СПбГУТ)))

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

8TH INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT 2019

VIII МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ»

АПИНО

ICAIT

СБОРНИК НАУЧНЫХ СТАТЕЙ

27–28 ФЕВРАЛЯ 2019 ГОДА

ПОДРОБНОСТИ НА САЙТЕ КОНФЕРЕНЦИИ

APINO.SPBGUT.RU

УДК 001:061.3(082)
ББК 72 А43

Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2019. Т. 1. 834 с.

ГЕНЕРАЛЬНЫЙ ПАРТНЕР

технологии бесконечности
КОМПАНИЯ «Т8»

ПАРТНЕРЫ КОНФЕРЕНЦИИ

Ростелеком

ROHDE&SCHWARZ

АРГУС НТЦ

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.

ISBN 978-5-89160-187-1

Научное издание
Литературное редактирование,
корректура Е. А. Аникевич
Оформление Г. И. Юрьев
Верстка Е. М. Аникевич
Подписано в печать 01.08.2019.
Вышло в свет 30.08.2019. Формат 60×90 1/8.
Уст. печ. л. 52, 13. Заказ № 052-ИТТ-2018.
пр. Большевиков, д. 22, корп. 1.
Россия, Санкт-Петербург, 193232

ИНФОРМАЦИОННЫЕ ПАРТНЕРЫ

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ ИНФОРМАЦИЯ КОСМОС

НАУЧНЫЙ ЖУРНАЛ ТУЗС «ТРУДЫ УЧЕБНЫХ ЗАВЕДЕНИЙ СВЯЗИ»

ИНФОРМАЦИОННАЯ ПОДДЕРЖКА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
научное рецензируемое издание • электронный научный журнал
Telecom IT — ISSN 2307-1303

СОДЕРЖАНИЕ

УДК 621.039; 654.926; 537.9; 621.3.011.732; 538.911
ГРНТИ 20.53.01

ТЕЛЕКОММУНИКАЦИОННАЯ СРЕДА В ЭПОХУ ИНФОРМАЦИОННОГО ОБЩЕСТВА: ИНТЕЛЛЕКТУАЛЬНЫЕ УСТРОЙСТВА И МАТЕРИАЛЫ ФУНКЦИОНАЛЬНОЙ ЭЛЕКТРОНИКИ

А. С. Багдасарян[1, 2, 3], В. В. Бутенко[1]

[1] Научно-исследовательский институт радио
[2] Институт радиотехники и электроники имени В. А. Котельникова Российской академии наук
[3] НПП «Технологии радиочастотной идентификации и связи»

Получение радикально новых возможностей перспективных технологий связи предполагает решение целого ряда фундаментальных и прикладных задач по поиску новых физических принципов генерации, передачи, приёма и обработки информации с использованием современных микро- и нано-технологий.

информационное общество, телекоммуникационная среда, функциональная электроника, интеллектуальные устройства, опаловые матрицы.

Введение

Одним из первых отечественных ученых, который обратил внимание на принципиально новую роль информации в современном мире, был академик Вадим Александрович Трапезников. Еще в 1966 г. известный ученый признал, что информация становится наиболее важным продуктом [1].

Сегодня уже ни у кого не возникает сомнение, что мир нарастающими темпами движется в эпоху постиндустриального развития, характерной особенностью которой является безусловная доминанта информационных процессов во всех сферах жизни и деятельности общества и человека. Эта доминанта и лежит в основе концепции новой исторической фазы возможного развития цивилизации, в которой главными продуктами производства становятся информация и знания. Эта фаза и есть информационное общество, основными отличительными чертами которого являются:

– открытость для всех;

– решающий вклад в устойчивое развитие обществаа и повышение качества жизни людей;

– создание условий для реализации потенциала каждого человека.

Эволюция роли и значения информации неизбежно повлекла и эволюцию телекоммуникаций как совокупности физической среды и способов передачи, приёма и обработки информации. При этом по мере развития общества развитие телекоммуникационных технологий происходит в темпе, опережающем реальные возможности общества по генерации и использованию информации. Период смены поколений телекоммуникационных технологий существенно уменьшается. В этом смысле телекоммуникации не только следуют в кильватере информационных потребностей общества, но уже в значительной мере определяют траекторию вектора развития цивилизации [2].

Получение радикально новых возможностей перспективных технологий связи предполагает решение целого ряда фундаментальных и прикладных задач по поиску новых физических принципов генерации, передачи, приёма и обработки информации [3, 4, 5]. Ведутся такие исследования в сфере функциональной электроники. Речь – прежде всего о технологиях на поверхностных акустических волнах (ПАВ).

Технологии ПАВ

Основоположники этой науки академик Юрий Васильевич Гуляев и академик Владислав Иванович Пустовойт знают и нас научили понимать, что преобразование электрической энергии в звук даёт ранее недоступные возможности по точности и скорости измерений и обработки информации [3]. И сегодня мы развиваем это учение в прикладных сферах. Области применения ПАВ-технологии в современном радиоэлектронном приборостроении и системах связи общеизвестны [4, 5, 6, 7, 8].

С середины 60-х годов прошлого столетия, благодаря классической работе Ю. В. Гуляева и В. И. Пустовойта [3], произошло становление и получило бурное развитие новое научное направление твердотельной функциональной электроники – «Акустоэлектроника» («Акустооптика»), включая наиболее значимое с практической точки применения «Пассивная Акустоэлектроника». За это время в рассматриваемой области представлены и защищены тысячи международных патентов, десятки тысяч научных публикаций, сотни внедрённых в производство изобретений. Предлагаемый специалистам в области инновационных технологий доклад является логическим продолжением успехов российских учёных. В нем представлены перспективы развития пассивной электроники в XXI веке, позволяющие проводить разработки новых классов и поколений устройств на поверхностных акустических волнах (ПАВ) с уникальными характеристиками, определяющими мировой уровень в рассматриваемой области знаний.

Основными приложениями функциональной электроники, рассмотренные в настоящей работе и которые в настоящее время исследуются и адаптируются к потребностям перспективных телекоммуникаций, являются:

– радиочастотная идентификация [4, 5] и мониторинг физических параметров критически важных объектов [6, 7];

– фильтрация сигналов, в том числе во входных каскадах с высоким уровнем мощности [8];

– отображение информации.

Система мониторинга (рис. 1) работает по принципу радиолокатора с пассивной целью [4, 5, 6, 7]. Датчик работает в разрешённых для SRD устройств диапазонах (например, ~433 МГц) в режиме линии задержки на ПАВ в разрешённых полосах частот (например, ~1 МГц). Приёмник этого диапазона имеет чувствительность P0 = 3 * 10–15 Вт = 150 дБ/Вт при отношении сигнала к шуму 10 дБ в рабочей полосе частот и расстоянии до 10 м. При использовании шумоподобных сигналов длины более миллиона, дальность надёжной работы дистанционного скрытного пассивного датчика увеличивается до 50 м. В этом случае один приёмник может обеспечить нормальную работу нескольких десятков кодированных сенсоров и обеспечить, например, надёжное обнаружение взрывчатых веществ в пунктах большой пропускной способности людей.

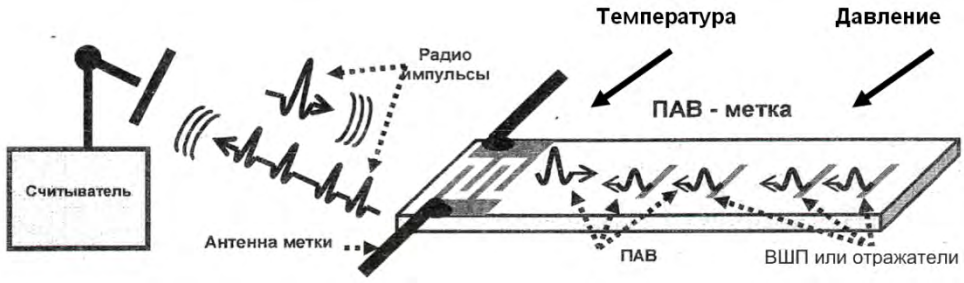


Рис. 1. Принципы построения систем радиочастотной идентификации и мониторинга физических параметров критически важных объектов

Датчик представляет собой пассивную структуру на ПАВ, подложка которой содержит встречно-штыревой преобразователь (ВШП) и множество отражающих полосок. Преобразователь подключён к антенне, согласованный в рабочем диапазоне частот. Акустические колебания возбуждаются преобразователем после облучения антенны электромагнитным сигналом в заданном диапазоне частот. В зависимости от внешнего воздействия (давления, температуры, радиационного излучения, изменение газового состава) среды, в которой находится сенсор, существенно изменяются физические характеристики ПАВ-структуры, приводящие к изменению скорости и условий распространения поверхностных акустических волн. В резуль-

тате, через 5–20 мкс в антенне появляется отражённый сигнал, который излучается в пространство и может быть успешно обнаружен приёмным мультипроцессорным устройством. Приёмное устройство принимает отражённый сигнал, проводит измерения его параметров и принимает решение, например, о наличии или отсутствии в газовой среде искомых веществ. Каждый сенсор имеет индивидуальные характеристики отражения сигнала.

Отличительными особенностями датчиков на ПАВ являются их устойчивость к радиации, невосприимчивость к электромагнитным помехам, отсутствие возможности клонирования, подделки, широкий температурный режим работы, невозможность обнаружения иными средствами, помимо средств, входящих в состав системы мониторинга с одновременной радиочастотной идентификацией.

Рис. 2. Пассивный ПАВ-датчик физической величины с внешней чувствительной нагрузкой

Датчик может также представлять собой линию задержки (ЛЗ) на ПАВ, содержащую два ВШП (рис. 2.). Первый преобразователь соединён с приёмо-передающей антенной, второй представляет собой отражательный ВШП, нагруженный на чувствительный элемент. Величина нагрузки Z, очевидно, зависит от измеряемого параметра (давления, влажности, температуры, интенсивности излучения и т.п.). При изменении величины нагрузки под действием измеряемой физической величины меняется коэффициент отражения ПАВ от отражательного ВШП [6].

Интеллектуальные ПАВ-устройства: новые возможности телекоммуникационных систем

На основе мировых тенденций одной из главных перспектив развития техники ПАВ является создание интеллектуальных устройств с новыми возможностями: балансных фильтров с самосогласованием и преобразованием импедансов, ПАВ-микросборок и модулей, платформ с интеграцией ПАВ-, WLP-, LTCC-технологий, радиочастотных меток (РЧМ) на ПАВ, объединенных с датчиками различных физических величин. В работе [9] для каждого типа таких устройств представлены количественные и качественные

характеристики как зарубежных, так и отечественных разработчиков, и производителей техники ПАВ. По прогнозам потенциальный объем выпуска пассивных РЧМ на ПАВ значительно превысит объем выпуска фильтров на ПАВ. Объединение РЧМ с различными датчиками приводит к созданию интеллектуальных устройств на ПАВ с возможностью измерения, например, давления, температуры, изгиба, и радиопередачи сигнала с метки, содержащего информацию о коде метки и измеряемых физических величинах (рис. 1, 2). Наилучшим решением для построения беспроводного высокотемпературного датчика является РЧМ, выполненная на кристалле лангасита, пьезоэлектрические свойства которого сохраняются до 1200 ºС. Известно успешное использование решетки из шести ПАВ-датчиков на лангасите, совмещенных с РЧМ на ПАВ на частоты 280–300 МГц, для измерения температуры в диапазоне 355–406 ºС на ТЭЦ вместо устаревших и громоздких термопар [10].

Снижение вносимого затухания в интеллектуальных устройствах на ПАВ возможно за счет согласования однонаправленного ВШП с антенной метки. В настоящее время эффективно применяется монтаж кристаллов РЧМ на ПАВ в многослойный корпус на основе LTCC с встроенной согласующей индуктивностью (рис. 3) [11]. Представленные решения, направленные на снижение вносимого затухания РЧМ на ПАВ, дополняют и расширяют возможности интеллектуального ПАВ устройства, совмещающего в одном корпусе датчик(и) и радиометку на ПАВ.

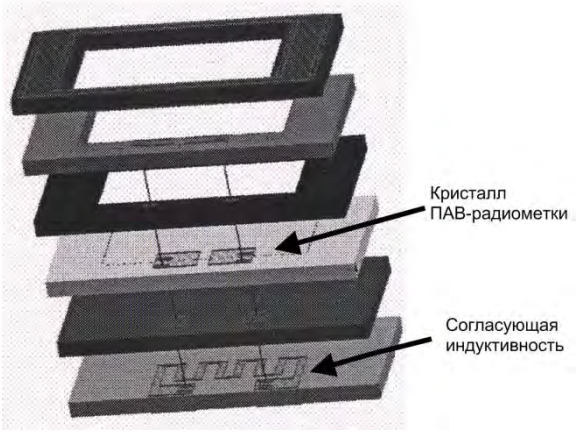


Рис. 3. Многослойная LTCC плата РЧМ на ПАВ с согласующей индуктивностью

Применение LTCC-технологии для монтажа кристаллов РЧМ на ПАВ обеспечило их высокие электрические характеристики, надежность, высокую степень миниатюризации и совместимость с технологией поверхностного монтажа. Нами найдены также новые конструктивно-технологические решения РЧМ с невзаимными СВЧ устройствами, в которых кодовая последовательность метки формируется за счет приема ПАВ (и преобразования по мере распространения в линии задержки поверхностных акустических волн в электромагнитный сигнал). Разработаны технологические основы получения нанокомпозитов на основе решетчатых упаковок микросфер кремнезема (рис. 4) для создания невзаимных устройств в составе РЧМ на ПАВ нового поколения [12, 13, 14].

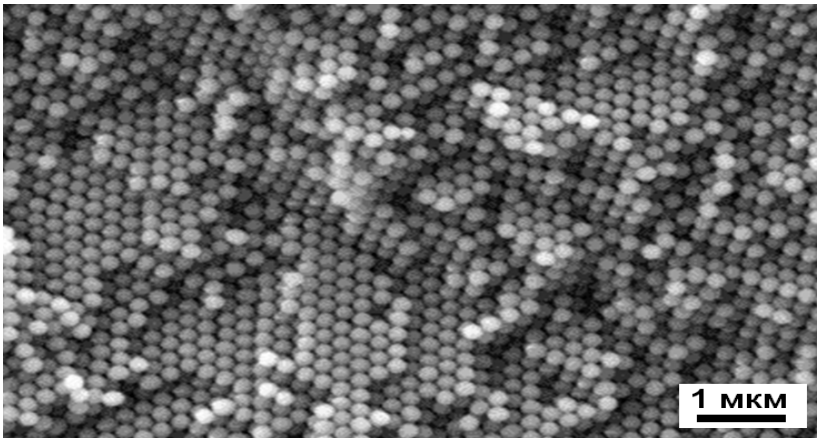


Рис. 4. Снимок (растровая электронная микроскопия) поверхности роста опаловой матрицы

Интеллектуальные ПАВ-устройства и опаловые матрицы: новые возможности в медицине

Все приведенные выше исследования носят междисциплинарный характер и находят применения не только в области телекоммуникационных технологий, но и в других областях сферы деятельности человека, например, в медицине. Так, одной из важных задач современной медицины является определение индивидуального сердечно-сосудистого риска. Существующие на сегодняшний день методы зачастую трудоемки и требуют дорогостоящего оборудования. Рассмотренные выше системы радиочастотной идентификации и мониторинга с использованием беспроводных датчиков призваны решить следующие задачи: прогнозировать опасные для жизни осложнения на ранних стадиях:

– обеспечить своевременность диагностики и проведения необходимых лечебных мероприятий;

– с помощью беспроводных технологий в режиме реального времени дистанционно оценивать параметры сердечно-сосудистой системы при проведении СМАД и ХМ ЭКГ;

– оценивать различия тонического состояния сосудов и вариабельность сердечного ритма; наблюдать изменения сердечного ритма и АД в режиме реального времени.

Данная скрининг-диагностика состояния сердечно-сосудистой системы открывает широкие функциональные возможности, в том числе, позволяя определять адаптированность к физическим нагрузкам. Все выше перечисленное помогает врачу оперативно отслеживать динамику показателей сердечно-сосудистой системы и принимать верное решение в отношение тактики ведения пациента, а также адекватно контролировать эффективность проводимых лечебных и спортивных мероприятий [15].

В работах [16, 17] проведены уникальные исследования на стыке нанотехники и медицины. (по предполагаемому использованию опаловых матриц в медицине). На рис. 5 и 6 представлены результаты этих исследований для:

1. Культивирования и размножения клеточной массы.
2. Генерирования (без применения рентгеновских трубок) импульсного рентгеновского излучения (объем излучателя – образца опаловой матрицы <1 мм3).

Рис. 5. Культивирование фибропластов человека на опаловых матрицах (7-ые сутки, МТТ-тест)

По первому направлению. Прогресс в реконструктивно-пластической хирургии в различных разделах медицины в значительной мере зависит от внедрения современных нано материалов в качестве трехмерных матриксов для клеточных и тканевых культур. Выбранный для технологической проработки метод формирования наноструктур обеспечивает получение на их основе биоматериалов нового поколения (с учетом результатов моделирования свойств живых биологических тканей) таким образом, чтобы, при необходимости, они могли замещать структурные и (по возможности) функциональные дефекты, возникающие при оперативных вмешательствах, а также иметь высокую биологическую безопасность. Одной их ключевых проблем создания биоискусственных органов и тканей является разработка матриксов (носителей) для клеток с использованием нано частиц различных материалов. Исследования возможностей дифференцировки стволовых клеток из костного мозга, жировой ткани, периферической крови и других источников позволяют надеяться на возможность восстановления, с использованием таких клеток, структурных и функциональных дефектов многих органов и тканей. Для разработки адекватных гибридных структур, необходим поиск в области моделирования, синтеза и изучения взаимодействия соответствующих биологических тканей и наночастиц как основы композиционных материалов [16].

По второму направлению. В результате взаимодействия импульсного лазерного излучения (наносекундного диапазона длительности) с опаловой матрицей (трехмерной фотонно фононной средой – решетчатой упаковкой наносфер SiO2) генерируется рентгеновское излучение, регистрируемое рентгеновской фотопленкой (см. Рис.6 с рентгеновской пленкой). Указанный способ дает возможность формировать импульсное рентгеновское излучение 10^{-3} рад, при этом, интегральная энергия в единичном·с расходимостью менее 1 импульсе составляет 0,4–0,5 Вт при длительности в доли миллисекунды, что дает мощность близкую к генерируемой микрофокусной рентгеновской трубкой [16, 17].

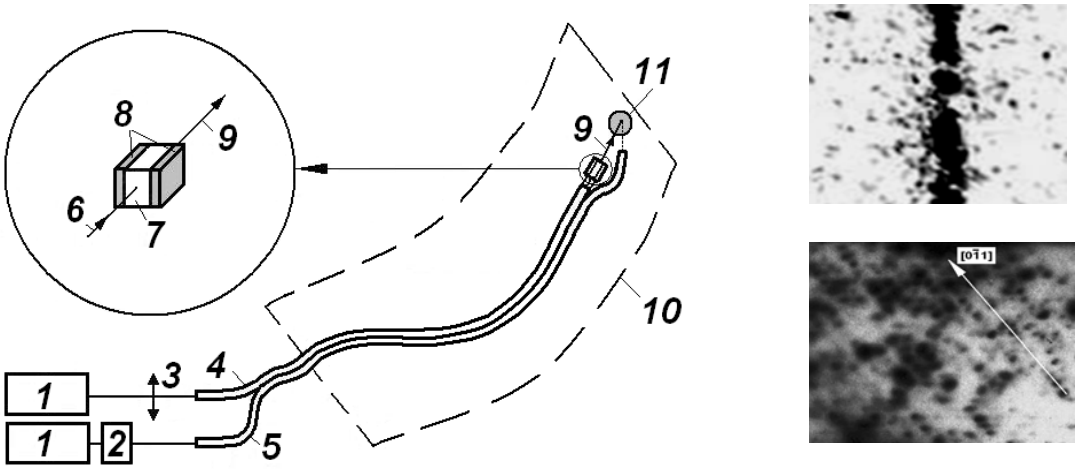


Рис. 6. Схема эндоскопического устройства для генерации направленного импульсного рентгеновского излучения: 1 – лазер; 2 – система изображения исследуемого объекта или регистрации спектров КР; 3 – оптическая система фокусирования лазерного излучения; 4, 5 – волоконно-оптические кабели; 6 – подвод лазерной накачки по оптическому кабелю; 7 – опаловая матрица (ОМ); 8 – пластины из пьезоэлектрических материалов; 9 – импульсное рентгеновское излучение; 10 – исследуемая полость; 11 – объект воздействия рентгеновского излучения

Есть основания полагать, что при надлежащем выборе параметров ОМ, параметров лазерного излучения, а также условий проведения эксперимента существует возможность для увеличения энергии квантов рентгеновского излучения до значений, которые позволят использовать данный способ его получения в промышленных и медицинских целях.

Работа выполнена при поддержке РФФИ (гранты № 18-07-00282 А и № 18-09-02076 МК).

Список используемых источников

1. Трапезников В.А. Управление экономики и технический прогресс // Труды III Международного конгресса Международной федерации по автоматическому управлению Лондон 20–25 июня 1966 г. М. : Наука, 1972. 499 с. http://trap-ipu.narod.ru /

2. Bagdasarian A. S., Bagdasarian S. A., Butenko V. V., Gulyaev Yu. V., Mkrtchyan A. R. Telecommunications Environment in the ERA of Information Society // 5th International Conference on «Electron, Positron, Neutron and X-ray Scattering under External Influences», Yerevan – Megri, Armenia 16–22.10.2017. P. 97.

3. Гуляев Ю. В., Пустовойт В. И. Усиление поверхностных волн в полупроводниках // ЖЭТФ. 1964. Т. 47. С. 2251–2253.

4. Багдасарян С. А., Гуляев Ю. В. Радиочастотная идентификация с использованием технологии ПАВ // Наука и технологии в промышленности. 2005. № 1. С. 54.

5. Багдасарян С. А., Николаева С. О., Подшивалова Г. В., Семенов Р. В. Оценка дальности действия систем радиочастотной идентификации в условиях природных и техногенных катастроф // Теория и техника радиосвязи. 2012. № 4. С. 11–16.

6. Багдасарян С., Днепровский В., Карапетьян Г., Нефедова Н., Синицына Т. ПАВ-датчики дистанционного контроля физических величин // Электроника: Наука, технология, бизнес. 2008. № 1 (83). С. 46–51.

7. Карапетьян Г. Я., Днепровский В. Г., Багдасарян С. А., Багдасарян А. С., Николаев А. Л., Кайдашев Е. М. Пассивный беспроводной датчик на поверхностных акустических волнах для измерения параметров газовых и жидких сред // Инженерный вестник Дона. 2012. № 2 (20). С. 186–190.

8. Багдасарян А., Багдасарян С., Карапетьян Г., Машинин О., Синицына Т. Импедансные ПАВ-фильтры для телекоммуникационных систем. Российский приоритет // Электроника: Наука, технология, бизнес. 2014. № 7 (139). С. 48–65.

9. Багдасарян А. С., Гуляев Ю. В., Доберштейн С. А., Синицына Т. В., Багдасарян С. А. Интеллектуальные устройства на ПАВ: Новые возможности // Техника радиосвязи. 2018. № 2 (37). С. 64–73.

10. M. Pereira da Cunha [et al.] Wireless Harsh Environment SAW Array System for Power Plant Application // Proc. IEEE Ultrasonics Symposium. 2014. P. 381–384.

11. Бутенко В. В. [и др.] Акустоэлектронные идентификационные метки в керамике LTCC // Труды научно-исследовательского института радио. 2013. № 1. С. 16–23.

12. Alexey Belyanin, Alexander Bagdasarian, Sergey Bagdasarian, Petr Luchnikov and Natalya Katakhova. Magnetic Nanocomposites Based on Opal Matrices // Key Engineering Materials Submitted Vol. 781, pp. 149–154 © 2018 Trans Tech Publications, Switzerland DOI 10.4028

13. Багдасарян А. С., Багдасарян С. А., Бутенко В. В., Карапетьян Г. Я. Датчик давления на поверхностных акустических волнах. Патент на полезную модель № 180995 03.07.2018. Бюл. № 19.

14. Багдасарян С. А. Радиочастотные компоненты на поверхностных акустических волнах с невзаимными СВЧ устройствами // Материалы Международной научно-технической конференции, 19–23 ноября 2018 г. М. : РТУ МИРЭА INTERMATIC, 2018. Ч. 3. С. 526–530.

15. Багдасарян А. С., Багдасарян С. А. Информационные технологии с использованием радиомониторинга в общей врачебной практике // Материалы Международной научно-технической конференции, 19–23 ноября 2018 г. М. : РТУ МИРЭА INTERMATIC, 2018. Ч. 3. С. 521–525.

16. Багдасарян А. С., Багдасарян С. А., Белянин А. Ф., Кащенко О. В., Павлюкова Е.Р. Информационные технологии для реализации пациент-ориентированного подхода в системе управления лечебно-диагностическим процессом у больных артериальной гипертензией // Доклад на VI Междисциплинарном конгрессе по заболеваниям органов головы и шеи. НМИЦ Нейрохирургии им. Н. Н. Бурденко. г. Москва, 17 мая 2018.

17. Багдасарян А. С., Белянин А. Ф., Багдасарян С. А. Эндоскоп направленного импульсного рентгеновского излучения // Материалы Международной научно-технической конференции, 19–23 ноября 2018 г. М. : РТУ МИРЭА INTERMATIC, 2018. Ч. 3. С. 646–649.

УДК 929
ГРНТИ 03.23.55

К 150-ЛЕТИЮ СО ДНЯ РОЖДЕНИЯ ОСНОВОПОЛОЖНИКА ЭЛЕТРОННОГО ТЕЛЕВИДЕНИЯ Б. Л. РОЗИНГА: ВЕХИ БИОГРАФИИ И НАУЧНОЙ РАБОТЫ

А. Б. Гехт, А. А. Гоголь

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

Цель, которую преследует эта статья – не только кратко рассказать о важнейших вехах научной биографии основоположника электронного телевидения Б. Л. Розинга, но и прояснить ситуацию с местом захоронения ученого. Существует точка зрения, гласящая, что созданный в 2005 г. мемориал якобы является кенотафом и что настоящая могила ученого осталась в прежнем, крайне запущенном виде.

Авторы данной статьи со всей ответственностью утверждают, что приведенная выше позиция глубоко ошибочна. На основе видеозаписи процесса перезахоронения Б. Л. Розинга авторы статьи доказывают, что останки ученого были перенесены из прежней могилы к месту его нынешнего погребения на Вологодском кладбище Архангельска, где был установлен памятник ученому, стоявшего у истоков современного телевидения.

электронное телевидение, Б. Л. Розинг.

XX век стал столетием острых противоречий в развитии человеческой цивилизации, столетием разочарований и вместе с тем надежд человечества, связанных, в первую очередь, с научно-техническим прогрессом, изменившим жизнь практически каждого человека на планете. Поиски новых путей, экспериментирование и революционное преобразование, многоликость, противоречивость – вот отличительные особенности науки XX века. Одним из важнейших достижений XX столетия стало открытие и широкое распространение телевизионного вещания, кардинальным образом изменившего способы и типы распространения информации в обществе. Многие ученые

и изобретатели своими идеями и открытиями способствовали развитию телевизионного вещания. У истоков создания телевидения стоял наш соотечественник, ученый Борис Львович Розинг, своими трудами подготовивший почву для дальнейшего совершенствования и развития электронного телевидения.

Несмотря на то, что в наши дни его изобретением ежедневно пользуются практически все жители Земли, имя этого человека по-прежнему недостаточно известно за пределами научного сообщества. Цель, которую преследует эта статья – кратко рассказать о важнейших вехах научной биографии Б. Л. Розинга, его великом вкладе в развитие современной науки.

Борис Львович Розинг, первый ученый, реализовавший на практике работу электронного телевидения, родился в Санкт-Петербурге в 1869 году в аристократической семье потомков голландского аптекаря, приглашенного работать в Россию во времена Петра I. В 1891 г. он с отличием закончил физико-математический факультет Санкт-Петербургского университета и начал свою научную и преподавательскую деятельность. Поисками способа электрической передачи изображения в Технологическом институте Санкт-Петербурга, где он работал с 1892 г., Борис Розинг занимался не один год. Еще в 1907 году он подал первую в мире заявку на патентование электронного телевидения [1, С. 42]. В силу различных причин открытие Розинга оказалось по достоинству оценено в первую очередь за рубежом: изобретение было запатентовано в 1908 г. в Англии и в 1909 г. в Германии, и лишь в 1910 г. – в России [1, С. 45].

Но главной датой в жизни Розинга – ученого является 9 (22) мая 1911 года. В этот день Борису Львовичу удалось успешно предать и получить точное изображение на экране пока еще простейшего устройства, бывшего прототипом кинескопа современного телевизора, которое ученый назвал «электрическим телескопом». Опыт Розинга состоял в следующем. Используя электронный луч, на экране осциллографической электронно-лучевой трубки появилось изображение, которое состояло из 4 белых полос на черном фоне [2, P. 18]. Среди тех, кто помогал Розингу с опытом, был тогда еще студент Санкт-Петербургского Технологического института Владимир Зворыкин – именно его, а не Розинга, через несколько десятилетий назовут отцом телевидения, хотя в основе работы всех воспроизводящих телевизионных устройств лежал принцип, открытый Борисом Львовичем в 1911г. [3].

Через год, в 1912 г., за свой успешный опыт Борису Львовичу была присуждена Золотая медаль Русского технического общества, а также премия имени К. Г. Сименса, что было отражено в протоколах собраний Русского Технического Общества [4]. Талантливый ученый получил заманчивое предложение из США, где ему предлагали все условия для дальнейшей научной работы, но Розинг отказался, не считая правильным продавать результаты своих научных трудов иностранцам [5].

