fluctuation compensation algorithm.

Aleksandrova A., Volkogonov V., Potomako D. Overview of Data Diode technologies and its Application in Information and Telecommunication Networks to Ensure Information Security. – PP. 42–46.
In today's world, where information plays a key role in various areas, ensuring its security is a prerequisite for the successful operation of organizations. In this regard, tools for ensuring information security are becoming more and more in demand. One such tool is the Data Diode.
Key words: unidirectional data transfer, mission critical, Data Diode.

Aleksandrova E., Kushnir D. Analysis of the Characteristics of Blockchain Formation with Arbitrary Data Storage. – PP. 47–52.
Blockchain as a technology is becoming more and more popular and in demand, which determines the need for its research, including in the educational process. Often blockchain is seen as a system of records about the transfer of certain values, but its application can be much broader, for example, it can be used to place some arbitrary data or information about documents. To investigate the principles of adding data to the blockchain, a Linux-capable application has been implemented that forms a training demo blockchain. The solution allows to analyze the basic properties of the blockchain when placing arbitrary data directly or using a universal resource pointer.
Key words: blockchain, application development, data storage, digital signature.

Alekhin R., Pestov I., Smirnov D., Shelkoplyasova P. Security Analysis of OpenStack Cloud Infrastructure During Emulation of DDoS Attacks on Infrastructure Nodes. – PP. 52–55.
Today, the use of cloud computing is becoming one of the most popular solutions. Regardless of the cloud infrastructure deployment model, system security is paramount. In connection with the development of technologies, as well as the geopolitical situation, the number of attacks on the Russian segment of the network, such as bringing systems to a denial of service, is growing. The most common type of such attack is a Distributed Denial of Service attack. It is important to be aware of the scope of this type of attack on the cloud infrastructure. During emulation of an attack on infrastructure nodes, all instances will be affected by the attack.
Key words: cloud technologies, cloud infrastructures, OpenStack, DDoS attack, information security.

Alimetov K., Tsvetkov A. Development of a Secure Instant Messaging System. – PP. 56–59.
The report describes the implementation of software with a graphical interface for secure messaging. The main purpose of the implemented software product is the secure transfer of symbolic information and files. In the process, it became necessary to solve problems with: the correct display of messages on all types of devices - from a personal computer to a smartphone; fast loading of correspondence without having to refresh the page every time; protection against various types of attacks (XSS, CSRF, etc.) and the security of storing credentials. The main idea is to use: security functions and a low-level API to protect against various types of attacks and cryptographic signature of data; modern methods of adaptive layout; permanent connections for message transmission. For this purpose, a web application with a hybrid layout, a JS frontend (VueJS) and a Python backend (Django) was implemented, in which http requests and websocket connections are used as the main method of data delivery
Key words: information security, secure application development, web application, end-to-end data encryption, messaging system.

Al-Kerea Z., Muthanna A., Yasir H. Standardization and Use Cases for xURLLC in 6G Networks. – PP. 60–64.

The three main service categories supported by 5G are eMBB, URLLC, and mMTC. Future *applications are specified as URLLC utilities if they need to reliably transfer data from one endpoint to another during URLLC support. There are many approaches to improve the reliability of the LTE control channel, such as the DCI duplication approach. Together (mMTC) and (URLLC), which seem to have a similar future potential. 5G networks will focus on Enhanced Mobile Broadband (eMBB). The ability to anticipate extreme or frequent events, scale the system, and implement additional diversity improvements effortlessly, latency and reliability constraints based on the value of the information, is also mitigated by this perspective, which eliminates them all. The article focuses on xURLLC applications that is to take the lead in building mission-critical applications for 5G and 6G networks.*

Key words: 3GPP, 5G, LTE, sTTI, URLLC, and New Radio.

Al-Kerea Z., Muthanna A., Yasir H. 5G Smart Edge Application Scenarios. – PP. 65–69.

As edge computing processes data at the edges of a network rather than transporting it across long distances first, this will increase demand for edge computing. The objective of this paper is to navigate the whole benefits of caching and computing edge as proving that 5G should be 10 times more effective than 4G. Also proving that the 'Network Edge' seems to be quite different conceptually from Edge Devices and Servers. We also will be revealing What kinds of workloads are we thinking of when we refer to Edge Servers or the Network Edge. As a conclusion application with extremely low latency needs can now be supported by mobile devices and edge servers when they are connected directly through wireless. A state-of-the-art network architecture called MEC was created to handle the unprecedented increase in compute demand and the increased expectations for computing-based user experiences. It aims to provide Cloud Computing capabilities and IT services close to end users by redistributing a large amount of processing and storage resources towards the network edges.

Key words: UAV, 5G, Artificial Intelligence, RAN, intelligent edge computing.

Альотум Ю. М. А. Биометрическая и поведенческая аутентификация и мягкая биометрия с использованием динамики нажатия клавиш и мыши. – С. 70–75.

Зависимость людей от веб-приложения и мобильных приложения для хранения и обработки конфиденциальной информации, необходимость ее защищать от хакеров. Поведенческие биометрические данные, такие как динамика нажатия клавиш и мыши, которые используют индивидуальный ритм набора текста и щелчков, могут использоваться для улучшения существующих методов безопасности, которые являются эффективными и дешевыми. Из-за баллистической полуавтономной натуры для поведения писать текст и использованных мыши, их трудно имитировать и полезные в качестве биометрических данных.

Ключевые слова: биометрическая аутентификация, динамика нажатия клавиш, динамика мыши, мягкая биометрия, непрерывная аутентификация.

Andreeva A., Kanaev A. Analysis of the Use of Digital Doubles in Railway Transport. – PP. 76–79.

Currently, there are more and more prerequisites for the implementation of the concept of Industry 4.0 in various sectors of the economy and everyday human life, including rail transport. The digital twin is one of the leading tools of this transformation. The use of digital doubles for

various railway transport facilities will make it possible to optimize the operation of this structure, optimally assign service life, prevent malfunctions, emergencies, etc.
Key words: digital twin, railway transport, industry 4.0, digitalization, modeling.

Arsirii A., Bylina M. Overview and Comparative Analysis of Modern Pressure Sensors. – PP. 80–84.
The article presents the main types of pressure sensors that have found application in various areas of technology and electronics, mainly in optoelectronics. The important principles and characteristics of their operation, as well as the range and scope of application, are discussed. The article also provides a characteristic of material groups that are used to achieve the functional properties of pressure sensors with different levels of sensitivity, accuracy class, energy consumption, autonomous operation, and more.
Key words: pressure sensors, operating principles, pressure sensors, materials.

Ahapkina A., Sposob S. Application of Mathematical Operations on Elliptic Curves to the Diffie-Hellman Protocol in Order to Increase the Reliability of Keys in VPN. – PP. 84–88.
In VPN the Diffie-Hellman algorithm is used to calculate public and private keys, but the reverse logarithm method allows you to calculate all key pairs in advance. The use of a method based on mathematical operations on elliptic curves does not allow calculating all n-bit key pairs in advance and, thus, allows increasing the level of reliability when using shorter keys.
Key words: VPN, Diffie-Hellman, elliptic curves, algorithm, mathematical operations.

Akhrameeva K., Burdin P. Application of Steganography in the Level Editor. – PP. 88–93.
The article discusses the possibilities of embedding information in game environment objects using the Valve Hammer Editor level editor. The tools for modifying game levels available in the editor are described and the possibility of their application in the context of steganography is analyzed. Practical examples of possible implementations of information embedding in the game level are given.
Key words: steganography, information embedding, level editor, computer games.

Akhrameeva K., Gerling E. Image Integrity Monitoring with Digital Watermarks. – PP. 94–97.
In today's world, more and more information is transmitted over communication channels such as the Internet. In this way, for example, medical images, schemes, topographic maps are transmitted. For such images, the problem of integrity control (invariability) in transmission is relevant. To solve this problem, this paper proposes the use of digital watermarks.
Key words: digital watermark, accurate authentication, integrity, embedding algorithm.

Akhrameeva K., Zhilyakov G. Research on the Possibility of Embedding Information in Images using Gan-Systems. – PP. 98–102.
This paper presents the result of artificial intelligence analysis of textual information embedding into colored images and extraction of secret information from resulting image by means of AI. In the beginning the program asks for a path, to the color image in which you want to put the message, then the text of the message. The program, designed to embed additional information, independently determines the pixels to implement the embedding, while ensuring

optimal protection against attacks, the best quality of the stegoobject, the embedded information, as well as acceptable quality for the extraction of the embedded information. Using several algorithms, the program ends up with a finished image with a secret message. To extract the message, you only need to specify the path to the image. Implementation of this method of attachment using artificial intelligence improves the quality of the obtained image, increases the resistance of the obtained images to primitive methods of stegoanalysis, and AI-based methods of stegoanalysis.
Key words: general adversarial networks; steganography; machine learning; GAN systems.

Babich V., Esalov K., Kozlova A. Application of Neural Networks for Analysis Heterogeneous Traffic. – PP. 103–107.
The ability to accurately classify traffic by type (audio, text, etc.) and social network (Facebook, Telegram, YouTube, etc.) is an important feature for Deep Packet Inspection technology. This article compares various methods of classifying heterogeneous traffic using machine learning models and neural networks.
Key words: analysis, traffic, classification, machine learning, neural networks.

Babkov I., Fedorova Z. Investigating Ways to Improve the Effectiveness of using SIEM-Systems in Organizations' Corporate Network. – PP. 108–111.
The article discusses the issues of choosing the optimal way to monitor the level of information security in organizations based on comparative analysis. Presented an overview of existing information security measures in the context of import substitution. A map of national and foreign SIEM systems solutions is provided.
Key words: information security, information systems, protection, SIEM-systems, DLP-systems, information security policy.

Baboshin V., Nogin S., Tsyvanyuk V. The Specifics of Modern Requirements for the Reliability of Data Processing Centers Implementing Cloud and Edge Computing. – PP. 111–115.
The specific requirements for the reliability of modern stationary and mobile data processing centers implementing cloud and edge computing are considered and systematized. These requirements affect both general aspects of the technical readiness of objects of this class, as well as aspects of reliability, maintainability and the level of maintenance of their software and hardware. The fulfillment of the considered requirements will ensure the unconditional reliability of the functioning of data processing centers focused on the implementation of cloud and edge computing.
Key words: reliability, data center, cloud and edge computing, requirements, maintainability, maintenance.

Bakatov V., Pomogalova A. Blockchain Oracles as a Key Security Element for Conversion in Cross-Chain Processes. – PP. 116–120.
The active development of modern technologies, in particular blockchain technology, leads to the development of new ways to integrate systems with each other. Bridges, or converters, are the most necessary and popular tool for enabling interaction between different blockchain networks. These software solutions allow the process of exchanging tokens from one blockchain network into tokens of the same name in another without losing the original quantity. This mechanism will not only ensure the equivalence of tokens in different networks, but also the

seamless interaction of the systems. Further development of such solutions will allow more complex operations than transferring tokens from one network to another. However, the issue of trust in such software solutions is critical because they are centralized. This paper examines the possibility of using oracles as a key mechanism to ensure the security and trust in cross-chain interoperability systems.
Key words: blockchain, oracle, TON, Ethereum, smart contract, bridge.

Barakat A., Petriv R. Exploring Defense Mechanisms against DNS Farming Attacks. – PP. 120–124.
In this article, we will talk about the DNS pharming attack, as well as the most popular methods for applying this attack, as well as the main methods for protecting your systems from this attack. After studying the causes of this problem and the solution, I am going to implement a Java application that will be able to detect any DNS poisoning on Windows computers, and this application will also fix or remove any DNS records that were added by a malicious source.
Key words: DNS, Pharming, Websites, IP address, HTTP, HTTPS

Batenkov K., Katkov O. Measuring the Readiness Parameters of Digital Channels and Paths. – PP. 124–127.
The quality parameters of digital channels and paths are considered in the form of the readiness time obtained by adding all the readiness periods in the measurement interval, and the unavailability time – by adding all the unavailability periods. It is indicated that the elements of the path are determined by geographical, not architectural considerations, and their boundaries do not necessarily coincide with the transmission rate of the considered through-path.
Key words: communication network, telecommunication network, quality indicator, digital path, end-to-end path.

Batin E., Katasonov A. Investigation of Backdoor Detection Methods Based on Passive Monitoring of Access Channels. – PP. 127–131.
In the modern world, our devices are increasingly being attacked by intruders. One of the tools used by hackers is a backdoor. A backdoor is a malicious computer program that provides an attacker with unauthorized access to an infected device by exploiting a security vulnerability. This study considers the task of identifying a class of backdoors that provide interactive access on non-standard ports by passively monitoring the access channel.
Key words: viruses, backdoors, information security, virus detection.

Bashmakov A., Ogoreltsev P., Skorykh M., Creating a Pipeline with automatic Web Application Vulnerability Testing for the Gitlab Software Code Repository Management Platform. – PP. 132–135.
The paper is devoted to developing a solution for automating application vulnerability testing In this work, an automated solution developed based on the DevOps GitLab lifecycle tool is proposed, which aims to minimize the risk of application vulnerabilities. The peculiarities of making a pipeline with automatic vulnerability test using GitLab life-cycle implementation platform and semgrep static code analysis tool are considered in the work. The peculiarities of the test creation are given, the template for vulnerability signatures searching is written, the test vulnerable web application is created, the pipeline functionality is shown.
Key words: web application vulnerabilities, GitLab, semgrep, automation.

Bekkel L., Maksimenko M., Nekrasov S. Development of a hardware-software complex for processing sensor network data. – PP. 136–139.
In this article, we consider the possibility of building a scalable smart home system. The system consists of a sensor network, a software package for managing the network and providing an application program interface for working with it, and an application that provides data and allows the end user to control sensors. The task set in this work is to create a complete smart home system for home use, with the possibility of subsequent expansion and the use of inexpensive hardware. To solve this problem, prototypes of sensors were developed on the Arduino hardware platform, as well as a software package for processing and presenting information from sensors.
Key words: internet of things, smart home, architecture, internet of things system, development

Belaya T., Berezin A. Classification and Analysis of Network Traffic Using Clustering Methods. – PP. 140–145.
The article deals with the solution of the problem of IP – network traffic classification using clustering methods. Classification of network traffic is necessary to solve problems of control and optimization, separation of traffic and data, as well as when making decisions for subsequent processing. Network traffic classification is used to solve specific problems, such as prioritizing the bandwidth for individual traffic, establishing rules for network management, ensuring network security. To solve the problem of network traffic classification, we consider the algorithms of cluster analysis, statistical methods of the parameters of flows extracted from the traffic, formulate the selection criteria and conditions of applicability of the classification method.
Key words: clustering, classification, network traffic.

Belozerov K., Kislyakov S. Distribution of Network Resources in a 5G Network Based on a Gaming Approach. – PP. 145–150.
Standardization of network slices, which are an important element of resource allocation in 5G networks, is considered a critical issue in the scientific community. In this regard, this study presents a method for allocating cache storage resources using game theory and bankruptcy games to improve the quality of the end user experience.
Key words: game theory, network slicing, 5G networks, network management.

Belyaev D., Rogalnikov I. Using the Capabilities of OpenSSL to Secure Instant Messaging System. – PP. 150–153.
This article focuses on the development of instant messaging system. To ensure security, it is proposed to use the capabilities of OpenSSL in operating system Astra Linux, and crypto library PyGOST. To establish trust in certificates, it is proposed to embed elements of Public Key Infrastructure in client and server software.
Key words: public key certificate, instant messaging system, key generation.

Belyaev P., Zikratov I., Zikratova T., Neverov E. Using the Bee Algorithm to Control UAV Swarms for Terrain Monitoring. – PP. 153–158.
The methods for controlling swarms of unmanned aerial vehicles during terrain monitoring planning are considered. It is shown that it is reasonable to use metaheuristic algorithms that can provide a reasonably good solution to the optimization problem in order to save resources.

The authors propose a two-stage algorithm for solving the problem of finding objects in the terrain, based on a beebee algorithm. The first stage involves preliminary monitoring of the area and mapping of "promising sites". In the second stage, swarm agents explore the identified "promising" areas. The results of the work can be useful to developers of algorithms for control of self-organizing UAV groups.
Key words: group robotics; swarm algorithms, metaheuristic algorithms; bee algorithm; monitoring; drones.

Berezin A., **Kuznetsov M.** Neural Network Training Platform Based on Binary Classifier. – PP. 158–162.
This report discusses a platform for practical training of students in neural networks based on a binary classifier. In the modern world, neural networks are ubiquitous for use in solving various problems, while they are quite complex technology, and this platform was developed for a better understanding and greater involvement of students in the basics of simple models of neural networks. One of these models are binary classifiers, on the basis of which you can clearly understand which parameters in one way or another affect the operation of neural models and apply this knowledge in the future.
Key words: neural networks, classifier, training platform.

Berezkin A., Vasiliev S., Nikolaeva L. Loss Function Analysis for Training Intelligent Face Identification Systems. – PP. 163–166.
The article discusses the concept of a loss function regarding the use of these functions for identifying persons in transport security systems. The loss function is a mathematical function that is used to calculate the errors of the function when comparing the answer received from the model with the correct answer. The higher the value obtained, the worse the face recognition model performs. The article provides an overview of the loss functions applicable to training a face recognition pipeline and notes the optimal solutions, taking into account the specifics of working with a large number of faces.
Key words: face recognition, face detection, biometrics vector, loss function, softmax loss, margin-based loss.

Berezkin A., Do P. H., Kirichek R. Overview of Solutions based on Artificial Intelligence to Minimize Delay in Satellite Communication Networks. – PP. 167–171.
This paper provides an overview of various solutions that leverage artificial intelligence (AI) techniques to minimize delays in satellite communication networks. The high latency associated with satellite communications can significantly affect the performance of various applications, such as real-time video streaming and telemedicine, leading to poor user experience. The use of AI in satellite communication networks can help overcome these challenges by optimizing various network parameters, such as bandwidth allocation, routing, and error correction. This paper discusses several AI-based solutions, including machine learning and reinforcement learning techniques, that have been proposed to enhance the efficiency and reliability of satellite communication networks. The advantages and limitations of these solutions are also discussed, along with potential areas for future research.
Key words: satellite communication network, delay minimization, artificial intelligence, predictive modeling, quality of service.

Birikh E., Bogomedova K., Sakharov D. Security Model for Medical Commercial Institutions. – PP. 172–176.
In this article, a security model for medical commercial enterprises was compiled, based on the threat model, the violator model and existing laws and decrees.
Key words: information security, security model, viruses, information leakage, data leakage, federal security service of Russia (FSB of Russia), Ministry of Finance of Russia, information security department.

Birih E., Saharov D., Tarov E. Application of Cryptographic Methods of Information Protection in Open Telecommunication Channels. – PP. 177–180.
The article discusses modern methods and algorithms on which cryptographic methods of information protection are based when it is transmitted over open telecommunication channels. The analysis of these methods is carried out. As a result of the analysis, measures are proposed to improve the security of information transmitted through open communication channels.
Key words: information security, cryptography, communication channels.

Bogomaz M., Kushnir D. Analysis of Possible Attacks on the Multilevel Blockchain Model. – PP. 181–185.
Because of its characteristics, blockchain technology is rapidly gaining popularity when it comes to securing various applications and services. This leads to the need for in-depth research into the security of blockchain itself. Because blockchain is a collection of different technologies, security issues at each level of the blockchain architecture must be considered separately. The study analyzes attacks on the multilayer blockchain model and proposes appropriate countermeasures against these attacks.
Key words: blockchain, multilevel blockchain model, blockchain attacks, blockchain security.

Bolotov T., Goikhman V. Analysis of the Principle of Establishing a Voice Connection in the WhatsApp Application. – PP. 186–190.
The purpose of the study is to analyze traffic in the WhatsApp application. In this article, based on an experiment, you need to determine the scenario for establishing a connection between a client and a server using the STUN protocol. The main attention is paid to the algorithm of the STUN protocol and the TURN server. The scientific novelty of the work lies in the fact that it uses statistical methods that have not previously been used to conduct such studies. As a result, during the experiments, an algorithm for establishing voice connections using instant messengers was identified using the WhatsApp application as an example.
Key words: analysis, traffic, WhatsApp, STUN, TURN.

Borovskaya Y. Analysis of Sensor Data Caching Policies and Algorithms in Information-Centric Networking ICN. – PP. 190–194.
The architectural and information integration of the Internet of Things and information-centric networking ICN provides a number of obvious advantages in terms of efficient storage and prompt provision of sensory data to the user. Analysis of Internet of Things traffic, as well as existing caching policies and algorithms for replacing data in cache memory shows the need to use new semantic algorithms to control the caching of sensory data. The task arises of de-

veloping a generalized algorithm for replacing data in cache memory, taking into account semantic tags, as well as in the future the task of analyzing and modeling the relevance status of this data.
Key words: information-centric networking ICN, content caching, CDN Cache, caching policy.

Bugrova E., Pestov I., Romanyuk E., Shestakova V. Monitoring of Cloud Infrastructure as a Means of Detecting Attacks on the Information System. – PP. 194–199.
Cloud infrastructures, like any other information systems, are objects of possible attacks by malicious actors. To detect and prevent such attacks, monitoring and analysis tools for cloud infrastructure are necessary. This article discusses monitoring cloud infrastructure using the Grafana system and its role in detecting attacks on information systems.
Key words: monitoring system, cloud infrastructure, attack detection, information security.

Budarny G., Dyusmetova A., Kazantsev A., Krasov A. Social Engineering: its Methods and Ways of Protection. – PP. 200–204.
In the modern world, where information is one of the most important resources, the issue of ensuring its security is extremely relevant. This is due to the steadily growing number of ways to steal personal data, the emergence of more and more sophisticated means to achieve this goal. The article considers such a technique as social engineering: its methods and methods of protection in each situation.
Key words: social engineering, information protection, information security, phishing, obfuscation, psychology.

Budarny G., Kamalova A., Krasov A. Comparison of Static and Dynamic Code Analysis and their Role in the DevSecOps Methodology. – PP. 204–208.
In today's world, security has become a top concern for companies. Cloud computing, Internet access, globalization and the use of mobile phones have changed the basic scenario that companies are used to operating in, adding many security risks to their systems and information. DevSecOps is a new work methodology that enhances the DevOps philosophy by adding a security component throughout the development process and helping to create a security culture at all levels of the company.
Key words: DevSecOps, development, information security, application security, secure development.

Bylina M., Glagolev S. Evaluation of Communication Quality in Modern High-Speed Fiber-optic Systems. – PP. 209–214.
In modern digital high-speed fiber-optic communication systems (FOCS) of large extent using the technology of dense multiplexing in the wave domain (DWDM), multilevel formats of amplitude, phase and combined quadrature-amplitude modulation (QAM) are used for signal generation, and coherent methods are used for their reception. To assess the quality of communication in the FOCS, the error coefficient or the Q-factor associated with it can be measured. The paper considers the features of determining these parameters in FOCS with QAM.
Key words: fiber-optic communication system, DWDM, quadrature-amplitude modulation, QAM, coherent reception, communication quality, error coefficient, Q-factor

Bylina M., Fraz A. Modern Optical Spectrum Analyzers and Possibilities to Improve their Characteristics. – PP. 214–219.
Optical methods of information transmission are widely used and are in great demand in telecommunications. To control the parameters of optical components and evaluate the quality of communication in fiber-optic systems, optical spectrum analyzers are needed. This article describes the areas of application, classification, parameters and principles of operation of spectrum analyzers. A comparative analysis of modern spectrum analyzers is presented, proposals for improving their characteristics are formulated.
Key word: optical spectrum analyzer, OSA, spectrum analyzer, spectrometer, OSA parameters, Fourier spectrometer, interferometer, spectrum, resolution improvement.

Valeev D., Kotenko I. Analysis of Approaches to Automatic Processing of Fuzz Testing Results. – PP. 219–224.
Modern approaches to the implementation of fuzz testing are so efficient that they often exceed the capabilities of the analysts responsible for their processing. These factors lead to an increase in the time between the detection of a defect and its correction, non-optimal prioritization of processing tasks, and the influence of the human factor. The paper analyzes available approaches to automating the processing of fuzz testing results and possible directions for the development of these techniques.
Key words: fuzzing, automatic defect processing, defect localization.

Vasilyev N., Gegelskiy M. Research of Issues of Relief Visualization for Solving the Problems of Radio Engineering. – PP. 225–229.
When solving radio engineering problems, one may encounter difficulties that cannot be solved without the use of a three-dimensional terrain model. This problem is relevant to this day, since solving problems by modeling requires not only correct mathematical calculations, but also requires taking into account the terrain on which the simulation takes place.
Key words: *relief, radio engineering, research.*

Vasin A., Elagin V. Analysis of Allocation of Virtualized Resources for Network Slices in Mobile Communication Networks. – PP. 229–233.
The emergence of a Network Slicing paradigm for 5G networks provides new opportunities for service providers to share cloud infrastructure. This article analyzes the existing models of dynamic scaling of virtual network function resources for Network Slicing. By implementing these models, cloud infrastructure providers can use predictive technologies to dynamically allocate network resources while meeting the service level agreements of network segments. LSTM models are used to predict the utilization of virtualized infrastructure resources. A generalized model of automated resource scaling based on the architecture of network functions virtualization is considered.
Key words: NFV, SDN, 5G, Network Slicing, ML, MANO, VNFM, NFVO, Bi-LSTM.

Vedenkin D., Gilfanova A. Application of the Quasi-QAM Modulation Method in the Problem of Increasing the Noise Immunity of a Digital Communication Channel. – PP. 234–258.
Wireless communication systems are becoming increasingly popular due to the fact that they provide high data transfer rates and low latency in real-time tasks. The development of existing

digital communication systems, improving the quality of communication, as well as offering new services, are associated with the need to solve problems of electromagnetic compatibility and stable operation in a complex signal-interference environment.
Key words: mathematical modeling, modulation, quadrature amplitude modulation, signal constellation, white noise, color noise.

Veras N., Konkov V., Makhonina E., Polyanicheva A. Vulnerability Study of the Microsoft Edge Browser for Windows Operating System BDU:2022-06064. – PP. 238–241.
The article discusses the vulnerability of the Microsoft Edge browser of Windows operating systems BDU:2022-06064, provides a description of current threats based on the exploitation of the vulnerability. Descriptions are given of ways to prevent information security violations, as well as recorded cases of network attacks carried out when an attacker exploited a vulnerability.
Key words: information security, web browser, Windows, information loss.

Веселов Д. А., Оводова Т. А., Веб-конструктор инфографики для торговых платформ. – С. 242–245.
В статье представлено новое приложение для повышения конкурентоспособности товаров с целью повышения коэффициента продаж и заинтересованности покупателей. Целью данного исследования является повышение коэффициента продаж товаров за счет использования разработанного веб-сервиса.Акцент делается на торговых платформах и возможностях увеличить продажи партнеров путем размещения красочных и информативных фотографий предлагаемых товаров. Предлагается создать веб-сервис инфографики, который позволит не только редактировать фотографии, загруженные локально, но и загружать все фотографии товаров с маркетплейса по артикулу и легко загружать их на маркетплейс.
Ключевые слова: веб-конструктор инфографики, веб-сервис инфографики, загрузка фотографий товаров, снижение трудоемкости и временных затрат, синхронизация с торговой платформой, использование API-ключей партнеров.

Vetrov N., Smirnov D. Security Threat Analysis. – PP. 246–250.
This article provides a brief overview of common vulnerabilities in SCADA systems used for process control. The main types of vulnerabilities are described, such as authentication, encryption, configuration errors, lack of security updates, and hardware and software components. The causes of these vulnerabilities, such as the use of weak passwords, suboptimal security policies, programmer errors and others, are considered.
Key words: SCADA, vulnerabilities, authentication, encryption, configuration, security updates, hardware and software components.

Vivchar R., Rumyantsev S. Software Development Methodology for Evaluating Risk Indicators of Management Decisions in Creating Modern Data Transmission Systems. – PP. 250–254.
The article presents a software development methodology for evaluating risk indicators of management decisions in creating modern data transmission systems. A methodology for assessing risk indicators has been defined. A software structure has been proposed and its technical part has been justified.
Key words: risk, simulation modeling, management decision, quality, situation.

Vikulov A., Skorobogatova S. A Study of the Error Vector of QAM Constellation Dependence on the Measured Signal-to-Noise Ratio in IEEE 802.11 Network. – PP. 255–259.
The paper focuses on determining the dependence of the error vector parameter on signal-to-noise ratio. The article reviews the signal quality parameters such as error vector magnitude and signal-to-noise ratio. The necessity of conducting an experiment with spectrum analysis is discussed. The results of the experimental study are used to investigate the type of correlation between the signal-to-noise ratio and the error vector magnitude.
Key words: EVM, RCE, SNR, spectrum analysis, constellation diagram, QAM, Wi-Fi.

Vinnikov S., Kovtsur M., Trezorov V. Investigation of the Impact of Attacks on a Wireless Network Based on Cisco Equipment. – PP. 260–265.
In today's realities, wireless networks occupy a significant place in everyone's life. This is due to the rapid growth of user needs, which in turn is the reason for the constant development of computers and telecommunications devices. With the rapid development of Wi-Fi equipment, an increasing number of errors and vulnerabilities are coming, which can have an extremely negative impact both on the work of ordinary users and on the entire business infrastructure due to the emergence of new threats to the security of wireless equipment. This paper presents a report on the study of the impact of various attacks on the infrastructure of Cisco wireless devices, which will give a general understanding of the operation and vulnerabilities of wireless equipment operating according to IEEE 802.11 standards.
Key words: wireless local area networks, network security, WLC, information attacks, Wi-Fi, denial of service.

Vitkova L. The Model of Information Attacks in the Media Space. – PP. 265–268.
In the modern mediatized world, the most important meanings are formed in the mass consciousness through the channels of mass media and social networks. At the same time, the problem of detecting information attacks in social networks is becoming particularly relevant. There is a question of revision of terminology, classification, identification of signs of information attacks, development of models, techniques and algorithms for their detection. The paper proposes terms and definitions that make up the conceptual apparatus common to the socio-humanitarian and technical sciences. A model of information attacks is also presented, which allows us to proceed to the selection of signs for detection and form requirements for algorithms for analyzing and evaluating information attacks.
Key words: information attacks, information space, information attack vector, media resource, social network analysis.

Vitkova L., Zrelova A. Modern Problems of Personal Data Protection in the Russian Federation. – PP. 268–272.
This article is devoted to the problem of personal data protection in the Russian Federation. Particular attention is paid to cybercrimes aimed at stealing and distributing databases of personal data of users that have occurred over the past year. It is noted that at the moment there is a tightening of requirements for personal data operators aimed at strengthening the protection of personal data subjects and ensuring privacy. The paper analyzes the changes made to the legislation of the Russian Federation on personal data after the frequent attacks on large companies and the leakage of personal information of users.
Key words: cyber attacks, personal data, analysis of legislation, leaks of personal data.

Vitkova L., Leshukova A. Detection of Objects in Images. – PP. 272–275.
Computer vision technologies make it possible to make life safer in modern realities. It only grows over the years. According to experts, the need for data technology will continue to grow. This is a fairly developed area, both in terms of productivity and quality. One of the most popular sections is Object Detection (object detection) - the definition of an object in an image or video stream. Over the past decades, it has been proposed to use a large number of methods and solutions to this problem. The detectors are based on a variety of computer vision algorithms, the main task is to teach the machine to recognize objects. This article will talk about one of the most applications of ultra-precise neural networks - the detection of objects in images. The article contains several data sets and presents metrics for evaluating the quality of detection. Several basic neural network type architectures have also been used for object detection, some of them have been disassembled and tested in practice.
Key words: detector, computer vision, metric, image, neural networks.

Vladimirov S., Volkov V. Control and Synchronous Audio Output Device for Dsee-65H Holographic Fan. – PP. 276–280.
The paper presents the structure and principle of building a control and synchronous audio output device for the Dsee-65H holographic fan. A block diagram of the control device has been developed and options for its implementation based on various hardware platforms have been proposed. Taking into account the peculiarities of the operation of the holographic fan, the principle of synchronous output of audio data was developed and tested. Directions for further development of the control device are presented.
Key words: holographic fan, data output timing, single-board microcomputer, Raspberry Pi.

Vladimirov S., Skakunov I., Trofimov V., Fischev E. The Use of the Gold Code for Network Coding in the Two-Way Relay Channel. – PP. 280–284.
The paper presents the option of applying an error correction Gold code formed by two maximum-length codes for network coding in a two-way relay channel. The principle of restoration of errored data with consideration to the Gold encoding and the network coding principles is shown. Mathematical modeling has been performed and probabilistic characteristics of various options for decoding the codeword are presented.
Key words: maximum-length code, Gold code, network coding, two-way relay channel.

Volkogonov V., Kazantsev A., Krivets A. Creation of the Alarm System Based on IoT Devices in the Yandex Smart Home Environment. – PP. 285–289.
To date, the high rate of development of cyber-physical systems allows integrating progressive engineering methods of protection into one's life, which leads to the limitation of the market for a large number of smart home systems and devices. But systems built for installation usually have limited functionality and the inability to fix or modify the device for environmental and safety conditions. In this regard, the idea arose to create their own burglar alarm system, which was combined with the "smart home" system from Yandex. The work goes through the process of independent implementation of the security system, its capabilities and ways to improve it, as well as the search engine of the project.
Key words: VK API, cyber-physical systems, burglar alarm, NodeMCU, OrangePi, smart home.

Volostnykh V., Vorobyov P., Kononov P. Processing by Technical Means of Official Documents of Limited Distribution. – PP. 289–293.
The article deals with the issues of processing official documents of limited distribution and official documents containing official secrets in the field of defense that are not classified as state secrets. The requirements for information systems designed for processing official documents of organizations and enterprises are outlined. The issues of transition to secure electronic document management are considered. Ways to ensure the security of documented information are proposed. The article may be useful to the management staff of enterprises and specialists of information security departments, as well as students and postgraduates of educational organizations.
Key words: information security, protection of information systems, information of limited distribution, official secrets in the field of defense, training of specialists, official documents, electronic document management.

Volostnykh V., Kononov P. Trends in the Development of the System of Interdepartmental Electronic Document Management in Higher Educational Organizations. – PP. 294–298.
The article discusses the tasks and objectives of interdepartmental electronic document management, discusses the features of the MADO system in relation to higher educational organizations, describes the current state of development and implementation of the system. Variants of the architecture of solutions for the implementation of MADO are proposed. The authors consider the features and advantages of the transition to interdepartmental electronic document management. The main prospects of development in this direction are also described.
Key words: interdepartmental electronic document management, electronic document management system, information security tools, higher educational organization, electronic signature.

Vorontsov A., Shemyakin S. Description of the Structure of a Secure Communication Channel with Authentication. – PP. 299–303.
In data transmission networks, the protection of transmitted messages is of great importance. Violators may use various methods of substitution of true messages or impose false messages. Message authentication mechanisms are used to protect against such actions. The article proposes the structure of a secure communication channel with noise-resistant coding and authentication to protect against the imposition and substitution of messages.
Key words: information security, secure communications, data transmission networks, authentication, cryptography.

Voroshnin G., Drepa V., Kovtsur M. Software Development for Penetration Testing of Wireless Networks of the IEEE 802.11 Family. – PP. 304–308.
Wireless Wi-Fi networks have become an integral part of almost everyone's daily life. They are used in the smallest home networks as well as in large corporate networks. However, very few users of wireless networks think about how is secured the data they transmit. The number of information security incidents increases every year. One of the most common targets for attacks is network equipment, which, in particular, provides clients with connectivity over IEEE 802.11 family networks. Along with the continuous improvement process of protocols and network security standards, the mechanisms of circumventing or breaking these standards are also being upgraded. Even the most advanced network equipment is susceptible to the simplest types of attacks that significantly reduce the quality of service. In this regard, the software development

for IEEE 802.11 family networks testing is relevant both to verify the network stability and to create methods to combat real-world cases of attacks.
Key words: information security, wireless network security, testing Wi-Fi networks.

Vybornova A., Elagin V., Korolev D. Implementation of the Docker Container System in Fog Computing. – PP. 308–313.
Modern devices involve an increasing reduction in their physical size, as well as a change in the technology implemented on their basis. The problem of the transition of modern networks based on virtual machines to an infrastructure based on Docker technology is the irrational use of microcomputer resources. Docker requires high performance, additional add-ons on the system leads to increased load and resource consumption. This article discusses different optimization techniques to speed up container deployment.
Key words: Docker, containers, Kubernetes, layers, image, orchestrator, fog computing.

Vybornova A., Leonova A. Review of Augmented Reality Glasses Models. – PP. 313–317.
The article provides a description of some of the popular augmented reality glasses from different manufacturers, namely Epson, Rokid and Microsoft, and their analysis. Various approaches to the development and creation of AR glasses are considered. The main components of augmented reality glasses necessary for their creation, relevant at the beginning of 2023, are derived.
Key words: AR glasses, augmented reality, augmented reality glasses.

Vybornova A., Nesterova Y. Image Reproduction with Augmented Reality Glasses: Technologies and Devices. – PP. 317–321.
The article discusses the main areas of application of augmented reality technology. The types of technology are presented and their characteristics are given. An overview of devices that support this technology and are on the market at the time of writing is given. The relevance of carrying out developments in the field of augmented reality is substantiated.
Key words: augmented reality, virtual reality, AR glasses, AR content, image reproduction.

Gavkalyuk B., Sineshchuk M., Shestakov A. Complex Methodology and Algorithms for Synthesis and Evaluation of Rationality of Options for Building Architectures of Departmental Organizational and Technical Systems of the "Cyberpolygon" Class. – PP. 322–327.
The article is devoted to the issues of methodological and algorithmic support of the process of formation of departmental organizational and technical systems of the "cyberpolygon" class. The procedures for the synthesis of an organizational and technical system are considered, taking into account the distribution of functions among the components of the departmental cyberpolygon, depending on the accepted version of the architecture and the strategy of its phased development (improvement, modernization). The procedures for evaluating the rationality of options for building departmental cyberpolygon architectures are investigated, taking into account the different contribution of quality criteria for solutions for the construction of such systems from the composition of multi-vector groups of quality criteria. A comprehensive methodology is proposed that can be used for a wide class of practical tasks in applied scientific research of organizational and technical systems, their functional subsystems, design and justification of development.
Key words: cyberpolygon, synthesis, complex methodology, algorithms.

Geraskin V., Ermolaev E., Kukunin D., Fedotov I. Performance Analysis of the Infiniband Network. – PP. 327–331.
With the development of neural network technologies and the concept of big data, there is a need for a high-performance data transmission network with low latency. One possible solution could be the InfiniBand network developed by IBTA. This data transmission network is based on the use of special adapters and switches. This paper presents the results of the analysis of the performance of InfiniBand based on Mellanox adapters when transmitting various types of traffic.
Key words: infiniband, point-to-point, high-speed network, computer network, RDMA.

Gerling E., Zebzeev E., Kistruga A. Research of the Features of Wireless Network Traffic Protection Based on WPA3. – PP. 332–336.
Wireless networks are an integral part of modern technologies. In particular, Wi-Fi is a technology of wireless data transmission technology from devices to a network according to the standards of the IEEE 802.11 family. Wi–Fi networks are the most common computer networks and are used around the world, both in private homes where one or more devices are supposed to be connected, and in large corporate networks companies, where the number of connected devices can be measured in hundreds. One of the main problems is ensuring secure transmission. The WPA 3 standard, introduced in 2018, is the latest Wi-Fi network security solution at the moment. This article discusses the mechanisms used in WPA3. The Simultaneous Authentication of Equals authentication process, also called SAE, is described.
Key words: WPA3, SAE, OWE, information security, network administration.

Goikhman V., Knyazeva V. The Research on the Practical Application of Digital Twin Theory. – PP. 336–341.
ITU-T is currently developing standards for the use of digital twins. A digital twin is a real-time representation of physical objects in the digital world. This technology has been used in many industries oriented towards Intelligent manufacturing and Industry 4.0. This article discusses the issues of practical use of digital twin theory and defines its areas of use in infocommunications.
Key words: infocommunications, artificial intelligence, neural networks, digital twin.

Гончаров С. В., Оводова Т. А. Подсистема детектора лжи на основе искусственного интеллекта. – С. 342–345.
В этой статье представлен взгляд на будущее детекции лжи. Сложность обычных процедур проверки на полиграфе сама по себе является препятствием для его применения в большем количестве уголовных дел и повседневных жизненных ситуаций. Автор вводит новое приложение искусственного интеллекта в повседневные аспекты нашей жизни, которое избавляет от человеческого фактора и делает процесс принятия решений намного быстрее, чем сейчас.
Ключевые слова: обнаружение фактора лжи, процедуры проверки на полиграфе, новое приложение для искусственного интеллекта, искусственный интеллект

Gorban S., Krasov A., Tsvetkov A. Evaluating the Effectiveness of Access Rights Control Mechanisms in the Linux OS. – PP. 345–348.
This article is devoted to the study of the effectiveness of the system of access rights. The article discusses the specifics of implementation and evaluation of the access rights system. The authors of the article use methods of analysis to evaluate the results of the system. The aim of the work is to conduct a study aimed at improving the functioning of the system.
Key words: access rights, Linux OS, security, administration.