Потрясения в жизни России начала XX века привели В. К. Зворыкина в США, где ему посчастливилось сделать впечатляющую карьеру в области развития средств телевещания. Его же учитель остался в России. В ходе революционных событий 1917 года Б. Л. Розинг оказался в Краснодаре, где и остался на несколько лет. Борис Львович Розинг был в числе группы ученых, по инициативе которых в Краснодаре был открыт Политехнический институт. Работая в этом учебном заведении преподавателем физики, Борис Львович получил ученое звание профессора, а также занял должность проректора [1, С. 64].

Живя в Краснодаре, ученый написал книгу «Электрическая телескопия (видение на расстоянии). Ближайшие задачи и достижения», которая была издана в Петрограде в 1923 году. Учёный как будто предвидел будущее. В своей книге он писал: «Несомненно, наступит, наконец, такое время, когда электрическая телескопия распространится повсеместно и станет столь же необходимым прибором, каким является в настоящее время телефон. Тогда миллионы таких приборов, таких "электрических глаз" будут всесторонне обслуживать общественную и частную жизнь, науку, технику и промышленность» [6].

В 1924 году Розинг занял должность старшего научного сотрудника Ленинградской экспериментальной электротехнической лаборатории, в которой имелась хорошая техническая база для его экспериментов. Борис Львович продолжал работать над усовершенствованием передающего и приемного устройства своего «электрического телескопа». В результате он создал несколько вариантов конструкций электронно-лучевой трубки. Тогда же исследовательская группа под руководством Б. Л. Розинга создала три различных прибора, облегчающих ориентировку незрячих среди тёмных и светлых предметов. Но в скором времени научная и преподавательская деятельность Бориса Львовича прервалась.

В 1930 г. Розинг был арестован за связи с людьми, обвиненными в контрреволюционной деятельности и в 1931 г. выслан на 3 года в северные районы СССР – сначала в Котлос, а затем в Архангельск [1, С. 81.]. Благодаря заступничеству друзей и коллег из числа научного сообщества, Розингу удалось устроиться на работу на кафедру физики в ЛАТИ, где он продолжил свою деятельность преподавателя и исследователя.

В 1932 году правительство СССР приняло решение развивать электронное телевидение. В качестве почетного гостя, читающего лекции по этому вопросу, в Москву и Ленинград приезжает ученый, ставший всемирно известным благодаря созданию лучевой передающей трубки – Владимир Зворыкин, когда-то ассистировавший Розингу во время его экспериментов с передачей изображения. Зворыкину удалось не только усовершенствовать, но и добиться широкого практического применения открытия своего учителя – Бориса Розинга.

Именно его открытие послужило отправной точкой для дальнейшего развития электронного телевидения. На его основе Зворыкин разработал второй важнейший компонент электронного телевидения – передающую телевизионную камеру и электронную систему телевидения с передающей электроннолучевой трубкой [7]. В последствии Зворыкин говорил, что он изобрел только иконоскоп и ни на что другое не претендует [2, PP. 138–139]. Но американские газеты уже назвали его отцом телевидения, совершенно не беря во внимание заслуги его предшественников. Сложилась необычная ситуация: ни научный мир, ни деловые круги, ни журналисты не оспаривали роли Бориса Львовича Розинга – в значительной степени, о нём, как об основоположнике электронного телевидения, просто забыли.

В ссылке ученый жил крайне скромно. Коллеги по кафедре, зная его затруднительное положение, помогали Борису Львовичу, принося ему домашнюю еду. О последних днях жизни ученого мы знаем немногое. Многолетняя напряженная работа и, в особенности трудные условия жизни в непривычном северном климате подкосили здоровье учёного. 20 апреля 1933 г., из-за произошедшего кровоизлияния в мозг его не стало. Б. Л. Розинг был скромно похоронен на окраине Вологодского (также известного как Кузнечевское) кладбища в Архангельске. На следующие четверть века имя Бориса Львовича было фактически забыто.

В 1957 году, на волне масштабной реабилитации жертв политических репрессий, Розинг был полностью реабилитирован [1, С. 85]. Постепенно жизнь и многосторонняя научная деятельность, творческий путь Бориса Львовича стали освещаться в литературе и в жизни научного сообщества. В 1964 г. вышла книга П. К. Горохова «Борис Львович Розинг – основоположник электронного телевидения», посвященная жизни и научной деятельности исследователя. В 1978 году на здании кафедры физики в ЛТИ была установлена мемориальная доска в память первой приемной электронно-лучевой трубки, изобретенной Розингом [8]. 28 ноября 2003 года на главном здании СПбГТИ по адресу Московский проспект, д. 26 была открыта мемориальная доска Розингу, выполненная по проекту художника Т. Н. Милорадовича [8].

Своего рода финальным аккордом в деле восстановления справедливости в отношении захоронения Б. Л. Розинга стало его перезахоронение, инициированное работниками местного областного телевидения. В 2004 году оргкомитет по созданию мемориала Б. Л. Розинга, возглавляемый Л. С. Филипповой, пригласил ректора СПбГУТ А. А. Гоголя принять участие в этом знаменательном событии и оказать посильную помощь. Для оказания содействия были привлечены различные коммерческие и общественные организации, такие как Российский фонд истории связи, Фонд помощи в развитии отечественной науки «Диполь», а также Попечительский совет СПбГУТ,

учрежденные Санкт-Петербургским государственным университетом телекоммуникаций им. проф. М. А. Бонч-Бруевича, Архангельская телевизионная компания, Архангельский государственный технический университет и другие организации [9]. В результате, 30 мая 2005 года Борис Львович Розинг был перезахоронен на Вологодском кладбище в Архангельске.

Существует точка зрения, гласящая, что созданный в 2005 году мемориал якобы является кенотафом и что настоящая могила ученого осталась в прежнем, крайне запущенном виде. Именно это утверждение приводится в очерке «Две могилы Бориса Розинга» [10]. Ссылка на этот очерк приводится и в специальной статье популярной интернет-энциклопедии Википедия, посвященной Б. Л. Розингу [11].

Авторы данной статьи со всей ответственностью утверждают, что приведенная выше позиция глубоко ошибочна.

По инициативе директора филиала ФГУП «Российская телевизионная и радиовещательная сеть» «Архангельский областной радиотелевизионный передающий центр» Мансура Акрамовича Салахутдинова велась видеосъемка процесса перезахоронения Б. Л. Розинга. Этот видеоисточник (доступный по ссылке http://www.sut.ru/index.php/teaching/ft/fakultetgf/kaf-history) наглядно демонстрирует, что останки ученого были перенесены из прежней могилы к месту его нынешнего погребения, где был установлен памятник ученому [12]. Таким образом, Борис Львович Розинг действительно захоронен в своем мемориале на Вологодском кладбища Архангельска.

В завершении этого очерка авторы выражают глубокую благодарность за всестороннюю поддержку директору филиала ФГУП «Российская телевизионная и радиовещательная сеть» «Архангельский областной радиотелевизионный передающий центр» Мансуру Акрамовичу Салахутдинову, а также ректору СПбГУТ профессору Сергею Викторовичу Бачевскому.

Имя Б. Л. Розинга, человека, жизнь и научная работа которого служат примером для современных преподавателей и учёных, с большим уважением вспоминают в стенах Санкт-Петербургского университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, сотрудники которого впоследствии продолжили и с большим успехом развили дело становления телевидения в России, начатое ещё Борисом Львовичем Розингом.

Список используемых источников

1. Горохов П. К. Борис Львович Розинг – основоположник электронного телевидения. М. : Наука, 1964.

2. Розинг Б. Л. Система электрической телескопии, основанная на применении пульсирующих и переменных токов // Электричество. 1911. № 15. С. 349–359.

3. Abramson A. Zworykin, Pioneer of Television. Urbana : University of Illinois, 1995.

4. Журнал общего собрания Русского Технического общества от 19 мая 1912 г. // Записки РТО. 1913. № 6–7. С. 61.

5. Вся Россия. Розинг. [Электронный ресурс] // Телеканал Россия-1. URL: http://russia.tv/video/show/brand_id/3966/episode_id/325609 (дата обращения 20.02.2019).

6. Розинг. Б. Л. Электрическая телескопия (видение на расстоянии). Ближайшие задачи и достижения. Петроград : Academia, 1923. С. 6.

7. Зворыкин В.К., Мортон Д. А. Телевидение. Вопросы электроники в передаче цветного и монохромного изображений. М. : Иностранная литература. 1956. С. 225.

8. Основоположник электронного телевидения Б. Л. Розинг. [Электронный ресурс] // СПбГТИ – Санкт-Петербургский государственный технологический институт. URL: http://www1.lti-gti.ru/museum/rozing.htm (дата обращения 20.02.2019).

9. Гоголь А. А. Памяти основателей теле- и радиовещания. Отчет о краткой командировке // Вестник ГФ СПбГУТ. 2005. № 2. С. 29.

10. Две могилы Бориса Розинга. [Электронный ресурс] // Архангельский некрополь. URL: http://arh-necropol.narod.ru/index/0-415 (дата обращения 30.03.2019).

11. Розинг, Борис Львович [Электронный ресурс] // Википедия. URL: http://ru.wikipedia.org/wiki/%D0%EE%E7%E8%ED%E3,_%C1%EE%F0%E8%F1_%CB%FC%E2%EE%E2%E8%F7 (дата обращения 30.03.2019).

12. Перезахоронение останков Б. Л. Розинга на Кузнечевском кладбище г. Архангельска 17 мая 2005 г. [Электронный ресурс] // Кафедра истории и регионоведения СПбГУТ. URL: http://www.sut.ru/index.php/teaching/ft/fakultetgf/kaf-history (дата обращения 30.03.2019).

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 654.027
ГРНТИ 49.27.31

ВЛИЯНИЯ ЭЛЕМЕНТОВ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ С ТЕХНОЛОГИЕЙ CARRIER ETHERNET НА ЗАДЕРЖКУ РАСПРОСТРАНЕНИЯ ТРАФИКА

Р. С. Абдусаламов, А. В. Ануфренко, О. В. Мордвинова, Р. К. Фомкин

Военная академия связи имени Маршала Советского Союза С. М. Буденного

Транспортные сети связи Carrier Ethernet могут создаваться на основе разных архитектур с огромным количеством входящих в них элементов. При прохождении трафика по направлениям транспортной сети неизбежно возникают различного рода задержки, связанные с его обработкой в каждом узле сети, а также при его распределении по сети. Для обеспечения требуемого качества обслуживания пользователей необходима возможность детального учета влияния функционирования элементов транспортной сети на задержку трафика, проходящего через нее трафика. Чему способствует разработка соответствующих имитационных моделей функционирования транспортной сети связи Carrier Ethernet.

узловая задержка, транспортная сеть связи, Carrier Ethernet, моделирование, узел агрегации.

Современные транспортные сети связи являются сложными объектами анализ которых требует учета большого количества параметров. Аналитические модели недостаточно детализируют процесс функционирования транспортных сетей, поэтому используют имитационное моделирование. С помощью имитационного моделирования на основе программы General Purpose Simulation System STUDIO [1] создана модель транспортной сети связи Carrier Ethernet. Разработанная модель помогает анализировать влияние элементов транспортной сети на задержку распространения трафика.

Моделируемая сеть Carrier Ethernet представляет из себя восемь узлов транспортной сети связи с полносвязной топологией. Трафик в транспортную сеть связи поступает из узла агрегации и представляет собой сочетание трафика Constant Bit Rate, Real Time – Variable Bit Rate и Unspecified Bit Rate. Из транспортной сети связи трафик попадает на другой узел агрегации.

Транспортная сеть представлена как объект, имеющий многослойную (многоуровневую) структуру. Модель функционирования сети учитывает узловую задержку и задержку в линии связи, а именно оптические и электрические преобразования сигнала, происходящие в этих элементах транспортной сети.

Временная модель оборудования Carrier Ethernet, учитываемая в имитационных моделях и описывающая слагаемые суммарной узловой задержки, представлена на рис. 1–2 [2, 3].

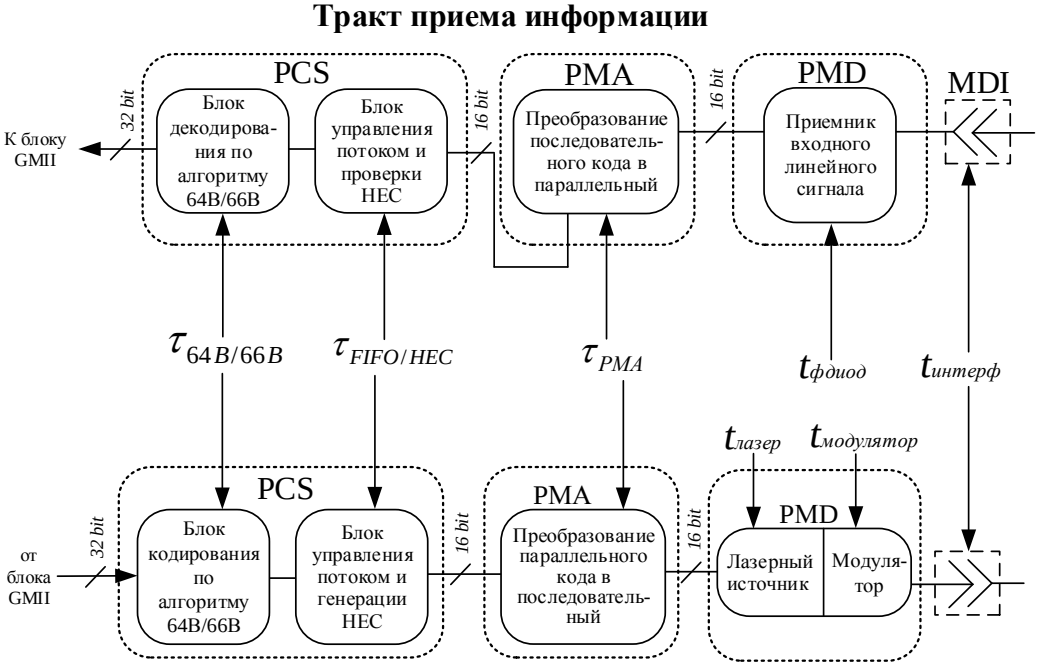


Рис. 1. Временная модель оборудования Carrier Ethernet в части MDI-PCS

Обобщенное представление слагаемых узловой задержки отображено на рис. 3 (см. ниже).

Аналитическое выражение для расчета общей узловой задержки, учитываемое в имитационной модели функционирования транспортной сети *Carrier Ethernet* имеет следующий вид [5]:

$$\tau_{CE} = \sum \tau_{\text{кан}}^{CE} + \sum T_{\text{физ}}^{CE} = \sum_{k} (n \cdot t_{\text{интерф}} + n \cdot t_{\text{ф.диод}} + n \cdot \tau_{PMA} + n \cdot \tau_{FIFO/HEC} + t_{\text{лазер}} +$$

$$+ t_{\text{модулятор}} + n \cdot \tau_{GMII} + n \cdot \tau_{RS} + n \cdot \tau_{\text{доступ}} + n \cdot \tau_{802.3\,MAC} + n \cdot \tau_{MAC_{CONTROL}} + n \cdot \tau_{LLC}),$$

где τ_{CE} – общая узловая задержка транспортной сети связи, k – количество сетевого оборудования на рассчитываемом участке сети, n – количество однотипных элементов в оборудовании, $t_{\text{интерф}}$ – задержки интерфейсов, $t_{\text{ф.диод}}$ – задержки оптических приемников, τ_{PMA} – задержка сериализации, $\tau_{FIFO/HEC}$ – задержка управления пакетом, $t_{\text{лазер}}$ – задержки источников лазерного излучения, $t_{\text{модулятор}}$ – задержки внешних модуляторов, τ_{GMII} – задержка гигабитного интерфейса, τ_{RS} – задержка согласования, $\tau_{\text{доступ}}$ – задержка управления доступом к физическому уровню, $\tau_{802.3\ MAC}$ – задержка процесса инкапсуляции кадра, τ_{LLC} – задержка процесса инкапсуляции пакета.

Рис. 2. Временная модель оборудования Carrier Ethernet в части GMII-LLC

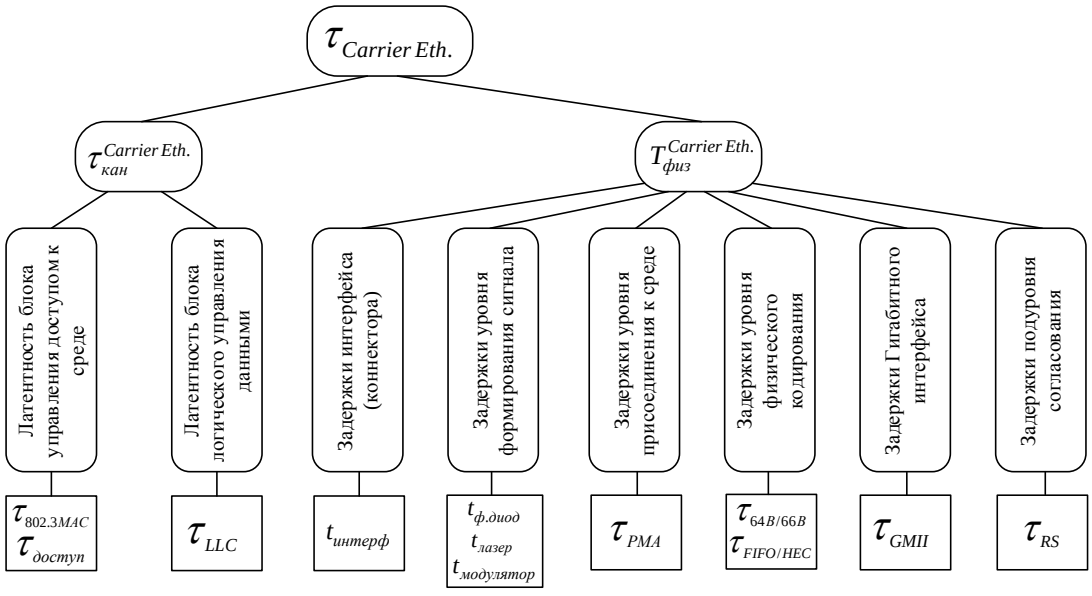


Рис. 3. Общая классификация узловой задержки для модели Carrier Ethernet

Функция, описывающая закон изменения сигнала в оптических линиях связи имеет следующий вид:

$$T_{\text{опт}}(\lambda) = \frac{l_{\text{опт}}}{v_{\text{гр}}(\lambda)} = \frac{N(\lambda) \cdot l_{\text{опт}}}{c} = \left[n - \lambda \frac{dn}{d\lambda}\right] \frac{l_{\text{опт}}}{c} =$$

$$= \left[\sqrt{1 + \sum_{i=1}^{3} A_i \frac{\lambda^2}{\lambda^2 - l_i^2}} - \lambda \frac{d\left(1 + \sum_{i=1}^{3} A_i \frac{\lambda^2}{\lambda^2 - l_i^2}\right)}{d\lambda} \right] \frac{l_{\text{опт}}}{c},$$

где $l_{\text{опт}}$ – оптическая длина линии, $v_{\text{гр}}(\lambda)$ – групповой показатель скорости света в среде передачи, $N(\lambda)$ – групповой показатель преломления среды распространения, c – скорость света в вакууме.

Следовательно, зная величины всех слагаемых и количество сетевого оборудования, можно вычислить задержку участка транспортной сети, построенного по технологии Carrier Ethernet.

Рассматриваемая модель транспортной сети связи представляет собой многофазную многоканальную систему массового обслуживания с ограниченными ёмкостями буферов (накопителей), то есть с отказами [6].

Структура моделируемого фрагмента транспортной сети приведена на рис.4.

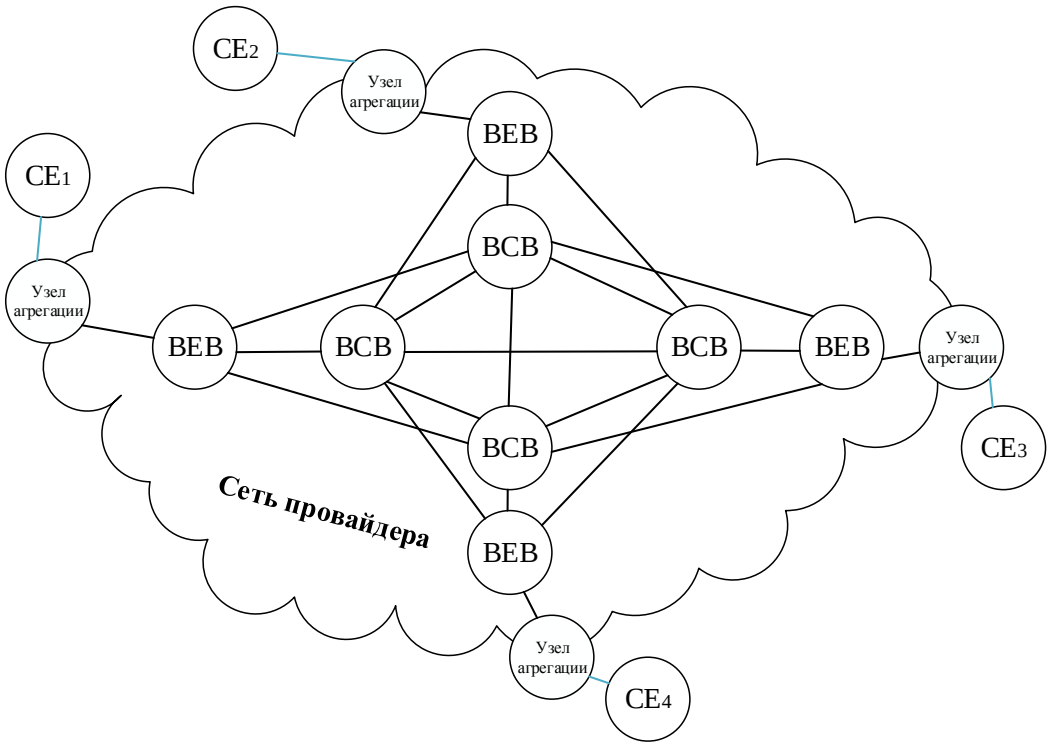


Рис.4. Структура моделируемого фрагмента транспортной сети

Сообщения поступают от 1 источника (узла агрегации) и проходят через различные по назначению узла транспортной сети Carrier Ethernet (BEB, BCB). Интервалы поступления сообщений распределяются по закону, который формирует модель узла агрегации. Интервалы между отказами, а также время восстановления работоспособности узлов транспортной сети связи распределяются по нормальному закону. Процесс отказа и восстановления элементов транспортной сети описан с учетом защитных механизмов сети связи (протокол *Ethernet ring protection protocol*). Сообщения проходят через транспортной сеть и попадают к получателю (на другой узел агрегации).

В результате разработанной модели проанализировано существенность влияния элементов транспортной сети связи на задержку, агрегированного трафика, проходящего через транспортную сеть связи:

1. Задержкой интерфейсов элементов транспортной сети можно пренебречь.

2. Задержка оптических усилителей является постоянной величиной и носит существенный для обеспечения QoS характер.

3. Задержки оптических приемников, источников лазерного излучения, внешних модуляторов являются постоянными величинами и носят несущественный для обеспечения QoS характер.

4. Задержка при инкапсуляции кадра Ethernet является непостоянной величиной и носит для обеспечения QoS существенный характер.

Разработанная модель транспортной сети Carrier Ethernet способствуют детальному анализу влияния параметров сети на задержку агрегированного трафика.

Список используемых источников

1. Девятков В. В. Среда имитационного моделирования GPSS STUDIO: руководство пользователя. Казань, 2019. 550 с.

2. ITU-T Recommendation G.8032. Transmission systems and media, digital systems and networks. – 2015.

3. 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. 145 с.

4. ITU-T Recommendation G.805. Generic functional architecture of transport networks. – 2000.

5. Фокин В. Г. Оптические системы передачи и транспортные сети. М. : Эко – Трендз, 2008. 288с.

6. Алиев Т. И. Основы моделирования дискретных систем. СПб: СПбГУ ИТМО, 2009. 363 с.

Статья представлена заведующим кафедрой «Электрическая связь» ПГУПС, доктором технических наук, профессором А. К. Канаевым.

УДК 004.4:004.7
ГРНТИ 49.27.99

АНАЛИЗ ВЕРОЯТНОСТИ ПОТЕРИ ПАКЕТОВ В БУФЕРЕ МАРШРУТИЗАТОРА С УЧЕТОМ ФРАКТАЛЬНОСТИ ТРАФИКА

Р. С. Абдусаламов, Р. К. Фомкин

Военная Академия Связи имени маршала Советского Союза С. М. Будённого

В статье проводится исследование зависимости фрактальности трафика от буферного запоминающего устройства маршрутизатора в основных системах массового обслуживания. В качестве исследуемой системы рассматривается сетевой трафик, где присутствует вспышки или всплеск на различных временных интервалах. Актуален вывод о целесообразности увеличения емкости буферного запоминающего устройства с целью уменьшения влияния фрактальности трафика.

самоподобный трафик, фрактальность трафика, показатель Хёрста, БЗУ – буферное запоминающее устройство.

На сегодняшний день большое внимание в исследовании инфокоммуникационных систем уделяется проблемам наличия свойств самоподобия. Однако это не дает однозначного вывода о самоподобной структуре таких систем, т. к. существуют ряд воздействий, которые могут приводить к таким же свойствам [1, 2].

Рассматривая в качестве исследуемой системы сетевой трафик, можно сделать вывод о самоподобной или фрактальной его природе на основе современных исследований. В нем присутствуют так называемые вспышки или пачки пакетов, наблюдаемые на различных временных интервалах. Из этого следует, что распространенные методы моделирования и расчета таких систем, основанные на использовании пуассоновских потоков, не дают полной и качественной картины происходящего в сети [3].

Известны несколько методов оценки самоподобия состояния систем. Самые популярные из них: анализ R/S-статистики; анализ графика изменения дисперсии; анализ, основанный на специфических свойствах; оценка Виттла; анализ, основанный на вейвлет-функциях [4]. R/S-метод не слишком точен, поскольку дает оценку только уровня самоподобности во временном ряде. Поэтому данный метод может использоваться только для про-

верки, является ли временной ряд самоподобным и если является, то получить грубую оценку *H*. Этот результат может быть использован для оценки показателя Хёрста.

На практике проверка на самоподобность и оценка показателя Хёрста является сложной задачей. Проблема в том, что на практике в основном исследуют конечный набор данных [1]. Из этого следует невозможность выявления самоподобности трассы трафика. При этом анализ реального трафика данных в существующих и перспективных ТКС показал некорректность использования во многих случаях пуассоновских моделей для определения их вероятностно-временных характеристик [5]. Но существует большое количество моделей оценки вероятности потери пакетов в результате переполнения буфера. Поэтому актуальна задача провести их сравнительный анализ и выработать рекомендации по их применению.

На сегодняшний день основной моделью является модель СМО M/M/1, предполагающая, что время поступления заявок и время их обслуживания распределены по экспоненциальному закону.

В исследуемой работе проанализирован маршрутизатор на магистральном уровне Cisco 4000, имеющий 3 слота и по 6 портов, буфер которого имеет объем B = 128 Мбит [3].

Для вычисления количества очередей в СМО используем выражение:

$$n = \frac{B}{L},$$

где L – размер IP-пакета.

При этом, размер IP-пакета будем считать максимальным L = 65535 байт.

$$n = 128 \cdot 1024 \cdot \frac{1024}{65535 \cdot 6 \cdot 2 \cdot 3}.$$

Пусть, согласно вычислениям следует, что $W_{sr} = 28$.

Воспользуемся формулой для вычисления вероятности потерь для различных W:

$$Ploss(po) \coloneqq \frac{(1 - po)}{(1 - po)^{W+1}} \cdot po^{W},$$

где $po = \frac{\lambda}{\mu} < 1$ – коэффициент загрузки канала обслуживания; λ – интенсивность входного потока; μ – интенсивность обслуживания выходного потока; W – емкость запоминающего устройства (ЗУ), измеряемая в пакетах. Зависимость вероятности потерь пакетов вычислено и показано (рис. 1).

Известно, что можно оценить вероятность потери пакета при помощи параметра самоподобия (параметра Хёрста). Тогда выражение вероятности потерь преобразуется к виду:

$$Ploss(po) := \frac{(1-po)}{(1-po)^{[(W+1)^{2(1-H)}]}} \cdot po^{W^{2(1-H)}}.$$

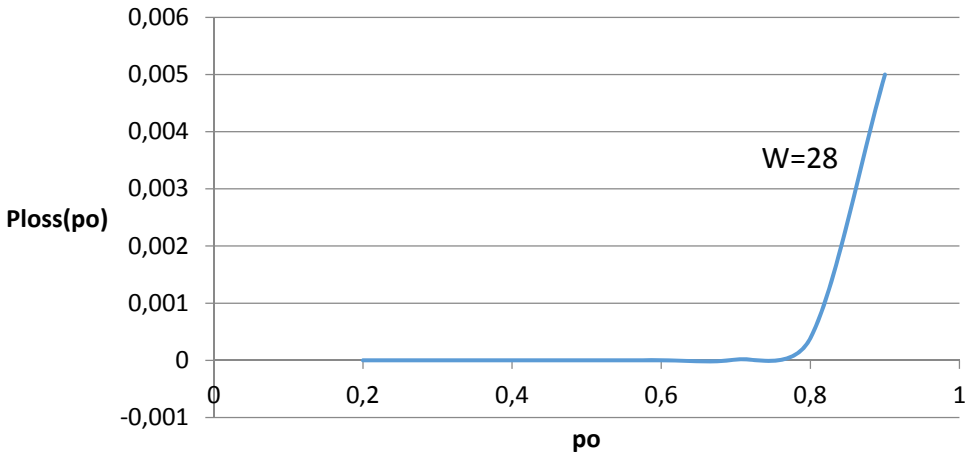


Рис. 1. Зависимость вероятности потерь пакетов при W = 28

Согласно полученному графику можно сделать вывод, что при увеличении очереди возрастает вероятность потерь пакетов (рис. 2).