Gorbulenko E., Mesnyankin E., Potapov S., Potapova N. Development of an Optical-Mechanical Path for Duplex Laser Space Communication. – PP. 349–354.
Different versions of the optical-mechanical path for duplex laser space communication (with a common transceiver channel and separated receiving and transmitting channels), estimated energy calculations, estimated calculations of weight and size characteristics are given in the paper, and an option of placing functional assemblies on board the spacecraft for devices with reduced weight and size characteristics for transmission large data volumes with high speed over distances from units to thousands of kilometers is proposed.
Key words: space laser communication, space optical communication line (SOCL), fiber-optic communication line (FOCL), optical-mechanical path, duplex communication.

Gorda M., Chechulin A. Review and Systematization of Software Tools Used to Investigate Cyber-Attacks. – PP. 355–359.
Despite the improvement of various means of information protection, every year, there is a more significant increase in the number of cybercrimes, some of which cannot be detected or prevented at the time of carrying out. Such cybercrimes are the object of research for cybercriminalists. As part of the investigation, specialists use specialized software that allows you to track the place and time of the crime and, sometimes, the criminal himself. The report will provide an overview and systematization of modern computer forensics software tools and analyze their advantages and disadvantages.
Key words: forensics, cyber forensics, investigation of cybercrimes.

Gorlov N. Monitoring of Physical Optical Access Network Environments. – PP. 360–364.
The report is devoted to the issues of monitoring in physical environments of optical access networks. The application of technology based on the principles of Mandelstam–Brillouin scattering is justified. The calculated relations allowing to estimate the basic functionality of Brillouin reflectometry in the time domain are presented. The possibility of monitoring the physical channels of the tree topology of the optical access network by Brillouin analysis in the time domain using finite reflections is analyzed.
Key words: monitoring, passive optical network, physical stress, Brillouin scattering, finite reflection method.

Gorlov N. Classification and Scope of Fiber-Optic Sensors Based on the Mandelstam-Brillouin Scattering Principle. – PP. 365–369.
The report is devoted to the classification and application of fiber-optic sensors based on the Mandelstam-Brillouin scattering principle. It presents a mathematical model of the process of obtaining measurement information based on the results of the analysis of the spectrum of the

backscattered signal. Of particular interest are fiber-optic sensors for monitoring the integrity of the pipeline and for security/perimeter fencing.
Key words: optical fiber, fiber-optic sensor, Mandelstam–Brillouin scattering, Brillouin frequency shift.

Grishin I., Kazakova A., Okuneva D. Operating Characteristics Analysis of the 2D-MUSIC Algorithm for FR2 in Next Genearaton Mobile Networks. – PP. 370–376.
The paper presents an analysis of 2D-MUSIC method of field processing in the opening of a planar antenna array, which allows determining the direction of reception of signals coming from user devices operating in the millimeter wavelength range in superdense networks and separated by angular coordinates from each other by an interval smaller than the Rayleigh resolution interval. These experimental results allow us to evaluate the real characteristics of the method under consideration.
Key words: 2DMUSIC, azimuth, elevation angle, user equipment, antenna array.

Guryanov I., Kaisina I. Prospects for the Use of Stereovision in UAVs. – PP. 376–381.
The article presents a generalized overview of various types of UAVs, lists the types of payloads and modern technologies. It is highlighted that increasing the autonomy of UAVs is considered a promising direction for the development of the industry. An important part of increasing autonomy, including in confined spaces, can be the use of stereo vision. The article assumes that stereo vision will be used to detect objects and measure the distance to them in order to prevent collisions. A stand for further testing of stereovision algorithms is presented.
Key words: unmanned aerial vehicle, stereo vision, autonomy.

Daleh Al-Magsoosi A. Approaches to eBPF Usage for Network Monitoring. – PP. 381–384.
Many cloud service providers are having trouble monitoring the network with popular eBPF-based monitoring tools that use Kubernetes and run on various kernel versions. Despite the interoperability issues, eBPF can be used to monitor cases where traditional tools fail. However, many lack understanding of the complexity, limitations, and potential risks of using this technology. In addition, only a small number of companies currently offer ready-to-use products. This paper will present the results of using the eBPF technology and several conclusions that were obtained as a result of the experiments.
Key words: cyber-attacks, anomalous data, containerization systems, ebpftrace.

Dementev R., Derzhko D., Ushakov I. Analysis of MPLS Impact on IPSEC Operation in a Service Provider's Network Using Domestic Network Equipment. – PP. 384–389.
At the current time, the problem of import substitution in Russian IT companies is acute. This article discusses aspects of the influence of multiprotocol label switching on the performance of an IPsec tunnel using the example of Eltex equipment. The network segment is presented and basic performance tests are carried out. In the future, research is planned in the field of implementation of the MPLS VPNL3, MPLS VPN L2 and MPLS TE services.
Key words: information security, import substitution, performance, fault tolerance, MPLS, IPsec, routing.

Demidov N. Some Aspects of the Study of Traffic Transmission of 3d Video Images. – PP. 389–394.
The article discusses various areas of use of 3D video images and substantiates the relevance of studying the features of this type of traffic. Some results of the study of 3D video traffic are presented. The experimental component of the study is described. The problems requiring solutions to obtain high-quality holographic video content are identified. Strategic directions of further stages in the experiment program are proposed for discussion.
Key words: holographic technologies, digital holography, 3D image traffic, 3D video stream traffic, video stream traffic, data transmission, communication networks.

Derkach A., Mikhailichenko A., Parashchuk I. The Current State of Methods for Analyzing the Effectiveness of Storage and Backup Systems for Data Centers. – PP. 394–398.
The state, conditions and features of the application of modern methods of analyzing the effectiveness of such complex information technology systems, which are information storage and backup systems for data processing centers, are considered. Variants of the formulation of classification features for the identification of such methods, which can be attributed to: the type of the efficiency indicator, the class of a priori uncertainty of the system functioning process, the dependence of the efficiency indicator on time, as well as the method of evaluating the effectiveness of systems of this class.
Keywords: efficiency analysis, method, performance indicators, storage and backup system, data center, requirements, method, classification feature.

Dmitrieva J., Elagin V. Parameters in SDN for Network Prediction. – PP. 399–403.
The article analyzes network element management and configuration protocol the SDN (Software Defined Networks). The OF-Config protocol is an accompanying OpenFlow protocol that dynamically supports the interaction of the controller and the OpenFlow switch. Network overload and failure can be avoided by using the OF-Config protocol and changing parameters. This article is devoted to the analysis of these parameters.
Key words: SDN, Software-Defined Network, OpenFlow, OF-Config.

Dmitrienko M., Erygin V., Semkina M. Targeting Problems for Multiple Objects using Rotation Strategies and Cluster Approach. – PP. 404–408.
This article discusses the problems of assigning targets to weapons for a defense system to counter numerous objects concentrated in a narrow area, such as low-altitude missile threats or swarms of unmanned aerial vehicles. Two algorithms for assigning weapon targets - a fixed rotation strategy and a rotation strategy – are proposed based on this formulation.
Key words: assigning a target to a weapon, the probability of defeat, a lot of aerial objects, operational strategy, modeling.

Dmintrienko M., Erygin V., Tuhbatullina E. The Application of Micro Coaxial Rotorcraft in Warfare: An Overview, Key Technologies, and Warfare Scenarios. – PP. 408–412.
The mode of future wars is mainly local wars and regional conflicts. This style of war is characterized by unpredictability and instability, which can happen anytime and anywhere. Once it happens, the battlefield is vast, short-range and fast-changing. In order to adapt to the characteristics of this kind of warfare, simple equipment and short reaction time have become two important factors in selecting weapons. Coaxial rotorcraft has been widely studied and applied

in future wars due to its convenient carrying, strong environmental adaptability, and rich load capacity. This paper conducts an overview of the Coaxial rotorcraft. Furthermore, we also identify its key technologies, warfare scenarios and future directions. We anticipate that this survey can shed new light on the coaxial rotorcraft systems.
Key words: unmanned aerial vehicle, military conflict, multifunctionality, control, data transmission, usability, microcoaxial rotorcraft.

Dong H., Kotenko I. Intrusion Detection based on Multi-Task Learning with Optimization of Uncertainty Losses. – PP. 412–417.
As the first and effective defense line for network and system, intrusion detection system require high accuracy and low false alarms. The paper proposes a hard parameter sharing Multi-task Learning (MTL) method for multi-class traffic classification, utilizing uncertainty-based loss optimization. Comparisons with single task learning (STL) models proves MTL can identify rare intrusions better.
Key words: cybersecurity, intrusion detection, deep learning, multi-task learning

Donskov E., Kotenko I. Algorithms for Detecting and Preventing Attacks on Intelligent Transport Systems using Blockchain Distributed Register Technology. – PP. 418–423.
Information transmission and storage systems are an integral part of human life. Every year, the development of systems, methods of storing and transmitting information develops taking into account emerging requirements - wired systems, wireless systems, systems of moving objects. In addition to the need to store and transmit information in specific conditions, the security of data storage and transmission plays an important role. Recently, the most popular trend in ensuring data security in such systems is a special case of distributed registry technologies – blockchain technology. As part of the work, the authors consider the security issues of integrating blockchain technology using the example of intelligent transport systems - one of the types of systems for moving objects. In addition to reviewing the main attacks that are most typical for such systems, taking into account the integration of blockchain technology, the authors consider algorithms for detecting attacks, as well as methods for preventing them.
Key words: intelligent transport system, blockchain.

Drepa V., Kovzur M., Petrova T. Estimation of Time to Block Illegitimate Access Points in the Corporate Network. – PP. 423–427.
One of the most common attacks on corporate networks today is connecting an illegitimate access point. It allows an attacker to gain access to a company's protected network, enabling him to launch various types of vulnerability scanners and to attack the network remotely, without being in the organization itself. Therefore, every company should be able to fight this attack effectively and, importantly, quickly. The report presents one method of blocking illegitimate access points in a corporate network. Theoretical and practical testing of estimating the time of finding a non-legitimate access point in a wired network, as well as it's cutting off from the enterprise network is carried out.
Key words: automation, Ansible, security, wireless rogue access points.

Dunaytsev R., Svetova A. MU-MIMO Technology in IEEE 802.11ac Networks. – PP. 428–432.
With the ratification of IEEE 802.11ac in 2013, it became possible using MU-MIMO technology to deliver data frames to multiple client stations simultaneously. To accomplish this, both the access point (or the Wi-Fi router) and the client stations must support beamforming in multi-user mode. How many Wi-Fi devices released today support MU-MIMO and how to detect its use in an IEEE 802.11ac network? This study is devoted to answering these questions.
Key words: IEEE 802.11ac, MU-MIMO, Wave 2, Wi-Fi 5.

Evtikhin E., Lepeshkin O., Ostroumov M., Ostroumov O., Sinyuk A. The Theorem on the Completeness of the Formation of the Communication System Functioning Profile. – PP. 433–437.
Modern communication systems are critical objects for control systems. Criticality is manifested in the potential for violation of the system functioning process due to the influence of various factors. It is proposed to use the profile of a communication system to control and ensure a stable process of its functioning. The presented theorem characterizes the completeness of the functioning profile, which makes it possible to describe the achievement of the intended purpose of the system.
Key words: critical information infrastructure, critical facility, communication system, profile, system operation process.

Edemskaya E., Puchkov V. Using Autitd for Logging in Linux Systems. – PP. 438–443.
One of the important components of the information security of the company's infrastructure is SIEM, an event management and security information system. Such a system can be divided into 2 main parts – a subsystem for collecting events and a subsystem for analyzing received events. The correct configuration of the first one will help to detect an intrusion at the early stages of penetration, will facilitate the writing of alarm events, and if an attacker was able to penetrate the company's infrastructure, it will allow you to figure out how and why this happened. The main tool for collecting system events in Linux systems is auditd. Based on this tool, others have been created, for example, audit beat, go-audit, which complement the main functionality of auditd. The paper discusses the basic principles of the basic logging tool, and also presents the auditd setting, which allows logging important events in the system.
Key words: logging, event collection, linux, auditd.

Elagin V., Zajac M. Analysis of the Possibilities of Applying Speech Analytics Technologies for CEM Tasks. – PP. 443–448.
This article is dedicated to the possibilities of applying speech analytics for Customer Experience Management tasks. The article discusses software that implements the concept of managing user experience. To present the tasks that speech analytics must solve, the customer lifecycle is considered, which includes 9 stages that should be relied upon when implementing auxiliary technologies. The article describes the principle of how speech analytics works for CEM tasks and the results of implementing it.
Key words: customer experience management, customer lifecycle, customer experience, loyalty, churn, speech analytics.

Elagin V., **Nekrasov V.** Analysis of the Requirements of Video Conferencing Systems to the width of the Transmission Channel. – PP. 448–453.
The demand for videoconferencing is growing every year. It is already hard to imagine a corporate environment without videoconferencing systems, they solve many communication tasks of state authorities and large corporations. The quality of group and personal video conferences is very important for every customer, and it directly depends on the bandwidth. In this article we analyzed the requirements of different videoconferencing systems to the bandwidth of the communication channel and looked at how the bandwidth affects the quality of the conference in practice.
Key words: video conferencing, channel width, bitrate, Wireshark.

Elagin V., Obukhov S. Artificial Intelligence in Post-NGN Networks. – PP. 454–456.
In order to effectively use all the technologies of 5G, 6G networks, it is necessary to quickly process intensive network traffic, configure networks, this is realized through the integration of auxiliary systems such as machine learning, neural networks and artificial intelligence. Artificial intelligence methods have great potential for solving the problems of intelligent resource allocation between base stations in 5G networks, are able to process a huge number of parameters, learn and adapt to changing conditions, and recognize patterns. They are able to realize the needs in the directions of high bandwidth and low latency. This article describes the main methods of machine learning, as well as some specific examples of artificial intelligence applications that can be used in post-NGN networks.
Key words: post-NGN, 5G, 6G networks, artificial intelligence, learning, deep learning.

Elagin V., Petrov M., Chekalov D. Analysis of the Access Network Load by Promising Services and QoS Provision. – PP. 457–460.
The purpose of the study is a comparative analysis of the traffic load of the access network by promising applications from B2C clients. The main object of research is the tariffs provided to B2C clients with a bandwidth of 300 Mbit/s and higher. In the article, based on the collected and analyzed statistics, it is required to determine the bandwidth effectively occupied by the client in the CNN for such tariff plans. The main conclusion is to justify the redundancy of such tariffs and, as a consequence, the redundancy of multiple excess capacities on the provider's equipment. Also, in the course of the study, the actual bandwidth occupied by the client was revealed.
Key words: broadband access, xPON, B2C client, Triple-play, FTTB, OLT.

Elagin V., Chipsanova E. Study of the Efficiency of the Hybrid Model of Mobile Edge Computing in 5G Networks. – PP. 460–465.
With the development of mobile and infocommunication networks, the development of edge computing systems is relevant. The hybrid model of mobile edge computing allows to correctly allocate resources, however, in order to deal with the hybrid model, you need to study the standard options for the location of edge servers. This article will analyze the location of edge servers, and will also consider the factors that affect their location.
Key words: 5G, MEC, server location, hybrid model.

Elagin V., Shalimov I. Models for Prediction of Failures in the Operation of Broadcast Equipment. – PP. 466–471.
The operation of broadcasting equipment is characterized by relatively low maintenance costs in case of timely detection of faults and their elimination through the use of spare parts, tools and accessories. However, when maintenance intervals are not followed, or when extraordinary network events occur, repairing or replacing equipment is costly.
Key words: failure modeling, digital television, probability, prediction.

Elagin V., Shchegolskiy Y. Review Machine Learning Methods for Analysis's Traffic Issues. – PP. 471–475.
Machine learning is a branch of artificial intelligence that focuses on creating systems that learn and evolve from the data they produce.
Machine learning technology has made it possible to perform some operations faster than humans. Over the years, the technology has improved and new algorithms have been invented to make it work. Nowadays, machine learning is used in many areas of human activity, including traffic analysis.
The article considers the tasks solved by machine learning methods. The algorithms used for traffic analysis are considered. Comparison of the given algorithms is carried out, and one, the most suitable for traffic analysis tasks is allocated.
Key words: machine learning, traffic analysis, traffic classification, clustering.

Elizarova L., Izrailov K. Classification of Information Security Areas using Categorical Division. – PP. 475–479.
The work is dedicated to the analysis of statistics of scientific publications on research aimed at solving problems in various areas of information security. These areas were obtained by the authors earlier using the apparatus of categorical division. The method of analysis is to search for scientific articles and assign them to the relevant areas. Conclusions are made regarding the current and future relevance of information security tasks.
Key words: information security, publication activity, forecasting.

Ershova T., Tcvetkov A. The Selection of Information Security Audit Method. – PP. 480–483.
With the rapid development of information technology threats to information security grows. The topic of security auditing, which is one of the most important ways to find vulnerabilities in time and prevent possible unauthorized actions in the future, becomes extremely relevant. The article deals with the methods of information security auditing.
Key words: information security audit, active audit, CRAMM, OCTAVE, RiskWatch.

Esalov K., Kuznetsov M., Romanenko K. Analysis of Machine Learning Models for Time Series Prediction. – PP. 484–488.
This report discusses the principles of analysis and methods of data preprocessing for forecasting time series, namely: the Box-Cox transformation, normalization and differentiation. To predict the future values of time series using machine learning models, regression models such as Linear Regression, Random Forest, and Gradient Boosting (CatBoost) were considered. As a result of the experiments, based on the data of past periods, it was possible to build a forecast of the time series for several values ahead and evaluate the effectiveness of the considered machine learning models.

Key words: machine learning, prediction, time series, data preprocessing.

Esalov K., Kuznetsov M., Romanenko K. Service for Identifying, Determining the Activity and Involvement of the user in the Process of Distance Learning. – PP. 489–492.
This article deals with the problem of evaluating participation in a videoconference, which is becoming increasingly relevant in connection with modern distance and mixed forms of education, as well as the spread of videoconferencing technologies. To solve this problem, a software product created in the Python programming language was developed. The development is based on computer vision technology for video analysis and determining the time of presence of participants in a video conference. When solving the computer vision problem, two neural networks were used, namely MTCNN for face detection and InceptionResnetV1 for face recognition. The results of the study show the high accuracy of the program and its applicability for automating the process of counting the time of people's presence at video conferences.
Key words: neural networks, face recognition, face detection, videoconferencing.

Zhavoronkova V., Tarabanov I. Crosschain Technology Research using the Polkadot Ecosystem as an Example. – PP. 493–497.
Blockchains are becoming increasingly popular in various areas of infocommunication technology in the modern world. This paper presents an overview of the Polkadot ecosystem using crosschain bridges, which allow solving the problem of scalability, interaction and information transfer between different blockchain networks. An analysis is presented that identifies network criteria for evaluating crosschain technologies. These criteria vary according to their functions, level of trust, direction of asset transfer, mechanisms, and degree of centralisation.
Key words: blockchain, crosschain, Polkadot, smart contract, token.

Zhernova K. Designing a Globally Optimal Human-Computer Interface. – PP. 497–500.
There are various methods for evaluating human-computer interfaces that can be used to evaluate the interface after taking steps to protect data during the interaction of the operator with the interface. Most often, the effectiveness of a human-computer interface is measured using formal metrics such as speed and accuracy, which are compared to those of other interfaces. You can also evaluate the usability of the interface using user surveys, video analysis of interface tests, and so on. A third possible way to evaluate a human-computer interface is to measure the distance between the effectiveness and usability metrics of the interface and the metrics of some globally optimal interface, that is, an interface that would be completely secure and yet sufficiently effective. The report considers the possibility of designing such a globally optimal interface.
Key words: human-computer interaction, information security, user interfaces, security assessment.

Zhernova K., Chechulin A. Methods for Searching for Vulnerabilities in the Unmanned Transport Environment of the "Smart City". – PP. 500–504.
An important part of the "smart city" is the unmanned transport environment. Protecting data exchange between unmanned vehicles and smart city infrastructure seems to be a significant task. An unmanned vehicle environment may have vulnerabilities that allow an attacker to attack unmanned vehicles and passengers, which can cause physical harm to road users, as well as financial loss. For this reason, the problem of finding and eliminating vulnerabilities in the

unmanned transport environment of the "smart city" is relevant. This report discusses various classes of methods for searching for vulnerabilities in the unmanned transport environment of the "smart city".
Key words: human-computer interaction, unmanned transport environment, "smart city", information security, user interfaces.

Zhigadlo V., Nosov M., Shinkarev S. Problems and Prospects of Development of Methods and Means of Processing Heterogeneous Data on the Parameters of Structural Reliability of Modular and Mobile Data Centers. – PP. 504–508.
Modern problems are investigated and a new approach to the development of methods and tools for processing large volumes of heterogeneous data on the values of structural reliability parameters of modular and mobile data centers is proposed. This approach includes six stages of creating appropriate methods that provide key target functions: data collection and preprocessing, rapid detection of accidents and failures, assessment of the level of structural reliability, as well as analysis and risk management of structural reliability violations of objects of this class. Modern (including intelligent) analytical methods and mechanisms are proposed by which these objective functions can be practically implemented.
Key words: heterogeneous data processing, structural reliability, modular data center, mobile data center, methods, tools, large amounts of data.

Zhikh D., Kislyakov S., Skorinov M. Application of RPA Technology to Optimize Service Quality Management Business Processes. – PP. 508–511.
The emergence of new technologies over the past few years has led to a transformation in service quality assurance.
As business process optimization becomes an integral part of digital transformation, companies are adopting robotic process automation to improve service quality. The application of this technology enables the use of software bots for simple tasks, while improving efficiency and reducing operational costs.
This report examines business processes related to service quality and approaches to automating these business processes using robotics.
Key words: business process, service quality management, Robotic Process Automation.

Zadboev V., Lipatnikov V., Melekhov K. Method for Determining in the Data Transmission Network the Chain of Routes to the Geographical Location of the Interface. – PP. 512–517.
Abstract: any network infrastructure needs to be protected from external threats, but this is still not enough, therefore it is necessary to stop any attempts to enter the internal network, the network, for example, by reverse attacking the attacker in order to calculate his location. Purpose: to increase the security of internal network traffic of the data transmission network of a critical facility by identifying intruders based on their IP addresses. Objective: to develop a system for determining the geographic location of an intruder and an algorithm for its actions.
Key words: attacker's location, IP address, threat model, external threats, data network, critical object, network scanning.

Zadorozhnyanya A. Self-driving Vechiles as Industrial Internet of Things. – PP. 517–522.
This article identifies sources that describe modern self-driving vehicles, promoting the development and development of the Industrial Internet. The Industrial Internet plays an

important role in the search for autonomous vehicles of the future. There are also method of network delay's decrease in unmanned vehicles as an Industrial Internet system. This allows them to reduce the load on the data network, optimize network usage and reduce network delay, which minimizes a risk of accidents.
Key words: IIoT, Industrial Internet, Industrial Internet of Things, SDV, self-driving vehicle, unmanned vehicles, autonomous vehicles, AV, BEV, battery electric vehicle, HEV, hybrid electric vehicle.

Zakharenkov N., Zakharenkov K., Lukin K., Stakheev I. Technical Aspects of an Implementation of Connector Using Expanded Beam Technology. – PP. 522–527.
An expanded beam connector is a collimator designed to transform a divergent light beam at an output of fiber-optic cable into an expanded beam of parallel rays. Based on theoretical modeling of the most important parameters of the expanded beam connector, which are significant challenges during the product development, technical aspects of its implementation were analyzed. An advantages, disadvantages, and field of application of this technology were also considered.
Key words: fiber-optic connectors, expanded beam technology, optical and geometric parameters.

Zakharenkov K., Zakharenkov N., Lukin K., Titova O. Problem of Measuring the Parameters of Micro-Optics Lenses used in Optical Transmission Systems. – PP. 527–532.
There are numerous devices for measuring the optical or geometric parameters of lenses. Micro-optical lenses and their assemblies are often used in optical transmission systems, and deviations in their parameters can greatly affect attenuation in the nodal system. The paper considers the types of lenses used in optical transmission systems and analyzes the suitability of these devices for measuring the focal length of such lenses. The conclusion is drawn about the shortcomings of the devices, and proposals are presented for developing or upgrading existing equipment.
Key words: optical and geometric parameters of lenses, effective focal length, back focal length, front focal length, focal length, micro-optics, lenses, ball lenses, optical fibers.

Zverev A., Shelukhin O. Modernization of the LAN Closed Loop System by Domestic Access Control Complexes. – PP. 533–537.
Implementation of a hardware-software encryption complex in local networks is a universal tool for ensuring the protection of a corporate network and confidential information. But an important factor is the training of specialists. When it comes to learning how to use this APCS, there is a need to create a virtual environment in which you can practice without violating the law and the integrity of computer networks and systems. To do this, it is possible to deploy the virtual infrastructure of the Continent, where you can learn how to configure the network devices of the complex and their protective mechanisms.
Key words: AKPSh Continent, industry 4.0, crypto-gateway, laboratory stand.

Zelichenok I., Kotenko I. Architecture and Implementation of the Prototype of the Module for Detecting Multi-Step Attacks using Short-Term and Long-Term Analysis. – PP. 537–541.
With a rapidly growing data flow, identifying subtle threats to information security, implemented at several stages, is becoming increasingly difficult. When automating the process of

multi-step attacks with a large data flow, the use of machine learning and big data processing technologies is important. The paper proposes the architecture of the multi-step attack detection module, which is based on these technologies and consists of two components: a short-term data analysis subsystem that detects attacks in real time, but limited by a short time window, and a long-term analysis subsystem that reconstructs scenarios based on the data provided by the module short term information. The machine learning model makes the final conclusion about the conducted multi-step attack. The initial implementation of this module is also presented.
Key words: information security, cyber-attacks, multi-step attacks, attack detection.

Zolotova D., Katasonov A. Comparative Analysis of Means to Limit Applications Launched by Users. – PP. 541–546.
Nowadays, with the increase in the volume of transmitted information, the requirements for ensuring the security of this data are also growing. Attackers are developing new methods of obtaining unauthorized access to operating systems in order to gain access and damage classified information. One of the most vulnerable nodes used by attackers is the company's staff, who can open an infected application or click on a phishing link. To ensure security against such attacks, it is proposed to use technologies to restrict users from running applications. In this work, the collection was carried out, the characteristic features were determined and a comparative table of means for limiting applications launched by users was compiled.
Key words: access restriction; applications; Deskman; Security Administrator. WinLock.

Zyleva P., Pestov I., **Tremel I., Yurova U.** Comparison of Virtualization Systems of Software Complex of Virtualization Tools "Brest" and VMware. – PP. 546–552.
Virtualization is increasingly being used in the IT field. It reduces the cost of maintenance, allows testing of new systems, improves security, helps to increase the adaptability, performance, availability, flexibility and scalability of the IT environment. In virtualization, the capabilities of the hardware are realized with the help of software and a virtual computer system is created. This allows IT departments to run multiple virtual systems (multiple operating systems and applications) on a single server. In connection with the departure of foreign suppliers of virtualization systems from the country, a comparative study of the Russian hardware virtualization system with departed foreign solutions is relevant in order to provide detailed information on similarities and differences in order to troubleshoot.
Key words: virtualization, hardware virtualization, PC SV "Brest", VMware, VMware vSphere, Astra Linux, import substitution, information security.

Zyleva P., Pestov I., **Tremel I., Yurova U.** Security Methods Astra Linux Special Edition. – PP. 553–558.
Stability, security, ease of use, data protection from unauthorized access are important for every user of an information system. Therefore, it is of particular importance for all users to fulfill the basic tasks of information security - protecting the confidentiality, integrity and availability of data. The fulfillment of these tasks is necessary, from ensuring the security of personal data, further to commercial secrets and up to state secrets. Astra Linux Special Edition is a special-purpose OS designed to create protected automated systems on its basis. Provides protection of confidential information and state secrets to the level of "special importance".

Key words: Astra Linux Special Edition, Security, Information Security Tools, Mandatory Integrity Control, Closed Software Environment, Application Isolation, Astra Linux Directory (ALD), Mandatory Access Control (MAC), Common User Space.

Zyleva P., Pestov I., Tremel I., Yurova U. Integration of the Client Machine on the Linux Operating System Into the Active Directory Domain. – PP. 559–564.

Most medium and large enterprises use Microsoft Active Directory to centrally manage access to resources owned by the organization. This has been the case for decades, and companies have invested heavily in creating automation tools and workflows aimed at improving the security and efficiency of their IT admin teams. According to the latest data, due to the withdrawal of key foreign IT vendors from the Russian market, the demand for the use of domestic operating systems has increased dramatically. Now this is due to security issues and Microsoft's position on working in the country, although the process itself began back in 2020. The most popular system remains Astra Linux, a UNIX–like OS based on the Debian distribution, which has been developed by Rusbitech since 2008. The transfer of enterprise IT systems will require setting up the correct interaction of the updated systems with the solutions that already exist, with all the resources that users use, so administrators are faced with the task of integrating Linux servers and workstations into the Active Directory domain environment.

Key words: Active Directory, Samba, Winbind, Kerberos, Domain, LDAP protocol, User Identifier UID, Group Identifier GID, Security Identifier SID, SMB (Server Message Block), CIFS (Common Internet File System), NSS (Name Service Switch).

Ibragimov R. Noise Immunity of Coherent Systems in Fiber-Optic Transmission. – PP. 564–567.

In view of the development of technology for coherent reception of an optical signal, one of the important criteria for operation is noise immunity. The importance of this criterion is due to the use of multilevel modulation formats (DP-16QAM, DP-32QAM, etc.), which are more susceptible to distortion due to closely spaced signal states. To improve the transfer characteristics of communication systems today is the use of cascaded coding schemes. Hybrid schemes that implement the joint operation of SD-FEC and HD-FEC can reduce the number of errors in the received signal.

Key words: backbone network, signal-to-noise ratio, noise tolerance, FEC.

Ignatieva D., Pestov I., Fedorova E., Fedotovskaya A. Big data Analysis for Information Security. – PP. 567–572.

The 21st century is the era of information flow. The data that humanity has accumulated over the past decade far exceeds the data that was available to humanity during the previous century. Society is "on the cusp of a huge wave of innovation, productivity and growth, as well as new ways of competing and creating value – all thanks to big data." Big data analysis has proven to be an effective tool in many areas of modern information processing, including information security. By providing more data and applying various analytical methods, all real and potential risks can be analyzed very quickly, many alternatives for protection and counteraction can be evaluated, more accurate forecasts of future development can be made, and more detailed expert opinions can be carried out. The purpose of the article is to study big data analytics. Tasks: overview of big data sources and methods of analyzing this data.

Key words: Big Data (BD), information security, big data analytics

Izrailov K., Ponomarev N., Tarov E. Analysis of Time Series Forecasting Models for Predicting Trends in the Development of Information Security Threats. – PP. 572–577.
The work is devoted to the task of predicting threats to information security. To do this, the analysis of existing time series forecasting models is carried out to identify trends in the development of threats. As a result of a criterion comparison of the above models, the most suitable of them were determined. A methodological scheme for the selection of forecasting models is proposed. The theoretical and practical significance of the research results, as well as the ways of its continuation are indicated.
Key words: information security, time series, forecasting, forecasting models.

Izrailov K., Umaraliev I. A Hypothetical Method of Recovery of Machine Code Architecture Modules to Identify High-Level Vulnerabilities. – PP. 577–581.
This work is devoted to the study of the author's method of restoring the architecture of programs from machine code in order to search for high-level vulnerabilities. A method is described for highlighting the connections of program modules, which allows you to restore the architecture itself. Working with the method of conditional access to the clustering of meta-information obtained from machine code. A graphical illustration of an example of cluster division of mutual calls of program functions in 2D space is given, and the results are analyzed.
Key words: information security, machine code, reverse engineering, software security, architecture restoration.

Izrailov K., Chasovskikh E. Comparative Analysis of Security Solutions from Unauthorized Software Distribution. – PP. 581–586.
The article is devoted to the field of software protection. The purpose of the work is to identify the most effective methods of protecting programs from unauthorized distribution. In the interests of this, a review and criterion comparison of protection methods is carried out. The results of the comparison are presented in tabular form, the most suitable solutions are determined. The work will continue to expand the methods of protection and the list of criteria to obtain more complete and accurate results of comparative analysis.
Key words: software protection, software, unauthorized distribution, unauthorized access.

Izrailov K., Yaroshenko A. Investigation of the Machine Learning Opportunities for Automatic Ranking of Vulnerabilities According to Their Text Description. – PP. 586–590.
The work is devoted to the search for vulnerabilities in the interfaces of the Smart City transport infrastructure. One of the urgent tasks of the study is the automatic identification and ranking of vulnerabilities to select the order of their neutralization. Moreover, only their textual description given by a person manually is taken as the initial data on vulnerabilities. For this, it is possible to apply various models and methods of machine learning. The course and results of the experiment for the Russian database of vulnerabilities are described. The performance of the following classifiers is compared: ExtraTreeClassifier, Svm.SVC, MLPClassifier, ExtraTreesClassifier, RandomForestClassifier. The obtained F-measure on average showed a value of ~0.65, which can be considered satisfactory, although it needs to be improved.
Key words: information security, vulnerabilities, ranking, smart city.

Ilina O., Kupchinenko O., Skoropad A. Network Traffic Analysis in a Modern Operating System. – PP. 590–595.
The tasks of network traffic analysis, the features of traffic analyzers, their general properties and differences are considered. The analysis of popular tools for monitoring and analyzing network traffic in a modern special-purpose operating system is carried out. The possibilities of graphical and console utilities for monitoring, analyzing and visualizing network traffic that can help identify problems in the operation of a local network are analyzed.
Key words: network traffic analysis, packet interception, network traffic monitoring, sniffer, network traffic analysis tools.

Ichetovkin E., Kotenko I. Analysis of Protection Methods Intrusion Detection Systems from Attacks on Machine Learning components. – PP. 595–600.
Intrusion detection systems are used to detect attacks on network devices. Among such systems, the most promising are heuristic-type intrusion detection systems with machine learning components based on neural networks. The machine learning components of intrusion detection systems, in turn, can be subjected to various attacks, which will compromise their work and, therefore, it will not be possible to guarantee the correctness of the attack detection result. For this reason, one of the most relevant cybersecurity tasks is to analyze methods for protecting intrusion detection systems from attacks on machine learning components.
Key words: machine learning, neural networks, intrusion detection system, protection against attacks on machine learning components.

Ichetovkin E., Kotenko I. Analysis of Attacks on Machine Learning Components of Intrusion Detection systems. – PP. 600–604.
When monitoring cybersecurity, it is extremely important that intrusion detection systems using machine learning components can adequately fulfill their mission of detecting the presence of intruders at an early stage of an attack, quickly isolating threats, and monitoring compliance with information security regulations. However, the adequate performance of intrusion detection functions cannot be guaranteed if the machine learning components themselves are subject to attacks (so-called adversarial attacks). To develop methods to counter such attacks, it is necessary to analyze attacks on machine learning components of intrusion detection systems. This article is devoted to this issue.
Key words: machine learning, neural networks, attacks on machine learning components.

Kazachenko I., Kushnir D. Analysis of Prospects of Blockchain Integration to Increase the Level of Information Security in 5G Networks. – PP. 604–609.
This article raises the question of the need to integrate blockchain technology in the fifth generation networks. The paper briefly describes the concept of blockchain technology, and also touches upon the advantages of blockchain integration as the main mechanism for ensuring information security in fifth generation networks in general, and for individual technologies in particular.
Key words: blockchain, 5G, cybersecurity, cloud computing, edge computing.

Kaisina I., Kuznetsov V., Tunguskova A., Shklyaev A. Review of Methods for Carrying Out Automatic Safe Landing of UAVs on Various Sites. – PP. 609–612.
The article discusses methods for landing unmanned aerial vehicles in order to deliver cargo. As a cargo, you can choose: food, medicine, parcels, various goods from shops, etc. Based on the analysis of methods and algorithms, technical perspective algorithms were selected for further implementation on a test bench and a series of experimental studies.
Key words: aerologics, unmanned aerial vehicle, safe landing, cargo delivery, payload, technical review system.

Kanaev A., Proshin F. Carrying PTP Messages Through OTN Based Network with Intermediate Nodes. – PP. 613–618.
The modern telecommunication networks operates at different layers ensuring the high capacity at the backbone parts and providing either services for users. The OTN technology makes it possible to achieve required parameters of traffic processing. It is necessary to guarantee at each node the precise time scale that is delivered due to a corresponding protocol. The Precision Time Protocol (PTP) is the most common method at Ethernet networks for providing the high precision and configuration simplicity. Using of this protocol within OTN is a way for increasing the network reliability and stability. This work aims to form and analyze a PTP algorithm. A model of node interaction is proposed. An influence of the processing stages on a precision and asymmetry is shown. The model parameters can be chosen that makes it possible to change network functioning conditions.
Key words: optical transport network, OTN, synchronization, PTP, synchronization channel, OSMC.

Kislyakov S., Lochkarev E. Identification of ODA Components for Workforce Management (WFM) System. – PP. 618–623.
This paper analyzes the "ARGUS Workforce Management" system with the aim of migrating it to the new Open Digital Architecture framework. Business function groups of the system, were identified in accordance with ODA Functional Architecture and mapped to the eTOM business functions of the same system, and ODA components were extracted. The interaction between the components, which is carried out through open software interfaces, was demonstrated.
Key words: Open Digital Architecture, ODA components, software, Workforce Management.

Kislyakov S., Sukhomlinov D. Allocation of ODA Components for Network Resource Inventory Accounting Systems. – PP. 623–627.
The world of infocommunication management is moving towards reformatting approaches to the development of support systems for operations and business. " NGOSS/Framework Program") for building automation information systems. One of the key ideas is the division of "monolithic" software into small self-sufficient software components.
The work is based on the ARGUS NRI network resource accounting system. To translate the NRI system, the principles of the open architecture of the ODA were used. The paper highlights the main components of the NRI system, their description and the necessary APIs for interaction with other components. An example of connecting components for a network resource accounting system to each other is shown.
Key words: open digital architecture, OSS/BSS, OSS components, Network Resource Inventory, open API.

Kistruga A., Kovtsur M., Sharapov R. Exploring Approaches for Analyzing WLAN Chipsets to Identify the Presence of Hardware Vulnerabilities. – PP. 628–631.
Nowadays, a huge number of people are using wireless data transmission technologies, in particular Wi-Fi. Connection through such networks is very convenient, and for this reason, a huge amount of data is transmitted in them. As a result, one of the biggest challenges is securing this data, especially for corporate networks, where protecting confidential information is very important. Broadcom is one of the world's largest suppliers of chipsets for wireless devices. Because their chipsets are so widespread, they can be easy prey for cybercriminals, and any vulnerability found in them is considered a high risk. In order to counteract the activity of an attacker, it should be possible to identify the vulnerabilities that a particular chipset has. Identifying them requires certain approaches to analyzing these chipsets, which are explored in this pape.
Key words: hardware vulnerabilities; chipset research; WiFi-exploit; broadcom; firmware; reverse engineering.

Kistruga A., Kryshchenko N., Minyaev A. Investigation of Attacks on IEEE 802.11 Wireless Networks with WPA3-SAE Authentication Mode. – PP. 632–637.
The security of IEEE 802.11 wireless networks is associated with many features of their structure and configuration used, which also includes the version of the security protocol selected on the device. This article examines the effectiveness of several types of attacks on a wireless access point and clients using WPA3-SAE security mode and WPA2-PSK/WPA3-SAE mixed mode for connection authentication. Attacks such as flood by association and deauthentication packages of the client are considered, as well as vulnerability of the mixed security mode is exploited. The vulnerability of security modes to the listed attacks is compared, taking into account different versions of the security protocol used by the client when connecting to a Wi-Fi network in transition mode.
Key words: wireless network security, WPA3-SAE, downgrade attack, association flood attack, deauthentication attack.

Klishin D., Chechulin A. Ontology of Information Security Models. – PP. 637–642.
The purpose of this work is to systematize the existing knowledge about information security models presented in standards and scientific research by identifying the basic concepts and unifying models to solve the problem of complexity: analysis, selection of an information security model relevant to the information infrastructure of the enterprise; assessment of the current level of information security of the enterprise.
In the work: the basic concepts and their properties used in information security documents describing information security models are identified; connections between concepts are formed; the formation of an ontology of information security models described in regulatory legal acts has begun.
Key words: information security model, information security level, standard, ontology, concepts of information security models, information security processes.