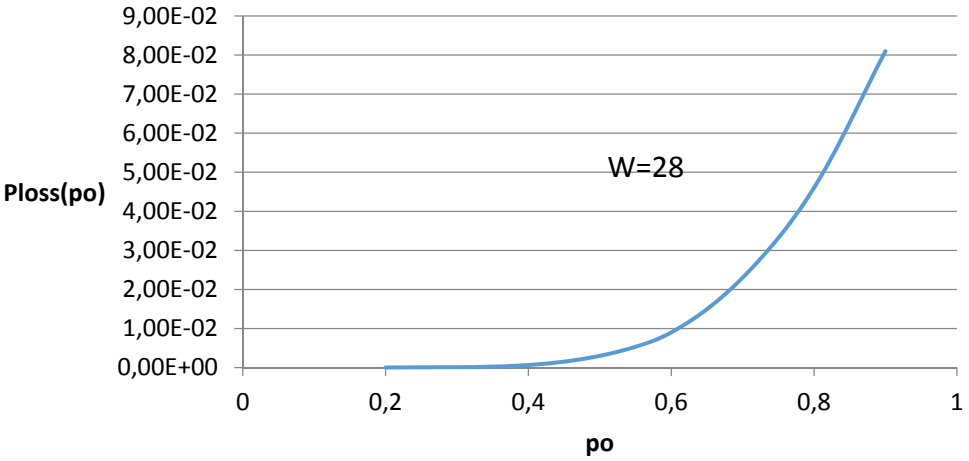


Рис. 2. Зависимость вероятности потерь пакетов при W = 28, H = 0,7

Наиболее качественную оценку дает модель СМО M/M/1. Она может быть использована как нижняя граница вероятности потери сообщений при соответствующем объеме БЗУ и известном коэффициенте загрузки канала ρ.

Но, согласно проведённымм исследованиям, самая высокая вероятность потери сообщений наблюдается при использовании СМО с показателем Хёрста 0,95. Также определено, что при увеличении фрактального трафика и роста коэффициента девиации, увеличивается вероятность потери пакета.

Однако влияние фрактальности снижается при увеличении емкости БЗУ. Полученные в ходе моделирования результаты подтверждают, что наиболее объективная оценка вероятности потери сообщения за счет переполнения БЗУ обеспечивается только при учете характера трафика, иначе возникнет большая доля погрешности в расчетах [4] (рис. 3).

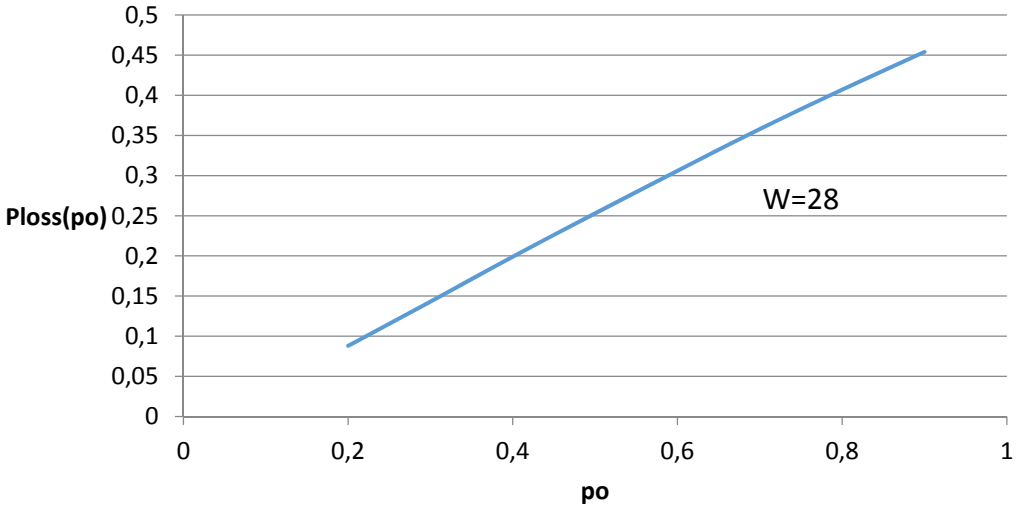


Рисунок 3. Зависимость вероятности потерь пакетов при *W*=28, *H*=0.95 [5]

При увеличении фрактального трафика и роста коэффициента девиации увеличивается вероятность потери пакета за счет переполнения БЗУ. Влияние фрактальности снижается при увеличении емкости БЗУ. Таким образом, актуален вывод о целесообразности увеличения емкости БЗУ с целью уменьшения влияния фрактальности трафика.

Список используемых источников

1. Олифер В. Г., Олифер Н. А. Компьютерные сети, 3-е издание. СПб. : Питер, 2006, С. 215–219.

2. Жданов А. Г., Расказов Д. А., Смирнов Д. А., Шипилов М. М. Передача речи по сетям с коммутацией пакетов IP-телефония. СПб. : СПбГУТ, 2001. 144 с.

3. Семенов Ю. В. Проектирование сетей связи следующего поколения. СПб. : Наука и техника, 2005, 105 с.

4. Абдусаламов Р. С. Исследование вероятности потери пакетов при увеличении фрактальности сетевого трафика // Студенческая наука для развития информационного общества. VIII Всероссийская научно-техническая конференция : сб. материалов. 2018. 545 с.

5. Briden, R. RFC1633 – Integrated Services in the Internet Archives: an Overview // Internet Archives [Electronic resource]. 2004. URL: http: //www.faqc .org/rfss225/rfc 1633.html.

Статья представлена заведующим кафедрой «Электрическая связь» ПГУПС, доктором технических наук, профессором А. К. Канаевым.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

В. С. Авраменко, Д. А. Бочкарев, А. В. Маликов

Военная академия связи им. Маршала Советского союза С.М. Буденного.

В современных инфокоммуникационных системах существует множество разнообразных предпосылок возникновения компьютерных инцидентов. Многообразие и разнородность сведений о событиях информационной безопасности создает новые требования к системам анализа и оперативного реагирования на компьютерные инциденты.

информационная безопасность, компьютерный инцидент, искусственный интеллект, искусственная нейронная сеть.

В настоящее время наблюдается рост числа инцидентов в инфокоммуникационных системах, приводящих к большим финансовым, коммерческим и репутационным потерям юридических и физических лиц, а в случае с органами государственной власти и субъектами критической информационной инфраструктуры – к угрозам безопасности личности, общества и государства [1].

В рамках проводимых в сфере информационной безопасности расследований часто фиксируются множественные случаи некорректного реагирования на инциденты, в ходе которых системными администраторами, сотрудниками подразделений информационной безопасности организаций или иными уполномоченными лицами были уничтожены криминалистически значимые данные, позволяющие привлечь к уголовной ответственности злоумышленников (была существенно снижена юридическая значимость данных, собранных в ходе внутреннего расследования инцидента), а также технические данные, позволяющие использовать их для анализа в целях предупреждения подобных компьютерных инцидентов в будущем.

Согласно оценкам экспертов, в области информационной безопасности, организации не могут быстро обнаруживать проникновения в сеть, более 92 % проникновений остаются незамеченными пострадавшей организацией [2]. Очевидно, что подразделения информационной безопасности должны играть более активную роль. Необходимо постоянно контролировать, что происходит внутри инфраструктуры и стремиться использовать

средства реагирования до того, как атаки смогут привести к компьютерным инцидентам и нанести серьезный ущерб.

В настоящее время расследование компьютерных инцидентов включает в себя технические мероприятия, цель которых состоит в сохранении криминалистически значимых данных и возможность исследования этих данных в будущем в рамках судопроизводства, а также организационные мероприятия, позволяющие снизить ущерб и предоставить следствию необходимые документы.

Такие технические мероприятия обеспечивают целостность потенциально имеющих отношение к инциденту данных путем отключения, упаковки, опечатывания, а затем надлежащего хранения носителей информации. Организационные мероприятия заключаются в уведомлении руководства организации, подразделений информационной безопасности о факте инцидента и сведениях технического характера [3].

Правила сбора и фиксации цифровых доказательств не установлены на законодательном и подзаконном уровне вследствие быстрой изменяемости информационных технологий, но вполне приемлемо разрабатывать и обобщать их на уровне ведомственных нормативных актов (либо на уровне нормативных актов конкретной организации). Однако качество таких документов напрямую зависит от уровня подготовленности технических специалистов в таких ведомствах и организациях и нередко остается низким.

Как правило, вышеуказанные мероприятия осуществляются вручную и зачастую хаотично. Системные администраторы и сотрудники подразделений информационной безопасности не знают, как реагировать на возникший инцидент, как обеспечить оперативный сбор достоверных данных, необходимых для проведения расследования. Недостаток этих сведений приводит к позднему реагированию на инцидент, в результате которого противоправные, а зачастую преступные действия злоумышленника реализуются, а информационные следы этих действий удаляются.

Ввиду разнородности используемых в инфокоммуникационных системах устройств, а также многообразия средств защиты информации, количество регистрируемых событий информационной безопасности столь велико и постоянно продолжает расти, что их обработка и анализ с целью выявления общих закономерностей, причин возникновения и сценариев развития имеют высокую трудоемкость.

С учетом большого числа событий, происходящих в инфокоммуникационных системах, необходимо проводить автоматический сбор и автоматизированный анализ сведений, описывающих события информационной безопасности.

Основными источниками сведений о событиях, которые следует анализировать для определения состояния инфокоммуникационных систем являются:

сведения о сетевом трафике;
сведения о процессах;
журналы маршрутизаторов;
журналы операционных систем;
журналы приложений;
журналы баз данных.

Существуют различные методы обработки данных: общие методы (прогнозная аналитика, имитационное моделирование, визуализация), методы искусственного интеллекта: глубинный анализ данных (*Data Mining*), машинное обучение (*Machine Learning*), в том числе и на основе искусственных нейронных сетей, генетические алгоритмы и др. Для оперативного и достоверного анализа событий информационной безопасности наиболее целесообразно использовать технологии искусственного интеллекта, что обусловлено следующими его свойствами: способность выделять необходимые для анализа сведения из значительного объема неинформативных (шумовых) входных сигналов, выявление и классификация скрытых закономерностей, отсутствие необходимости жесткой формализации решаемых задач, адаптивность к изменениям среды функционирования.

Обычно схема реализации технологии искусственного интеллекта включает в себя следующие процессы:

загрузка данных в систему и их предварительная обработка;

извлечение признаков (классификация, преобразование «сырых» данных, позволяющее использовать их для обработки алгоритмами искусственного интеллекта);

обучение модели с использованием признаков;

тестирование модели (ее упрощение или усложнение, добавление новых признаков, новых источников данных, комбинирование моделей);

внедрение лучшей модели (моделей) в рабочую инфокоммуникационную систему;

загрузка в модель рабочей системы реальных данных.

Таким образом, можно выделить следующие ключевые компоненты, обеспечивающие функционирование системы искусственного интеллекта: обучающий набор данных (датасет), признаки классификации, алгоритмы.

На сегодняшний день основные проблемы функционирования систем искусственного интеллекта в области информационной безопасности возникают на этапе формирования обучающих наборов данных. Это объем и характер данных (объем данных прямо пропорционально влияет на эффективность алгоритма машинного обучения), а также качество набора данных (зачастую наборы данных для обучения неполны, неточны и разноформатны). Также остро стоит проблема создания внутренних датасетов, собираемых и хранящихся внутри организации – это требует значительных дисковых ресурсов, однако повышает эффективность машинного обучения.

Особенности классификации признаков заключаются в их многообразии. Так, web-запросы могут анализироваться по более чем 500 признакам (длина запроса, URL, whois, сертификаты TLS, типы MIME и др.), а файлы в процессе исполнения – по более чем 190 признакам [4].

Алгоритмы искусственного интеллекта имеет следующие особенности. Во-первых, для решения различных задач для различных данных следует применять различные алгоритмы, так как не существует универсального алгоритма. Но также и одну задачу можно решить с помощью разных алгоритмов. Во-вторых, в процессе рабочего функционирования модель не обучается, она итеративна и требует регулярного обновления. В-третьих, выбор алгоритма является компромиссом между точностью предсказания, скоростью работы и сложностью модели. И наконец, решающим в определении эффективности работы системы является качество обучающего набора данных. Вариант применения искусственных нейронных сетей в задаче анализа компьютерных инцидентов безопасности представлен в [5].

Следует отметить то, что системы с искусственным интеллектом также могут подвергаться компьютерным атакам. Они могут следующую направленность: извлечение данных и моделей из системы, «обман» моделей, изменение функционирования модели на этапе обучения путем изменения обучающего набора данных.

Таким образом, использование методов искусственного интеллекта в целях диагностирования компьютерных инцидентов, как основной составляющей процедуры их расследования, способно вывести защищенность инфокоммуникационных систем на качественно новый уровень, однако требует тщательного планирования с учетом аспектов потребления ресурсов и безопасности.

Список используемых источников

1. Positive Technologies, Актуальные киберугрозы. III квартал 2018 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q3 (дата обращения 24.01.2019).

2. Gartner, «Critical Capabilities for Security Information and Event Management», URL: https://www.gartner.com/doc/3894576 (дата обращения 24.01.2019).

3. Межрегиональная общественная организация «Союз ИТ-директоров». «Инциденты информационной безопасности. Рекомендации по реагированию». URL: http://www.expo-itsecurity.ru/upload/iblock/215/recommendations_SMALL_FIN_3.pdf (дата обращения 24.01.2019).

4. Jinrong Bai, Junfeng Wang, Guozhong Zou. A Malware Detection Scheme Based on Mining Format Information // The Scientific World Journal, 2014. URL: https://www.hindawi.com/journals/tswj/2014/260905/ (дата обращения 24.01.2019).

5. Авраменко В. С., Маликов А. В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей // Сборник трудов конференции «Региональная информатика и информационная безопасность». Выпуск 4. СПб. : СПОИСУ, 2017. 533 с. (С. 24–26).

УДК 004.056
ГРНТИ 81.93.29

АРХИТЕКТУРА СИСТЕМЫ ВИЗУАЛИЗАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ СЕНСОРНЫХ ЭКРАНОВ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ

С. А. Агеев, А. Ю. Иванов, М. В. Коломеец, В. И. Комашинский, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Использование сенсорных экранов совместно с системами дополненной реальности в системах поддержки и принятия решений на основе визуальной аналитики по сравнению с использованием обычных LCD-дисплеев позволяет более эффективно производить анализ состояния компьютерной сети. Для их совместного использования необходимо разработать такую архитектуру, которая позволит визуализировать и управлять данными в режиме реального времени сразу на нескольких типах устройств. включая сенсорный экран, LCD-дисплей и очки дополненной реальности. В работе предлагается концепция построения и архитектура системы поддержки и принятия решений на основе визуальной аналитики, которая реализует сразу несколько способов представления информации на разных устройствах.

визуальная аналитика, архитектура систем, информационная безопасность, сенсорные экраны, дополненная реальность.

Системы поддержки и принятия решений используют визуализацию данных в случаях, когда анализ, мониторинг или принятие решений должны совершаться человеком. Системы визуализации сталкиваются с очевидными трудностями, когда анализу подлежит большое количество многомерных данных, которые оператору сложно воспринимать.

Так может происходить во множестве различных задач обеспечения информационной безопасности, например, при анализе защищенности компьютерных сетей [1], обнаружении сетевых атак [2], проектировании безопасных встроенных систем [3].

Решения, основанные на использовании дополненной реальности для визуальной аналитики [4], а также основанные на сенсорных экранах для управления [5] позволяют более эффективно (с точки зрения восприятия пользователем информации) визуализировать информацию в сравнении с использованием стандартных дисплеев.

Для совместного использования дополненной реальности и сенсорных экранов, когда отображение данных происходит в очках дополненной реальности, а управление за счет жестов на сенсорном экране, необходимо использовать распределенную архитектуру, которая позволит обеспечить достаточную гибкость при настройке как методов управления, так и методов отображения.

В работе предлагается концепция построения и возможная архитектура системы поддержки и принятия решений на основе визуальной аналитики, которая реализует сразу несколько способов представления информации на разных устройствах: в очках дополненной реальности и на сенсорном экране.

Ключевым элементом такой архитектуры являются контейнеры. Контейнеры являются специально выделяемой областью памяти, в которую можно загружать данные по определенному шаблону и после – визуализировать ее (рис. 1).

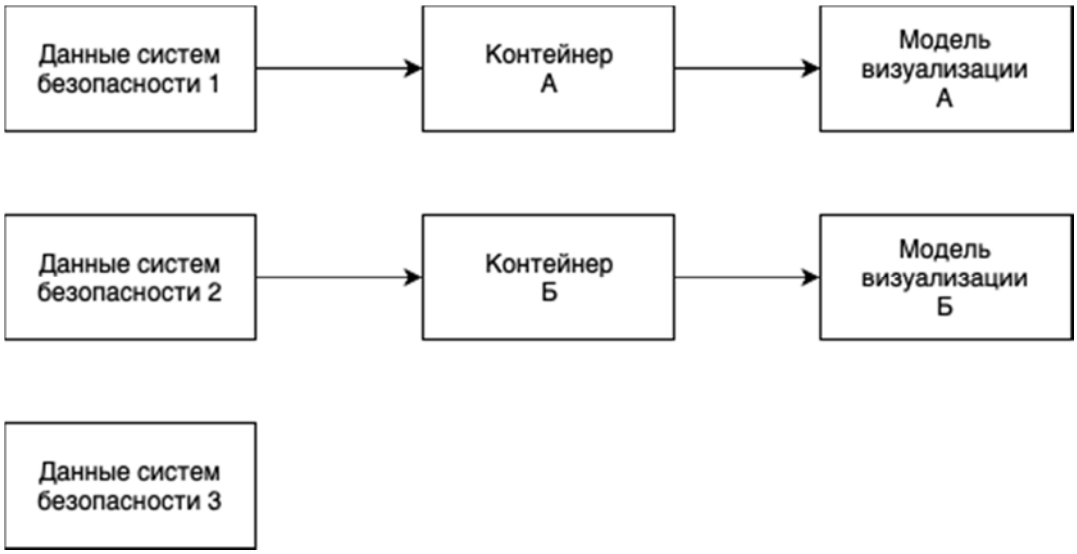


Рис. 1. Контейнерная архитектура (данные от источников передаются в контейнеры, после чего визуализируются)

Количество типов контейнеров равняется количеству типов моделей визуализации. Данные от систем загружаются в контейнер, после чего отображаются в системе визуализации.

При этом, источник данных для контейнера можно менять (рис. 2), тем самым обеспечивая гибкость системы и повторяемость моделей визуализации [6, 7]. Таким образом одну и ту же модель визуализации можно использовать для различных источников данных.

Рассмотрим пример реализации данной архитектуры.

Модель визуализации демонстрируется с использованием очков дополненной реальности, в то время как команды контейнеру данных отправляются с помощью жестов на планшете.

Изначально, пользователь создает контейнер данных в системе. После создания контейнера система открывает к нему доступ (API), с помощью которого можно загружать данные в контейнер посредством HTTP запросов.

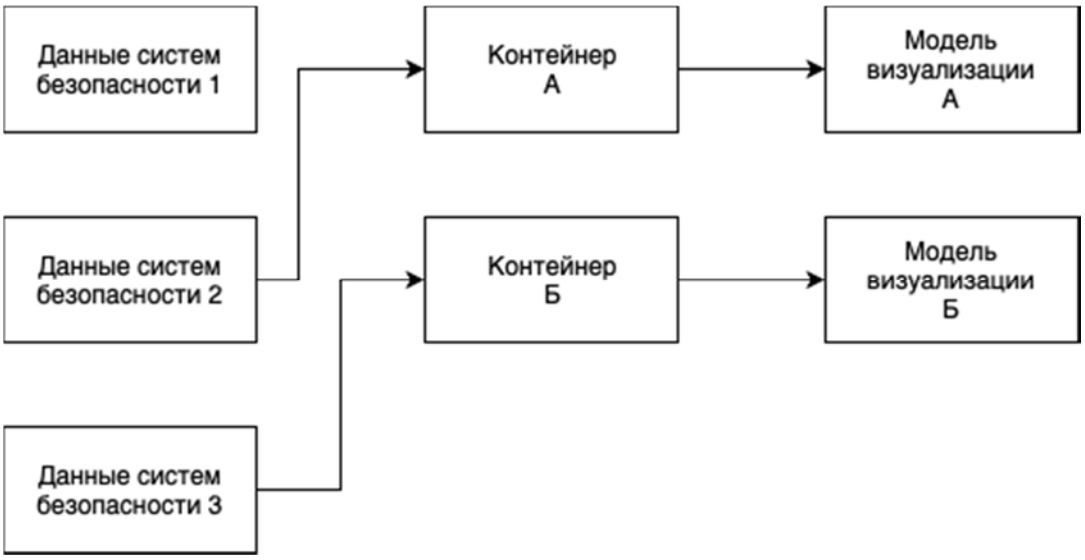


Рис. 2. Повторное использование контейнеров (контейнеры перепривязываются к другим источникам данных, обеспечивая повторяемость использования моделей визуализации).

Каждому контейнеру назначается специальный HTTP-адрес (*адрес_устройства/имя_котейнера*).

При переходе по этому адресу система показывает пример поддерживаемой структуры данных в формате JSON.

Все данные, которые будут впоследствии передаваться по этому адресу должны соответствовать структуре, предоставленной системой.

Пример JSON структуры для контейнера, который поддерживает визуализацию линейного графика приведен в листинге 1.

Листинг 1 – пример JSON-структуры линейного графика

```
{
  "count":[12, 7, 10, 11],
  "time":[1552668182, 1552668282, 1552668382, 1552668482, 1552668582],
}
```

Системы безопасности загружают данные при помощи POST-запросов. Преимуществом контейнеров также является то, что данные визуализации с их помощью отображаются в динамическом виде.

Визуализация сама распознает, что данные в контейнере были изменены, и тем самым анимирует изменения графиков.

Таким образом команды, вводимые на сенсорном экране планшета, изменяющие контейнер данных, динамически отображаются в виде анимации в очках дополненной реальности.

Таким образом, предложенная архитектура обеспечивает необходимую гибкость при визуализации данных от разных источников, и ее можно использовать при реализации систем поддержки и принятия решений, основанных на визуальной аналитике с использованием дополненной реальности и сенсорных экранов.

Работа выполнена при финансовой поддержке РФФИ (проект № 18-07-01488).

Список используемых источников

1. Котенко И. В., Степашкин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды Института системного анализа Российской академии наук. 2007. Т. 31. С. 126–207.

2. Браницкий А. А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

3. Котенко И. В., Десницкий В. А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд. 2011. № 3 (39). С. 68–75.

4. Коломеец М. В., Котенко И. В., Чечулин А. А. Использование виртуальной и дополненной реальности для визуализации данных кибербезопасности // Защита информации. Инсайд.2017. № 5 (77). С.58–63.

5. Котенко И. В., Коломеец М. В., Комашинский В. И., Бушуев С. Н., Гельфанд А. М. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция. Санкт-Петербург, 24–26 октября 2018 г.: материалы конференции. СПб. : СПОИСУ. 2018. С.143–144.

6. Котенко И. В., Коломеец М. В., Бушуев С. Н., Гельфанд А. М. Методы человеко-машинного взаимодействия на основе сенсорных экранов в ситуационных центрах безопасности // Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). Санкт-Петербург. 2–4 октября 2018. СПб. : АО «Концерн «ЦНИИ «Электроприбор», 2018. С. 660–664.

7. Чечулин А. А., Коломеец М. В., Котенко И. В., Бушуев С. Н. Архитектура прототипа системы визуализации неформализованных данных // Математические методы в технике и технологиях – ММТТ-29. XXIX Международная научная конференция, 31 мая – 3 июня 2016 года, Санкт-Петербургский государственный технологический институт, Санкт-Петербург, Россия. 2016. Т. 4. С. 142–144.

УДК 654.1
ГРНТИ 50.41.23

ИМПЛЕМЕНТАЦИЯ ЭЛЕМЕНТОВ IOT В МЕХАНИЗМЫ ИЗМЕРЕНИЯ ПОЛЬЗОВАТЕЛЬСКОГО ОПЫТА КЛИЕНТА ОПЕРАТОРА СВЯЗИ

В. А. Акишин[1,2], С. В. Кисляков[1,2], Дан. А. Терентьев[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]ООО «Научно-технический центр АРГУС»

В настоящее время операторы связи (и другие участники рынка, предоставляющие B2C услуги) все больше заинтересованы во внедрении и развитии механизмов измерения клиентской лояльности с целью контроля оттока и повышения прибыли, получаемой с каждого клиента. Поэтому сегодня приобретают большую популярность подходы к достижению указанных целей, основанные на управлении клиентским опытом – впечатлениями клиента от контакта с компанией на протяжении всего жизненного цикла их взаимодействия. Бурное развитие концепции Интернета Вещей даёт новые возможности в части управления клиентским опытом (Customer Experience Management, CEM). В данной работе рассматривается возможные решения на стыке CEM/IoT (Internet of Things) для повышения точности идентификации клиента оператора связи.

Customer Experience Management, Internet of Things.

О рыночной ситуации

На настоящее время Россия обладает одним из самых высоких показателей проникновения мобильной связи среди населения в мире – 89 %. При этом количество мобильных подключений составило 255,4 млн. Таким образом проникновение sim-карт достигло 179 % [1]. Этому предшествовал период наращивания абонентской базы и агрессивной ценовой политики. Поэтому к периоду 2016 года рынок исчерпал возможности роста для подобной стратегии. Операторы столкнулись с падением ARPU (*Average Revenue Per User*) и необходимостью находить новые драйверы роста [1]. В 2018 г. количество смартфонов в России превысило 29 млн устройств, из них доля устройств с поддержкой LTE составила около 80 % [2]. Фокус операторов с этого времени переносится на цифровых клиентов и увеличение совокупной прибыли компании, получаемой от одного клиента за все время их взаимодействия (LTV) для фиксации роста. В таких условиях ключевыми стали два вектора развития: оптимизация трат в традиционных направлениях бизнеса и наращивание компетенций в перспективных digital-

направлениях, таких как IoT, больших данных, облачных сервисов, OTT-приложений (*Over The Top*), финансовых услуг. Отмена легальных ограничений на переход клиентов между операторами, а также распространение MVNO-операторов, которые обладают более гибкими возможностями по внедрении новых услуг, повышают вероятность оттока клиентов крупных операторов связи [3]. Исходя из данной ситуации на российском рынке телекоммуникационных услуг, и смягчении ценовой конкуренции стратегическими направлениями для операторов стали: повышение качества и оптимизация трат в традиционных направлениях бизнеса, и наращивание компетенций в перспективных digital-направлениях [2].

Таким образом, телекоммуникационные операторы все больше заинтересованы во внедрении и развитии механизмов измерения клиентской лояльности с целью контроля оттока и повышения средней прибыли, получаемой с каждого клиента (ARPU) и прибыли за все время взаимодействия (LTV). Это делается на основе систем управления клиентским опытом (CEM) – впечатлениями клиента от контакта с компанией на протяжении всего жизненного цикла их взаимодействия. Сбор, обработка и правильная интерпретация данных о клиентском опыте позволяет персонифицировать взаимодействие с клиентом, повышая эффективность техник поднятия суммы продажи (*Up-Sell*) и перекрёстные продажи (*Cross-sell*).

Идентификация клиента

TMForum описывает более 400 метрик, используемых для управления клиентским опытом, большая часть из них подразумевает идентификацию обращения. Это может быть или CustomerID, либо Enterprise CustomerID [4].

Традиционные CRM системы используются для того, чтобы отражать транзакции однозначно идентифицированных клиентов. Наиболее просто можно идентифицировать клиента при онлайн обращении. В CRM фиксируется номер телефона, либо e-mail адрес клиента, оставившего заявку/совершившего покупку. Хотя фактически данные о клиенте появляются уже при первом переходе на сайт. Это данные об устройстве, информация об источнике перехода и т. п. В таком случае, данные о клиенте попадают в DMP (*data management platform*) компании, через пиксель (*pixel tag*) для дальнейшего взаимодействия. В конечном итоге, современные платформы помогают получить и максимально проанализировать пользовательское подведение на онлайн площадках бизнеса [5]. Совокупность данных передаваемых с онлайн площадок и «офлайн» точек, можно объединять в CDP (*customer data platform*). При «офлайн» обращении определить клиента становится сложнее. Здесь наиболее частым инструментом идентификации служит карта лояльности клиента, либо номер телефона. Но при этом

определение клиента происходит только на конечном этапе взаимодействия – моменте совершения покупки. Даже внедрение сложных скриптов действий сотрудников офисов продаж не позволит проанализировать все точки контакта с клиентом. Соответственно, ставится задача идентифицировать клиента уже на начальном этапе цикла взаимодействия. Широкое распространение цифровых устройств и услуг, предоставляемых оператором связи, меняет концепцию взаимоотношений оператора и клиента. А развитие Internet of Things открывает новые возможности для создания новых инструментов управления клиентским опытом.

Имплементация элементов IoT в CEM

Возможным решением представляется использование в Wi-Fi сканеров в салонах продаж. Данные устройства позволяют сканировать устройства с Wi-Fi модулем (смартфоны, планшеты, ноутбуки). Все устройства с включённым Wi-Fi делают запросы в фоновом режиме для объявления своего присутствия. Клиентские устройства используют два метода обнаружения точек доступа: пассивное и активное сканирование. В первом случае устройство клиента пассивно ищет маяки точек доступа, расположенных поблизости, и на их основе выбирает к какой сети подключиться. При активном сканировании устройство клиента, который ищет доступные сети, само отправляет запросы. Запросы устройства могут быть следующими: направленными на определенную сеть с указанием ее SSID или широковещательными, то есть для любой сети в пределах зоны доступа. Запрос включает в себя идентификатор сети (SSID), который, как правило, является строкой в удобном для чтения формате, и MAC-адрес устройства. Некоторые устройства также делятся списком предпочтительных сетей (PNL). При включенном Wi-Fi мобильные устройства рассылают запросы с частотой, установленной производителем, но как правило период не превышает 60 секунд. Процесс получения и анализа клиентских адресов показан на рис. 1.

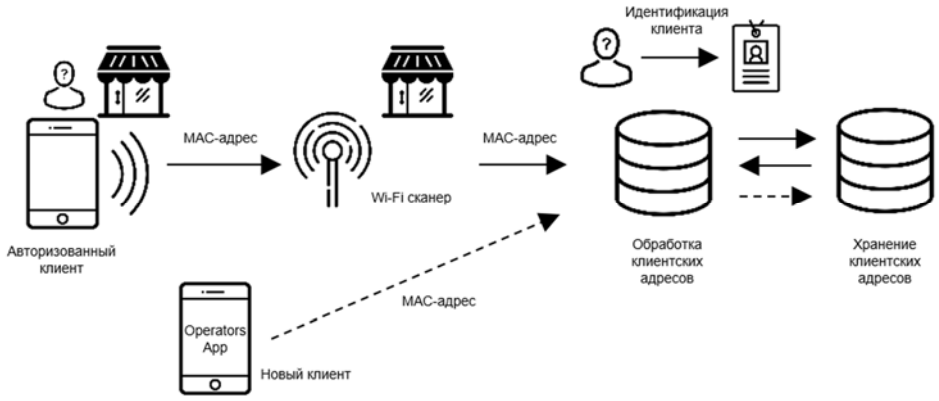


Рис. 1. Процедура получения и анализа клиентских адресов

Таким образом сканер позволит собирать данные клиентов на выбранном радиусе работы устройства: MAC, PNL и SSID.

Собранные MAC-адреса могут передаваться в системы таргетинга рекламы. Но для оператора связи более предпочтительным может быть сценарий при котором, клиент может быть определен благодаря соотнесению адреса, с адресом, полученным оператором заранее. Следовательно, клиент может быть идентифицирован при визите в офис продаж, а персонализированные предложения для клиента будут сразу направлены в приложение для управления услугами. Данные собираемые сканером, также могут использоваться для получения важных инсайтов о распределении аудитории точек продаж оператора связи.

Производитель устройства может быть определен по MAC-адресу, при сравнении первых 3 байтов с перечнем IEEE OUI (*Organizationally Unique Identifier*). Это может быть использовано для определения материального состояния клиента и их дальнейшей категоризации.

Перспективным представляется механизм определения информации о владельце устройства на основе анализа SSID из списка PNL. 36,2 % устройств выдают список PNL. И хотя многие из них содержат названия доступных публичных точек доступа или же пользователи сами меняют названия своих домашних сетей (что в дальнейшем можно использовать для глубокого анализа), большое количество домашних сетей содержит названия провайдеров услуг фиксированной связи [6, 7]. Для операторов, предоставляющих конвергентные пакеты услуг связи (как собственные сети ШПД, так и работающие по модели FVNO), открываются возможности контроля клиентов, пользующимися услугами других провайдеров фиксированной связи, и формирования персональных конкурентных предложений.

На основе описанных процессов была сформирована функциональная схема работы комплекса с имплементированными элементами Интернета вещей (рис. 2, см. ниже).

Каждый слой описывает логику работы на определенном этапе процесса работы системы при обнаружении клиента. Данные о клиенте собираются с IoT устройств и систем поддержки бизнес-процессов. Слой обработки и анализа данных на основе всех поступивших факторов позволяет сформировать блок клиентских данных, базируясь на которых можно строить персонифицированную коммуникацию с клиентом.

Заключение

Сложившаяся ситуация на рынке мобильной связи, вынуждает операторов изменять стратегию развития. Построение долгосрочных взаимоотношений с клиентом стало основной задачей. И системы управления клиентским опытом являются основным инструментом построения такого

взаимодействия. Описанное в статье решение по применению элементов IoT, позволяет охватить новые точки контакта с клиентом, повышая точность идентификации клиента. Wi-Fi сканер является инструментом, позволяющим дополнить портрет клиента, основываясь на новых клиентских данных.

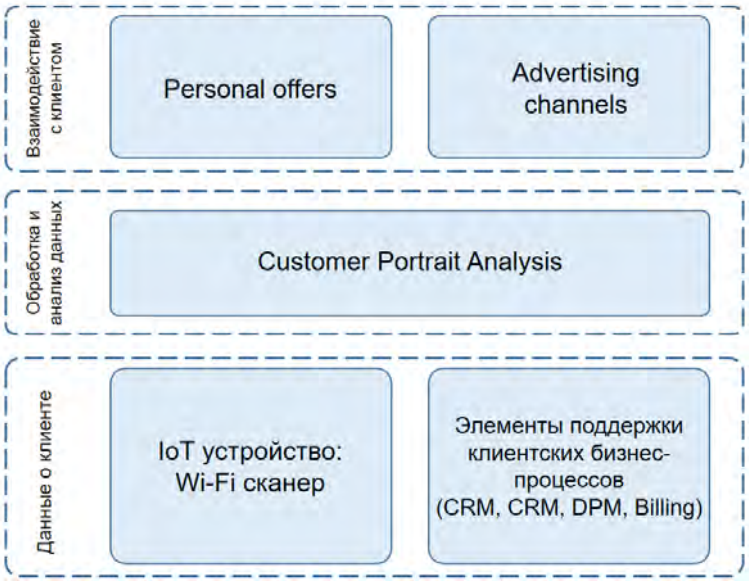


Рис. 2. Функциональная схема комплекса

Список используемых источников

1. 2017. Годовой отчет. ПАО Мегафон. М., 2017. 154 с.
2. 2017. Годовой отчет. ПАО МТС (Мобильные ТелеСистемы). М., 2017. 280 с.
3. Ланкевич К., Хабаев Н., Скоринов М. OSS комплекс как инструмент контроля лояльности клиентов оператора связи // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. № 5. С. 36–40.
4. TM FORUM. GB962A_Lifecycle_Metrics_R15.0.1. TM Forum; Декабрь, 2015.
5. Плащкевич С. CDP vs CRM vs DMP в чем же разница? [Электронный ресурс] // medium.com. Платформа журналистики 2018. Режим доступа: https://medium.com/
6. Гольдштейн А., Скоринов М., Феноменов М. Big Data – как выпустить джинна из бутылки? // Технологии и средства связи. 2015. № 5. С. 34–38.
7. Marco V. Barbera [and others]. Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes // IMC '13 Proceedings of the 2013 conference on Internet measurement conference – 2013. P. 265–276.

УДК 681.7
ГРНТИ 49.44

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ИНТЕГРАЛЬНО-ОПТИЧЕСКОГО МУЛЬТИПЛЕКСОРА ДЛЯ СИСТЕМЫ DWDM

Д. Д. Алексеева, М. С. Былина

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

Для транспортных сетей наиболее перспективной является технология плотного спектрального уплотнения, реализуемая с помощью оптических мультиплексоров и демультиплексоров. Наилучшими на сегодняшний день характеристиками обладают интегрально-оптические MUX/DEMUX, на основе массива планарных волноводов. В работе было проведено экспериментальное исследование параметров 40-канального DEMUX AWG с разносом каналов 100 ГГц: вносимых потерь и переходного затухания на дальний конец.

волоконно-оптические системы передачи, технология спектрального уплотнения, мультиплексирование, демультиплексирование, мультиплексор на основе планарных волноводов, AWG, DWDM.

Мультиплексор/демультиплексор (MUX/DEMUX) на основе фазированной решетки волноводов (*Arrayed-Waveguide Grating*, AWG) широко используется в оптических сетях с применением технологии спектрального мультиплексирования (*Wavelength Division Multiplexing*, WDM), которая позволяет увеличить пропускную способность одного оптического волокна. На рис. 1 (см. ниже) представлена конструкция AWG демультиплексора, который состоит из входных и выходных планарных волноводов, двух пластин и фазированной решетки, образованной группой планарных волноводов разной длины, причем длины любых двух соседних волноводов отличаются на одну и ту же величину ΔL [1].

Излучение мультиплексированного сигнала из входного волновода попадает в 1-ю пластину, образуя расходящийся пучок, который затем попадает во все волноводы фазированной решетки. В пластине 2 сигналы, прошедшие по каждому из волноводов решетки, интерферируют, в результате чего происходит фокусировка излучения в выходные волноводы.

В работе было проведено экспериментальное исследование демультиплексора для системы DWDM, предназначенного для демультиплексирования 40 каналов с интервалом между ними 100 ГГц. Измерялись вносимые

демультиплексором потери при разделении группового сигнала по отдельным каналам. Схемы измерения представлены на рис. 2.

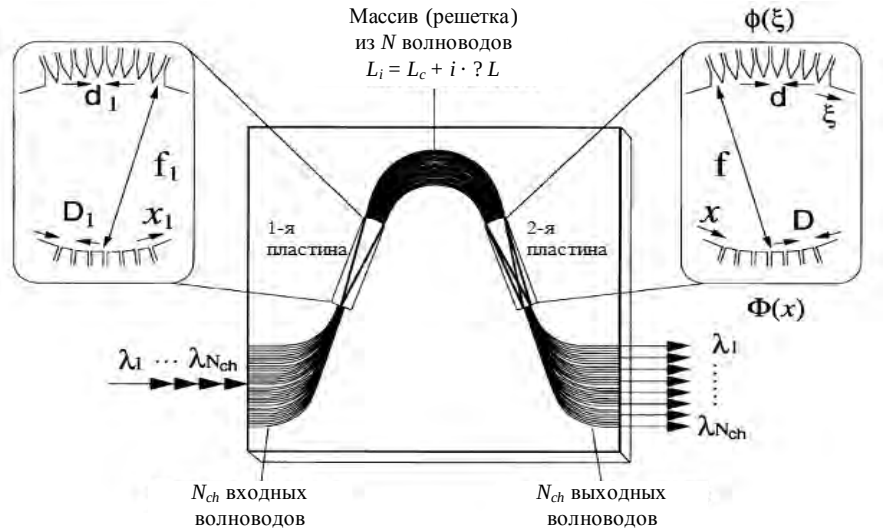


Рис. 1. Демультиплексор AWG

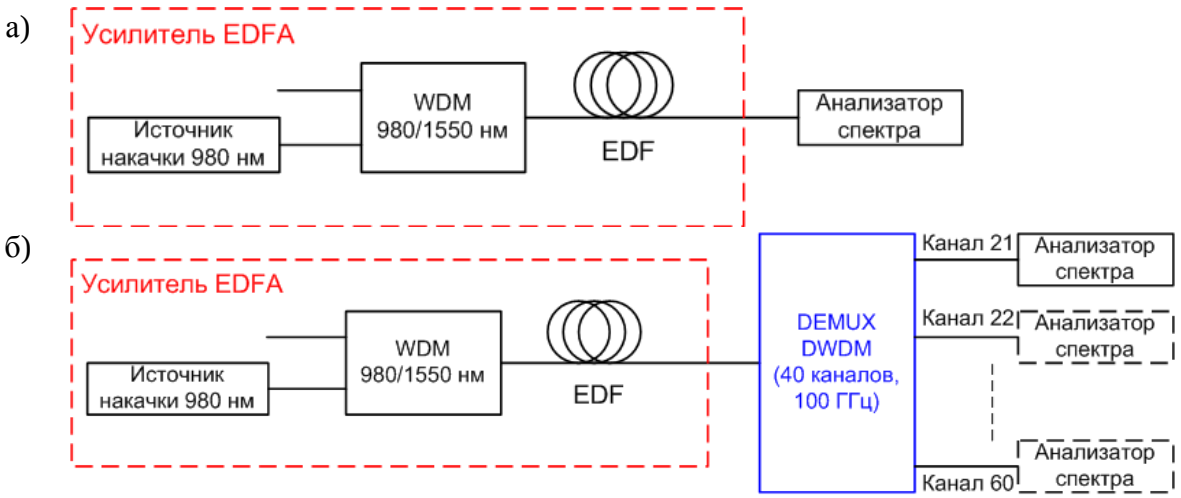


Рис. 2. Схемы измерения вносимых потерь при демультиплексировании

В качестве группового сигнала был использован широкополосный шум усиленного спонтанного излучения (УСИ) оптического усилителя (*Erbium Doped Fiber Amplifier*, EDFA) на основе волокна, легированного ионами эрбия (*Erbium Doped Fiber Amplifier*, EDF).

Для генерации УСИ в EDFA вводилась накачка на длине волны 980 нм (рис. 2а). Мощность накачки составляла 100 мВт. Фотоны с этой длиной волны активно поглощаются ионами эрбия, которые в отсутствие усиливаемого сигнала отдают поглощенную энергию в виде шума – спонтанно излучаемых фотонов в спектральном диапазоне DWDM. Спонтанно излучаемые фотоны вызывают вынужденное излучение, которое, таким образом,

усиливает возникшее спонтанное излучение. Полученное излучение принято называть шумами УСИ [2].

Для определения вносимых потерь проводились измерения:

– мощности излучения $P_{in\,i}$ в каждом спектральном канале на входе демультиплексора (в схеме на рис. 2а),

– мощность излучения $P_{out\,i}$ в полосе i-го канала на каждом из выходов демультиплексора (в схеме на рис. 2б).

Для измерения мощности излучения в спектральных диапазонах отдельных каналов использовались спектрограммы, зарегистрированные с помощью анализатора спектра.

На рис. 3 представлена спектрограмма шумов УСИ на выходе EDFA, зарегистрированная в схеме на рис. 2а. Вертикальная ось прибора была проградуирована в дБм/нм, для определения мощностей излучения мы перешли к мВт/нм (рис. 4) [3]. Для измерения мощностей $P_{in\,i}$ использовалась следующая методика:

– увеличивался фрагмент спектрограммы, соответствующий i-му спектральному каналу;

– по увеличенному фрагменту определялась средняя плотность мощности излучения $p_{in\,i}$ в канале в мВт/нм;

– рассчитывалась мощность $P_{in\,i}$ по выражению:

$$P_{ini} = p_{ini} \cdot \Delta\lambda_i ,$$

где $\Delta\lambda_i$ – ширина полосы канала, измеренная по спектрограмме i-го канала, зарегистрированной в схеме на рис. 2б [4]. Результаты измерений представлены в таблице.

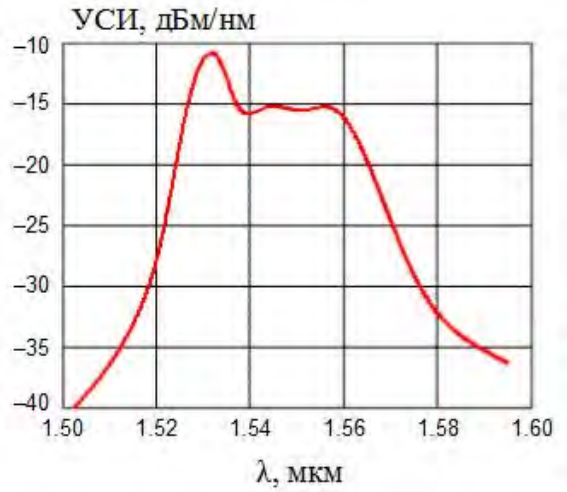


Рис. 3. Спектрограмма шумов УСИ

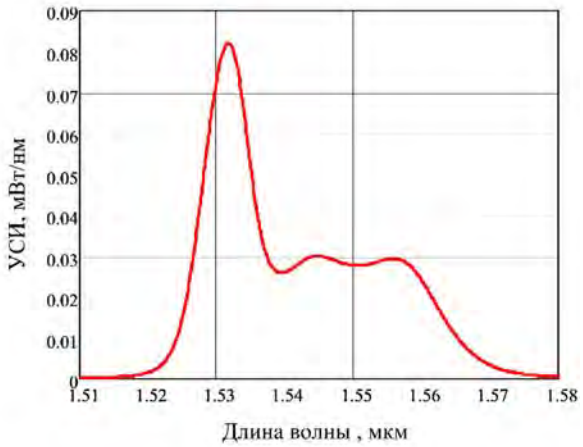
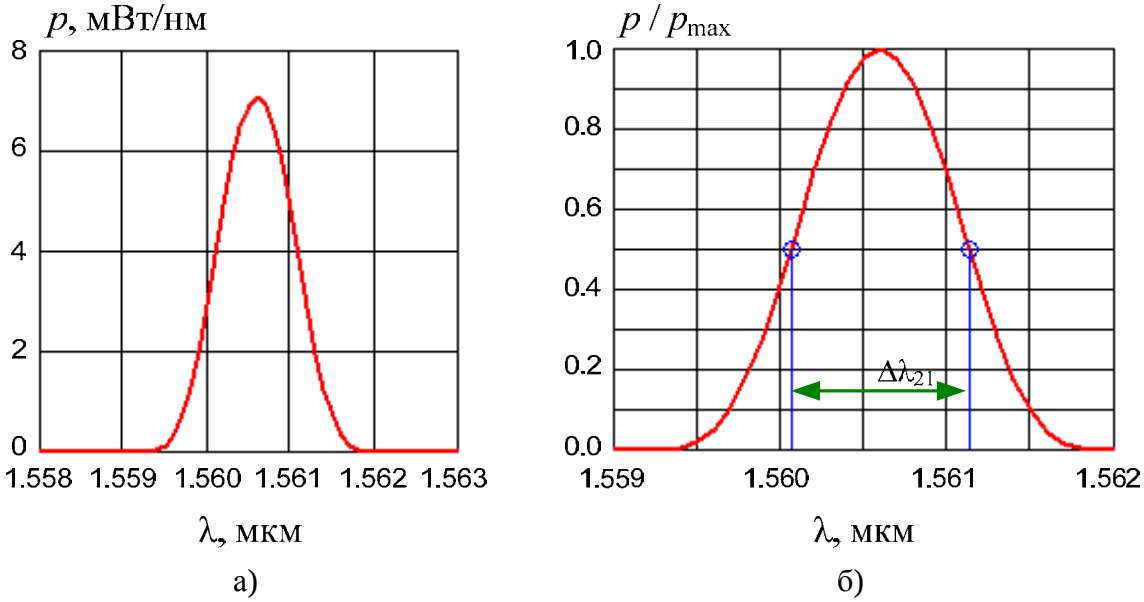


Рис. 4. Спектрограмма шумов УСИ, преобразованная для определения мощностей излучения в спектральных каналах

ТАБЛИЦА. Результаты исследования вносимых потерь при демультиплексировании широкополосного сигнала

№ канала	Длина волны, мкм	Мощность УСИ в полосе канала $P_{in\ i}$, мкВт	Мощность демульт. сигнала в канале $P_{out\ i}$, мкВт	Потери при демультиплексир. $a_{IL\ i}$, дБ
21	1.5606	24.38	7.501	5.119
22	1.5597	26.48	9.871	4.286
23	1.5589	28.35	12.505	3.555
24	1.5582	29.96	12.551	3.778
25	1.5574	31.39	14.319	3.408
26	1.5565	31.45	13.557	3.655
27	1.5557	31.86	14.922	3.294
28	1.5549	31.69	13.859	3.593
29	1.5541	31.03	11.953	4.143
30	1.5533	30.60	14.631	3.204
31	1.5525	30.47	14.385	3.261
32	1.5517	30.63	14.255	3.222
33	1.5509	30.08	14.081	3.296
34	1.5501	29.83	13.483	3.449
35	1.5493	30.87	13.372	3.633
36	1.5485	30.67	14.631	3.214
37	1.5477	31.02	13.342	3.664
38	1.5469	31.91	14.094	3.549
39	1.5461	32.37	16.747	2.865
40	1.5453	32.21	17.135	2.741
41	1.5445	32.70	16.635	2.935
42	1.5437	32.97	17.979	2.634
43	1.5429	31.60	17.192	2.644
44	1.5421	33.23	13.934	3.774
45	1.5413	29.42	12.740	3.635
46	1.5405	29.10	16.395	2.492
47	1.5397	28.16	14.366	2.923
48	1.5389	31.51	19.403	2.106
49	1.5381	29.73	16.486	2.561
50	1.5374	32.92	17.519	2.739
51	1.5366	37.26	21.034	2.483
52	1.5358	45.78	27.760	2.172
53	1.5350	56.13	37.362	1.768
54	1.5342	64.80	51.041	1.036
55	1.5335	77.04	59.963	1.088
56	1.5327	85.32	66.669	1.071
57	1.5319	85.68	92.681	0.341
58	1.5311	84.52	85.899	0.070
59	1.5303	85.12	69.313	0.892
60	1.5295	70.87	107.817	0.822

Для определения мощностей излучения $P_{out\ i}$ в схеме на рис. 2б были зарегистрированы спектрограммы оптических сигналов на каждом из 40 выходов демультиплексора, по которым определялись ширина полосы $\Delta\lambda_i$ и мощность в каждом канале $P_{out\ i}$ (рис. 5). Для измерения мощностей $P_{out\ i}$ использовалась та же методика, что и для измерения $P_{in\ i}$.



а) б)

Рис. 5. Спектрограмма на выходе 21-го канала (а)
и определение ширины 21-го канала (б)

В таблице представлены результаты измерений $P_{out\ i}$, а также результаты расчетов вносимых потерь по выражению:

$$a_{ILi} = 10\lg\left(\frac{P_{ini}}{P_{outi}}\right).$$

Из таблицы видно, что с увеличением номера канала (уменьшением длины волны) потери уменьшаются. Максимальные потери (около 5 дБ) наблюдались при демультиплексировании 21 канала с самой большой длиной волны (1560,6 нм).

Список используемых источников

1. Фриман Р. Волоконно-оптические систему связи: пер. с англ. «РИЦ Техносфера». М. ; Техносфера, 2007. 512 с.

2. Аснис Л. Н., Денисюк И. Ю. Технологии спектрального мультиплексирования для оптической связи. СПб. : ИТМО, 2008. 105 с.

3. Жирар А. Руководство по технологии и тестированию систем WDM / ред. А. В. Шмалько / пер. с англ. под ред. А. М. Бродниковского, Р. Р. Убайдуллаева, А. В. Шмалько. М. : EXFO, 2001. 252 с.

4. Листвин В. Н., Трещиков В. Н. DWDM системы. М. : Наука, 2013. 267с.

УДК 621.397
ГРНТИ 49.37.29

ИССЛЕДОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ УСКОРЕНИЯ ВИДЕОТРАФИКА С ИСПОЛЬЗОВАНИЕМ ГРАНИЧНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

М. Аль-Свейти, А. С. А. Мутханна

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

Ожидается, что к 2021 году 80 % мирового интернет-трафика будет приходиться на видео, поэтому для ускорения видео требуется достичь лучшее качество восприятия. Существует множество методов моделирования видеотрафика; в этой статье мы рассмотрим последние и наиболее распространенные модели. Мы также изучаем и анализируем последние механизмы и методы, разработанные для ускорения видео. Кроме того, ускорение видео анализируется с точки зрения 5G на основе объявленных ITU и 3GPP спецификаций.

IoT, 5G, MEC, граничные вычисления.

Введение

Граничные облачные вычисления как эволюция облачных вычислений приносят хостинг приложений из централизованных данных расположен вплоть до края сети, ближе к потребителям и данным, генерируемым приложениями. Граничные вычисления признаны одним из ключевых технологий для достижения требуемой показатели производительности (KPI) 5G [1], особенно в том, что касается низкой задержки и эффективности использования полосы пропускания. Однако не только передовые вычисления в телекоммуникационных сетях являются техническим инструментом для выполнения сложных KPI, он также играет существенную роль в трансформации телекоммуникационного бизнеса, где телекоммуникационные сети превращаются в универсальные сервисные платформы для промышленности и других специфических отраслей.

В обозримом будущем ожидается, что пятое поколение сети 5G будет отвечать требованиям различных сегментов рынка [2, 3], путем внедрения совершенно новых вариантов услуг и функций. Новые виды услуг будут не только взаимодействовать с нынешним рынком услуг, которые предоставляют операторы связи, но и активно развивать их. Предполагается, что системы 5G будут предоставлять новые типы служб и приложений с определенными требованиями и методами развертывания данной сети, в том числе и приложение видео трафика.

В статье предлагается применять метод граничных вычислений для улучшения качества восприятия и ускорения видео в будущих сетях.

Метод ускорения видео на основе граничных вычислений

Преимущества граничных вычислений:

– уникальное качество восприятия;

– услуги, адаптированные под индивидуальные потребности и предпочтения;

– эффективное использование радио и сетевых ресурсов;

– инновационные приложения и услуги для абонентов мобильной связи;

– предприятия и вертикальные сегменты.

Категории сценариев обслуживания:

1. Услуги, ориентированные на потребителя.
2. Услуги оператора и сторонних организаций.
3. Улучшения производительности сети и качества восприятия (QoE).

Услуги, ориентированные на потребителя

Расширенная реальность (рис. 1):

– приложение MEC анализирует выходные данные камеры устройства и точное местоположение; объекты, просматриваемые на камере устройства, накладываются на них с помощью локального контента дополненной реальности(3);

– обеспечивает уникальное впечатление посетителя от посещения музея или других интересных мест (в помещении или на открытом воздухе);

– обеспечивает низкую задержку и высокую скорость обработки данных.

Рис. 1. Метод интеллектуальной системы ускорения видео

Услуги оператора и сторонних организаций

Видеоаналитика (рис. 2):

– распределенная аналитика потоков видео в прямом эфире на мобильном фронте;

– события запускаются автоматически (например, движение, отсутствие объектов, скопление людей и т. д.); позволяет быстро обнаруживать и запускать действия;

– оптимизация транзитных и транспортных мощностей;

– применимо к общественной безопасности, «умные» города.

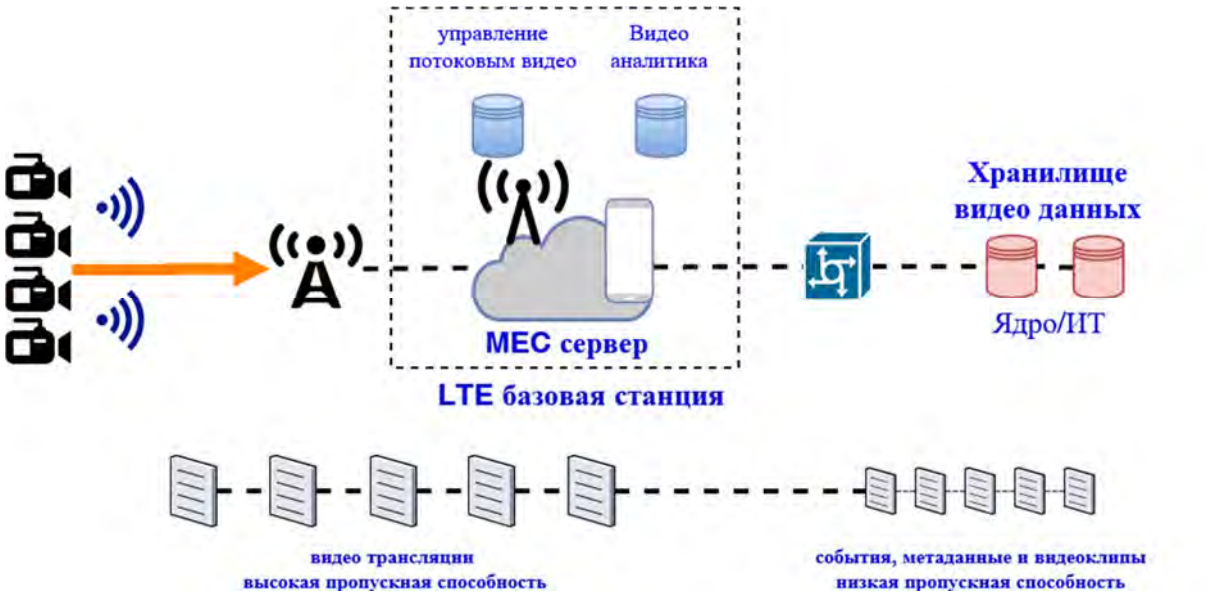


Рис. 2. Система для приложений виртуальной реальности

Улучшения производительности сети и QoE

Интеллектуальное ускорение видеосигнала (рис. 3):

– приложение Radio Analytics обеспечивает видеосервер индикацией предполагаемой пропускной способности, доступной через интерфейс радиосвязи вниз по каналу связи [4];

– эта информация может использоваться для содействия принятию решений по контролю перегруженности ПТС, а также для обеспечения соответствия кодирования на уровне приложения расчетной пропускной способности радиосвязи;

– обеспечивает улучшенное качество видео и пропускную способность.

Группа ISG MEC работает над созданием спецификаций нормативных групп, которые позволят эффективно и беспрепятственно интегрировать приложения от поставщиков, поставщиков услуг и третьих лиц на платформах MEC с участием многих поставщиков.

Рис. 3. Оптимизация контента сети с учетом радикализации

Заключение

Граничные вычисления для мобильных устройств дополняют SDN и NFV и способствуют трансформации сети мобильной широкополосной связи в программируемый мир, гарантируя, что высокоэффективное функционирование сети и предоставление услуг, личный опыт, и новые возможности для бизнеса.