Kovalev I., Pantyukhin O., Paschenko V., Solodukhin B. Issues of Quality Assessment of Software Tools of Automated Systems. – PP. 642–645.
Evaluation of the quality of software tools of automated systems for various purposes is a complex process, the basis of which is the choice of quality indicators. A feature of software

development is the need for strict compliance with state standards both in the field of software quality and in the development of automated systems.
Key words: software, software tools, quality assessment, state standard, quality indicators.

Kovalev I., Parashchuk I., Smirnov A. Analysis of the Main Characteristics of the Quality of Software for Managing Modern Infocommunication Networks. – PP. 645–649.
The analysis of the role and place of software in the structure of the process of automated management of modern infocommunication networks is carried out. Taking into account the analysis of existing domestic and international standards, the key characteristics of the quality of software tools in the interests of managing complex objects of this class are formulated. The possible indicators allowing to obtain qualitative and quantitative estimates of the quality of software for automated management of modern infocommunication networks are considered.
Key words: software, automated management, infocommunication networks, quality characteristics, quality indicator.

Kovaleva A., Kulikovskaya A., Sargsyan A., Kholodenok E., Shemyakin S. Attacks using Vulnerability Associated with Kaspersky VPN Secure Connection Secure Remote Access and Methods to Counter Them. – PP. 649–654.
This article describes a number of vulnerabilities related to the operation of information systems. In this article, the analysis of vulnerabilities and attacks performed by exploiting these vulnerabilities was applied. Examples of attacks performed by exploiting these vulnerabilities are given. The article also describes measures to counter these vulnerabilities. Based on what is described in this article, we can conclude that the most common causes of vulnerabilities, as a rule, include: errors in the design and use of software; unauthorized introduction and subsequent use of the software; the introduction of malware; human factor. Timely response to the emergence of certain vulnerabilities and following the recommendations for their elimination contribute to maintaining the overall level of information security at the proper level.
Key words: information security; vulnerability, cyber attack, information system, monitoring.

Kolomiitsev R., Petriv R. Comparative Analysis of the OS for Security Testing. – PP. 654–658.
Security testing is aimed at identifying deficiencies in information systems, and can be performed in remote and low-maintenance network segments using software and hardware probes, which use specialized open source operating systems as software. The paper analyzes the operating systems, describes their advantages and disadvantages.
Key words: security testing, operating systems, hardware and software probe, single-board platforms.

Korzhik V., Lapshin A., Razumov D., Yakovlev V. Research of an Attach on a Numerical Key Distribution Protocol Bases on Majority Processing of Raw Key Bits Intercepted by an Eavesdropper. – PP. 658–663.
We consider a numerical key distribution protocol between two users connected by a constant-parameter channel, consisting of a raw key bit generation protocol and a two-iteration preferred improvement of the main channel (PIMC) protocol. A protocol attack is investigated, which consists of an attacker not using two-step decoding of transmitted blocks, but using one-step majority decoding of raw key bits intercepted during two iterations of the PIMC protocol.

Based on simulations, the key sequence error probabilities of the legitimate user and the intruder are found. Estimates of complexity of such an attack were made.
Key words: cryptography, key distribution protocol, eavesdropper.

Kosov N., Petrov I. Research of the Main Aspects Necessary when Creating an Enterprise Information Security Policy. – PP. 664–669.
This article presents and characterizes the important points of information security policy development, discusses the simplest ways to improve the effectiveness of enterprise protection and the actions of intruders that can lead to the collapse of the enterprise. Special attention is paid to the policies that are inherently related to the information security policy and the changes in the two thousand twenty-second year are affected.
Key words: information security; information security policy at the enterprise; authority policy, access control policy; hierarchical structure.

Kotenko I., Levshun D. Algorithm for Cause-and-Effect Correlation of Security Events in Cyber-Physical Systems on the Basis of Intelligent Graph-Oriented Approach. – PP. 669–674.
Security analytics tools for cyber-physical systems, in particular those operating in such important areas as industry, energy, medicine and others, should provide continuous monitoring of security. Information about the current security state of a system is typically logged as security events. This study proposes an algorithm for causal correlation of security events in cyber-physical systems based on an intelligent graph-oriented approach. The algorithm includes the generation of a security event sequence graph based on data mining. An experimental evaluation of the proposed algorithm is carried out using a dataset of the industrial cyber-physical system.
Key words: security events, correlation of security events, event graphs.

Kotenko I., Parashchuk I., Saenko I. The Content and Features of the Key Stages of the Development of Methods and Models for Processing Data on Cybersecurity Incidents in Departmental Infocommunication Networks**.** – PP. 674–678.
The content and essence of the key stages of the development of models, methods and algorithms for intelligent analytical processing of large arrays of heterogeneous data on cybersecurity incidents in departmental information communication networks are considered. The features of methodological techniques, mathematical methods and private technologies of artificial intelligence used in solving such problems are investigated and substantiated, which allow to increase the reliability and operativeness of decision-making on the protection of information, telecommunications and other critical resources in networks and systems of this class.
Key words: incident, analytical data processing, cybersecurity, method, model, artificial intelligence, infocommunication networks.

Kotenko I., Popkov I. Methodology of Automated Forensic Data Collection in Threat Hunting Processes. – PP. 679–683.
Threat hunting involves retrospective analysis of host and network telemetry within the chosen infrastructure compromise hypothesis. The use of forensic data collection techniques can expand the range of data analyzed. This paper proposes a methodology for automated selective

collection of forensic data to enhance the informativeness of data stored in SIEM. The collection of such data as MFT tables, traffic dumps, RAM and system calls based on the anomaly of previous events on the host is considered.
Key words: information security event monitoring, proactive incident detection, proactive threat detection, forensics.

Kotenko I., Popkov I. Analysis of Current Research Trends in the Topic of Threat Hunting. – PP. 683–687.
Threat hunting is an iterative process comprised of a group of interrelated threat management processes covering various areas of an organization's information security. The article analyzes the most important stages of Threat hunting from the point of view of current trends - infrastructure inventory, formation of penetration hypotheses, collection and correlation of telemetry data, and documentation of results. In each of these stages, current research problems and directions for solving them have been highlighted.
Key words: information security event monitoring, proactive incident detection, proactive threat detection

Kravets E. Measurement of Mechanical Oscillations in High-Precision Crystal Resonators. – PP. 688–692.
The design of new crystal resonator topologies requires studying the amplitudes and frequencies of oscillations of the resonator's surface. This paper presents solutions employing optical interference to measure amplitudes and frequencies of mechanical oscillations, and provides estimation of the possible range of measurements. Based on the analysis, it is proposed that the heterodyned light beam interferometer be used to optically measure the amplitude of superficial oscillations in the resonator, and the acousto-optic light modulator be used to shift the frequency of the optical signal.
Key words: resonator, Michelson interferometer, acousto-optic modulator.

Kravtsova V., Uchinin A., Tcvetkov A. Deploying a Group Domain Policy Taking as an Example a Commercial Organization. – PP. 692–697.
In today's world of rapidly developing technologies, virtualization mechanisms have become an important part of computer technology. Containerization technology is inextricably linked with the concept of virtualization. This technology allows you to provide an isolated launch of applications and work environments. The relevance of containerization is explained by the optimization of the work and testing of the application, the speed of their scaling and deployment. The purpose of the article is to describe the containerization mechanism, its operation and features, and methods for protecting containers.
Key words: containerization, virtualization, Linux, Astra Linux, Docker, cgroups, namespaces.

Kravtsova V., Ushakov I. Anomaly Detection in Computer Networks using Big Data Methods. – PP. 697–701.
Methods for committing cyber attacks are becoming more sophisticated every day. Protection options developed on the basis of signatures become unreliable. Network anomaly detection solutions monitor corporate networks for abnormal behavior to detect new threats and take timely action. A large amount of computation and constant changes in the distribution of network data make it difficult to analyze the data and detect anomalous behavior within it. From

this we can conclude that solutions for working with big data have become an integral part of the work on the implementation of information protection. This article will explore the study of network traffic anomalies using big data.
Key words: anomalies, intrusion, big data, neural networks.

Kravtsova V., Ushakov I. Building Secure Network Connections on the Basis of Domestic Equipment. – PP. 702–706.
VPN connections are necessary not only for remote work and anonymization of traffic, but also for organizing encrypted data exchange within wide networks of various enterprises. The drivers of the VPN gateway industry will be IoT devices, 5G technologies. New niches for cryptographic protection tools can be APCS and extractive industry enterprises. In connection with the current situation in the world, there is also a need to use Russian-made devices for these purposes.
Key words: crypto gateway, VPN, tunneling, VRRP, IPSEC, IKE.

Krasov A. Network Steganography Based on Fountain Codes. – PP. 707–711.
This paper presents a method for creating a steganographic channel using a fonetic code. The fountain code is used to transmit broadcast traffic in channels with an unknown loss rate. Since parts of the secret message are also lost when the carrier packet is lost, reliable transmission is ensured by using a second fountain code. In this way it is possible to create multi-layer steganographic channels that can be used in broadcast networks. This method opens up the possibility of bypassing echeloned security systems, and can also be used to deliver secret messages to a group of people.
Key words: network steganography, fountain code, hidden network storage channel, multilevel steganography.

Krasov A., Polyanicheva A., Safina A. The Use of IP PBX Agat CU in the Conditions of Import Substitution. – PP. 711–715.
Due to the current political situation and the current sanctions, the need for import substitution in Russia is becoming increasingly urgent. There are several manufacturers of domestic equipment on the Russian market, such as "Eltex", "Agat RT", "Multicom", etc. In the framework of this work, the software IP PBX Agat CU is considered in detail.
Key words: IP telephony, IP PBX, telecommunication equipment, import substitution.

Krasov A., Salita A. Comparison of the Effectiveness of Network Steganography Methods. – PP. 716–719.
New encryption algorithms are being developed to meet the ever-increasing demands for confidentiality of transmitted information. However, confidential information transmission can also be ensured by using network steganography techniques. This paper compares the performance of some of the most common network steganography techniques – packet header embedding, LACK and RSTEG.
Key words: network protocols, transport protocols, network analysis, network security.

Крюкова Е. С., Паращук И. Б., Смирнов А. А. Программные средства инфокоммуникационных сетей и систем хранения данных: нечеткая идентификация уязвимостей. – С. 719–723.

Рассмотрен методологический подход, позволяющий описать признаки уязвимостей в программных средствах инфокоммуникационных сетей и сетей хранения данных, позволяющий идентифицировать угрозы. Предложен метод решения задач идентификации объектов и процессов в условиях нечеткости их наблюдаемых признаков. Он основан на устранении нечеткости идентификации уязвимостей программного обеспечения, использует нечеткие и лингвистические переменные при обработке нечетких знаний о характеристиках потенциальных уязвимостей. Предполагается, что это позволит повысить достоверность контроля защищенности программных средств.

Ключевые слова: программные средства, угрозы, уязвимости, безопасность, инфокоммуникационная сеть, система хранения данных, нечеткие множества, идентификация.

Kuznetsov D., Tsvetkov A. Using Forced Access Control to Ensure Container Security. – PP. 723–727.

Containerisation is already an integral part of our world. In addition to all its benefits and features, it is also dangerous and has a number of vulnerabilities. Indeed, it almost always requires some sort of privilege to run or run containerized applications, and using root is very common. This article describes how enforced access control systems, using SELinux as an example, can strengthen container security and create a defense in depth.

Key words: information security, containerisation, SELinux, vulnerabilities.

Kuzmina O., Minyaev A., Sakharov D. Research of the IEEE 802.11mc Standard and its Applicability in the Information Security Framework of an Enterprise Wireless Network. – PP. 727–731.

Today's enterprise networks can reach a large scale. As the number of users on enterprise networks grows, so does the likelihood of an attack. Identifying the location of enterprise wireless clients is one way to create geo-zones to control employee movement in a given area. This approach to information security will allow the enterprise to provide the necessary level of wireless network security. The report presents a study of IEEE 802.11mc standard and its applicability within the framework of ensuring information security of an enterprise wireless network. Requirements for network clients and wireless equipment are considered.

Key words: wireless networks, location detection, LBS, Wi-Fi RTT.

Kutluyarova A., Malakhov V., Rogozinsky G. Systematization of Computer Music Technologies. – PP. 732–735.

The question of systematization of the field of computer musical technologies is considered. The description of the systems and the processes they perform using the EDF0 notation is given. A classification is proposed according to the types of objects and subjects involved in the processes, as well as according to the type of the core that performs the main functions.

Key words: computer music technology, sound object, EDF0.

Kutuev T., Petriv R. Comparative Analysis of Software and Hardware Solutions for Implementing Firewalls Based on Open Source Code. – PP. 736–740.
Due to the withdrawal of large foreign vendors of network equipment from the domestic market, support for purchased and used products is being discontinued. Therefore, there is a necessity to create a firewall with the possibility of easy software distribution and user support. Such a system can be a solution based on single-board computing platforms using open-source software.
Key words: single-board computer, freely distributed software, firewall, open-source software.

Kushnir D., Mikhailova Z. Blockchain Transactions and Alternative Technologies. – PP. 740–745.
The article presents a description of blockchain technology, its features, components and algorithms. It also lists options for possible vulnerabilities and threats to components and algorithms of this technology and ways to solve them in the future. Further, a comparative characteristic of alternative technology - a database is presented and the optimal ways of using both systems are revealed. Next is a description of the new Tracechain technology. In conclusion, a comparative analysis of blockchain and TraceChain technology is given.
Key words: blockchain, cryptographic protection, ECDSA blockchain vulnerabilities, algorithm, DDoS attack, PoS, smart contract, database, TraceChain.

Kushnir D., Nechaev A. Research on Vulnerabilities of Software and Hardware Clients of Blockchain Networks. – PP. 745–750.
The technology of blockchain has gained wide popularity thanks to cryptocurrencies. Along with the opportunities that cryptocurrencies provide, additional security problems arise for systems that use them. One of the attack vectors on these systems is the search for vulnerabilities in cryptocurrency clients, both software and hardware. Today, a whole range of typical attacks on each type of client is known, as well as universal attacks on both types of clients. Since clients are an integral part of virtually all blockchain systems, it is necessary to define criteria for their security and analyze existing implementations to determine the resilience of any blockchain solutions.
Key words: blockchain, vulnerability, crypto wallet, software wallets, hardware wallets.

Kushnir D., Nikonov E. Design Features of P2P Blockchain Network. – PP. 750–754.
The basis of the possibilities of projects based on blockchain technology is the interaction of the participants that make up the P2P network, which means that there is no mandatory separation of participants by roles. Network nodes are directly connected to each other, each of them can act both as a server and client. A study was made of building such a network based on the design of a full-fledged node with the implemented functions of interaction with other participants.
Key words: blockchain, distributed ledger, blockchain network, information security, key, signature.

Kushnir D., Platonova T. Quantum Computer Programming and Emulation in Information Security. – PP. 754–758.
At present, quantum technologies continue to actively develop. They require new approaches to realization of usual tasks in the field of calculations and communications. So, special programming languages have been developed to work with quantum computers. In addition, due to limited access to physical quantum technologies, tools for emulation of quantum computing have now been developed. The research of development of programs for quantum computers and work with emulators is carried out on the basis of Python programming language with the use of Qiskit library. The possibility of conducting research in the field of quantum programming for the subsequent solution of problems in the field of information security is shown.
Key words: quantum computer, cubit, gate, quantum computing, programming languages.

Lapteva T., Muthanna A. S. A. Analysis of Methods for Improving the Performance of Vehicle Networks Based on the Boundary Computing System. – PP. 759–764.
Connected vehicles is one of the main announced use cases of the fifth generation (5G) cellular system. It is a new era of communication that is known as vehicular networks and comes with many forms and services. Vehicular networks provide all services associated with the deployment of autonomous vehicles and the exchanged data between nearby vehicles. Such systems require full coverage, ultra-high reliability and availability, ultra-low latency, and high system flexibility as per the 3rd Generation Partnership Project (3GPP) and the International Telecommunication Union (ITU). Introducing MEC to the access network of the vehicular network to provide the computing resources at the edge of the network will be the first part of this work. This will reduce the end-to-end latency, reduce the network congestion, achieve higher reliability, and increase the network flexibility.
Key words: edge multicomputing, vehicle networks, internet of things.

Lebedev N., Svechnikov D. Ensuring the Protection of Information in a Mixed Network Domain. – PP. 764–767.
This article focuses on the option of organizing information security in a mixed network domain, including workstations running Windows and Astra Linux. The proposed solution will allow processing restricted access information that does not contain information constituting a state secret in automated systems of different security classes due to the integrated use of the information protection subsystems of the Astra Linux SE OS, Secret Net Studio, Secret Net LSP and the Sobol trusted download tool.
Key words: information security, information protection, monitoring, response to information security incidents

Levshun D. Approach to Simulation Modelling of Critical Infrastructure Facilities for Cyber-physical Attacks Analysis. – PP. 767–770.
Critical infrastructure facilities are an integral part of key sectors of the economy and are directly related to the livelihoods of people. Disruption of these facilities functioning leads not only to financial and reputational damage, but also affects the economy as a whole. At the same time, the number of cyber-physical attacks on information resources is growing rapidly. One of the possible ways to analyze the security of critical infrastructures is their modeling. This paper proposes an original approach to simulation modeling of such objects for the analysis of cyber-physical attacks. The novelty of this approach lies in the dynamic analysis of attacks using information about the processes and resources of the system, detection of conflicts and

boundary conditions, multi-agent modeling, event modeling, modeling attackers with different levels of competence and access rights, modeling attacks and their consequences.
Key words: information security, critical infrastructure facility, cyber-physical attack, simulation modelling.

Lepeshkin O., Ostroumov O., Pirogov O., Chernykh I. Continuity and Autonomy of System Functioning – Elements of Its Functional Stability. – PP. 770–775.
Any control system complex technical objects, critically important objects at the present stage of technology development use lines, nodes, a communication system. One of the properties of a communication system is the continuity and autonomy of the system functioning, which characterize the ability to perform the system functions, the performance of which is described by the system functional stability. The paper considers ensuring the functional stability of a complex technical system.
Key words: critical information infrastructure, critical facility, functional stability, continuity, autonomy, communication system, control system, tasks, functions.

Makarova A., Smirnov D., Tsvetkov A., Chumakov I. Consideration of the Components of the FreeIPA Trusted Relationships Technology, as Well as the Question of the Feasibility of Transitioning to This Solution. – PP. 775–778.
The topic of a centralized system for user management and identification, as well as the creation of a set of group policies and access control to network devices, is an important aspect of ensuring network security. Currently, there is no perfect solution in the world that includes the operation of all operating systems under one technology for building trusted relationships in the network. By considering this issue, it will be possible to create a system that supports all operating systems, including the operation of group policies in the network and access control to network resources, which will increase the level of security in organizations that use various OS variants in their production.
Key words: trusted relationships, FreeIPA, Windows AD, information security.

Makolkina M., Pankov B. Identification of Requirements Imposed by Holographic Traffic to Communication Networks. – PP. 778–783.
The telecommunications development strategy of the current decade includes a direction for the global and widespread introduction of telepresence services based on holography technology and its capabilities for building three-dimensional copies of a person, using avatar robots and manipulating devices with the possibility of combining them into logical groups and communities. Undoubtedly, due to the lack of knowledge of physical principles and the lack of technological solutions in the field of reproducing holographic devices, the tasks set will not be implemented at once, as a result of this, it is necessary now to start forming a list of network requirements for telepresence services, further imposed on the parameters of communication lines of the Russian Federation, functional capabilities of telecommunications equipment and traffic characteristics of 3D images. The relevance of the research direction is due to the need to gain an understanding of the required efficiency of network interfaces, protocols, as well as the topology and principles of organizing control, switching and routing components with practical explanations on the required levels of quality of service (QoS) and quality of experience (QoE) in the mass implementation of holographic services telepresence.
Key words: telepresence, holography, 3D imaging, augmented reality, avatar robots, 2030 networks, 6G, 3D, HTC.

Markelova M., Shelehov A. Simulation-Based Delay Estimation in Multiple Access Networks. – PP. 784–789.

*This study is devoted to the development of a mathematical model of multiple access networks with different topologies with the possibility of considering the correlations between nodes. At the first stage, simulation modeling was carried out using the NS-3 network simulator. As a result of modeling, files with network traffic data dumps in *.pcap format were obtained, which can be used for further statistical analysis. Thus, a tool is proposed for generating implementations of traffic data in a network with dependent nodes.*

Key words: multiple access networks, delay estimation, NS-3 simulator.