Мобильные граничные вычисления являются одними из ключевых архитектурных концепций и технологий для 5G, позволяющая удовлетворить некоторые требования, как высокие требования к ожидаемой пропускной способности и задержкам передачи данных в сетях 5G, масштабируемость и автоматизация [5]. Данные технологий также обеспечивает дополнительную конфиденциальность и безопасность, а также обеспечивает существенная экономия средств.

Список используемых источников

1. A. Ateya, A. Muthanna, I. Gudkova, A. Abuarqoub, A. Vybornova and A. Koucheryavy. Development of Intelligent Core Network for Tactile Internet and Future Smart Systems // Journal of Sensor and Actuator Networks, Vol. 7 (1), Jan. 2018.

2. Abdelhamied A. Ateya; Ammar Muthanna; Maria Makolkina; Andrey Koucheryavy. Study of 5G Services Standardization: Specifications and Requirements // 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT): 2018 Pp: 1–6.

3. Manariyo, S., Khakimov, A., Pyatkina, D., Muthanna, A. Optimization Algorithm for IPTV Video Service Delivery over SDN Using MEC Technology // 2018 Lecture Notes inComputer Science. Pp: 419–427.

4. Makolkina M., Muthanna A., Manariyo S. Quality of Experience Estimation for Video Service Delivery Based on SDN Core Network // Lecture Notes in Computer Science. 2017. 10531. Pp. 683–692.

5. ETSI White Paper “Mobile Edge Computing – a key technology towards 5G“. Technical Requirements, including use cases (GS MEC 002).

УДК 621.391.63:681.7.068 *Приглашенный доклад*
ГРНТИ 49.44.31

МОДЕЛИРОВАНИЕ МАЛОМОДОВОЙ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ С КОМПЕНСАЦИЕЙ ХРОМАТИЧЕСКОЙ ДИСПЕРСИИ И ДИФФЕРЕНЦИАЛЬНОЙ МОДОВОЙ ЗАДЕРЖКИ НА ФИЗИЧЕСКОМ УРОВНЕ

В. А. Андреев, А. В. Бурдин, В. А. Бурдин, Е. Ю. Еремчук

Поволжский государственный университет телекоммуникаций и информатики

В работе представлены результаты имитационного моделирования двумодовой волоконно-оптической линии связи с компенсацией хроматической дисперсии и дифференциальной модовой задержки на физическом уровне. Моделирование осуществлялось на основе решения системы связанных нелинейных уравнений Шедингера методом расщепления по физическим процессам. Модель маломодовой ВОЛС учитывала фактор нелинейности, дисперсию, дифференциальную модовую задержку и случайные связи мод.

маломодовые оптические волокна, связь мод, дифференциальная модовая задержка, хроматическая дисперсия, система связанных нелинейных уравнений Шредингера, вероятность ошибок.

К настоящему времени стандартные одномодовые оптические волокна (ОВ), на которых построены современные сети связи, уже практически приблизились к пределу своих возможностей по увеличению пропускной способности, который определяется так называемым «нелинейным пределом Шеннона» [1, 2, 3]. Для преодоления этого предела предполагается использовать системы пространственного мультиплексирования, которые требуют применения новых типов ОВ [1, 2, 3, 4, 5, 6]. Это могут быть либо многосердцевинные либо маломодовые ОВ. На сегодняшний день лучшие показатели при практической реализации демонстрируют многосердцевинные ОВ [7, 8]. Однако, с точки зрения построения сетей связи более перспективны маломодовые решения [4]. Но для их практической реализации необходимо решить ряд проблем. Одним из наиболее существенных факторов, ограничивающих применение маломодовых ОВ, является совместное действие связи мод с дифференциальной модовой задержкой (ДМЗ), хроматической дисперсией (ХД) и нелинейностью. В общем случае, распространяющиеся в ОВ кабелей связи моды можно рассматривать либо как собственные моды, либо как линейно-поляризованные моды, либо

как вихревые моды [9]. При этом, каждую линейно-поляризованную моду можно представить в виде суммы собственных мод или же суммы вихревых мод. В свою очередь каждую вихревую моду также можно представить в виде суммы собственных мод или же суммы линейно-поляризованных мод. Пространственные мультиплексоры ввода/вывода вихревых мод не требуют специальных способов обработки сигналов. Однако из-за модовых связей вихревые моды отличаются большими потерями. Как следствие, пока реализация систем передачи на этих модах ограничена достаточно малыми расстояниями [10, 11]. При использовании пространственных мультиплексоров ввода/вывода линейно-поляризованных мод опять-таки из-за связей мод необходимо применение системы MIMO и, соответственно, специальных алгоритмов обработки сигналов [9, 12]. При этом требования к вычислительным ресурсам MIMO растут с увеличением дифференциальной модовой задержки, что при существующих возможностях средств вычислений ограничивает дальность передачи в этом случае. Для снижения требований к вычислительным ресурсам, в первую очередь, предпринимаются попытки создать ОВ с минимизированной ДМЗ [13]. Также, известны способы, заключающиеся в том, что вдоль волоконно-оптической кабельной линии с некоторым периодом включаются устройства компенсации ДМЗ [12, 14, 15, 16, 17]. В частности, устройства на основе набора волоконно-оптических линий задержки. Для двумодовых линий предлагаются также схемы скрещивания (переключения) мод. Очевидно, что применение подобных схем влияет и на качество передачи волоконно-оптической линии связи (ВОЛС). Естественно возникает интерес по определению возможностей такого подхода к повышению качества передачи информации и оцениванию степени его снижения, если это происходит. Из опыта эксплуатации одномодовых ВОЛС хорошо известна эффективность дисперсионного управления волоконно-оптических линий передачи на плотных картах [18, 19]. В [20] показано, что даже при компенсации ХД на грубых картах при размещении модулей компенсации на линейных оптических усилителях через 100 км динамический диапазон маломодовой ВОЛС протяженностью 1000 км увеличивается на 3–4 дБ. Можно предположить, что дисперсионное управление на плотных картах для таких линий будет еще эффективнее. Все вышесказанное и определило рассматриваемую в данной работе задачу – исследование методами имитационного моделирования функционирования маломодовой ВОЛС с компенсацией ХД и ДМЗ на физическом уровне в зависимости от длины секции компенсации.

Для сравнения качества работы маломодовой линии передачи как в [21] использовали концепцию порога эффективности корректирующих кодов (FEC limit) [22]. По результатам моделирования строили зависимости вероятности ошибок (BER) в оптическом модовом канале на приёме от пиковой мощности на передаче, по которым оценивали динамический

диапазон, полагая, что для значений BER ниже порога сигнал на приеме полностью восстанавливается. Значение порога BER полагали равным $4{,}7 \cdot 10^{-3}$ [22].

Процесс распространения сигнала в маломодовом ОВ с учетом линейных и нелинейных связей мод, дисперсии, ДМЗ и нелинейности описывали системой связанных нелинейных уравнений Шредингера [23], которые решали методом расщепления по физическим процессам [21, 23, 24, 25]. Применяемые модель и алгоритм подробно описаны в работе [25].

В данной работе рассматривалась двумодовая ВОЛС протяженностью 1000 км, с установленными через каждые 100 км эрбиевыми оптическими усилителями. Среднее значение строительной длины оптического кабеля принималось равным 5 км. Моделирование производилось для оптического сигнала с форматом модуляции DP-DQPSK для канальной скорости 100 Гбит/с по двумодовому ОВ.

Результаты моделирования подтвердили возможность увеличения динамического диапазона двумодовых магистральных ВОЛС за счет компенсации ХД на линейных оптических усилителях. Для рассматриваемых ВОЛС с длиной усилительных участков 100 км, динамический диапазон увеличивается на 3–4 дБ. Для таких ВОЛС при отклонениях длины усилительных участков от 100 км не более чем на 5 % изменение динамического диапазона не превышает 0,5 дБ. Для рассматриваемых ВОЛС с компенсацией ХД на оптических усилителях и последующей компенсацией на дальнем конце ВОЛС при остаточной ХД на усилительных участках до 5 % уменьшение динамического диапазона составляет не более 1,0 дБ. Все это свидетельствует о потенциальных возможностях компенсации ХД на линейных оптических усилителях для маломодовых ВОЛС большой протяженности.

Результаты моделирования для двухмодовой ВОЛС с дисперсионным управлением на плотных картах показали следующее. В среднем динамический диапазон рассматриваемой ВОЛС увеличивается с уменьшением длины участка компенсации. При длине участка компенсации 10–20 км динамический диапазон увеличивается на 1–1,5 дБ. При длине участка компенсации, равной строительной длине оптического кабеля, динамический диапазон увеличивается до 2,5 дБ или более. Однако это справедливо только для принятой модели оптического усилителя в предположении, что все потери секции компенсируются. Учитывая затраты, вносимые потери, технические трудности внедрения и столь малый эффект при плотном управлении дисперсией ВОЛС, крайне сложно говорить о перспективах его практической реализации.

Результаты моделирования показали, что при компенсации ХД только на приеме на дальнем конце линии применение компенсации ДМЗ на ли-

нейных оптических усилителях может привести к уменьшению динамического диапазона линии до 1,7 дБ. При компенсации и ДМЗ и ХД на линейных оптических усилителях изменения динамического диапазона из-за применения компенсации ДМЗ по абсолютной величине не превышали 0,5 дБ. При компенсации ХД на линейных оптических усилителях и компенсации ДМЗ на плотных картах при включении схем компенсации в муфтах кабельной линии на усилительном участке при уменьшении длины секции компенсации (до величины равной одной-двум строительным длинам кабеля) динамический диапазон сначала увеличивается, а с дальнейшим уменьшением секции компенсации (до значений менее строительной длины кабеля) уменьшается. При этом изменения динамического диапазона по абсолютной величине не превышают 1 дБ.

Все это позволило сделать вывод о том, что выбор методов и схем компенсации ДМЗ в первую очередь должен определяться условиями выравнивания групповых задержек мод в целях снижения требований к вычислительным ресурсам для MIMO. Но при этом целесообразно контролировать изменения динамического диапазона ВОЛС, особенно в случае компенсации ХД только на приеме в конце линии.

Список используемых источников

1. Essiambre R.-J., Kramer G., Winzer P. J., Foschini G. J., Goebel B. Capacity Limits of Optical Fiber Networks // J. Lightwave Technology, 2010, v. 28 (4), pp. 662–701.

2. Ellis A. D. The nonlinear Shannon limit and the need for new fibres // Proc. of SPIE, 2012, v. 8434, pp. 84340H.

3. Richardson D. J., Fini J. M., Nelson L. E. Space-division multiplexing in optical fibres // Nature Photonics, 2013, v. 7, pp. 354–362.

4. Li A., Chen X., Amin A.A., Ye J., Shieh W. Space-division multiplexed high-speed superchannel transmission over few-mode fiber // J. Lightwave Technology, 2012, v. 30 (24), pp. 3953–3964.

5. Андреев В. А., Бурдин А. В., Бурдин В. А. Маломодовый режим передачи по оптическим волокнам: применение на высокоскоростных ВОЛС // Электросвязь. 2013. № 126. С. 27–30.

6. Richardson D. J. New optical fibres for high-capacity optical communications // Phil. Trans. R. Soc. 2016. A 374, pp. 20140441.

7. Mizuno T., Shibahara K., Ye F., Sasaki Y., Amma Y., Takenaga K., Jung Y., Pulverer K., Ono H., Abe Y., Yamada M., Saitoh K., Matsuo S., Aikawa K., Bohn M., Richardson D. J., Miyamoto Y., Morioka T. Long-haul Dense Space-division Multiplexed Transmission Over Low-crosstalk Heterogeneous 32-core Transmission Line Using a Partial Recirculating Loop System // J. Lightwave Technology, 2017, v. 35 (3), pp. 488–498.

8. Rademacher G., Luis R. S., Puttnam B. J., Eriksson T. A., Agrell E., Aikawa K., Furukawa H., Awaji Y., Wada N. 159 Tbit/s C+L Band Transmission over 1045 km 3-Mode Graded-Index Few-Mode Fiber // Proc. 41st Optical Fiber Communication Conference and Exhibition (OFC) OSA, 2018, pp. Th4C.4.

9. Rusch L. A., Rad M., Allahverdyan K., Fazal I., Bernier E. Carrying data on the orbital angular momentum of light // IEEE Communications Magazine, 2018, v. 56 (2), pp. 1–10.

10. Zhu L., Zhu G., Wang A., Wang L., Ai J., Chen S., Du C., Liu J., Yu S., Wang J. 18 km low-crosstalk OAM+WDM transmission with 224 individual channels enabled by a ring-core fiber with large high-order mode group separation // Optics Letters, 2018, v. 43, pp. 1890–1893.

11. Ingerslev K., Gregg P., Galili M., Da Ros F., Hu H., Bao F.; Usuga Castaneda M. A., Kristensen P., Rubano A., Marrucci L., Ramachandran S., Rottwitt K., Morioka T., Oxenløwe L. K. 12 Mode, MIMO-Free OAM Transmission // Proc. Optical Fiber Communications Conference and Exhibition (OFC) OSA, 2017, pp. M2D.1.

12. Arık S. O., Keang-Po H., Kahn J. M. Group Delay Management and Multiinput Multioutput Signal Processing in Mode-Division Multiplexing Systems // J. Lightwave Technology, 2016, 34 (11), pp. 2867–2880.

13. Grüner-Nielsen L., Sun Y., Nicholson J. W., Jakobsen D., Jespersen K. G, Lingle R., Palsdottir B. Few Mode Transmission Fiber With Low DGD, Low Mode Coupling, Low Loss // J. Lightwave Technology, 2012, 30 (23), pp. 3693–3698.

14. Ye F., Warm S., Petermann K. Differential Mode Delay Management in Spliced Multimode Fiber Transmission Systems // OSA OFC/NFOEC Technical Digest, 2013, pp. OM3B.3.pdf.

15. Maruyama R., Kuwaki N., Matsuo S., Ohashi M. Two mode optical fibers with low and flattened differential modal delay suitable for WDM-MIMO combined system // Optics Express, 2014, 22 (12), pp. 14311–14321.

16. Arık S. O., Keang-Po H., Kahn J. M. Delay Spread Reduction in Mode-Division Multiplexing: Mode Coupling Versus Delay Compensation // J. Lightwave Technology, 2015, 33 (21), pp. 4504–4512.

17. Rademacher G., Warm S., Petermann K. Nonlinear interaction in differential mode delay managed mode-division multiplexed transmission systems // Optics Express, 2015, 23 (1), pp. 55–60.

18. Madani F. M., Kikuchi K. Design Theory of Long-Distance WDM Dispersion-Managed Transmission System // J. Lightwave Technology, 1999, v. 17 (8), pp. 1326–1335.

19. Suzuki M., Edagawa N. Dispersion-Managed High-Capacity Ultra-Long-Haul Transmission // J. Lightwave Technology, 2003, v. 21 (4), pp. 916–929.

20. Andreev V. A., Burdin V. A., Bourdine A. V., Dashkov M. V. Simulation of two-mode fiber optic link with chromatic dispersion compensation at line amplifiers // IEEE Conference Proceedings Systems of Signals Generating and Processing in the Field of on Board Communications, 2018, pp. 1–4.

21. Ferreira F., Jansen S., Monteiro P., Silva H. Nonlinear Semi-Analytical Model for Simulation of Few-Mode Fiber Transmission // IEEE Photonics Technology Letters, 2012, v. 24 (4), 240–242.

22. Alvarado A., Agrell E., Lavery D., Maher R., Bayvel P. Replacing the Soft-Decision FEC Limit Paradigm in the Design of Optical Communication Systems // J. Lightwave Technology, 2015, v. 33(20), pp.4338–4352.

23. Agrawal G. P. Nonlinear fiber optic. NY: Academic Press, 2013. 648 p.

24. Mumtaz S., Essiambre R-J., Agrawal G. P. Nonlinear propagation in multimode and Multicore fibers: generalization of the Manakov equations // J. Lightwave Technology, 2013, v. 31 (3), pp. 398–406.

25. Андреев В. А., Бурдин А. В., Бурдин В. А., Дашков М. В. Моделирование межмодовых связей при прогнозах вероятностей ошибок маломодовых линий передачи // Вычислительные технологии. 2018. Т. 22 (6). С. 4–11.

УДК 654.9
ГРНТИ 47.53.31

ПЕРЕДАЧА ВЫСОКОКАЧЕСТВЕННОГО ВИДЕОСИГНАЛА ПО ВОЛОКОННО-ОПТИЧЕСКОЙ СЕТИ С CWDM

Е. И. Андреева[1], В. П. Валюхов[2], В. Д. Купцов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский политехнический университет Петра Великого

Разработан, исследован и конструктивно исполнен комплект модулятора и демодулятора для передачи изображения студийного качества с использованием частотной модуляции оптического сигнала для волоконно-оптических систем, работающих на базе спектрального уплотнения. Реализован волоконно-оптический канал передачи полного цветового высококачественного телевизионного изображения со звуковым сопровождением в действующей сети в режиме спектрального уплотнения.

видеосистемы, волоконно-оптические сети.

Волоконно-оптические системы передачи телевизионных изображений находят широкое применение в различных сферах современной деятельности человека: в сетях кабельного телевидения, в системах обеспечения безопасности объектов, для управления технологическими процессами и движущимися объектами, для организации видеоконференцсвязи и дистанционного обучения и т. д. Требования к качеству передаваемого видеосигнала постоянно повышаются. Растут требования и к среде передачи информации для обеспечения широкополосности и снижения затухания. Вследствие этого широкополосный волоконно-оптический кабель является удобной средой для передачи телевизионных изображений, в том числе на дальние расстояния.

Использование технологии спектрального мультиплексирования значительно расширяет возможности систем передачи движущихся изображений. Одним из примеров может служить применение принципов спектрального уплотнения категории CWDM (*Coarse Wavelength Division Multiplexing*), позволяющей в несколько раз увеличить число видеоканалов, передаваемых по одному волокну, тем самым повысить эффективность использования каждого волоконного канала и рентабельность системы. Такое решение может использоваться в любых сетях, где уже задействованы все каналы, и для организации временных видеоконференций и т. п.

Технология CWDM – системы с разреженным спектральным уплотнением в диапазонах O, E, S, C и L. Частотный разнос каналов 20 нм, позволяющий мультиплексировать до 18 каналов в диапазоне от 1270 до 1610 нм. Частотный план для CWDM систем определяется стандартом ITU G.694.2. Область применения технологии CWDM – как правило, городские сети с расстоянием до 50 км.

Кроме малогабаритных модемов передачи ТВ сигналов с использованием ЧИМ [1, 2], разработаны модемы передачи телевизионного сигнала студийного качества с цифровым кодированием. Для волоконно-оптических линий передачи телевизионных сигналов в цифровой форме применяется раздельное кодирование составляющих цветового сигнала. Сигнал яркости и два цветоразностных сигнала кодируются независимо, а затем 3 потока видеоданных мультиплексируются (объединяются) в один общий цифровой поток. В качестве базовой частоты дискретизации выбрана частота цветовой поднесущей стандарта NTSC – 3,375 МГц. Частоты дискретизации сигналов яркости и цветности принято записывать в формате трех чисел, означающих номер гармоники 3,375 МГц для дискретизации:

1) яркостного сигнала,

2) цветоразностного сигнала C_{Blue},

3) цветоразностного сигнала C_{Red}.

Например, формат 4:2:2 означает дискретизацию сигнала яркости с частотой 13,5 МГц, обоих цветоразностных сигналов – с частотой 6,75 МГц. Таким образом, суммарная скорость дискретизации в этом формате составит 27 МГц, а потоковая скорость передачи данных в последовательном интерфейсе составит более 270 МГц. Стандартизована иерархия частот дискретизации сигналов яркости и цветности, соответствующая коэффициентам 1, 2, 4, 8. Функции цифровой обработки видеосигнала осуществляет видеопроцессор.

Фотоприёмное устройство (ФПУ) в волоконно-оптических сетях должно обладать рядом повышенных технических характеристик: широким динамическим диапазоном, оптимальной амплитудно-частотной характеристикой, малым энергопотреблением, технологичностью при серийном производстве и т. д. Основной характеристикой ФПУ является чувствительность, так как именно она непосредственно влияет на дальность передачи информации в системе при заданной мощности оптического излучения в передатчике. Фундаментальное ограничение на чувствительность ФПУ накладывают внутренние шумы входящих в его состав элементов. Построение и оптимизация ФПУ волоконно-оптических сетей передачи видеосигнала на основе метода эквивалентных канонических шумовых схем [3] позволило повысить чувствительность фотоприёмных устройств путем обоснованного выбора формы амплитудно-частотной характеристики ФПУ, пара-

метров фотодетектора и усилителя фототока. Использование в ФПУ интеграторов фототока [4] с минимальным временем интегрирования позволяет проектировать дуплексные волоконно-оптические сети, в которых во встречном направлении по отношению к видеосигналу транслируются относительно низкоскоростные сигналы управления и интеллектуальной настройки видеокамер. Метод расчета чувствительности фотоприёмного устройства интегрирующего типа на основе свертки автокорреляционной функции и импульсной характеристики цепи позволяет провести обоснованный выбор параметров фотоинтегратора с целью достижения высокой чувствительности ФПУ [5].

В качестве источника оптического излучения наряду с лазерами CWDM могут быть использованы волоконно-оптические светодиоды. При проектировании мощных светодиодов принципиальной является оптимизация растекания тока и тепла в светодиодных чипах при предельно жёстких условиях их работы. В [6] проведено сравнительное исследование тепловых характеристик, а также распределения тока и интенсивности электролюминесценции в InGaN/GaN светодиодах вертикальной и face-up конструкций. Светодиоды вертикальной конструкции позволяют эксплуатацию при больших плотностях тока без особого влияния на ресурс и ухудшение энергетических свойств в связи с более однородным распределением плотности тока по площади кристалла [6].

Дополнительно к практическим вопросам оптимизации чувствительности ФПУ при внедрении студийных модемов передачи телевизионных сигналов потребовалось решение проблем:

а) мультиплексирования 4-х каналов передачи стереофонического звука и 2-х каналов передачи данных со скоростью 2,048 Мбит/с с низким уровнем (ниже –70 дБ) перекрестных искажений между каналами,

б) обеспечения требований электромагнитной совместимости. Эти проблемы решены моделированием в пакетах SPECCTRA Quest SI Expert (компания CADENCE), Protel DXP (компания ALTIUM), что обеспечило высококачественную разводку многослойных печатных плат.

В результате создан студийный волоконно-оптический модем передачи видеосигнала в цифровой форме в реальном масштабе времени без потерь информации ВОМ-124, внешний вид которого представлен на рис. 1, структурная схема – на рис. 2.

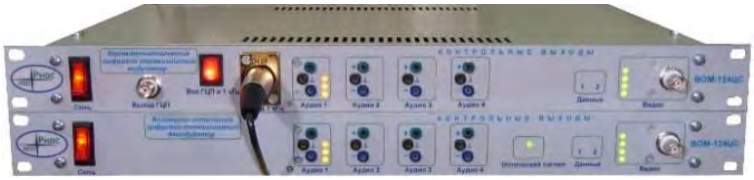


Рис. 1. Студийный волоконно-оптический модем передачи видеосигнала в цифровой форме ВОМ-124

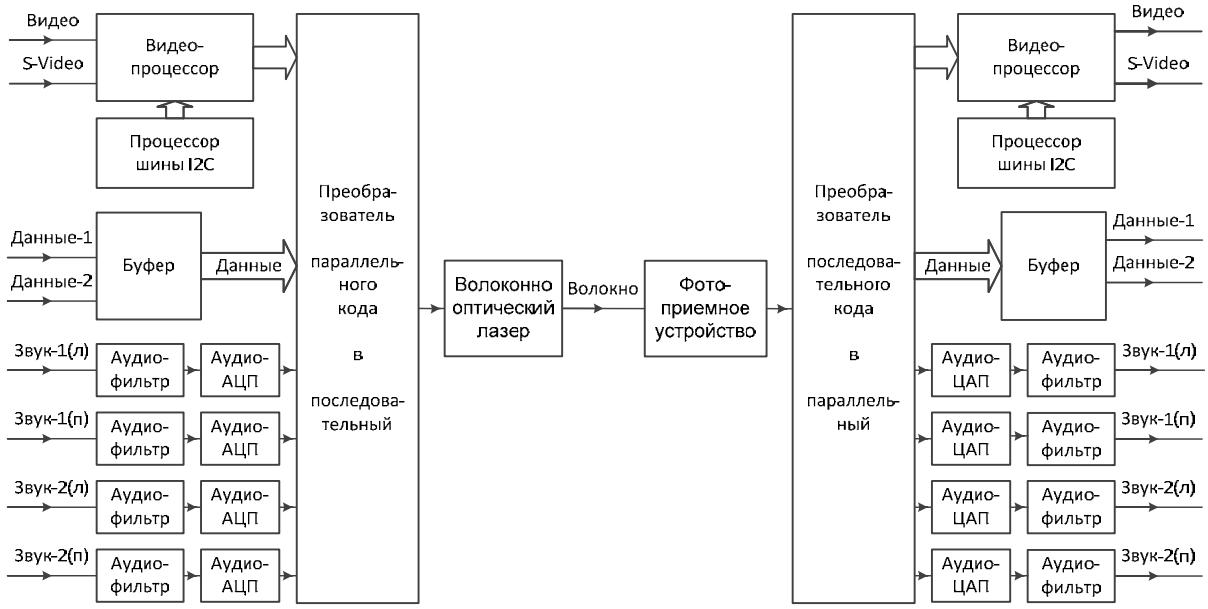


Рис. 2. Структурная схема цифровой волоконно-оптической системы передачи видеосигнала

Активная часть телевизионной строки видеосигнала оцифровывается 9-битным АЦП со скоростью выборок 27 МГц (цветовое разложение YUV 4:2:2), кадровые и строчные синхроимпульсы передаются кодовыми комбинациями, запрещенными для отсчетов видеосигнала. Четыре аудиосигнала оцифровываются 24-битными АЦП со скоростью выборок 48 кГц, что соответствует отношению сигнал/шум свыше 100 дБ. Потоки видео, данных (2 канала по 2,048 Мбит/с) и аудио мультиплексируются в последовательный код. Преобразователи параллельно-последовательного и последовательно-параллельного кодов для надежной синхронизации используют преобразование 16В-18В. Для настройки видеопроцессора используется интерфейсная шина I2C, управляемая PIC-процессором.

Новизна данной разработки состоит в том, что впервые в Российской Федерации была разработана и внедрена цифровая система передачи видеосигнала с частотой оцифровки телевизионного сигнала 27 МГц в соответствии со стандартами ITU-R BT 601 и ITU-R BT 656, что соответствует уровню профессионального студийного качества.

Дальность передачи мультиплексированного потока с отношением сигнал/шум 72 дБ составляет до 40 км при использовании лазера и одномодового волокна. Модемы ВОМ-124 внедрены в Центре Междугородной Связи «телецентра на Чапыгина, 6» в Санкт-Петербурге, а также в телестудиях регионального телевидения в г. Уфа, Гомеле и др.

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 1. Активное оборудование // 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. 57–61.

2. Андреева Е. И., Купцов В. Д., Валюхов В. П., Сумкин В. Р. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 2. Тестирование // 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. 61–66.

3. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемных устройств волоконно-оптических линий связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. №6 (113). С. 31–36.

4. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемного устройства на основе интегратора фототока // Электромагнитные волны и электронные системы. 2014. Т. 19. №7. С. 16–23.

5. Kuptsov V. D., Valyukhov V. P., Katelevsky V. Y., Rybin E. N. Light scattering by aerosol particles and air in the molecular condensation nuclei (MCN) detector // Proceedings of SPIE – The International Society for Optical Engineering 4. 2014. С. 92050Q.

6. Aladov A. V., Chernyakov A. E., Zakgeim A. L., Kuptsov V. D., Valyukhov V. P. Spatial distribution of current density and thermal resistance of high-power alingan vertical and face-up light-emitting diodes // Proceedings of SPIE - The International Society for Optical Engineering 7. Сер. "Optical Design and Testing VII". 2016. С. 100210X.

УДК 654.9
ГРНТИ 47.53.31

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ НА ВОЛОКОННОЙ ОПТИКЕ С ИСПОЛЬЗОВАНИЕМ СПЕКТРАЛЬНОГО УПЛОТНЕНИЯ

Е. И. Андреева[1], В. П. Валюхов[2], В. Д. Купцов[2], В. Р. Сумкин[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский политехнический университет Петра Великого

Представлена модель волоконно-оптической системы видеонаблюдения с использованием спектрального уплотнения каналов. Показано, что применение метода спек-

трального уплотнения видеоканалов может существенно повысить как рентабельность вновь создаваемых систем, так и оптимизировать наращивание сегментов уже существующих систем.

охранные системы, видеосистемы.

На сегодняшний день большое внимание уделяется системам обеспечения безопасности. Использование видеокамер с высоким разрешением, контроль на большой протяженности также предполагает использование оптических методов передачи видеосигнала.

Применение волоконно-оптических систем видеонаблюдения в сфере безопасности позволяет существенно расширить контролируемое пространство. Расстояния от видеокамер до контрольного пункта составляет от нескольких километров до 10 километров и выше при использовании одномодового кабеля. В случае протяженного периметра наблюдения становится существенной не только стоимость активного оборудования, но и самого оптического кабеля. Важное значение принимает топология построения сети и организация подключения отдельных камер для рационального экономически рентабельного использования кабеля [1].

Подключение каждой видеокамеры к отдельному волокну целесообразно при компактном их расположении по территории замкнутого объекта и относительно небольшой удаленности от контрольного пункта наблюдения. Преимущества оптических систем позволяют осуществлять удаленный контроль. В таких системах наглядно демонстрируются возможности активного оборудования и широкополосности волоконных световодов, в частности – в режиме спектрального уплотнения.