Metelkov A., Shestakov A. Cyberpolygons and Testing Grounds: Foreign Experience of Information Protection and Systems from Cyber Threats. – PP. 789–794.

The article considers the foreign experience of using the technology of cyber polygons and test benches in protecting information and systems from cyber threats. The experience of the USA and other countries in the use of cyber polygons for training in the conditions of digital transformation, hybrid wars in cyberspace requires deep understanding and consideration in the development of similar systems in the Russian Federation, government agencies and higher educational institutions. According to the results of the study, on the basis of program-targeted approaches to the problems of cyber polygons implemented by the Ministry of Finance of Russia, and taking into account precedents in world practice, it is possible to develop departmental technologies, for example, in the Ministry of Emergency Situations of Russia.

Key words: cyberpolygon, threats, computer attacks, resilience, security measures.

Mikhailichenko A., Pantyukhin O., Parashchuk I. A Variant of the Formulation of Probabilistic Partial and Complex Indicators of the Technical Reliability of Mobile Data Centers. – PP. 795–799.

A possible approach to the formulation of a probabilistic complex indicator of the technical reliability of mobile data centers based on the joint conditional probability of meeting the requirements for deviations of its particular reliability indicators characterizing the parameters of reliability, durability, maintainability and preservation of an object of this class is considered. The analysis of potential options for the formulation of particular indicators and prospects for the application of this approach to solve the problems of reliable and operational assessment and forecasting of the reliability of modern mobile data centers is carried out.

Key words: technical reliability indicator, mobile data center, requirements, deviations, conditional probability, maintainability.

Михайличенко А. В., Паращук И. Б. Процедуры гранулярного выбора анализируемых параметров технической надежности современных дисковых систем хранения данных. – С. 799–803.

Рассматриваются вопросы обоснованного, достоверного выбора анализируемых параметров технической надежности дисковых систем хранения данных, используемых, например, в современных мобильных дата-центрах. Реализовано формальное описание подхода к гранулярному выбору наполнения множеств таких параметров, состав которых необходимо формировать с учетом неточных, «зашумленных» нечетко заданных исходных данных. Предложенный подход призван выступать в качестве системы поддержки принятия решений в интересах формулировки безызбыточной, но полной и

обоснованной системы контролируемых параметров, что, в свою очередь, призвано повысить точность и оперативность решения задачи анализа технической надежности систем такого класса.
Ключевые слова: анализируемые параметры, дисковые системы хранения данных, техническая надежность, неточные, "зашумленные" нечетко указанные исходные данные, нечеткость.

Mikhailov P., Muthanna A. Research of Virtualization Architecture and Live Migration for Future Generation Communication Networks. – PP. 803–808.
One of the main implementations of next-generation communications networks is based on low latency, which will allow quick access to different services. And to achieve the minimum time to access an application or service from Internet of Thing devices. Data processing will require servers for fog computing, but then we are faced with the question of how to place the required applications on demand, as applications are originally in the cloud. In this article we will try to consider how services can migrate between clouds.
Key words: Internet of Thing, Fog computing, service migration.

Mihaljov O., Ryabov M. Electronic Warfare Methodology for Deploying a Wi-Fi Software Suppressor. – PP. 809–813.
Some notable examples have focused on electronic warfare. For example, the US military has invested heavily in automation through drone programs only for competitors such as the Iranians to create strategies to interfere with these systems. Iran managed to capture a top-secret American reconnaissance drone by tricking it into descending in the wrong place, jamming its control signals and providing it with fake GPS data. This article focuses on an electronic warfare approach for deploying a Wi-Fi jamming software suppressor. A Wi-Fi jamming software jammer can disable targets using DoS pursuit mode. The article describes a methodology for how software can also be used to suppress wireless signals.
Key words: Wi-Fi, Wireless, Wi-Fi Jammer, Electronic Warfare, wireless attacks.

Murashkin N., Pomogalova A. Creation of Blockchain Consensus Algorithm Based on Mobile Devices. – PP. 813–817.
Nowadays blockchain technology becomes an important part of life of humanity all over the world. There are acute problems of financial transactions, data security and confidentiality. Blockchain stopped to be mysterious and difficult, entered in mobile cryptowallets and accounts of digital exchanges, which are accessible by finger's touch at any place in the world. Modern mobile devices' capacity surpassed capacity of computers ten years ago, so it goes without saying: technical progress is unstoppable. But why is blockchain something powerful and available only for owners of super-performing devices? This work appears to be analysis of reasons and possibilities of blockchain consensus algorithm creation based on mobile devices.
Key words: blockchain, Ethereum, mobile apps, smartphone, consensus algorithm, Proof-of-Work, Proof-of-Stake.

Pavlov I. Optical Properties of Water and Their Dependence on the Type of Aquatic Environment. – PP. 817–823.
The development of underwater optical communications will ensure the study of the seabed, observation of deep-water and oceanic oil pipelines, underwater zoological life, communication with submarines and unmanned systems, etc. Optical communication is strongly affected by the characteristics of the water channel, as well as the turbidity and salinity of the water, which can reduce performance. In addition to turbidity and salinity, impurities and water molecules have an effect, so the underwater environment must be considered as a complex and dynamic environment. To gain a deeper understanding of the underwater environment and channel characteristics, extensive field studies are required. This article presents the optical properties of water and also discusses the optical properties for different types of water.
Key words: electromagnetic wave, radio frequency wave, data transmission rate, optical wireless communication, water environment.

Pavlov I. A Brief Overview of the Use of Radio Frequency and Optical Spectra in Underwater Wireless Communication. – PP. 823–828.
Underwater communication technologies have come a long way with the implementation of wireless technologies that use acoustic waves or electromagnetic waves. The latter can be implemented in the radio frequency spectrum or in the optical spectrum. Electromagnetic waves provide high-speed data transmission and high-speed communication. Moreover, underwater radio frequency communication provides a smooth transition between water and air, and it is not affected by the turbidity properties of water. Wireless communication in the optical spectrum has high bandwidth and low cost. For this reason, the review in this article is devoted to various aspects of underwater wireless communication using radio frequency and optical spectra.
Key words: electromagnetic wave, radio frequency wave, data transmission rate, optical wireless communication, water environment.

Parashchuk I., Sayarkin V., Seleznev A. Analysis and General Classification of Cybersecurity Risks for Document Management Automation Systems Based on Modern Infocommunication Networks. – PP. 828–832.
The analysis is carried out and the distinctive features of threats and the facets of possible damage caused by the main cybersecurity risks for document management automation systems based on modern infocommunication systems are considered. It is assumed that taking into account these features and classification features will increase the degree of validity of decisions on the development and technical implementation of high-quality cybersecurity subsystems for automated processing of electronic documents using channels and paths of modern infocommunication networks.
Key words: infocommunication network, document management automation system, electronic document, risks, cybersecurity.

Parashchuk I., Sundukov V. Stages of Development of Models and Methods of Multi-Factor Authentication of Users as Elements of the Policy of Differentiation of Access Rights to the Resources of Infocommunication Networks. – PP. 833–837.
The physical essence and functional content of the stages of development of modern models and methods of multi-factor authentication of users within the framework of the policy of the restriction of access rights of these users to the resources of infocommunication networks are

considered, analyzed and systematized. The analysis of possible private models and methods allowing to assess the quality of authentication, optimize and adapt the procedures of this multi-factor authentication process of network users is carried out.
Key words: infocommunication networks, models, methods, access rights differentiation policy, multi-factor authentication, user, stage, resources.

Parashchuk I., Chechulin A. Neuro-fuzzy Vulnerability Detection Method for Monitoring the Security of Processes and Means of Human–Intelligent System Interaction within the Framework of the "Smart Transport" Concept**.** – PP. 837–841.
A new, neuro-fuzzy method of detecting vulnerabilities of processes and means of interaction (interaction interfaces) of the "human – intelligent system" class in modern intelligent transport systems focused on the concept of "Smart Transport" is proposed. This method exploits the advantages of neuro-fuzzy networks, is considered as an element of security policy and is implemented within the framework of procedures to increase the reliability of security control of such objects. The practical use of this method will eliminate the complex uncertainty (of a joint type: fuzziness and incompleteness and inconsistency) of the source data that occurs when solving problems of searching for vulnerabilities of intelligent interfaces of this type in the real conditions of the implementation of the "Smart Transport" concept.
Key words: neuro-fuzzy networks, smart transport, intelligent transport system, interface, vulnerability, detection, method

Pekin D., Fedorova E., Tsyganov V., Sharapov R., Shemyakin S. Description of Vulnerabilities of Information Systems CVE-2022-1525, CVE-2022-1368, CVE-2022-1522, CVE-2022-38138 and Methods of Countering Them. – PP. 841–847.
The purpose of this article is to describe a number of vulnerabilities related to the operation of information systems. In this article, the analysis of vulnerabilities and attacks performed by exploiting these vulnerabilities was applied. Examples of attacks performed by exploiting these vulnerabilities are given. The article also describes measures to counter these vulnerabilities. Based on what is described in this article, we can conclude that the most common causes of vulnerabilities, as a rule, include: errors in the design and use of software; unauthorized introduction and subsequent use of the software; the introduction of malware; human factor. Timely response to the emergence of certain vulnerabilities and following the recommendations for their elimination contribute to maintaining the overall level of information security at the proper level.
Key words: information security; vulnerability, cyber attack, information system, monitoring.

Pestov I., Yurova U. Integration of a Linux Client Machine Into an Active Director Domain. – PP. 847–852.
Modern society is rapidly developing in the direction of a fully connected intellectual world, and such trends put forward unprecedented requirements for the reliability and safety of consumer goods. New smartphones are entering the technology market every day. The development of portable devices with a Linux operating system, with touch control, has made significant progress over the past few years. When planning to buy a mobile phone, whether new or used, people take into account certain parameters, such as color, size, characteristics, quality of the camera, processor and memory. But the most ignored part is the operating system. The article

provides a comparative analysis of modern Linux-based mobile operating systems on the market, such as Sailfish OS, Ubuntu Touch, HarmonyOS, as well as issues of their privacy and security
Key words: operating system (OS), mobile platform, microkernel, Linux, Sailfish OS, Ubuntu Touch, HarmonyOS, security.

Petrov I., Shemyakin S. Pseudorandom Numbers and a Pseudorandom Sequence Generator. – PP. 853–857.
This article shows a method for obtaining a pseudorandom sequence with the help of a user, two basic requirements for a sequence of random numbers, the basic properties of any periodic binary sequence, tests used to check the quality of generators and the basic requirements that cryptographically stable pseudorandom sequence generators and the gammas obtained with their help must satisfy.
Key words: pseudorandom sequence generator, random numbers, cyclicity, balance, correlation, graphical tests, statistical tests, cryptographically stable pseudorandom sequence generators.

Petrov I., Shemyakin S. Research of the Main aspects of Astra Linux, the First Acquaintance with the Operating System and its Installer, Why Government Agencies Switch to Astra Linux, Whether it is Worth Switching to Ordinary Users. – PP. 857–861.
This article provides information containing: what is the Astra Linux operating system in general and the general-purpose Astra Linux "Eagle" Common Edition operating system in particular, the features of the Astra Linux installer, information about the repository and its security, user convenience when using Astra Linux, why government agencies and the commercial sector are switching to it, and why it is the main domestic operating system.
Key words: Astra Linux, Astra Linux "Eagle" Common Edition, operating system, Astra Linux installer, repository, Astra Linux security.

Petrova T., Sakharov D., Tasyuk A. Analysis of the Features of the Construction of Modern Distributed Computing Networks that Affect the Security of Information. – PP. 861–864.
Information security in modern distributed computing networks is a complex problem that is affected by various functions, such as network segmentation, access control, identity and access management solutions, endpoint security and intrusion detection systems. These functions play a crucial role in protecting confidential information from unauthorized access and other security threats.
Key words: information security, distributed computing network, information warfare, cyber conflict, cyber threats.

Ponamarenko E. Overview of Approaches to Measuring the Quality of Service and Perception in Tactile Internet Systems. – PP. 864–869.
With the development of cellular communications and the achievement of fifth-generation mobile networks, Tactile Internet (TI) technologies are given considerable attention. In any system it is important to consider the parameters and characteristics to measure the quality of service and user perception. The subject of the study is a review of approaches to measuring the quality of service and perception in TI systems. Research method: collection and analysis of available research on the topic of measuring the quality of service and perception in TI systems. The

main results. Various methods and approaches to measuring the quality of service and perception are described. Practical significance. Based on the proposed approaches, it is possible to develop new methods and/or improve existing ones.
Key words: Tactile Internet, haptic interactions, kinesthetic information, tactile codec, quality of service, quality of perception.

Popova V., Chechulin A. Distinctive Features of Critical Infrastructure Object Systems in the Context of the Problem of Countering Cyberattacks. – PP. 870–872.
The critical infrastructure nuclear sector has unique characteristics and requires a special approach to ensuring the cybersecurity of facilities. The potential feasibility of a cyber threat to control systems of industrial facilities of critical infrastructure has been confirmed both in the course of experiments conducted by various structures responsible for the security of these systems, and by cybersecurity incidents that have already occurred. This study analyzes and systematizes the distinctive features of critical infrastructure objects according to the proposed criteria, which ultimately will allow us to determine the types of possible cyber-attacks and effectively counter them.
Key words: critical infrastructure facilities; vulnerability analysis; open databases.

Pronichev V., Ushakov I., Filyova V. Security Functions Realization on Eltex ESR Routers. – PP. 873–877.
A layered approach to routing security allows for robust protection against major network threats. Particular attention is paid to the multifunctionality of ESR Series routers, which allows you to combine various tools to ensure network security across the board. The article considers ESR routers functions that provide security against potential attacks, and justifies the competitiveness of domestic routers in the market under conditions of import substitution.
Key words: routers, security features, import substitution, comparative analysis.

Pschelko N., Sanin Yu. Increasing the Speed of Digital Signal Processing Through the Use of Codes of the Residual Class System. – PP. 877–880.
Currently, discrete wavelet transformations and, in particular, a method of signal processing using discrete wavelet transform in finite Galois fields are used in solving digital signal processing problems related to their processing and signal compression. It is shown that these transformations are carried out on the basis of wavelets and provide higher accuracy of transformations in comparison with traditional approaches, however, they require the selection of values of the used bases of the system of residual classes. The development of an algorithm for finding the bases of a system of residual classes makes it possible to quickly calculate a given number of bases for various types of wavelets in order to calculate a discrete wavelet transform.
Key words: digital signal processing, discrete wavelet transform, residual class system.

Salman W. Evaluation the Complexity of the Method Verifying the Correctness of Filling Out a Ballot by a Voter in a Remote Electronic Voting System. – PP. 880–885.
A method that allows the supervisory authority to make sure that the voter voted correctly for each candidate is investigated. The peculiarity of solving this problem is that the verification is carried out using an encrypted ballot and the supervisory authority does not know how the voter voted. To solve the problem, the methods zero- knowledge proof and the properties of

homomorphic encryption are used. The complexity of the implementation of this method has been assessed.
Key words: remote voting system, verification the proof of correctness filling the ballot, zero-knowledge proof.

Salman W., Yakovlev V. Method of Checking the Correctness of Filling Out the Ballot in the Remote Electronic Voting System. – PP. 885–890.
A method has been developed to verify the correctness of filling out the ballot as a whole, which has a low complexity on the blockchain side. Evaluations the complexity of calculations the formation proof of the correctness filling out of the ballot by the voter and evaluations the complexity of verifying the proof by the controlling party are obtained. The description of the method is accompanied by a numerical example of the correct filling out of the ballot.
Key words: remote voting system, verification the proof of correctness filling the ballot, zero-knowledge proof, scheme El-Gamal.

Saltykov A., Slepogin A. Overview of Higher-Speed 50G-PON Systems. – PP. 891–895.
The report provides an overview of the 50 GPON high-speed system. The purpose of the work is to familiarize students with the purpose, principle of operation and technical characteristics for a 50 Gb/s line rate passive optical network (PON) system. Attention is paid to fundamental advances in the field of optical transceivers working in combination with an improved error correction procedure and coding, as well as key innovations in the activation procedure, which operates on the basis of competition (contention-based operation) and advanced cryptographic features. With these improved capabilities, 50G-PON systems are ready for increased requirements to provide new high-quality services.
Key words: 50-GPON, contention-based operation, fiber optic transmission system equipment, communication organization scheme, fiber optic communication line.

Semenov A., Sokolov E. Performance Estimation Method for Symmetrical Cable Path in Structured Cabling System. – PP. 896–900.
A method for estimating Shannon capacity of symmetrical cable paths of the high-speed information cable systems is considered. The possibility of determining this parameter from the PSNEXT characteristic of a linear cable is shown. The prevailing influence of near-end crosstalk on the capacity of the cable system is substantiated. The growth of the influence of connectors on the throughput of the cable path as its class increases was established, i.e. increasing the maximum information transfer rates guaranteed to be supported by the SCS.
Key words: symmetrical cable path, crosstalk, Shannon capacity, class combination, structured cabling systems.

Skorykh M. Using JA3 Hashes as Indicators of Compromise. – PP. 901–905.
The paper considers an approach to detecting computer attacks and incidents in encrypted HTTPS traffic. The relevance of the topic is due to the complexity of the analysis of encrypted network traffic by modern intrusion detection systems. In the course of the work, the process of generating a JA3 hash is considered in detail. A stand was demonstrated with emulation of computer attacks on web resources using the Burp Suite software, as well as infection of nodes with known types of malicious software: Cobalt Strike, Merlin, Metasploit. The possibility of

detecting simulated computer attacks and incidents using the JA3 hash as an indicator of compromise is shown, the advantages and disadvantages of this method are listed, and further research directions are listed.
Key words: JA3 hash, HTTPS, network traffic, anomaly detection, intrusion detection systems, malware, Cobalt Strike, Metasploit, Burp Suite, Merlin.

Tarov E., Shemyakin S., Yakovlev V. Solving a System of Equations Based on the Chinese Remainder Theorem using the Montgomery Algorithm. – PP. 906–910.
A method of applying the Montgomery algorithm to reduce the computational costs of modular calculations when solving a system of equations based on the Chinese remainder theorem is considered. The software implementation of the proposed method in Python has shown that the use of the Montgomery algorithm significantly increases the speed of solving the system for large-bit numbers in comparison with the standard algorithm.
Key words: information security, cryptography, modular arithmetic, Montgomery algorithm.

Uchinin A., Tsvetkov A. Researching the Main Characteristics and Functional Capabilities of SIEM Systems. – PP. 910–916.
In the modern world of rapidly developing technologies, the mechanisms for protecting the information structure of an enterprise have acquired an important role among computer technologies.
With the development of technology, methods of obtaining unauthorized access and attacks on corporate networks have also evolved. In this regard, the protection of networks within enterprises became more complex and complex, began to include an increasing number of different systems that prevent harm to the network infrastructure. The number of information events in corporate networks may be too large to analyze each system separately. The task of structuring and correlating information received from various network security services was solved by SIEM systems that collect and analyze this information in real time.
Key words: *SIEM, information security, information, data, information security systems, control, incident.*

Fomin A. Current Status of Network Coding Applications in Wireless Data Networks Overview. – PP. 917–921.
The article provides a brief overview of current research in the network coding field in wireless data networks, which has been carried out over the past 10 years, and reviews the existing protocols based on the network coding method. The features of the reviewed studies are highlighted and their significance is given. The presentation has been grouped according to the years of research.
Key words: wireless networks, network coding, protocols.

Fomin S., Shvidkiy A. Analysis of the Mechanisms for Maintaining the State of the Cloud Service Infrastructure. – PP. 922–926.
This article describes several approaches to automated maintenance of a deployment, about common problems with a standard type of deployment. Service deployment mechanisms are increasingly being used these days. Ready-made services require the creation of a state in the environment. The purpose of this work is to study the security state that will respect the state of the service, a description of state maintenance methods. An analysis of various situations is

carried out to identify the consequences of a cloud service, as well as the most appropriate mechanisms for solving the identified problems.
Key words: deployment, Ansible, GitLab, Terraform.

Tcvetkov A. Analysis of Existing Protection Mechanisms and Attacks in Operating Systems. – PP. 927–931.
Ensuring security in a modern operating system depends to a greater extent on the quality of the implemented mechanisms laid down initially during development. Such errors can be both unintentional in nature and pursue certain goals: undocumented collection of information and statistics about the system, gaining access to computing resources, etc. Due to the fact that the probability of the existence of such vulnerabilities in the deployed system is not zero, it is necessary to analyze the existing basic means of ensuring information security, as well as countering unauthorized behavior of users and processes.
Key words: operating system, access control, unauthorized access attack, privileges.