Технология спектрального уплотнения, или спектрального мультиплексирования (WDM – *Wavelength Division Multiplexing*), позволяет передавать по одному волокну сигналы на многих длинах волн. Емкость волоконно-оптической линии возрастает при этом пропорционально числу спектральных каналов. Наиболее широко используются технологии CWDM (*Coarse Wavelength Division Multiplexing*).

Количество активных каналов CWDM-системы зависит от типа используемого волокна. Стандартные волоконные световоды (SF – *standard fiber*) оптимизированы для использования во втором окне прозрачности 1260–1360 нм (окно прозрачности O). В стандартных световодах, параметры которых соответствуют стандарту G.652A, B, область вблизи «водяного» пика поглощения 1383 нм (окно прозрачности E) обычно не используется вследствие относительно больших потерь. На практике этот тип потерь существенно зависит от технологии изготовления волокна и имеет тенденцию к снижению. Для современного одномодового волокна у большинства компаний величина этого пика лежит в пределах 0,4–0,6 дБ/км. Для волокон,

специализированных для работы в широком спектральном диапазоне эта величина снижена.

Например, в волокнах типа AllWave производства компании Lucent Technologies и SMF-28e производства компании Corning величина потерь в окне прозрачности E не превышает 0,31 дБ/км. Параметры этих световодов соответствуют рекомендациям G.652C и G.652D (ZWPF – *Zero Water Peak Fiber*; LWPF, *Low Water Peak Fiber*, волокно со сглаженным «водяным» пиком на длине волны 1383 нм), формируя практически гладкую кривую затухания в диапазоне 1300–1620 нм, близкую к кривой релеевского рассеяния.

Следует также учитывать, что при использовании стандартного одномодового волокна, как правило, не используется диапазон коротких длин волн, меньших 1300 нм, из-за больших потерь на рассеянии.

Топология волоконно-оптической системы видеонаблюдения с использованием технологии CWDM

Для организации видеонаблюдения протяженного объекта наиболее часто используются топологии типа «дерево» и «шина». Типовое решение на базе волоконно-оптической технологии в системе охранного видеонаблюдения представлено на рис. 1 (см. ниже).

Для подключения группы удаленных видеокамер может использоваться технология CWDM-уплотнения. Модемы-передатчики 1 работают на выбранных длинах волн. Источники для CWDM-систем представляют собой лазеры с распределенной обратной связью (DFB, *Distributed Feedback*). Они отличаются узкой спектральной полосой и высокой термостабильностью. Установка 4-х или 8-ми канальных мультиплексоров на периметре и аналогичных демультиплексоров на контрольном пункте позволяет увеличить емкость каждого волокна в соответствующее число раз. Достижимая дальность рассчитывается с учетом вносимых потерь от 0,5 до 1 дБ на спектральный канал. Важным достоинством системы является возможность использования универсальных модемов-приемников 5.

При необходимости подключения отдельного сигнала в уже работающий волоконный канал могут использоваться стандартные спектральные фильтры (рис. 1б). Однако их включение сопровождается вносимыми потерями, которые должны также учитываться при расчете энергетического бюджета. В некоторых системах видеонаблюдения протяжённого объекта возникает необходимость передачи управляющих сигналов к видеокамерам и поворотным устройствам, на которых расположены видеокамеры. Управляющие каналы относительно узкополосны и фотоприемные устройства, чувствительность которых определяет дальность передачи, могут быть выполнены на основе интеграторов фототока [2, 3].

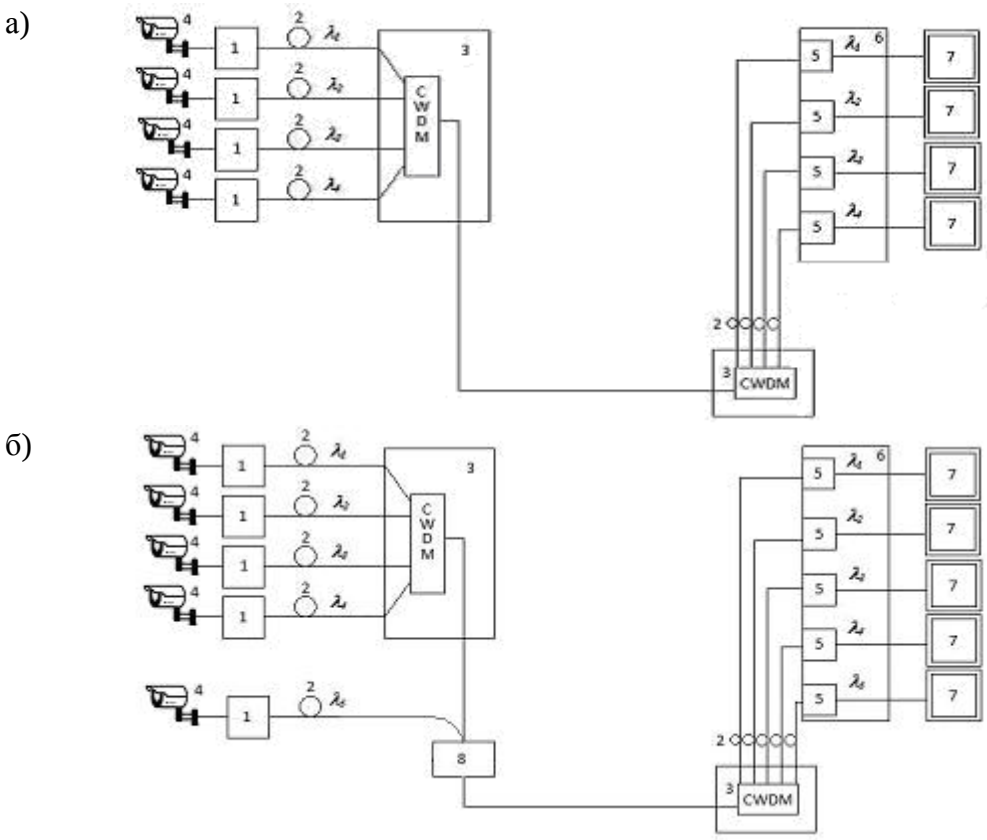


Рис. 1. Волоконно-оптическая система охранного телевидения с CWDM-уплотнением: 1 – волоконно-оптический модем-модулятор, 2 – одно/двухволоконный оптический кабель, 3 – оптический кросс с CWDM-мультиплексором/демультиплексором, 4 – видеокамера, 5 – волоконно-оптический модем-демодулятор, 6 – аппаратура обработки и хранения видеосигналов, 7 – монитор, 8 – CWDM фильтр

Монтаж

Для видеонаблюдения протяженного объекта наиболее целесообразно использование схемы построения, представленной на рис. 1а. В качестве модемов-передатчиков и модемов-демультиплексоров использовались модемы ОМД-1с, разработанные с учетом успешной эксплуатации предшествующих аналогов [4].

Основные характеристики модема ОМД-1с:

– модуляция видеосигнала при передаче – частотно-импульсная;
– длина волны оптического излучения – 1,31 мкм*);
– дальность передачи (SSMF-волокно G.652) – 10 км;
– энергетический бюджет линии – 16 дБ;
– отношение сигнал/шум по видео сигналу – 60дБ;
– напряжение питания – +9В (нестабилизированное);
– ток потребления каждого блока – 250 мА;
– габаритные размеры (без источника питания) – 130×70×30 мм;
– температурный диапазон – (–25°С ÷ +55°С).

*) энергетический бюджет и дальность передачи приведены для указанной длины волны источника излучения. Для повышения дальности используется методика оптимизации чувствительности фотоприёмного устройства на основе метода эквивалентных канонических шумовых схем [5]. Для повышения емкости волоконного канала в качестве источников в модеме-модуляторе используются лазеры с длиной волны, соответствующей шкале CWDM.

Гибкий бронированный кабель для финишной разводки

Для финишной разводки оптики на отдельно стоящие модемы и их группы до четырех штук удобно использовать бронированный кабель типа ОКМБ-03. Конструкция этого кабеля проста и надежна (рис. 2).

Особенностью кабеля марок ОКМБ-03 является отсутствие трубчатого полимерного модуля с оптическими волокнами, расположенными в нем свободно и заполненного гидрофобным компаундом. Основой данного типа кабеля является металлическая трубка, изготовленная из шести стальных оцинкованных канатных проволок (рис. 2) с прочностью не менее 1770 Н/мм^2. Наружный диаметр каждой из проволок от 0,5 до 1,35 мм. Волокна в 900-микронном лаковом покрытии в количестве от одного до четырех без дополнительного модуля армируются и герметично укладывается под полимерную герметичную оболочку, не поддерживающую горение.

Рис. 2. Конструкция кабеля ОКМБ-03: 1 – волоконный световод, 2 – гидрофобный заполнитель, 3 – броня из тонкой оцинкованной проволоки, 4 – защитное полимерное покрытие

Из-за отсутствия полимерного модуля в этом кабеле могут быть использованы волокна с рабочей температурой до 150, 200 и 300°С и защитные оболочки из высокотемпературных полимерных материалов, материалов с низким дымо- газовыделением (LSZH) не распространяющих горение, например, кремний органической резины, фторопласто- содержащих полимерных композиций, полиуретанов и др. Указанные особенности позволяют изготавливать высокотемпературные и огнестойкие модификации оптических кабелей.

Наружный диаметр кабеля 2,5 мм, что дает преимущество при прокладке в труднодоступных или сильно изогнутых участках. Кроме того,

при одноволоконном исполнении он может быть оконцован разъемом как обычный патчкорд, рис. 3. При необходимости кабель может изготавливаться с использованием герметичных разъемов, а также стойких к изгибу волоконных световодов. Так, в соответствии со стандартом (рекомендации МСЭ-Т G.652.D и G.657.A.1) такие одномодовые световоды допускают изгиб до радиуса 10 мм с приростом потерь не более 0,5 дБ/км.

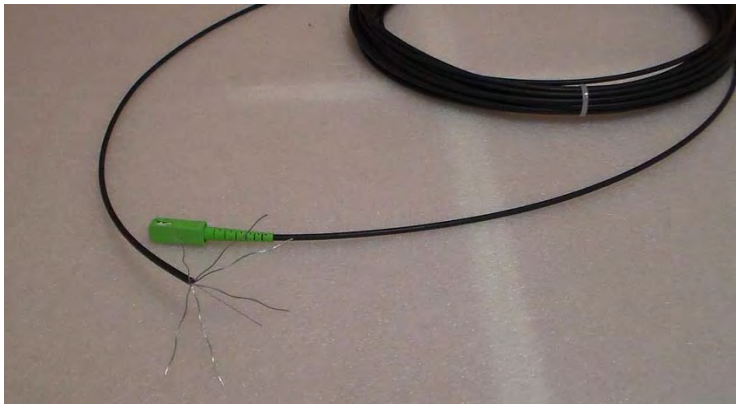


Рис. 3. Соединительный волоконно-оптический шнур на основе кабеля ОКМБ-03 в одноволоконном исполнении, снабженный оптическим коннектором

Апробация модемов в условиях объекта подтвердила качество установленного оборудования, удобство обслуживания, правильность технического решения.

Список используемых источников

1. Андреева Е. И., Купцов В. Д., Валюхов В. П., Сумкин В. Р. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 2. Тестирование // 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. 61–66.

2. Купцов В. Д., Валюхов В. П. Чувствительность фотоприемного устройства на основе интегратора фототока // Электромагнитные волны и электронные системы. 2014. Т. 19. №7. С. 16–23.

3. Kuptsov V. D., Valyukhov V. P., Katelevsky V. Y., Rybin E. N. Light scattering by aerosol particles and air in the molecular condensation nuclei (MCN) detector // Proceedings of SPIE – The International Society for Optical Engineering 4. 2014. С. 92050Q.

4. Андреева Е. И., Купцов В. Д., Валюхов В. П. Волоконно-оптическая система видеонаблюдения производственного объекта: функции охраны и технологического контроля. Часть 1. Активное оборудование // 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. 57–61.

5. Купцов В. Д., Валюхов В. П. Чувствительность фотоприёмных устройств волоконно-оптических линий связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. № 6 (113). С. 31–36.

УДК 621.396.2
ГРНТИ 49.13.13

МОДЕЛЬ КАНАЛОВ «НАПРАВЛЕНИЯ ВНИЗ» БАЗОВОЙ СТАНЦИИ UMTS-СИГНАЛОВ

О. М. Андреева, П. О. Поляков

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Стандарт UMTS относится к третьему поколению стандартов сотовой связи. Основным отличием от предыдущих стандартов является внедрение технологии широкополосного множественного доступа с кодовым разделением каналов. Стандарт UMTS является основой работы крупнейших поставщиков связи на территории России, таких как «МТС», «Билайн» и «Мегафон». Стандарт позволяет поддерживать скорость передачи информации на теоретическом уровне до 21 Мбит/с, что позволяет пользователям проводить сеансы видеоконференций посредством мобильного терминала, выполнять быструю загрузку музыкального и видеоконтента, получать доступ к сети Интернет.

В данной работе рассматривается модель формирователя физических каналов сигнала UMTS в направление вниз. Предложенный принцип моделирования позволяет упростить имитацию эфирной обстановки.

стандарт UMTS, кодовое разделение каналов, синхронизация.

В стандарте UMTS выделяют три вида каналов: логические, транспортные и физические [1]. Первые два из вышеперечисленных каналов необходимы для определения методов и путей передачи актуальной информации, в то время как физические каналы служат для ее непосредственной пересылки.

В данной работе рассматриваются лишь физические каналы каждого слота:

1) Выделенный физический канал (DPCH). Структура канала показана на рис. 1. На рис. 1 $N_{\dots}$ – число бит для каждого битового блока в канале. Битовый блок TFCI указывает соответствие скоростей (количество чипов в секунду) выделенных физических каналов. Блок бит TPC необходим для определения, требует ли базовая станция увеличить или уменьшить мощность сигнала. Блоки Data1 и Data2 нужны для хранения информации абонента, передающейся по каналу, а блок Pilot служит для кодирования информации о количестве бит, отводимых на каждый из описанных блоков канала. Коэффициент расширения спектра данного канала и число бит

для каждого блока информации $N_{\dots}$ определяются необходимой скоростью передачи и являются параметрами моделирования.

2) Общий пилотный канал (CPICH). Используется для определения скремблера базовой станции. По каналу всегда передаются логические нули. Канал расширен ортогональным кодом, коэффициент расширения которого также является параметром модели.

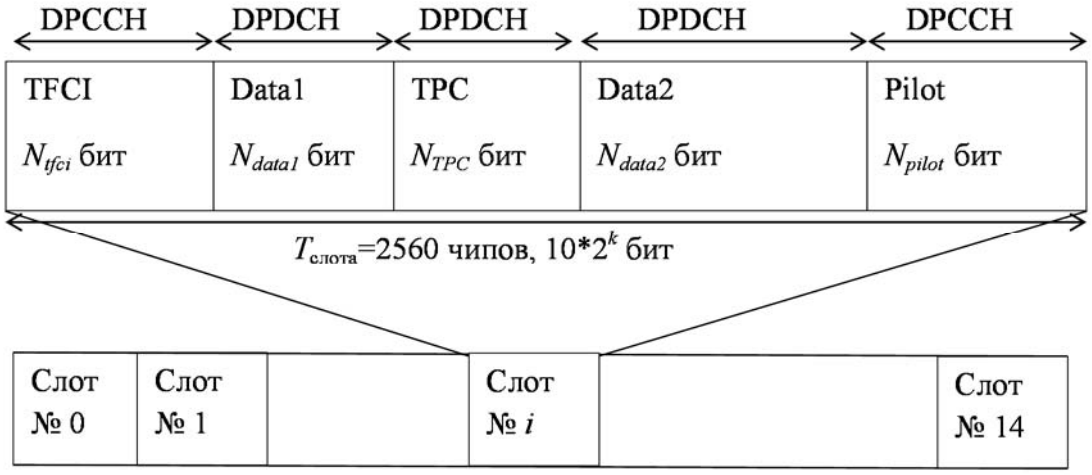


Рис. 1. Структура DPCH

3) Общий канал управления (P-CCPCH). Структура канала показана на рис. 2, где 256 чипов (2 бита), обозначенных как *Tx**OFF* обозначают отсутствие передачи данных, а 18 оставшихся бит служат для передачи служебной информации.

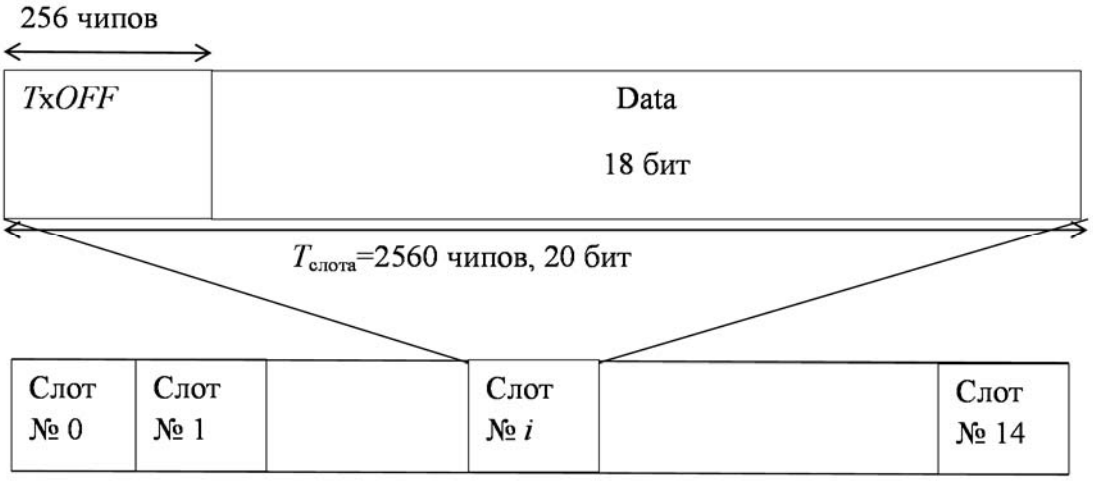


Рис. 2. Структура канала P-CCPCH

4) Канал синхронизации (SCH), включающий в себя два подканала: канал первичной синхронизации (PSCH) и вторичный канал синхронизации (SSCH). Структуры каналов показаны на рис. 3. PSCH-канал передает в начале каждого слота синхронизирующую последовательность, длиной 256 чипов. Канал SSCH передает в начале каждого слота один из 16 взаимнортогональных синхрокодов. Синхрокод выбирается в зависимости от номера слота в соответствие с кодовой группой сигнала. Всего в стандарте предусмотрено 64 кодовых группы, нумерующихся от 0 до 63 кодовой группы. И синхропоследовательность, и синхрокод являются параметрами модели.

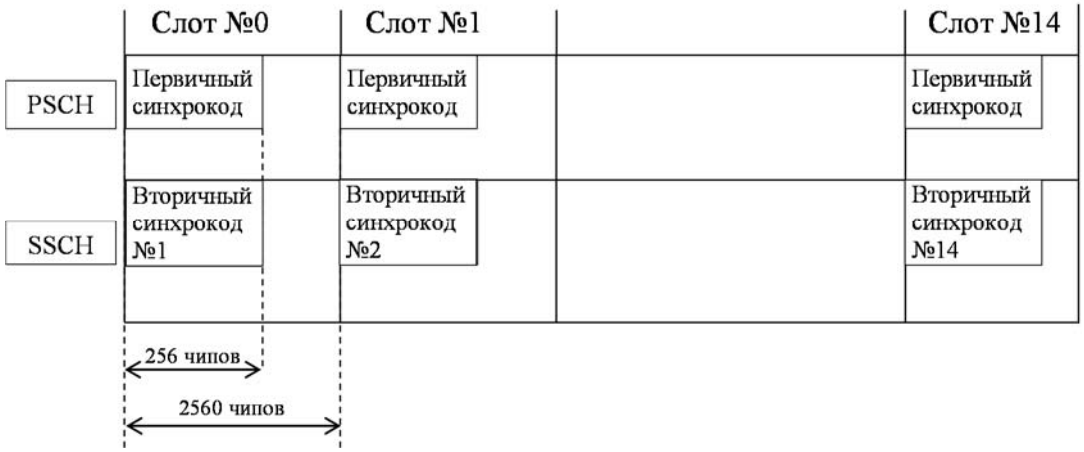


Рис. 3. Структура канала SCH

5) Канал индикации вызова (PICH). Структура канала достаточно проста: из трехсот бит используются для передачи служебной информации 288, а оставшиеся 12 бит не используются.

В данной модели, в соответствии со стандартом UMTS, при формировании каналов используется технология широкополосного множественного доступа с кодовым разделением каналов (WCDMA – *Wideband Code Division Multiple Access*), поэтому после формирования содержимого вышеописанных каналов необходимо осуществить их QPSK-модуляцию, расширение и скремблирование (кроме каналов PSCH и SSCH). Третий шаг – суммирование всех каналов, составляющих сигнал.

Структурная схема модели представлена на рис. 4. На данной схеме блоки DPCH, PICH, CPICH, CCPCH, и следующий блок (Re/Im, разделение на мнимые и вещественные части) производит QPSK-модуляцию каналов. В блоке расширения происходит умножение каналов на соответствующие каналообразующие коды, и сложение вещественной части с мнимой, формируя комплексный отсчет – чип сигнала. Затем расширенные и скремблированные последовательностью *Sc* каналы, вместе с каналами P-SCH и S-SCH поступает на сумматор, формируя выходной сигнал $S_{вых}$.

Созданная модель в соответствии с технологией WCDMA позволяет выбирать различные скорости для выделенных абоненту каналов, количество выделенных каналов, моделировать различные варианты сигнально-шумовой обстановки. Также, за счет включения каналов синхронизации, данная модель может служить в качестве проверочного сигнала для различных алгоритмов синхронизации.

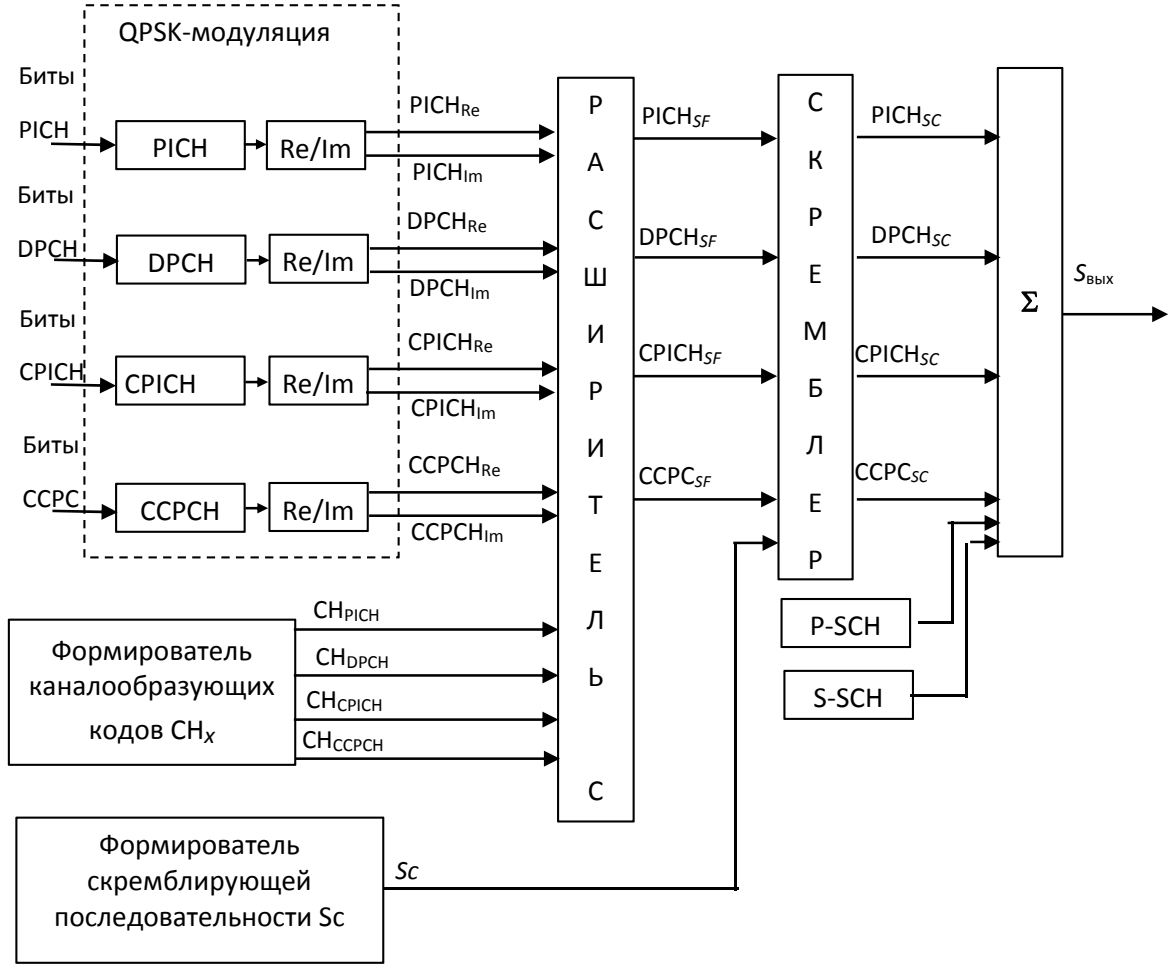


Рис. 4. Структурная схема формирования модели сигнала

Список используемых источников

1. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Spreading and modulation (FDD) //3GPP TS 25.213 – 2011.

УДК 004.056.53
ГРНТИ 81.93.29

РАЗРАБОТКА МЕТОДОЛОГИИ ЗАЩИЩЕННОГО КОНТРОЛЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКОВ ГОСУДАРСТВЕННЫХ СЛУЖБ

В. И. Андрианов, О. М. Виноградова

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

На всех стадиях развития информационных технологий было очевидно, что данные, хранимые и обрабатываемые в электронном виде, необходимо защищать, однако первоначально был отдан приоритет внешним угрозам. На сегодняшний день проблема защиты от внутренних угроз так же набирает значительный оборот, так как с развитием данных технологий и их постепенных внедрением во все большее количество компаний, а как следствие, увеличение осведомленности о существующих проблемах. Дополнительно также важно подразумевать в государственных службах наличие систем обеспечивающих надежную работу сотрудников, которые могут быть потенциальными нарушителями для систем контроля учета рабочего времени, состоящих из перечисленных систем защиты информации.

DLP, SIEM, защита данных, криптография, аутентификация.

Важным шагом в укреплении позиций компании в области ИБ становится внедрение DLP-системы. Это программное решение призвано противостоять утечкам конфиденциальной информации и при грамотном внедрении, подготовке процедурных документов и необходимых частных политик, все это позволит существенно снизить вероятность несанкционированного перемещения конфиденциальных данных вовне [1].

При принятии решении внедрять DLP-системы следует сделать «три шага»:

1) Оценить вероятность наступления события. (сколько раз в год происходит утечка информации).

2) Оценить возможный ущерб. (Сколько нам это будет стоить?).

3) Сопоставить полученную цифру со стоимостью внедрения системы.

Если цифра ущерба хотя бы примерно равна стоимости внедрения DLP-системы, то ее внедрение без сомнения оказывается прибыльным. По данным компании SearchInform, основанным на исследованиях Ponemon Insitute, средняя стоимость утечки информации в мире составляет $2,7 млн. И эта цифра, к сожалению, год за годом лишь увеличивается.

Перейдем непосредственно к описанию DLP-системы, которое показано на рис. 1.

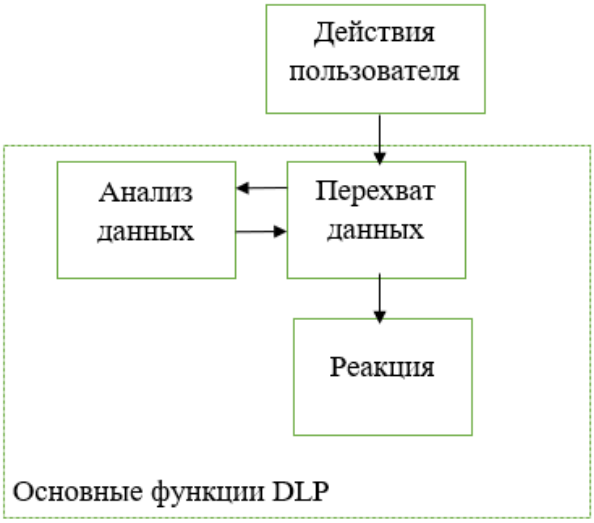


Рис. 1. Принцип функционирования DLP-системы

Если говорить об истории развития DLP-технологий, то первыми появились технологии сетевого мониторинга без возможности блокировки утечки через сетевые протоколы (HTTP, SMTP и т. п.). В дальнейшем производители соответствующих решений стали добавлять функции блокировки информации при передаче данных через сеть [2].

По данным глобального исследования компании InfoWatch в 2016 году было задокументировано 840 случаев утечки информации. Из них, как показано на рис. 2–67 % составляют внутренние нарушения безопасности, при этом 51 % внутренних нарушений являются преднамеренными (рис. 2).

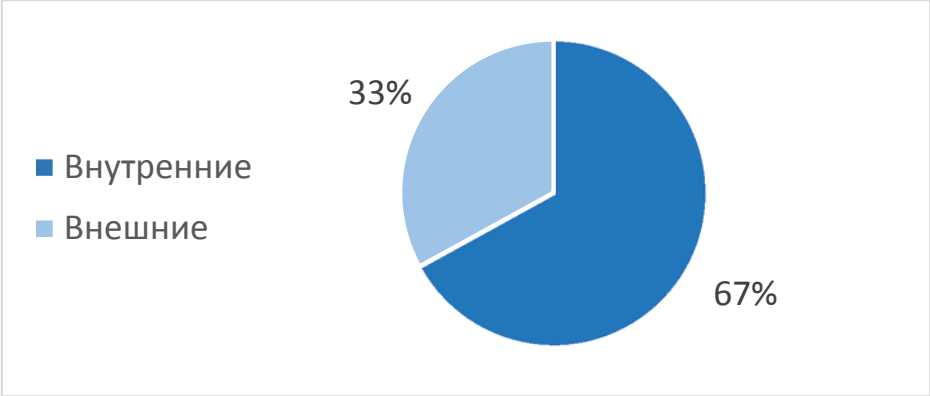


Рис. 2. Распределение вектора утечек

Рис. 2. Виновники утечек

При этом доля утерянных персональных данных равняется 87,5 %, 6,2 % – платежная информация, 4,6 % – коммерческая тайна и 1,7 % составляет государственная тайна.

Для осуществления контроля учета рабочего времени предлагается внедрение программно-аппаратных систем SIEM [3]. Разработкой SIEM-систем занимаются в том числе такие известные компании, как IBM, McAfee, Symantec, однако их решения не могут быть применены для анализа безопасности в ИВ по ряду следующих причин:

1. Отсутствие общепринятых критериев оценки уровня безопасности и определения понятия события безопасности в ИВ.

2. Необходимость формирования события безопасности из данных от устройств внутреннего нарушителя.

3. Большие объемы гетерогенных полуструктурированных и неструктурированных данных, поступающих синхронно и асинхронно от устройств внутреннего нарушителя различного типа [4]. Существующие SIEM-системы не в состоянии эффективно обрабатывать плохо структурированные данные высокой размерности, порождаемые большим количеством разнообразных устройств. В связи с этим возникает задача разработки методологического и математического обеспечения SIEM-систем для ИВ, позволяющего:

1) формализовать понятия события и инцидента безопасности для внутреннего нарушителя и систем межмашинного взаимодействия (M2M);

2) обеспечить сокращение размерности и обработку больших массивов гетерогенных неструктурированных и полуструктурированных данных;

3) выявлять и анализировать инциденты безопасности в внутреннего нарушителя.

Потому для формализации понятий события и инцидента безопасности в государственных службах первоначально требуется создать методику, описывающую предметную область с точки зрения взаимодействующих устройств [5]. В данной статье представлена математическая модель взаимодействия устройств, на основе которой формализовано понятие события контроля учета рабочего времени, а также доказана достаточность анализа синхронизации разных механизмов работы систем защиты информации для осуществления данного контроля.

Для синхронизации разных программных средств необходимо представить уровень предоставления угроз (рис. 3) и уровень предоставления инцидентов (рис. 4).

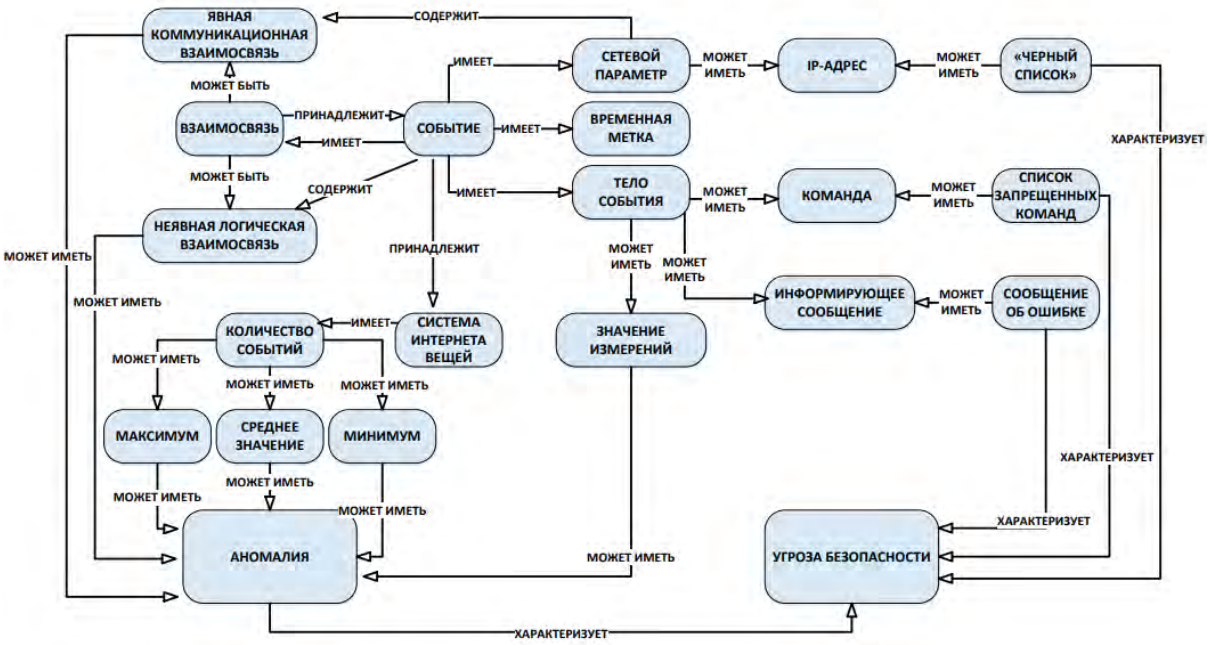


Рис. 3. Уровень представления угроз

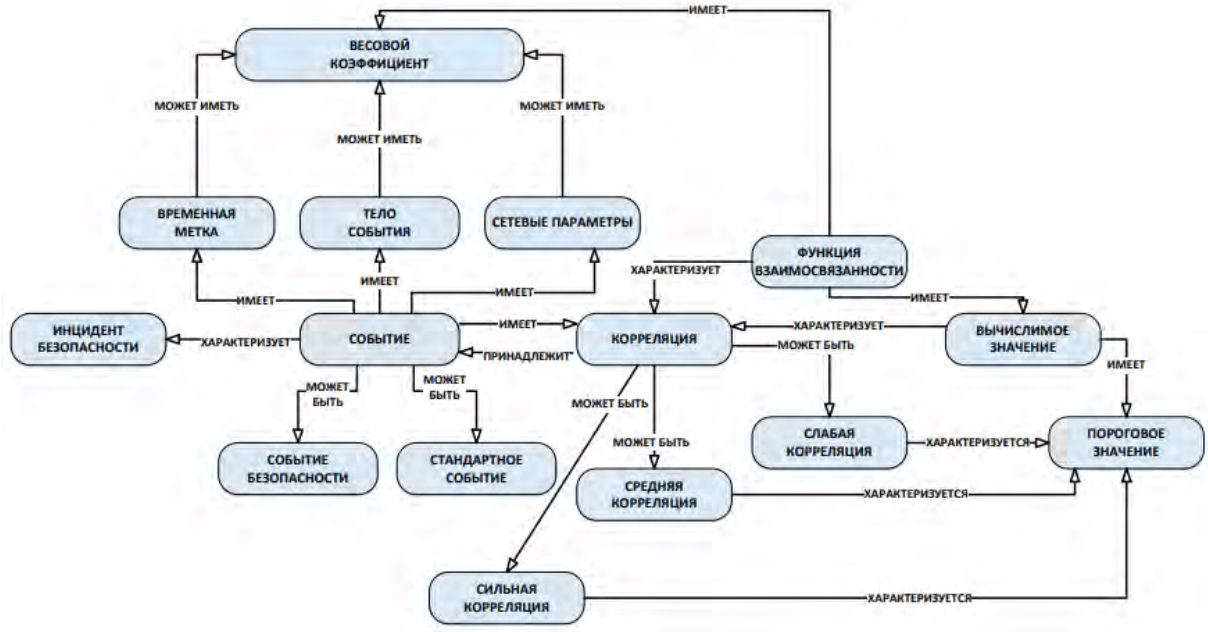


Рис. 4. Уровень представления инцидентов

Методика, учитывающая данные уровни, позволит агрегировать разные состояния больших массивов данных для систем контроля учета рабочего времени сотрудников [6]. В соответствии с синхронизацией DLP и SIEM, для сокращения размерности пространства сообщений, с целью последующей его трансформации в пространство событий, требуется выполнить два этапа агрегации (в соответствии с временным параметром и в соответствии с типом устройства) и этап нормализации, разделяющий этапы

агрегации. На рис. 5 представлена общая схема процесса предварительной обработки данных от устройств ИВ, состоящая из следующих этапов:

1) агрегация сообщений в соответствии с временным параметром;
2) нормализация сообщений;
3) агрегация сообщений в соответствии с типом устройства;
4) формирование событий из сообщений.

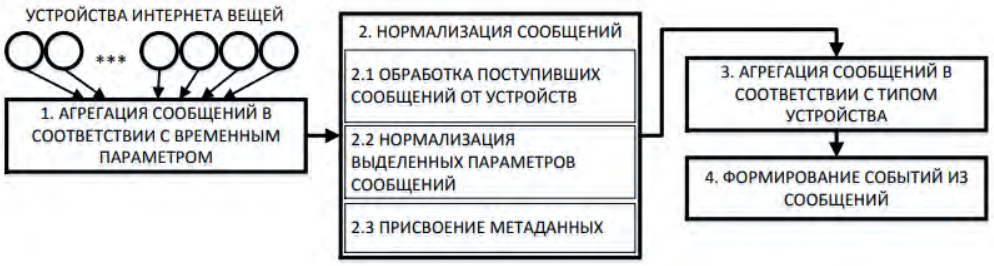


Рис. 5. Взаимосвязь разработанных математических методов агрегации больших массивов данных.

Соответственно получается, что первичная агрегация в памяти может производиться с разной интенсивностью в зависимости от устройства [7]. Также имеет значение возможная потеря данных, так как до занесения агрегированного значения в хранилище обработка происходит в оперативной памяти и в случае сбоя поступившие сведения могут быть потеряны (рис. 6).

Рис. 6. Схема агрегации сообщений в методике по времени

Итого, Разработанная методика предметной области контроля учета рабочего времени позволила сформулировать требования к разработке SIEM-системы и DLP для выявления и анализа инцидентов безопасности [8]. На уровне представления устройства был получен 87 перечень основных источников угроз безопасности, связанных с конечным устройством ИВ. На уровне представления пространства сообщений и пространства событий были сформулированы требования к процессу преобразования данных, заключающиеся в агрегации по времени и по объекту, разделяемых этапом нормализации. На уровне представления угроз безопасности были сформированы требования для выявления инцидентов, заключающиеся в корреляции событий с использованием правил, в статистической корреляции событий и в интеллектуальном выявлении неявных взаимосвязей между устройствами. На уровне представления инцидентов были сформулированы требования, заключающиеся в кластеризации событий и их корреляции друг с другом на основе оценки схожести событий по определенным параметрам.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности: учебное пособие. Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». Санкт-Петербург, 2012.

2. Ушаков И. А., Котенко И. В., Крылов К. Ю. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // Информационная безопасность регионов России (ИБРР-2015): материалы конференции. 2015. С. 75–76.

3. Дешевых Е. А., Ушаков И. А., Чечулин А. А. Интеграция SIEM-систем с системами корреляции событий безопасности, основанных на технологии больших данных // Информационные технологии в управлении (ИТУ-2016): материалы 9-й конференции по проблемам управления. 2016. С. 684–687.

4. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

5. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. 2018. № 3 (15). С. 47–54.

6. Штеренберг С. И. Методика построения поисковой системы для примитивной программы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 52–57.

7. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Методология управления потоками трафика в программно-определяемой адаптивной сети // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 4. С. 3–8.

8. Печенкин А. И., Лаврова Д. С. Обнаружение инцидентов безопасности в Интернете Вещей // Проблемы информационной безопасности. Компьютерные системы. СПб. : Изд-во Политехн. Ун-та. 2015. № 2. С. 69–79.

УДК 004.352.4
ГРНТИ 50.09.53

БИОТМЕТРИЯ В СКУД

Н. Э. Арбузова[1], С. В. Прудников[2], В. Ю. Тесаков[3], С. В. Шипулин[4]

[1]ООО «Холдинговая компания СевЗапСтрой»
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]ООО «Равелин»
[4]Управление Роскомнадзора по Северо-Западному федеральному округу

Данная статья посвящена внедрению биометрических методов распознавания. Как известно именно биометрические методы распознавания применяются людьми в повседневной жизни. Так мы узнаем знакомых нам людей по лицу, голосу, по походке и т. п. Полиция определяет преступников по отпечаткам тоже достаточно давно. Такой способ удобен, надежен, практичен. И уже много лет биометрические технологии применяются в СКУД. Все прекрасно понимают, что это такое, как они работают. Но, что удивительно, до сих пор это так и не вошло в массовую практику. По итогам последних опросов, только 11 % инсталляторов используют биометрические технологии более, менее регулярно на своих объектах.

электронные средства биометрической идентификации человека, контроллер, СКУД, системы контроля доступа, аутентификация, интеграция, алгоритмы и программное обеспечение, верификация (подтверждение).

Критерии биометрической идентификации

Для определения эффективности СКУД на основе биометрической идентификации используют следующие показатели:

FAR – коэффициент ложного пропуска;

FMR – вероятность, что система неверно сравнивает входной образец с несоответствующим шаблоном в базе данных;

FRR – коэффициент ложного отказа;

FNMR – вероятность того, что система ошибётся в определении совпадений между входным образцом и соответствующим шаблоном из базы данных;

график ROC – визуализация компромисса между характеристиками FAR и FRR;

коэффициент отказа в регистрации (FTE или FER) – коэффициент безуспешных попыток создать шаблон из входных данных (при низком качестве последних);

коэффициент ошибочного удержания (FTC) – вероятность того, что автоматизированная система не способна определить биометрические входные данные, когда они представлены корректно;

ёмкость шаблона – максимальное количество наборов данных, которые могут храниться в системе.

В России использование биометрических данных регулируются статьей 11 Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 г.

До сих пор электронные средства биометрической идентификации не добились такого успеха, как природа. Они не могут с точностью 98–99 % идентифицировать человека. Только разработчики технологии 3D распознавания лиц, утверждают, что могут работать в режиме идентификации и не требуют использования карт. Остальные рекомендуют использовать свои средства в режиме верификации (подтверждения) при поднесении карты пользователем. Напрашивается вопрос: Зачем платить дважды? Вот инсталляторы и используют средства биометрии только на наиболее ответственных точках доступа, проектируемых объектов. Практически все производители биометрических средств, предлагают какие-то свои контроллеры и решения. Это, абсолютно оправдано с точки зрения коммерческой деятельности, но что делать с тысячей объектов, где уже спроектированы и установлены системы контроля доступа. Представим, что у заказчика даже есть серьезные основания усилить системы идентификации с помощью биометрии. Но перед ним встает выбор – выкинуть все и поставить новое замечательное, или оставить все как есть. А заказчик, как известно чаще всего выбирает по качеству и цене! [1, 2, 3, 4, 5, 6, 7].

Но нельзя не отметить, что разработчики биометрических считывателей стараются найти общий язык с производителями средств СКУД, но для интеграции возникают некоторые барьеры. Например, китайские производители просто недостаточно понимают, что это такое и постоянно предоставляют SDK с ошибками или не полные. И российские разработчики средств биометрического контроля, как и большинство разработчиков, пишут документацию по мере ее необходимости. Описание средств интеграции далеко не на первом месте. Вот и получается, что производитель средств сетевых СКУД не только должен очень хотеть, но и изрядно поработать, чтобы произвести интеграцию со средствами биометрической идентификации.

Следующая, и, безусловно, важная причина - недоверие у самих заказчиков, опыта еще недостаточно и отсюда психологический барьер. Только несколько лет назад технологии биометрической идентификации стали использоваться в массовом сегменте (смартфоны, банкоматы, заграничные паспорта и т. д.). Только сейчас приходит понимание, что средства биометрической идентификации можно использовать в быту. Даже тогда, когда

других вариантов идентификации вообще нет, приходится слышать «а работать то будет?». Современные отечественные производители средств сетевых СКУД, постоянно на своих семинарах информируют пользователей о новых возможностях, приводят примеры удачных внедрений. Но в основном это информация представляется инсталляторам, а не конечным пользователям.

Вот и приходится самим производителям биометрических средств, пропагандировать свой продукт самостоятельно. Конечно, без поддержки более многочисленной армии инсталляторов, возможности их ограничены. И без этой поддержки многие идут по пути готовых решений, и иногда еще более теряют. И конечно – цена. Для проведения биометрической идентификации требуется обрабатывать значительное количество данных и вести большой объем вычислений, следовательно, контроллер считывателя должен иметь хорошее быстродействие. Стоимость устройства пропорциональна стоимости основного процессора и памяти – вот и получается, что данное решение получается не дешевым. А еще производители заталкивают в него, на всякий случай и дополнительные возможности. Вернемся к тому, что заказчики все выбирают по цене. Что остается инсталлятору – предлагать биометрические решения «на всякий случай», и только в редких случаях, из-за невозможности другого решения.

Из вышесказанного может сложиться печальная перспектива. Но на самом деле, на сегодня рынок готов применять биометрические технологии идентификации, как элемент сетевых СКУД. Знаний, предложений, реализованных проектов – достаточно. Главная задача производителя средств СКУД для успешной реализации проектов с использование средств биометрической идентификации – грамотно произвести интеграцию. Поскольку именно он (производитель средств СКУД) отвечает за работоспособность системы в целом.

Предлагается показать последовательность выбора партнеров для интеграции – производителя средств биометрической идентификации.

Во-первых, надо определиться с тем, что на рынке востребовано. Согласно последним исследованиям основную долю рынка применяемых биометрических считывателей занимают считыватели по отпечатку пальцев. Затем с большим отрывом считыватели по рисунку вен и по лицу. В целом, это три направления закрывают потребности 90 % рынка. Можно еще упомянуть идентификацию по радужной оболочке глаз – но сегодня это очень дорого.

Далее среди средств идентификации по отпечаткам пальцев выбираются наиболее популярные. Понятно, чем дешевле считыватель, тем выше на него спрос. Но при этом должен соблюдаться определенный уровень качества, т. е. оборудование должно себя уже неплохо зарекомендовать

на практике у пользователей. Самые популярные решения считывателей отпечатков пальцев предлагают производители из России и Китая. Причем последние, явно выигрывают по цене и на сегодня занимают около 50 % рынка.

Однако, первый же опыт работы с китайскими производителями показал, что получить от них SDK и объяснения как с ним работать, очень сложно. Второе место по популярности недавно заняли считыватели по рисунку вен. Есть качественный производитель в России, хорошие отзывы, продвинутое руководство в компании. Но цена изделия составляет 70 тыс. руб. Хотя стоит заметить зарубежные аналоги как минимум не дешевле. И во многих случаях это оправдано: качество считывания лучше, меньше ошибок, неприхотливы к испачканным рукам и влажности. Внедрение подобных решений происходит, как правило под заказ поэтому производители приняли решение отложить интеграцию до появления какого-то конкретного заказа.

Самым удобным способом биометрической идентификации является идентификация по лицу. На сегодняшний день в этом сегменте разработано достаточно большое количество решений. Можно разделить их на две группы: комплексные решения (телевизионная камера, сервер обработки данных) и законченное решение (встроенная телевизионная камера, контроллер, коммутирующее реле).

При комплексном решении достигается наилучшее качество идентификации, поскольку нет ограничений на вычислительные мощности средств обработки данных. Сигнал с датчика (телевизионной камеры) передается на сервер, который производит вычисления и после этого может выдать решение об аутентификации. Алгоритмы и программное обеспечение протестировано на объектах. Основная сложность применения – высокая стоимость конечного решения, но – возможна только «программная» интеграция. При этом нарушается один из основных законов работы СКУД, а именно – «контроллер должен работать автономно, в т. ч. в случае пропадании связи с сервером управления». Конечно для ряда категорий объектов, можно обеспечить все необходимые условия, но не для массового рынка. Интеграция с подобной системой возможна при наличии только конкретного заказчика и только конкретной задачи.

Второй вариант – законченное решение, которое широко представлено на рынке китайскими производителями. Надежность идентификации такого устройства приемлемо. Устройство может применяться в составе сетевых СКУД за счет наличия выход Wiegand. Однако использование этого устройства имеет некоторые особенности. Во-первых, это создание биометрических шаблонов. В инструкции: «При вводе изображения в память считывателя людям, имеющим рост 150–180 см рекомендуется встать в полуметре от устройства, которое монтируется на стене, на высоте примерно 120 см.

Во время ввода и проверки шаблона необходимо сохранять спокойное состояние, чтобы обеспечить в дальнейшем корректное распознавание лиц при проходе через точку доступа. Для каждого пользователя в базу заводится несколько изображений лица с различным наклоном головы вверх и вниз при ракурсе съемки анфас. Для более точного позиционирования лица при фиксации кадров необходимо следовать голосовым инструкциям, воспроизводимым устройством, а набор шаблонов, сделанных под разными углами, поможет точнее идентифицировать лицо во время проверки».

Особенность в том, что данную процедуру необходимо провести перед каждым устройством. Если таких устройств несколько – это выливается в длительный процесс с привлечением значительного административного ресурса. В исследуемых продуктах централизованное занесение шаблонов невозможно. Напрашивается вывод, данные устройства можно эффективно использовать только в автономном режиме, либо в случае очень небольшого количества пользователей. Отсутствие SDK на данном этапе пока тормозит развитие. Но это направление очень перспективное.

Заключение

В настоящий момент совершенствование биометрических технологий происходит высокими темпами. И первые результаты, это повышение надежности и снижение стоимости для традиционных технологий: распознавания по отпечатку пальца, лицу и рисунку вен. С другой стороны, постоянно развивается элементная база и повышается скорость обработки данных, что очень стимулирует интеграцию с сетевыми СКУД. Использование биометрических технологий в быту (смартфоны, паспорта и т. д.) повышает их привлекательность и доверие у заказчиков. Все это затронет не только развитие биометрических считывателей. Данные события приведут к технологическим изменениям и совершенствованию имеющихся на рынке систем контроля доступа. Улучшение качества взаимодействия разработчиков сетевых средств СКУД и средств биометрической идентификации неизбежно. Как быстро это произойдет, зависит от настойчивости лидеров рынка, и все это в целом приведет к повышению комфортности и безопасности проживания людей.

Список используемых источников

1. ГОСТ Р ИСО/МЭК19794-2-2005.
2. ГОСТ Р 54412-2011/ISO/IEC/TR 24741:2007.
3. Вихман В., Якименко А. Биометрические системы контроля и управления доступом в задачах защиты информации. Новосибирск : Изд-во НГТУ, 2016. 54 с. ISBN 978-5-7782-2955-6.

4. Вихман В., Якименко А. Внедрение биометрической идентификации в системы контроля и управления доступом. учебно-метод. пособие. Издательство: «Новосибирский государственный технический университет», 2016. ISBN 978-5-7782-3020-0.

5. Гинце А. Биометрия: куда пойдет развитие рынка // Системы безопасности. 2004. № 1. С. 54.

6. Купцов Р. Р. Анализ современных методов биометрической идентификации СКУД [Электронный ресурс] // Студенческий: электрон. научн. журн. 2018. № 8 (28). URL: https://sibac.info/journal/student/28/103920 (дата обращения 05.12.2018).

7. Харитонов А. В. Обзор биометрических методов идентификации личности // Кибернетика и программирование. 2013. № 2. С. 12–19. DOI: 10.7256/2306-4196.2013.2.8300. URL: http://e-notabene.ru/kp/article_8300.html

УДК 004.421
ГРНТИ 28.23.37

ВЫДЕЛЕНИЕ ОПИСАННЫХ ПИКСЕЛЬНЫХ МАСОК ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ НА ОСНОВЕ АРХИТЕКТУРЫ U-NET

П. А. Арепьев, Е. В. Каляшов, А. А. Савельева, А. В. Тарлыков

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

В статье рассмотрен процесс построения и оптимизации сети для выделения описанных вокруг объекта масок различной формы – круглых, прямоугольных, в форме описывающего многоугольника. Рассмотрены вопросы генерации данных для обучения сети и доработки архитектуры сети для работы с объектами разного масштаба. Приведены результаты работы на модельном примере.

свёрточная нейронная сеть, u-net, обучение, маски, подготовка данных.

В работе рассматривается вопрос построения с использованием свёрточной нейронной сети пиксельных масок определённой формы, описанных вокруг типового объекта – летательного аппарата. Соответственно сети приходится решать одновременно две задачи – поиск типового объекта на изображении и построение вокруг него соответствующей маски. Использование в качестве типового объекта летательных аппаратов ведёт к определённым сложностям, связанным с большим набором масштабов, а также возможных проекций и ориентаций летательных аппаратов на изображении. Для решения указанной проблемы с использованием нейронной сети необходимо подготовить большой набор обучающих данных, включающий проекции летательных аппаратов в максимально возможном диапазоне ориентаций

и масштабов. Также актуальным становится вопрос обобщения – возможности нейронной сети абстрагироваться от изображений проекций конкретных летательных аппаратов, использовавшихся в процессе обучения и перенести процесс построения масок на другие типы летательных аппаратов.

Для решения данной задачи в работе использовался специально сгенерированный синтетический набор данных с изображениями проекций летательных аппаратов. Построение подобного набора для обучения сети является практически единственным выходом, так как создание большого набора проекций в ручном режиме (путём фотографирования и разметки данных) является весьма сложной задачей. В ходе построения обучающего набора использовалось специально разработанное программное обеспечение, предназначенное для работы с доступными трёхмерными моделями летательных аппаратов, принимая на вход набор параметров и фалов с моделями, оно обеспечивало построение проекций летательного аппарата в заданном диапазоне углов ориентации и положений в кадре. Также программное обеспечение обеспечивало построение необходимых видов описывающих масок, предназначенных для обучения нейронной сети [1].

В ходе данной работы было использовано три модели летательных аппаратов для обучения сети (A6M2N, B707, F16), для каждой модели было сгенерировано 3000 изображений проекций (всего 9000 изображений) разрешением 1024×768 пикселей. В качестве фоновой подложки было использовано семь сильно отличающихся изображений неба аналогичного разрешения. Сеть обучалась предсказывать следующие типы масок – контурную, описывающий круг и прямоугольник, описывающий многоугольник (рис. 1). В качестве метрики качества (функции подобия) выступал коэффициент Дайса [2]. В процессе обучения использовалась аугментация для изображений (вариации цвета и яркости) объектов и фона (вариации цвета, яркости, геометрические искажения) [3].

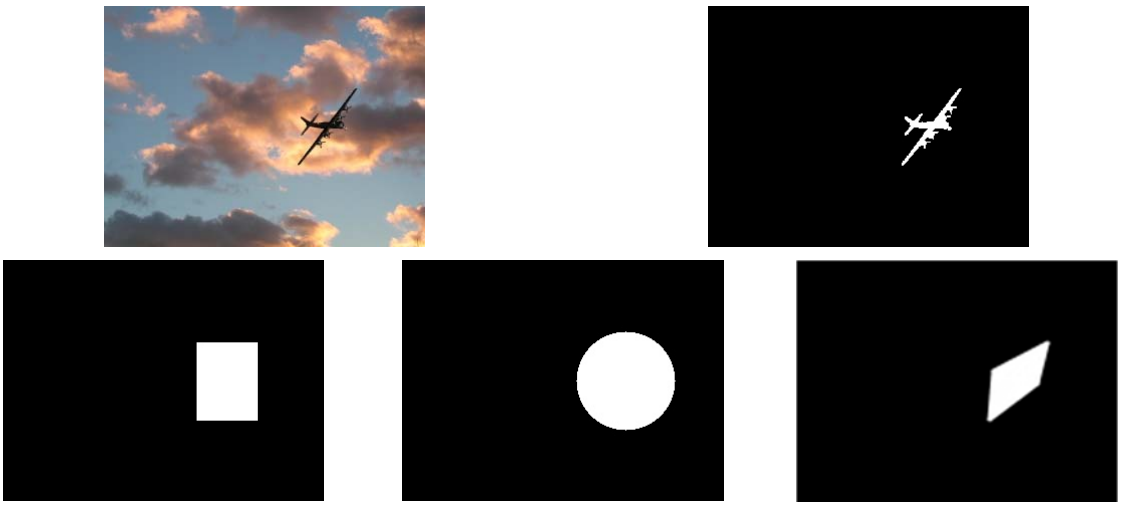


Рис. 1. Пример построенной проекции и набора масок

В качестве первого шага был проведён эксперимент с использованием базовой архитектуры сети U-Net [4], успешно зарекомендовавшей себя для сегментации медицинских изображений. Так как изображения летательных аппаратов характеризуются большой изрезанностью контура проекций, для улучшения качества обучения было решено доработать архитектуру сети для работы с изображениями высокого разрешения – 1024×768 пикселей (предварительные эксперименты показали существенное снижение результатов сегментирования при снижении разрешения исходных изображений).

Для тестирования обученной сети был подготовлен набор, состоящий из 180 изображений (60 изображений на каждую модель летательного аппарата). Результаты тестирования приведены в таблице 1.

ТАБЛИЦА 1. Качество сегментирования (значение коэффициента Дайса)

Вид маски	Среднее	Минимальное	Максимальное
Контур	0,923	0,772	0,971
Многоугольник	0,959	0,852	0,984
Прямоугольник	0,937	0,655	0,984
Круг	0,915	0,536	0,970

Можно отметить большой разброс минимальных и максимальных значений функции подобия на тестовом наборе. Детальный анализ результатов показал, что минимальные значения функции подобия для контурных масок наблюдались в случае малых размеров проекций моделей. Данный результат понятен, учитывая, что при малой площади предсказанной маски даже небольшие абсолютные отклонения в предсказаниях дают значительные относительные ошибки (коэффициент Дайса). Для случая же остальных видов масок, наоборот, худшие значения соответствовали большим размерам проекций (рис. 2).