Tsurbelev A., Shvidky A. Analysis of Cloud System Deployment Mechanisms Using the Infrastructure as Code Approach. – PP. 932–935.
Cloud systems in the modern world are becoming increasingly popular in various fields of information and communication technologies. This article discusses the approach of infrastructure deployment (Infrastructure as Code), which allows you to solve the problems of configuration, scalability and interaction of its various components. A comparative analysis of the currently existing deployment tools according to various criteria, their main advantages and disadvantages is carried out.
Key words: information technologies, cloud provider, Infrastructure as Code.

Shterenberg S. Simulation of an Intelligent Intrusion Detection System Based on Machine and Deep Learning. – PP. 935–940.
It is known that the number of smart devices is currently steadily growing. The need to protect them is growing, algorithms and methods of attacking systems that contain the fundamental elements of the development of artificial intelligence (hereinafter – AI) are becoming more complicated. It means that in the course of the development of AI, it becomes necessary to develop a unified methodology for building information security systems (hereinafter referred to as SPI) aimed at protecting any intelligent systems and devices. A special place in the design is occupied by the "immune systems" of cybersecurity, which will include various components from "threat knowledge" to Big Data processing. This article will be about modeling such systems.
Key words: SIEM, IDS, artificial intelligence, machine learning, deep learning.

АВТОРЫ СТАТЕЙ

АБРАМОВ Сергей Степанович — академик МАС, доктор технических наук, доцент, заведующий кафедрой радиотехнических устройств и техносферной безопасности, профессор кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, abramov@sibsutis.ru

АБРАМОВА Евгения Сергеевна — кандидат технических наук, доцент, доцент кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, evgenka_252@mail.ru

АБРАМОВА Елизавета Андреевна — студентка группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, abramowa400@gmail.com

АВРАМЕНКО Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АГАЕВ Руслан Ильхамович — студент группы ИКБ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agaev.0250@yandex.ru

АДАМ Юрий Александрович — студент группы V42041 национального исследовательского университета ИТМО, инженер лаборатории квантовых коммуникаций университета ИТМО, iaadam@itmo.ru

АДЬОТУМ Юсеф Мохаммед Абд Аллх — студент аспиранта, кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yousefot49@gmail.com

АЛЕКСАНДРОВА Агата Георгиевна — студентка группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agatka.aleksandrova27@mail.ru

АЛЕКСАНДРОВА Екатерина Алексеевна — студентка группы ИКБ-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekalex4@gmail.com

АЛЕХИН Роман Вячеславович — техник кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman2001-10@outlook.com

АЛИМЕТОВ Камиль Самирович — студент группы ИКБ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kamil.alimetov@mail.ru

АЛЬ-КЕРЕА Захраа Ахмед — аспирант кафедры сетей связи и передачи данных Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, eng-za@mail.ru

АНДРЕЕВА Арина Руслановна — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения императора Александра I, arinrus9@gmail.com

АРСИРИЙ Алла Ивановна — кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ars-alla@rambler.ru

АХАПКИНА Анастасия Михайловна — курсант 3-го курса военного факультета Белорусского государственного университета информатики и радиоэлектроники, anastasia.akhapkina2018@yandex.by

АХРАМЕЕВА Ксения Андреевна — кандидат технических наук, доцент, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oklaba@mail.ru

БАБИЧ Василий Николаевич — студент группы ИКТУ-03 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, babichvn22@mail.ru

БАБКОВ Иван Николаевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ib9809@mail.ru

БАБОШИН Владимир Александрович — кандидат технических наук, доцент, доцент кафедры восстановления устройств автоматики, телемеханики и связи на железных дорогах Военного института (железнодорожных войск и военных сообщений) Военной академии материально-технического обеспечения им. генерала армии А.В. Хрулева. boboberst@mail.ru

БАКАТОВ Виталий Николаевич — магистрант, студент группы ИКПИ-292м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bakatovvitalij@gmail.com

БАРАКАТ Абдельрахман Юсеф Хадер — студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ayb.jo.93@hotmail.com

БАТЕНКОВ Кирилл Александрович — доктор технических наук, доцент, профессор кафедры прикладной математики МИРЭА – Российского технологического университета, pustur@yandex.ru

БАТИН Евгений Александрович — студент группы ИКБ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zhenya-batin@mail.ru

БАШМАКОВ Алексей Васильевич — доцент кафедры комплексного обеспечения информационной безопасности 95 Санкт-Петербургского государственного университета морского и речного флота имени адмирала С.О. Макарова, abashm@mail.ru

БЕККЕЛЬ Людмила Сергеевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, milla.beckel@gmail.com

БЕЛАЯ Татьяна Иоанновна — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, studentszip@yandex.ru

БЕЛОЗЕРОВ Клим Владимирович — студент группы ИКТК-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, milk8490@gmail.com

БЕЛЯЕВ Дмитрий Леонидович — кандидат технических наук, доцент сотрудник Академии Федеральной службы охраны Российской Федерации, bdl33@academ.msk.rsnet.ru

БЕЛЯЕВ Павел Юрьевич — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, monoe1337@gmail.com

БЕРЕЗИН Александр Юрьевич — аспирант, ассистент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, berezinalexhdr@gmail.com

БЕРЕЗКИН Александр Александрович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aa.berezkin@mail.ru

БИРИХ Эрнест Владимирович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, be1982@mail.ru

БОГОМАЗ Мария Эдуардовна — студентка группы ИКТЗ-21м кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maria.bogomaz15@gmail.com

БОГОМЕДОВА Карина Магомедовна — студент группы ИКБ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, thenadka@gmail.com

БОЛОТОВ Тимофей Вячеславович — студент группы ИКТК-96 Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, bolotov.t56@gmail.com

БОРОВСКАЯ Яна Александровна — аспирант кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики, yana.borovskaya.98@mail.ru

БУГРОВА Екатерина Сергеевна — студентка ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bugrova.es@sut.ru

БУДАРНЫЙ Глеб Сергеевич — студент группы ИКБ-91 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, budda.gleb1901@yandex.ru

БУРДИН Павел Павлович — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neutrieman@gmail.com

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент, заведующая кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

ВАЛЕЕВ Денис Рашидович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, lemniscatta.den@gmail.com

ВАСИЛЬЕВ Никита Алексеевич — младший научный сотрудник научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vasn2020@mail.ru

ВАСИЛЬЕВ Сергей Александрович — магистрант 1 курса кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vasiliev_1999@gmail.com

ВАСИН Антон Сергеевич — аспирант кафедры инфокоммуникационных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antoshca-vasin@yandex.ru

ВЕДЕНЬКИН Денис Андреевич — кандидат технических наук, доцент кафедры радиофотоники и микроволновых технологий Казанского национального исследовательского технического университета им. А.Н. Туполева-КАИ, denis_ved@mail.ru

ВЕРАС Никита Александрович — студент группы ИКТЗ-94 Санкт-Петербургского государственного университета Телекоммуникаций им. профессора М. А. Бонч-Бруевича, makhonina.y@inbox.ru

ВЕСЕЛОВ Даниил Алексеевич — студент 1-го курса магистратуры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; daniil.veselov2012@yandex.ru

ВЕТРОВ Николай Сергеевич — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikolaj.vetrov.2012@mail.ru

ВИВЧАРЬ Роман Михайлович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ВИКУЛОВ Антон Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, asv012016@gmail.com

ВИННИКОВ Семен Андреевич — студент группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций, vinnikovsema@mail.ru

ВИТКОВА Лидия Андреевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; старший научный сотрудник Лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра российской академии наук vitkova@comsec.spb.ru

ВЛАДИМИРОВ Сергей Сергеевич — доктор технических наук, доцент, доцент кафедры сетей связи и передача данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВОЛКОВ Владислав Дмитриевич — студент группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladislavvolkovn1@yandex.ru

ВОЛКОГОНОВ Владимир Никитич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, volkonogov.ikss@yandex.ru

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, научный сотрудник научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, ra1alo@mail.ru

ВОРОБЬЕВ Павел Владимирович — младший научный сотрудник Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, akvalangist.sobaken@gmail.com

ВОРОНЦОВ Андрей Анатольевич — студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vorontsov.andrey000@yandex.ru

ВОРОШНИН Григорий Евгеньевич — студент группы ИКТБ-18м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, voroshnin.g@yandex.ru

ВЫБОРНОВА Анастасия Игоревна — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.vybornova@spbgut.ru

ГАВКАЛЮК Богдан Васильевич — кандидат технических наук, доцент, начальник Санкт-Петербургского университета ГПС МЧС России, rector@igps.ru

ГЕГЕЛЬСКИЙ Максим Александрович — оператор роты (научной) главного управления связи военных сил Российской Федерации, vasn2020@mail.ru

ГЕРАСЬКИН Валерий Кириллович — магистр кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, geraskin.valery@gmail.com

ГЕРЛИНГ Екатерина Юрьевна — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, gerlingeu@gmail.com

ГИЛЬФАНОВА Альмира Фанисовна — аспирант кафедры радиофотоники и микроволновых технологий Казанского национального исследовательского технического университета им. А. Н. Туполева-КАИ, gilfanovaaf@stud.kai.ru

ГЛАГОЛЕВ Сергей Федорович — кандидат технических наук, доцент, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, GlagolevSF@yandex.ru

ГОЙХМАН Вадим Юрьевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vg@sotsbi.ru

ГОНЧАРОВ Савелий Васильевич — студент 1-го курса магистратуры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича; saigon2000@inbox.ru

ГОРБАНЬ Сергей Андреевич — студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gsa.work4409@yandex.ru

ГОРБУЛЕНКО Егор Андреевич — младший научный сотрудник научно-исследовательской лаборатории 42 лазерно-локационных систем АО «НИИ ОЭП», GorbulenkoEA@niioep.ru

ГОРДА Максим Дмитриевич — аспирант Санкт-Петербургского Федерального исследовательского центра Российской академии наук, m.gorda.lengu@ya.ru

ГОРЛОВ Николай Ильич — доктор технических наук, профессор, профессор кафедры фотоники в телекоммуникациях Сибирского государственного университета телекоммуникаций и информатики, gorlovnik@yandex.ru

ГОРЯЧКИНА Анастасия Олеговна — студентка группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, NGoryachkina01@mail.ru

ГРИШИН Илья Владимирович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i.v.grischin@mail.ru

ГУРЬЯНОВ Илья Сергеевич — студент группы Б19-282-1 Ижевского государственного технического университета им. М. Т. Калашникова, ilyaguryanov2018@gmail.com

ДАЛЕХ АЛЬ-МАГСУСИ Алаа Абдулхуссейн — аспирант факультета безопасности информационных технологий Национальный исследовательский университет ИТМО, adleah@uowasit.edu.iq

ДЕМЕНТЬЕВ Роман Игоревич — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hjvf128@mail.ru

ДЕМИДОВ Николай Александрович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, deminickal@outlook.com

ДЕРЖКО Дмитрий Ярославович — студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dimaderzhko@gmail.com

ДЕРКАЧ Алексей Евгеньевич — соискатель (аспирант) кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ДМИТРИЕВА Юлия Сергеевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitrieva_spbgut@bk.ru

ДМИТРИЕНКО Михаил Евгеньевич — кандидат физико-математических наук, преподаватель 31 кафедры Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, midmitrienko@mail.ru

ДО Хао Фук — магистр компьютерных наук, аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. Бонч-Бруевича, haodp@dau.edu.vn

ДОНСКОВ Евгений Андреевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, radion2002@gmail.com

ДРЕПА Владислав Евгеньевич — студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladikdrepa@mail.ru

ДУН Хуэйяо — аспирант факультет безопасности информационных технологий Национальный исследовательский университет ИТМО, hydong@itmo.ru

ДУНАЙЦЕВ Роман Альбертович — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.dunaytsev@spbgut.ru

ДЮСМЕТОВА Азалия Айдаровна — студент группы ИКБ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dyusmetova_azaliya@mail.ru

ЕВТИХИН Иван Олегович — аспирант Российской академии народного хозяйства и государственной службы, ivanevtihin@ya.ru.

ЕДЕМСКАЯ Екатерина Дмитриевна — студентка группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekaterina.edemskaya51@gmail.com

ЕЛАГИН Василий Сергеевич — кандидат технических наук, доцент, доцент кафедры инфокоммуникационных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elagin.vas@gmail.com

ЕЛАГИН Владислав Михайлович — студент группы ИКТУ-97 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elaginvlad04@gmail.com

ЕЛИЗАРОВА Лия Романовна — студентка группы ИКБ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elizarovaaliya@gmail.com

ЕРМОЛАЕВ Егор Евгеньевич — магистр кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egoulya@mail.ru

ЕРШОВА Татьяна Владимировна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ershova.tatiana.9@yandex.ru

ЕРЫГИН Вадим Викторович — гражданский преподаватель Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vadimerygin@yandex.ru

ЕСАЛОВ Кирилл Эдуардович — начальник Научно-образовательного центра «Инфокоммуникационных технологий и нейрокогнитивных архитектур»; ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kesalov@sut.ru

ЖАВОРОНКОВА Вера Владимировна — студентка группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, osminag.very@gmail.com

ЖЕРНОВА Ксения Николаевна — кандидат технических наук, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zhernova@comsec.spb.ru

ЖИГАДЛО Валентин Эдуардович — доктор технических наук, доцент, советник генерального директора ЗАО «Институт телекоммуникаций», председатель Экспертного совета при Санкт-Петербургском государственном унитарном предприятии «Санкт-Петербургский информационно-аналитический центр», zve@mail.ru

ЖИЛЯКОВ Глеб Витальевич — студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zgv00@bk.ru

ЖИХ Дарья Валентиновна — студент группы ИКТС-13м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dariazhih@yandex.ru

ЗАДБОЕВ Вадим Александрович — оператор научной роты Военной орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного, zadboev89@mail.ru

ЗАДОРОЖНЯЯ Алина Александровна — аспирант кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zadorozhniaia.aa@sut.ru

ЗАХАРЕНКОВ Константин Александрович — студент группы ИКТС-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zacharenkov28@mail.ru

ЗАХАРЕНКОВ Никита Александрович — студент группы ИКТС-81 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zakharenkov.wittgen@gmail.com

ЗАЯЦ Максим Петрович — студент группы ИКТС-13м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maksim-zajac29@yandex.ru

ЗВЕРЕВ Артем Михайлович — магистр группы М092201(71) Ордена Трудового Красного Знамени Московского технического университета связи и информатики, zverev_sh4w@vk.com

ЗЕБЗЕЕВ Егор Алексеевич — студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, zebzeev.avis@gmail.com

ЗЕЛИЧЕНОК Игорь Юрьевич — аспирант, младший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zelichenok@spb.comsec.ru

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, профессор, декан факультета информационных систем и технологий, профессор кафедры информационных управляющих систем, zikratov.ia@sut.ru

ЗИКРАТОВА Татьяна Викторовна — преподаватель Военного института (военно-морской политехнический) ВУНЦ ВМФ «Военно-морская академия», ztv64@mail.ru

ЗОЛОТОВА Дарья Сергеевна — студентка группы ИКБ-92 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, oblachko4@gmail.com

ЗРЕЛОВА Анастасия Леонидовна — студентка группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastyzr@gmail.com

ЗЫЛЕВА Полина Сергеевна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. polina-zyleva@mail.ru

ИБРАГИМОВ Роман Захирович — кандидат технических наук, доцент кафедры фотоники в телекоммуникациях Сибирского государственного университета телекоммуникаций и информатики, ibragimov@sibsutis.ru

ИГНАТЬЕВА Дарья Александровна — студентка группы ИКТЗ-21М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, miss.ignateva.14@mail.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, konstantin.izrailov@mail.ru

ИЛЬИНА Ольга Борисовна — кандидат географических наук, доцент, старший преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, nastik94@yandex.ru

ИЧЕТОВКИН Егор Андреевич — аспирант Санкт-Петербургского Федерального исследовательского центр Российской академии наук, ichetovkin.e@iias.spb.su

КАЗАКОВА Алина Юрьевна — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kazakovlina@yandex.ru

КАЗАНЦЕВ Алексей Анатольевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kazantsev.ikss@yandex.ru

КАЗАЧЕНКО Ирина Олеговна — студентка группы ИКТМ-22м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kazachenko_ira22@mail.ru

КАЙСИНА Ирина Алексеевна — кандидат технических наук, доцент кафедры Сетей связи и телекоммуникационных систем Ижевского государственного технического университета им. М. Т. Калашникова, kaisina.irina.al@yandex.ru

КАМАЛОВА Анастасия Олеговна — студентка группы ИКБ-02 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kamalovan002@mail.ru

КАНАЕВ Андрей Константинович — доктор технических наук, профессор, профессор кафедры Электрическая связь Петербургского государственного университета путей сообщения императора Александра I, kanaevak@mail.ru

КАРГИНА Дарья Андреевна — студентка группы V33021, лаборант лаборатории квантовых коммуникаций Национальный исследовательский университет ИТМО, dakargina17@gmail.com

КАТАСОНОВ Александр Игоревич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksasha716@yandex.ru

КАТКОВ Олег Николаевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

КИРИЧЁК Руслан Валентинович — доктор технических наук, доцент, ректор Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirichek@sut.ru

КИСЛЯКОВ Сергей Викторович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; бизнес-аналитик НТЦ Аргус, s.v.kislyakov@gmail.com

КИСТРУГА Антон Юрьевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.kistruga@gmail.com

КЛИШИН Данил Владимирович — аспирант факультета безопасности информационных технологий Национальный исследовательский университет ИТМО, dvklishin@itmo.ru

КНЯЗЕВА Виктория Юрьевна — студентка группы ИКТМ-12м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, knyazevavu@gmail.com

КОВАЛЕВ Игорь Станиславович — кандидат военных наук, доцент, доцент кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, iskova@yandex.ru

КОВАЛЕВА Александра Александровна — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, niktoto2002@mail.ru

КОВЦУР Максим Михайлович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxkovzur@mail.ru

КОЗЛОВА Алена Игоревна — студентка группы ИКПИ-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kozlovap.alyona@yandex.ru

КОЛЕСНИК Арсений Сергеевич — студент группы V33021, лаборант физико-технического мегафакультета Национального исследовательского университета ИТМО, arsenic.kl@gmail.com

КОЛОМИЙЦЕВ Руслан Константинович — студент группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, russlankot@mail.ru

КОНОНОВ Павел Александрович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kononov.pa@spbgut.ru

КОНЬКОВ Владимир Владимирович — студент группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. профессора М. А. Бонч-Бруевича, nik.veras@mail.ru

КОРЖИК Валерий Иванович — доктор технических наук, профессор, профессор кафедры безопасности информационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korzhikvalery@gmail.com

КОРОЛЕВ Даниил Сергеевич — студент группы ИКТУ-97 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dany.coroleov@yandex.ru

КОСОВ Никита Алексеевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, IL111111@mail.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича ivkote@comsec.spb.ru

КРАВЕЦ Елена Валентиновна — кандидат технических наук, доцент кафедры радиосвязи и вещания Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, helen-kravetz@yandex.ru

КРАВЦОВА Валерия Андреевна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kravtsova_valeria@mail.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, Заслуженный работник высшей школы РФ, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРИВЕЦ Андрей Сергеевич — студент группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krivets_2002@mail.ru

КРЫЩЕНКО Наталья Игоревна — студентка группы ИКБ-92 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krynatal@mail.ru

КРЮКОВА Елена Сергеевна — кандидат технических наук, преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, e.kkrukovaa69@yandex.ru

КУЗНЕЦОВ Вадим Сергеевич — заместитель директора по инновациям ООО «Беспилотные системы», kvs@unmanned.ru

КУЗНЕЦОВ Даниил Денисович — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daniil.kuznecov20011@gmail.com

КУЗНЕЦОВ Максим Сергеевич — студент группы ИКПИ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mkgs210@gmail.com

КУЗЬМИНА Ольга Ивановна — студентка группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Olgakuzmina2000@mail.com

КУКУНИН Дмитрий Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Coux@ya.ru

КУЛИКОВСКАЯ Альбина Павловна — студентка группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, panasenkoks@mail.ru

КУПЧИНЕНКО Ольга Павловна — преподаватель кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, k-olga102@yandex.ru

КУТЛЫЯРОВА Александра Александровна — студентка Санкт-Петербургского государственного института кино и телевидения, mr_echelon@mail.ru

КУТУЕВ Тимур Тагирович — студент группы ИКТЗ-94 Санкт-Петербургского государственного университета Телекоммуникаций им. профессора М. А. Бонч-Бруевича, Afanimmailab@gmail.com

КУШНИР Дмитрий Викторович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry.kushnir@gmail.com

ЛАПТЕВА Татьяна Владимировна — студентка группы ИКМ-13з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 1978.laptevat.v@mail.ru

ЛАПШИН Алексей Сергеевич — Студент группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ISpeedCore97I@yandex.ru

ЛЕБЕДЕВ Никита Андреевич — сотрудник Академии Федеральной службы охраны Российской Федерации, sda33@academ.msk.rsnet.ru

ЛЕВШУН Диана Альбертовна — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, gaifulina@comsec.sbp.ru

ЛЕВШУН Дмитрий Сергеевич — кандидат технических наук, старший научный сотрудник Санкт-Петербургского Федерального исследовательского центр Российской академии наук, levshun@comsec.spb.ru

ЛЕОНОВА Алина Александровна — студентка группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, leonova_alina15@mail.ru

ЛЕПЕШКИН Олег Михайлович — доктор технических наук, доцент, доцент Инженерно-строительного института Санкт-Петербургского Политехнического университета Петра Великого, lepechkin1@yandex.ru

ЛЕШУКОВА Анастасия Михайловна — студентка магистратуры 1 курса кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, n.leshukova98@gmail.com

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник Военной орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛОБАЦКИЙ Иван Аркадьевич — первый заместитель директора Санкт-Петербургского государственного казенного учреждения «Городской мониторинговый центр»

ЛОЧКАРЕВ Егор Андреевич — студент группы ИКТК-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lo4karev.egor00@mail.com

ЛУКИН Игорь Андреевич — курсант кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, ugo.lukin@gmail.com

ЛУКИН Константин Игоревич — кандидат технических наук, доцент, заведующий кафедрой специальных средств связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ki@supertel.ru

МАКАРОВА Александра Дмитриевна — студентка группы ИКБ-04 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, madweb@lenta.ru

МАКОЛКИНА Мария Александровна — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makolkina.ma@sut.ru

МАКСИМЕНКО Мария Эдуардовна — студентка группы ИКТЗ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mariyamaximenko@mail.ru

МАЛАХОВ Владислав Евгеньевич — аспирант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, vlamalakho95@gmail.com

МАРКЕЛОВА Мария Анатольевна — младший научный сотрудник НОЦ «Цифровые телекоммуникационные технологии» Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), MAMarkelova@etu.ru

МАХОНИНА Елена Александровна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета Телекоммуникаций им. профессора М. А. Бонч-Бруевича, No0boT2001@mail.ru

МЕЛЕХОВ Кирилл Витальевич — адъюнкт Военной орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С. М. Буденного, kirill_melehov@bk.ru

МЕСНЯНКИН Евгений Петрович — старший научный сотрудник научно-исследовательской лаборатории 42 лазерно-локационных систем АО «НИИ ОЭП», MesnyankinEP@niioep.ru

МЕТЕЛЬКОВ Александр Николаевич — кандидат юридических наук, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России, metelkov5178@mail.ru

МИНЯЕВ Андрей Анатольевич — кандидат технических наук, доцент кафедры защищённых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev.a@gmail.com

МИХАЙЛИЧЕНКО Антон Валерьевич — адъюнкт (аспирант) кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С.М. Буденного, toni09_91@mail.ru

МИХАЙЛОВ Павел Павлович — студент группы ИКМ-13з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sour-cattail.0w@icloud.com

МИХАЙЛОВА Зоя Владимировна — студент группы РК-21м Санкт-Петербургского государственного университета, wzeymix@gmail.com

МИХАЛЕВ Олег Александрович — кандидат технических наук, заместитель начальника научно-исследовательского центра Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vasn2020@mail.ru

МУРАШКИН Никита Анатольевич — студент группы ИКПИ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, niwhalea23@gmail.com

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сети связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

НАСЕДКИН Борис Александрович — аспирант факультета фотоники, научный сотрудник лаборатории квантовых процессов и измерений национального исследовательского университета ИТМО, banasedkin@itmo.ru

НЕВЕРОВ Евгений Андреевич — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, datnever@yandex.ru

НЕКРАСОВ Вадим Николаевич — студент группы ИКТК-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nekrasoww645@gmail.com

НЕКРАСОВ Сергей Германович — студент группы ИКВТ-01 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, poshta-nekrasov@yandex.ru

НЕСТЕРОВА Яна Олеговна — студентка группы ИКТИ-25м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yana031999@gmail.com

НЕЧАЕВ Андрей Александрович — студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lcme.nechaev@mail.ru

НИКОЛАЕВА Лада Андреевна — магистрант 1 курса кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nicklada94@gmail.com

НИКОНОВ Евгений Русланович — студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, NIKKSTUDIO3023@gmail.com

НОГИН Сергей Борисович — кандидат технических наук, доцент, доцент кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

НОСОВ Михаил Иванович — доктор технических наук, доцент, старший научный сотрудник научно-исследовательского центра Михайловской военной артиллерийской академии, mikhail.nosov.64@mail.ru

ОБУХОВ Станислав Андреевич — аспирант группы 2215А-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stasstas1155@yandex.ru

ОВОДОВА Татьяна Александровна — старший преподаватель кафедры иностранных и русского языков, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, ovodova@bk.ru

ОГОРЕЛЬЦЕВ Павел Анатольевич — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, paul.ogorelcev@gmail.com

ОКУНЕВА Дарина Владимировна — кандидат технических наук, декан факультета инфокоммуникационных сетей и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, darina_okuneva@mail.ru

ОСТРОУМОВ Максим Александрович — начальник отделения кафедры безопасности инфокоммуникационных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, coj1991@mail.ru

ОСТРОУМОВ Олег Александрович — кандидат технических наук, докторант кафедры техносферной безопасности Инженерно-строительного института Санкт-Петербургского политехнического университета Петра Великого, oleg-26stav@mail.ru

ПАВЛОВ Иван Иванович — академик МАС, кандидат технических наук, доцент, доцент кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, iipavlov02@mail.ru

ПАВЛОВА Мария Сергеевна — доцент кафедры радиотехнических устройств и техносферной безопасности Сибирского государственного университета телекоммуникации и информатики, mspavlova@ngs.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, p_oleg99@mail.ru

ПАНЬКОВ Богдан Олегович — студент группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i@m-pankov.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ПАЩЕНКО Василий Владимирович — кандидат технических наук, доцент кафедры назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного

ПЕКИН Денис Игоревич — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denis-pekin2000@yandex.ru

ПЕСТОВ Игорь Евгеньевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pestovie@outlook.com

ПЕТРИВ Роман Богданович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petriv@sut.ru

ПЕТРОВ Илья Игоревич — студент группы ИКБ-92 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, IL111111@mail.ru

ПЕТРОВ Максим Александрович — студент группы ИКТК-96, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petrovmaksim01@mail.ru

ПЕТРОВА Татьяна Васильевна — студентка группы ИКТБ-28м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tanya26012001@mail.com

ПЕТРОВА Татьяна Сергеевна — магистрант кафедры защищенных средств связи Санкт-Петербургского государственного университета лекоммуникаций им. проф. М. А. Бонч-Бруевича,

ПИРОГОВ Олег Евгеньевич — курсант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, zerostar019@icloud.com

ПЛАТОНОВА Татьяна Андреевна — студент группы ИКБ-95 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, heh.heh2018@yandex.ru

ПОЛЯНИЧЕВА Анна Валерьевна — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polavaly@gmail.com

ПОМОГАЛОВА Альбина Владимировна — старший преподаватель кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного политехнического университета, a.l.b.i.n.a@bk.ru

ПОНАМАРЕНКО Екатерина Сергеевна — аспирант кафедры Сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, katerinochka-rinochka2010@yandex.ru

ПОНОМАРЕВ Николай Александрович — студент группы ИКБ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikapon13@gmail.com

ПОПКОВ Илья Александрович — аспирант факультета безопасности информационных технологий Национального исследовательского университета ИТМО, popkov.ilya.alexandrovich@yandex.ru

ПОПОВА Валерия Олеговна — аспирант факультета безопасности информационных технологий Национального исследовательского университета ИТМО, lerapopova236@gmail.com

ПОТАПОВ Сергей Леонтьевич — старший научный сотрудник – начальник стенда научно-исследовательской лаборатории 42 лазерно-локационных систем АО «НИИ ОЭП», PotapovSL@niioep.ru

ПОТАПОВА Нина Ивановна — кандидат технических наук, начальник научно-исследовательского и испытательного отдела 4 лазерных и световых технологий – начальник научно-исследовательской лаборатории 42 лазерно-локационных систем АО «НИИ ОЭП», PotapovaNI@niioep.ru

ПОТОМАКО Денис Олегович — студент группы ИКТБ-27м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, den.potomako@mail.ru

ПРОНИЧЕВ Владислав Дмитриевич — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nggajloy@gmail.com

ПРОШИН Федор Алексеевич — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, fedorproshin@gmail.com

ПУЧКОВ Владимир Викторович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, puchkov-81@bk.ru

ПЩЕЛКО Николай Сергеевич — доктор технических наук, доцент, главный научный сотрудник АО «НИИ «Рубин», nikolsp@mail.ru

РАЗУМОВ Дмитрий Александрович — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dmitry.razumov1257@yandex.ru

РОГАЛЬНИКОВ Игорь Юрьевич — сотрудник Академии Федеральной службы охраны Российской Федерации, shliapin1995@mail.ru

РОГОЗИНСКИЙ Глеб Гендрихович — доктор технических наук, профессор кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, начальник НОЦ «Медиацентр» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gleb.rogozinsky@gmail.com

РОМАНЕНКО Кирилл Андреевич — студент группы ИКПИ-05 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kirill2922293@mail.ru

РОМАНЮК Егор Олегович — студент ИКТБ-27 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pomidorych2000@gmail.com

РУМЯНЦЕВ Сергей Олегович — студент группы ИКПИ-96, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergey.rumy@gmail.com

РЯБОВ Михаил Михайлович — оператор роты (научной) ГУС ВС РФ mihail32799msk@yandex.ru/vasn2020@mail.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук; профессор кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, ibsaen@mail.ru

САЛИТА Андрей Сергеевич — магистр кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, salita@internet.ru

САЛМАН Васан Давуд — аспирантка кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, wasan.salman@mail.ru

САЛТЫКОВ Антон Радиевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anton.saltykov@gmail.com

САНИН Юрий Васильевич — кандидат технических наук, доцент, ведущий научный сотрудник АО «НИИ «Рубин», Y.V.Sanin@rubin-spb.ru

САРКИСЯН Артём Арменович — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, temik777rus@gmail.com

САФИНА Аделина Ильзаровна — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bratz-200101@mail.ru

САХАРОВ Дмитрий Владимирович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sguard7@mail.ru

САЯРКИН Виталий Андреевич — курсант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, vitaliysayarkin@gmail.com

СВЕТОВА Анастасия Васильевна — студент группы ИКТУ-98 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastya_sv00@mail.ru

СВЕЧНИКОВ Дмитрий Александрович — кандидат технических наук, доцент сотрудник Академии Федеральной службы охраны Российской Федерации, sda33@academ.msk.rsnet.ru

СЕЛЕЗНЕВ Андрей Васильевич — кандидат технических наук, начальник отдела военно-технической информации Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, andrsel@mail.ru

СЕМЁНОВ Андрей Борисович — доктор технических наук, профессор кафедры механизации и автоматизации строительства Национального исследовательского Московского государственного строительного университета, andre52.55@mail.ru

СЕМКИНА Маргарита Руслановна — курсант учебной группы 3182 Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, semkinamargarita931@gmail.com

СИНЕЩУК Максим Юрьевич — Заместитель начальника центра информационных и коммуникационных технологий – начальник отдела связи и сетевых технологий Санкт-Петербургского университета ГПС МЧС России, smaxim@inbox.ru

СИНЮК Александр Демьянович — доктор технических наук, доцент, профессор кафедры общепрофессиональных дисциплин Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, eentrop@rambler.ru

СКАКУНОВ Игорь Рустамович — студент группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ighor.skakunov@mail.ru

СКОРИНОВ Максим Юрьевич — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; главный специалист АО «Нэксайн», maksim.skorinov@nexign.com

СКОРОБОГАТОВА Светлана Алексеевна — студентка группы ИКТГ-24м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skorobogatova_sa@mail.ru

СКОРОПАД Александр Витальевич — ведущий инженер НИЛ № 4131, НИО № 413, НТЦ № 41 Санкт-Петербургского филиала – «ЛОНИИР» (ФГБУ НИИР), sav01236@yandex.ru

СКОРЫХ Марк Андреевич — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mark.skorykh@bk.ru

СЛЕПОГИН Антон Юрьевич — студент группы ИКТФ 26-М Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antoha0517@mail.ru

СМИРНОВ Александр Андреевич — адъюнкт кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, alexsmirrrrn@yandex.ru

СМИРНОВ Даниил Николаевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ylcreate1@gmail.com

СОКОЛОВ Евгений Глебович — аспирант кафедры многоканальных телекоммуникационных систем Ордена Трудового Красного Знамени Московского технического университета связи и информатики, e.g.sokolov@gmail.com

СОЛОДУХИН Борис Владимирович — кандидат военных наук, доцент, старший преподаватель кафедры Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного

СПОСОБ Сергей Павлович — магистр технических наук, старший преподаватель кафедры связи военного факультета Белорусского государственного университета информатики и радиоэлектроники, sposob.sergey@gmail.ru

СТАХЕЕВ Иван Геннадиевич — кандидат технических наук, доцент кафедры специальных средств связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kisasig@yandex.ru

СУНДУКОВ Вячеслав Алексеевич — курсант Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, slava.sundukov.2014@mail.ru

СУХОМЛИНОВ Даниил Игоревич — студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d.sukhomlinov.spb@gmail.com

ТАРАБАНОВ Илья Федорович — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarabanov.if@spbgut.ru

ТАРОВ Евгений Викторович — студент группы ИКБ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tarov25@mail.ru

ТАСЮК Александр Андреевич — аспирант кафедры защищенных средств связи Санкт-Петербургского государственного университета т е

ТИТОВА Ольга Викторовна — кандидат технических наук, доцент кафедры специальных средств связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olga1110.spb@mail.ru

ТРЕЗОРОВ Владислав Игоревич — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций, trezorov.v.i@yandex.ru

ТРЕМЕЛЬ Ирина Сергеевна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича. irina.tremel@yandex.ru

ТРОФИМОВ Владислав Витальевич — студент группы ИКТИ-15м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladislav.trofimov.1998@yandex.ru

ТУНГУСКОВА Анастасия Михайловна — студентка группы М22-282-1 Ижевского государственного технического университета имени М. Т. Калашникова, anastasiya.tunguskova@mail.ru

ТУХБАТУЛЛИНА Эвелина Фанилевна — курсант учебной группы 3182 Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, Tuxbatullina2003@mail.ru

УМАРАЛИЕВ Игорь Васильевич — студент группы ИКБ-91 Санкт-Петербургского государственного университета Телекоммуникаций им. профессора М. А. Бонч-Бруевича, i.umaraliev.spb@mail.ru

УЧИНИН Андрей Сергеевич — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andrey.uchinin@gmail.com

УШАКОВ Игорь Александрович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakov.ia@sut.ru

ФЕДОРОВ Павел Олегович — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного политехнического университета, pavel_lenin@mail.ru

ФЕДОРОВА Злата Анатольевна — студентка группы ИКТЗ-21м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zf_sweetday@mail.ru

ФЕДОРОВА Екатерина Сергеевна — студентка группы ИКТБ-28М Санкт-Петербургского государственного политехнического университета, chukina.es@yandex.ru

ФЕДОТОВ Илья Олегович — магистр кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fedotow.ilja@gmail.com

ФЕДОТОВСКАЯ Анастасия Дмитриевна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ananas3302@mail.ru

ФИЛЕВА Виктория Сергеевна — студентка группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.s.fileva@yandex.ru

ФИЩЕВ Егор Дмитриевич — студент группы ИКТГ-14м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, trhb421@gmail.com

ФОМИН Артем Игоревич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fomin.artem633@gmail.com

ФОМИН Савелий Павлович — студент группы ИКТК-96 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saveliyf@inbox.ru

ФРАЗ Алексей Вячеславович — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, frazalex@yandex.ru

ХОЛОДЁНОК Елена Сергеевна — студентка группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kkholodenok@gmail.com

ЦВЕТКОВ Александр Юрьевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aleksandr.tcvetkov@sut.ru

ЦУРБЕЛЕВ Андрей Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andrei.tsurbeleff@yandex.ru

ЦЫВАНЮК Вячеслав Александрович — кандидат военных наук, старший научный сотрудник, старший научный сотрудник Научно-исследовательского центра связи ВУНЦ ВМФ «Военно-морская академия» МО РФ, ciwoniuk@mail.ru

ЦЫГАНОВ Владимир Александрович — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vovan300401@gmail.com

ЧАСОВСКИХ Екатерина Ильдаровна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета Телекоммуникаций им. профессора М. А. Бонч-Бруевича, feofanova_e_i@mail.ru

ЧЕКАЛОВ Дмитрий Александрович — студент группы ИКТК-95, Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chekslovda.psk@gmail.com

ЧЕРНЫХ Илья Сергеевич — начальник отделения кафедры Безопасности инфокоммуникационных систем специального назначения Военной орденов Жукова и Ленина Краснознаменной академии связи имени Маршала Советского Союза С. М. Буденного, fes90@list.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент, доцент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; ведущий научный Санкт-Петербургского Федерального исследовательского центра Российской академии наук, chechulin@comsec.spb.ru

ЧИПСАНОВА Елена Валерьевна — бакалавр, студентка кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lenchip@mail.ru

ЧУМАКОВ Игорь Владимирович — студент группы ИКБ-04 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, i@ichumakov.ru

ШАЛИМОВ Илья Сергеевич — студент группы ИКМ-21з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilya28092000@gmail.com

ШАРАПОВ Роман Игоревич — студент группы ИКТЗ-93 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sharapov.roman@list.ru

ШВИДКИЙ Артём Александрович — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shvidkiy@sut.ru

ШЕЛЕХОВ Антон Алексеевич — аспирант кафедры радиотехнических систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), antshel27@gmail.com

ШЕЛКОПЛЯСОВА Полина Евгеньевна — студентка группы ИКТЗ-16 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kuolya20112@gmail.com

ШЕЛУХИН Олег Иванович — доктор технический наук, заведующий кафедры «Информационная безопасность» Ордена Трудового Красного Знамени Московского технического университета связи и информатики, sheluhin@mail.ru

ШЕМЯКИН Сергей Николаевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, s4421764@ya.ru

ШЕСТАКОВ Александр Викторович — доктор технических наук, старший научный сотрудник, ведущий научный сотрудник, п омощник начальника Санкт-Петербургского университета ГПС МЧС России, alexandr.shestakov01@yandex.ru

ШЕСТАКОВА Валерия Алексеевна — инженер кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shestakova.va@spbgut.ru

ШИНКАРЕВ Семен Александрович — кандидат технических наук, доцент, доцент кафедры автоматизированных систем специального назначения Военной орденов Жукова и Ленина Краснознамённой академии связи имени Маршала Советского Союза С. М. Будённого, se_men82@mail.ru

ШКЛЯЕВ Александр Вячеславович — студент группы Б20-282-1 Ижевского Государственного Технического Университета имени М. Т. Калашникова, sasha-shklyaev@bk.ru

ШТЕРЕНБЕРГ Станислав Игоревич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shterenberg.stanislaw@yandex.ru

ЩЕГОЛЬСКИЙ Юлиан Евгеньевич — студент группы ИКТК-96 Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yulik.shchegolskiy@gmail.com

ЮРОВА Ульяна Сергеевна — студентка группы ИКТЗ-94 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. u_yurova@mail.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, viyak@bk.ru

ЯРОШЕНКО Александр Юрьевич — начальник отдела организации защиты информации Департамента информационных технологий и связи МЧС России, alexagz@mail.ru

ЯСИР Хуссейн Али Ясир — аспирант кафедры сетей связи и передачи данных Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, eng-hu@mail.ru

АВТОРСКИЙ УКАЗАТЕЛЬ