а) б) в) г)

Рис. 2. Пример результата сегментации с использованием базовой архитектуры сети, виды масок: а) контурная, б) многоугольник, в) прямоугольник, г) круг

Подобное поведение сети можно объяснить ограниченной глубиной базовой сети, которая не позволяет эффективно выделять признаки для объектов крупного масштаба, и предсказания описывающих масок (круговой и прямоугольника) значительно ухудшаются для случаев крупных изображений объекта. Пример подобного поведения сети можно увидеть на рис. 3.

Рис. 3. Ошибки предсказания базовой сети для разных масштабов

Для решения проблемы с высоким значением ошибки и улучшения способностей сети к сегментации различных типов масок была произведена доработка сети – увеличена глубина (части энкодера и декодера) с 4 до 6 слоёв с постепенным уменьшением разрешения. Необходимо отметить, что суммарный размер параметров доработанной модели увеличился в несколько раз и составил примерно 90 Мб. Для тестирования доработанной версии сети использовался тот же набор изображений, что и в случае начальной версии. Результаты тестирования приведены в таблице 2. Сравнение среднего значения функции подобия (к-та Дайса) для исходной и доработанной сетей приведено на рис. 4.

ТАБЛИЦА 2. Качество сегментирования доработанной сетью

Вид маски	Среднее	Минимальное	Максимальное
Контур	0,922	0,752	0,971
Многоугольник	0,966	0,849	0,989
Прямоугольник	0,980	0,864	0,995
Круг	0,957	0,789	0,988

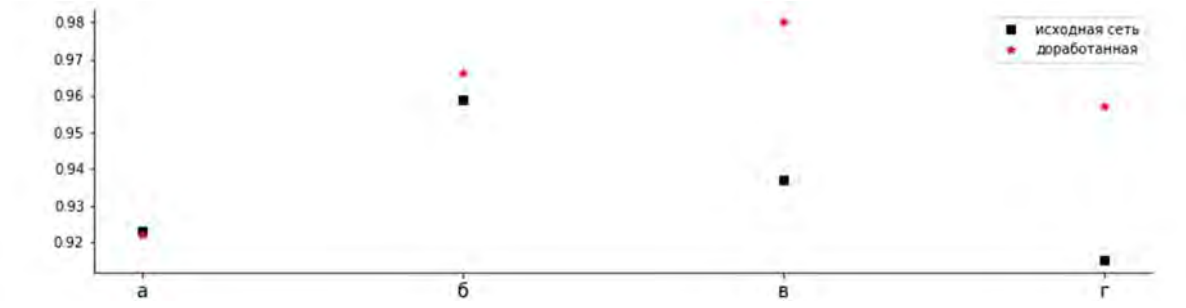


Рис. 4. Качество (к-т Дайса) построенной маски для исходной и доработанной сетей, точки: а – контурная, б – многоугольная, в – прямоугольная, г – круглая маски

Можно отметить, что качество нахождения контура объекта у доработанной сети осталось на уровне базовой сети, однако качество выделения остальных типов масок существенно выросло. Пример с результатами работы доработанной сети представлены на рис. 5, все изображения соответствуют приведённым на рис. 2 (полученным с использованием базовой сети).

а) б) в) г)

Рис. 5. Результат сегментации с использованием доработанной архитектуры сети, виды масок: а) контурная, б) многоугольник, в) прямоугольник, г) круг

Таким образом, можно сделать вывод, что нейронные сети, использующие даже базовую архитектуру U-Net, являются эффективным средством сегментации изображений. Однако для достижения оптимального результата в случаях разномасштабных объектов и такого усложнения задачи, как построение описывающих масок, может потребоваться доработка и модификация архитектуры. Также важно заметить, что существенное влияние на качество сегментации оказывает разрешение входных данных.

Список используемых источников

1. Каляшов Е. В., Савельева А. А., Тарлыков А. В. Использование синтетических данных для обучения нейронной сети классификации летательных аппаратов // 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. 432–437.

2. Sørensen–Dice_coefficient [Электронный ресурс] // Электрон. дан. 2018. URL: https://en.wikipedia.org/wiki/Sørensen–Dice_coefficient, свободный. Загл. с экрана. Яз. англ.

3. Aysegul Dundar, Ignacio Garcia-Dorado. Context Augmentation for Convolutional Neural Networks [Электронный ресурс] // Электрон. текстовые дан. 2017. URL: https://arxiv.org/abs/1712.01653, свободный. Загл. с экрана. Яз. англ.

4. Olaf Ronneberger, Philipp Fischer, Thomas Brox. U-Net: Convolutional Networks for Biomedical Image Segmentation [Электронный ресурс] // Электрон. текстовые дан. 2015. URL: https://arxiv.org/abs/1505.04597, свободный. Загл. с экрана. Яз. англ.

Статья представлена проректором по информатизации СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 28.23.37

ОЦЕНКА СПОСОБНОСТИ К ОБОБЩЕНИЮ НЕЙРОННОЙ СЕТИ СЕГМЕНТАЦИИ ЛЕТАТЕЛЬНЫХ АППАРАТОВ, ОБУЧЕННОЙ НА ОГРАНИЧЕННОМ НАБОРЕ СИНТЕТИЧЕСКИХ ДАННЫХ

П. А. Арепьев, Е. В. Каляшов, А. В. Тарлыков, А. А. Швидкий

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

В статье исследуется вопрос применимости свёрточной сети, обученной на ограниченном наборе синтетических данных, для сегментации реальных объектов поверх различных фонов. Представлены методы генерации данных для обучения сети. Рассмотрен вариант подготовки обучающих данных с использованием самой сети. Приведены результаты тестирования сети на модельном примере.

свёрточная нейронная сеть, обучение, подготовка данных.

В ходе работы исследуется задача использования свёрточной нейронной сети, обученной сегментации объектов с использованием набора данных ограниченного объёма, для сегментации других объектов близкого типа. В качестве объектов для сегментации выступали изображения летательных аппаратов на фоне небосвода. Для получения обучающего набора данных необходимого объёма было использовано специальное программное обеспечение, предназначенное для построения проекций трёхмерных моделей и наложения их на необходимые фоновые изображения [1]. Использование подготовленного таким образом обучающего набора данных является неизбежным следствием невозможности нахождения в открытом доступе массивов данных требуемого вида.

Для построения нейронной сети использовалась архитектура U-Net [2]. Базовая архитектура была доработана для поддержки изображений необходимого разрешения, также сеть была расширена – добавлены два слоя для улучшения выделения объектов крупного масштаба. Для начального обучения нейронной сети было использованы следующие типы моделей летательных аппаратов – A6M2N, B707, F16. Для построения основного набора обучающих данных было сгенерировано 9000 проекций указанных выше моделей (3000 проекций для каждой), использовавшееся разрешение изображений – 1024×768 пикселей. В качестве фонов для наложения проекций было использовано семь фотографий неба, изображения были также

приведены к разрешению 1024×768 пикселей, все фоновые изображения подвергались аугментации [3] – вертикальным и горизонтальным отражениям, масштабированию, модификациям цветового тона и насыщенности. В процессе обучения сети ставилась задача предсказывать контурную маску объекта. Точность предсказания оценивалась с использованием коэффициента Дайса [4].

В ходе тестирования сети использовались два набора данных: основной тестовый набор – изображения проекций для исходных объектов (A6M2N, B707, F16) и дополнительный – для объектов B29, F4u1, FW3FL. В качестве фонов для построения тестовых наборов выступали семь исходных фонов из основного обучающего набора и дополнительный набор из семи альтернативных изображений. Для оценки способности сети к обобщению сравнивались результаты сегментирования на исходном и дополнительном наборах объектов, фоновые изображения также варьировались. Результаты сегментирования основного набора объектов и фонов приведены в таблице 1. Пример сегментации изображений с наложенной полупрозрачной маской приведён на рис. 1.

ТАБЛИЦА 1. Качество сегментирования на исходном наборе объектов и фонов

Тип объекта	Среднее	Минимальное	Максимальное
A6M2N	0,922	0,836	0,967
B707	0,918	0,820	0,959
F16	0,927	0,752	0.971

Рис. 1. Сегментация объектов исходного набора

Для определения влияния фона на успешность сегментации использовались изображения объектов основного набора, но с наложением на дополнительный набор фонов. Сравнительные результаты приведены в таблице 2.

Можно отметить, что качество сегментации практически не изменилось при замене фоновых изображений, что говорит о возможности использования сети для функционирования в незнакомом окружении. Примеры сегментации можно видеть на рис. 2.

ТАБЛИЦА 2. Сегментирование исходного набора на новых фонах (к-т Дайса)

Тип объекта	Среднее	Минимальное	Максимальное
A6M2N	0,919	0,838	0,972
B707	0,924	0,857	0,967
F16	0,927	0,779	0,970

Рис. 2. Примеры сегментации объектов основного набора поверх фонов из дополнительного набора

Возможность сети сегментировать неизвестные ей объекты оценивалась с использованием дополнительного набора моделей (B29, F4u1, FW3FL) и, одновременно, дополнительного набора фоновых изображений. Данные по качеству сегментации сведены в таблицу 3, примеры сегментации представлены на рис. 3.

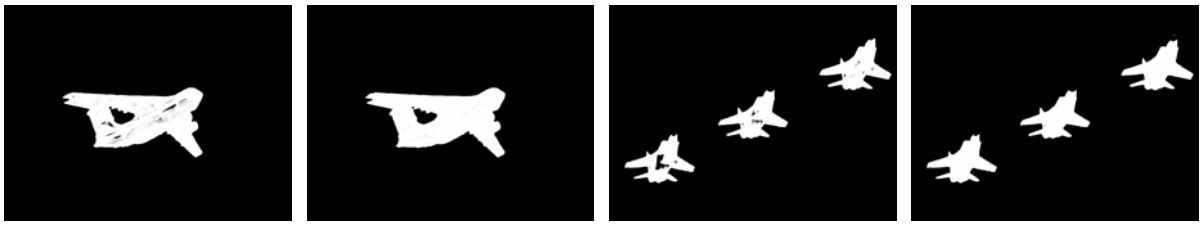
ТАБЛИЦА 2. Сегментирование дополнительного набора объектов на дополнительном наборе фонов (к-т Дайса)

Тип объекта	Среднее	Минимальное	Максимальное
B29	0,902	0,824	0,958
F4u1	0,920	0,852	0,971
FW3FL	0,924	0,818	0,965

Рис. 3. Примеры сегментации тестовых изображений неизвестных сети моделей с использованием второго набора фоновых изображений

В данном случае качество сегментации незначительно ухудшилось, но осталось в приемлемых рамках, что говорит о достаточно высокой обобщающей способности сети.

Дополнительно в ходе работы был проведён эксперимент по сегментации объектов неизвестного типа (не участвовавшего в процессе обучения) на изображениях видеопотока с низким уровнем чёткости и неизвестным фоном. Начальный вариант обученной сети показал способность находить объекты, но качество предсказанных масок оказалось невысоким, с рваными пробелами, что связано с низким качество исходных изображений и их низким контрастом. Тем не менее, за счёт хорошей обобщающей способности исходной сети, небольшое дообучение позволило решить данную проблему – была отобрана часть корректно предсказанных сетью масок и сеть была дообучена на изображениях с этими же масками. Подобное дообучение позволяло существенно улучшить предсказание для всего набора изображений видеопотока. Изменение предсказанных масок после дополнительного обучения сети приведены на рис. 4.



а) б) в) г)

Рис. 4. Качество сегментации первичным вариантом сети – а), в) и после дополнительного обучения – б), г)

Подводя итог, можно отметить, что свёрточные нейронные сети, используемые для сегментации изображений, обладают значительными обобщающими способностями. Данное свойство позволяет использовать для обучения сети генерируемые синтетические изображения с ограниченным наборами трёхмерных моделей и фоновых изображений. В дальнейшем сеть способна выделять широкий круг объектов на искусственных и естественных изображениях. В случае низкого качества входных данных сеть может быть достаточно легко дообучена под конкретную задачу с помощью обучающего набора, генерируемого самой сетью, в результате качество сегментации повышается. С подобным подходом устраняется необходимость в получении труднодоступных фото и видеоматериалов с качественной разметкой.

Список используемых источников

1. Каляшов Е. В., Савельева А. А., Тарлыков А. В. Использование синтетических данных для обучения нейронной сети классификации летательных аппаратов // 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.432–437.

2. Olaf Ronneberger, Philipp Fischer, Thomas Brox. U-Net: Convolutional Networks for Biomedical Image Segmentation [Электронный ресурс] // Электрон. текстовые дан. 2015. URL: https://arxiv.org/abs/1505.04597, свободный. Загл. с экрана. Яз. англ.

3. Aysegul Dundar, Ignacio Garcia-Dorado. Context Augmentation for Convolutional Neural Networks [Электронный ресурс] // Электрон. текстовые дан. 2017. URL: https://arxiv.org/abs/1712.01653, свободный. Загл. с экрана. Яз. англ.

4. Sørensen–Dice_coefficient [Электронный ресурс] // Электрон. дан. 2018. URL: https://en.wikipedia.org/wiki/Sørensen–Dice_coefficient, свободный. Загл. с экрана. Яз. англ.

Статья представлена проректором по информатизации СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 621.39, 654.739
ГРНТИ 49.33.29, 49.33.33

МОДЕЛЬ ОЦЕНКИ ВРЕМЕНИ ДОСТАВКИ ДАННЫХ В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ

Т. Н. Астахова[1], Д. М. Воробьева[2], М. О. Колбанёв[3], А. А. Шамин[1]

[1]Нижегородский государственный инженерно-экономический университет
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Изучение способов экономии энергии отдельными устройствами для увеличения времени их функционирования беспроводных сенсорных сетей без перезаряда батареи является одной из первостепенных задач. В работе построена модель для оценки вероятности времени доставки сообщений, что позволяет повысить точность оценок качества функционирования беспроводной сенсорной сети.

беспроводная сенсорная сеть, вероятностно-энергетические характеристики, время доставки сообщений, мощность сигнала на передающей антенне.

К числу наиболее актуальных направлений исследования беспроводных сенсорных сетей относится изучение способов экономии энергии отдельными устройствами для увеличения времени их функционирования без перезаряда батареи [1].

В фиксированных сетях связи, использующих системы с центральной батареей, связность узлов сети обусловлена топологией сети, т. е. способом соединения сетевых элементов друг с другом. Передача данных между стационарно расположенными терминалами обеспечивается здесь оконечными станциями и транзитными узлами и может быть блокирована только в случае перегрузки сети или отказа ее элементов:

– разрывы соединений в моменты окончания запаса энергии батареи одного из сетевых элементов;

– невозможность установления соединений из-за ограниченной мощности сигнала на передающей антенне сенсорного устройства и слишком больших расстояний от него до соседних сетевых элементов.

Связность, как показатель качества функционирования беспроводной сенсорной сети, представляет собой обобщение другой характеристики беспроводной сенсорной сети – времени жизни сети, под которой понимают интервал времени с момента запуска сети в эксплуатацию до момента разряда батареи у любого из сетевых устройств с автономным питанием [2]. Время жизни сети можно рассматривать как частный случай связности, когда прерывается информационное взаимодействие с одним из сетевых устройств. Связность сети, в отличие от времени жизни сети, характеризует сеть в целом, а не свойства ее отдельных элементов. Она дает возможность исследовать как процессы задержки и блокировки информационного обмена из-за недостаточной мощности радиопередатчика, так и процессы функционирования сети при восстановлении энергопитания сетевых элементов, временно прекративших свою работу. Каждое сенсорное устройство нуждается в энергии электрической батареи, главным потребителем которой оказывается радиопередатчик.

Рассматривается беспроводная сенсорная сеть, в которой все сенсорные узлы разделены по какому-либо принципу на группы или кластеры. Принципы разделения устройств на группы могут быть различными: географические координаты, типы сенсоров, уровни энергопотребления, емкости электрических батарей и пр. В каждом кластере одно из сенсорных устройств выполняет роль головного кластерного узла [3]. Предположим, что сенсорные устройства образуют сенсорное поле точек, распределенных на плоскости по закону Пуассона, и имеется возможность передавать блоки данных от сенсорных устройств через дополнительные транзитные узлы. Также будем предполагать, что мощность, которую использует сенсорный узел при передаче данных, ограничена величиной $P_{\text{пер}}$, и что каждое сенсорное устройство знает направление для передачи блока данных к головному

узлу. Дополнительно предположим, что сенсорное устройство расположено в центре круга, и что в этом круге можно выделить сектор, ориентированный в направлении головного кластерного узла.

Согласно вышеуказанным предположениям среднее время доставки блока данных T [с] от сенсорного до головного кластерного узла определяется из следующего соотношения:

$$T = \frac{e^{\frac{1}{4}A^2 P_{\text{пер}} \alpha\lambda}\left(\sqrt{\pi}\ \text{erf}\left(\frac{1}{2}A\sqrt{\alpha\lambda}\sqrt{P_{\text{пер}}}\right)A\sqrt{\alpha\lambda}\sqrt{P_{\text{пер}}} + 2e^{-\frac{1}{4}A^2 P_{\text{пер}}\alpha\lambda}\right)}{e^{\frac{1}{4}A^2 P_{\text{пер}}\alpha\lambda}\sqrt{\pi}\ \text{erf}\left(\frac{1}{2}A\sqrt{\alpha\lambda}\sqrt{P_{\text{пер}}}\right)A\sqrt{\alpha\lambda}\sqrt{P_{\text{пер}}} - 2e^{\frac{1}{2}A^2 P_{\text{пер}}\alpha\lambda} + 2} t,$$

где $A = \frac{\gamma}{4\pi\sqrt{P_{\text{пр}}}}\sqrt{C_{\text{пер}} C_{\text{пр}}}$, $C_{\text{пер}}$ – коэффициент усиления передающей антенны, $C_{\text{пр}}$ – коэффициент усиления приёмной антенны, $P_{\text{пр}}$ [Вт] – мощность радиосигнала на принимаемой антенне, γ [м] – длина волны передаваемого радиосигнала, α [рад] – угол сектора в радианах, r [м] – радиус круга (определяется по формуле Фрииса [4], в пределах которого может вестись продуктивная передача блока данных от сенсорного устройства транзитному узлу), λ – плотность размещения сенсорных узлов на поле точек, $\text{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2} dt$ – функция ошибок.

На рис. 1 представлена зависимость среднего времени доставки от потребляемой мощности передающей антенны $P_{\text{пер}}$.

Построена модель для оценки вероятности времени доставки сообщений, учитывающая мощность сигнала на выходной антенне, взаимное расположение сенсорного устройства и головной станции, и другие параметры, что позволяет повысить точность оценок качества функционирования беспроводной сенсорной сети.

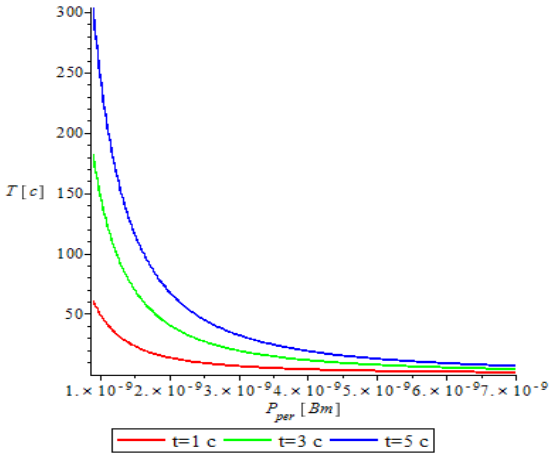


Рисунок. Зависимость среднего времени доставки от мощности радиопередатчика $P_{\text{пер}}$ при фиксированном t

Список используемых источников

1. Верзун Н. А., Колбанёв М. О., Шамин А. А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях // Информационные технологии и телекоммуникации. 2017. № 1. С. 88–96.

2. Ерохин С. Д., Махров С. С. Протоколы маршрутизации в беспроводных сенсорных сетях: основанные на местоположении узлов и направленные на агрегацию данных // T-Comm – Телекоммуникации и Транспорт. 2013. № 3. С. 44–47.

3. Кучерявый А. Е., Салим А. Выбор головного узла кластера в однородной беспроводной сенсорной сети // Электросвязь. 2009. № 8. С. 32–36.

4. Уоллес Р. Максимальная дальность связи по радиоканалу в системе: как этого добиться? // Новости электроники. 2015. № 11. С. 3–13.

УДК 621.39, 654.739
ГРНТИ 49.33.29, 49.33.33

ХАРАКТЕРИСТИКИ ЭНЕРГОПОТРЕБЛЕНИЯ УМНЫХ ВЕЩЕЙ

Т. Н. Астахова[1], Д. М. Воробьева[2], М. О. Колбанев[3], А. А. Шамин[1]

[1]Нижегородский государственный инженерно-экономический университет
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

В статье исследуются вероятностно-энергетические характеристики, которые зависят от пространственных параметров сети и технических характеристик сенсорных устройств, позволяющие определять взаимную зависимость энергетических и информационных параметров, а также предоставляющие возможность оценки времени жизни сенсорной сети.

вероятностно-энергетические характеристики, беспроводная сенсорная сеть, мощность радиосигнала, плотность распределения, пуассоновское поле точек, распределение, топология сети, умные вещи, энергоэффективность передачи.

Рассматривается интернет вещей, терминалы которого – умные вещи или сенсорные устройства – имеют автономное питание и взаимодействуют друг с другом через эфирные сети [1, 2]. Увеличение времени жизни сети такого типа прямо зависит от экономии заряда аккумуляторов сенсорных устройств, а главным потребителем энергии аккумуляторов являются радиопередатчики, которым на передачу одного бита требуется примерно в миллион раз больше энергии, чем при обработке этого бита в микропроцессоре.

Совокупные затраты электроэнергии в сети зависят не только от интенсивности информационного взаимодействия терминалов, но и от плотности умных вещей в сенсорном поле и критерия выбора транзитного узла протоколами маршрутизации.

Моделью сенсорного поля выбрано поле точек, которые случайным образом распределены в пространстве, а основной характеристикой – плотность поля, измеряемая средним числом точек, находящихся на единице площади (объема). Предполагается, что рассматриваемое сенсорное поле состоит из однородных сенсоров, у которых:

– вероятность появления того или иного числа точек в любой области плоскости (пространства) не зависит от того, сколько точек попало в любые области, не пересекающиеся с данной;

– вероятность попадания в элементарную область двух или более точек пренебрежимо мала по сравнению с вероятностью попадания одной точки.

Такое сенсорное поле можно описать пуассоновским полем точек.

Для указанных условий получены функции распределения вероятности случайной величины мощности излучающей антенны сенсорного устройства, достаточной для передачи блока данных на приемную сторону, и общего энергопотребления устройств этой сети при информационном взаимодействии.

Согласно применяемым протоколам маршрутизации всепроникающих сенсорных сетей возможны различные варианты ретрансляции блоков данных при передаче от умной вещи к базовой станции: первому, второму и так далее «соседу» (рис. 1).

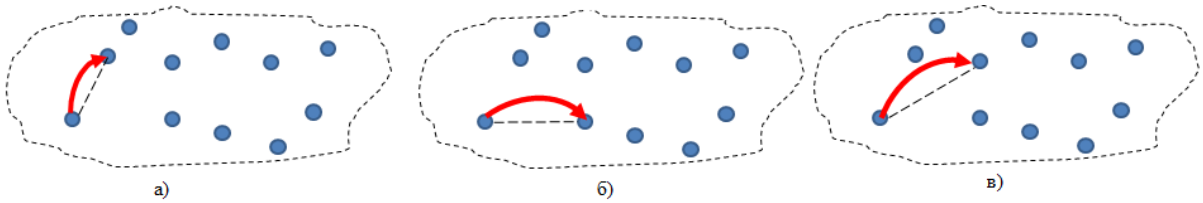


Рис. 1. Возможные варианты ретрансляций блоков данных:
через ближайшую (а); вторую (б), третью (в) умную вещь

В работе построена математическая модель физического процесса информационного взаимодействия в ББС в случае пуассоновского поля точек (сенсорных узлов) и для различных вариантов ретрансляций блоков данных – первому, второму и четвертому соседу [3, 4, 5].

Выражение для расчета средней энергии, затрачиваемой на передачу блока данных ближайшему объекту, второму и четвертому сенсорному узлу, соответственно:

$$\overline{e_1} = \frac{2P_{\text{пр}}\pi^2 f\lambda b\left(\left\lceil R\sqrt{\nu}\right\rceil + 1\right)}{\nu\, \mathrm{C}_{\text{пр}}\mathrm{C}_{\text{пер}}{v_c}^2},$$

$$\overline{e_2} = \frac{9P_{\text{пр}}\pi^2 f\lambda b\left(\left\lceil\frac{2}{3}R\sqrt{\nu}\right\rceil + 1\right)}{2\,\nu\,\mathrm{C}_{\text{пр}}\mathrm{C}_{\text{пер}}{v_c}^2},$$

и

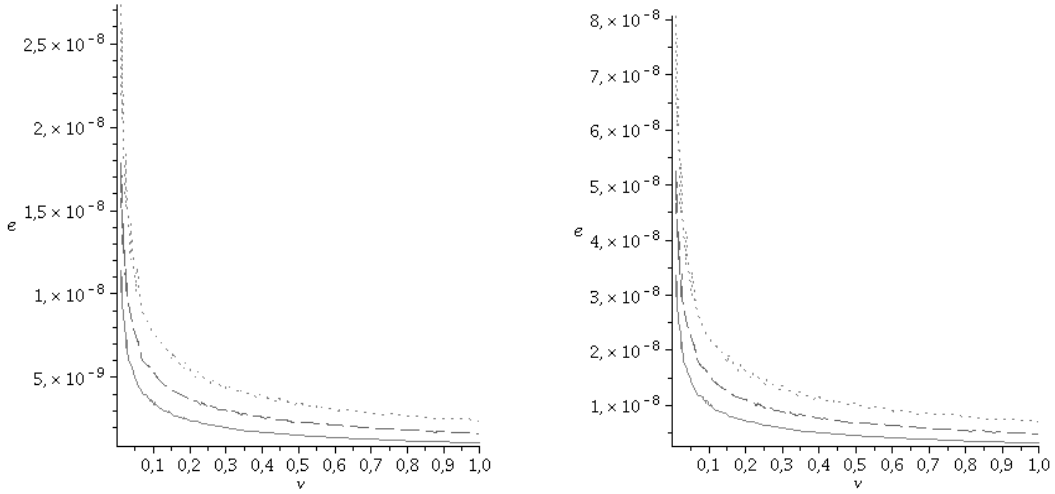
$$\overline{e_4} = \frac{1225\cdot P_{\text{пр}}\pi^2 f\lambda b\left(\left\lceil\frac{16}{35}R\sqrt{\nu}\right\rceil + 1\right)}{128\cdot\nu\,\mathrm{C}_{\text{пр}}\mathrm{C}_{\text{пер}}{v_c}^2},$$

где $P_{\text{пр}}$ [Вт] – мощность радиосигнала на принимаемой антенне, f [Гц]–частота радиосигнала, λ [блок/с] – интенсивность передачи блоков, b [бит] – длина передаваемых блоков, v_c [м/с] – скорость света, $C_{\text{пер}}$ – коэффициент усиления передающей антенны, $C_{\text{пр}}$ – коэффициент усиления приёмной антенны, R [м] – радиус круга, в пределах которого может вестись продуктивная передача блока данных от сенсорного устройства транзитному узлу, ν [1/м^2] – плотность размещения сенсорных узлов на поле точек.

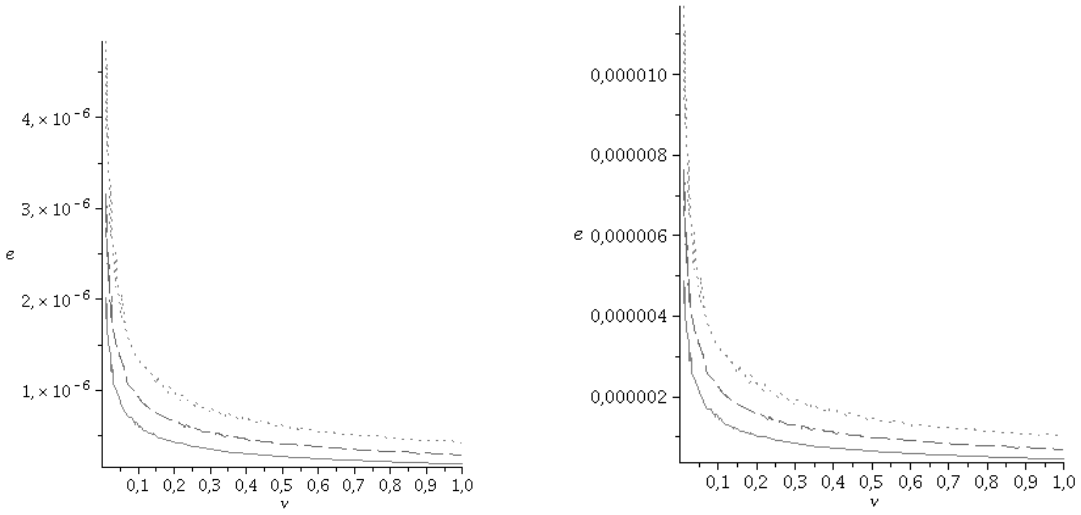
Применяя вышеприведенные выражения, проведем численный расчет и анализ влияния параметров рассматриваемой беспроводной сенсорной сети и умных вещей на требуемую мощность радиосигнала на передающей антенне объекта беспроводной сенсорной сети.

На рис. 2 представлена зависимость энергопотребления от плотности распределения умных вещей на плоскости при разных вариантах передачи для различных значений частот сигнала.

На рисунке 3 показано влияние длины передаваемых блоков на энергопотребление одним сенсорным устройством при значениях частоты сигнала $f = 13{,}56\cdot10^6$ Гц и интенсивности передаваемых блоков λ = 1 блок/с при плотности распределения узлов ν = 0,01 1/м^2.

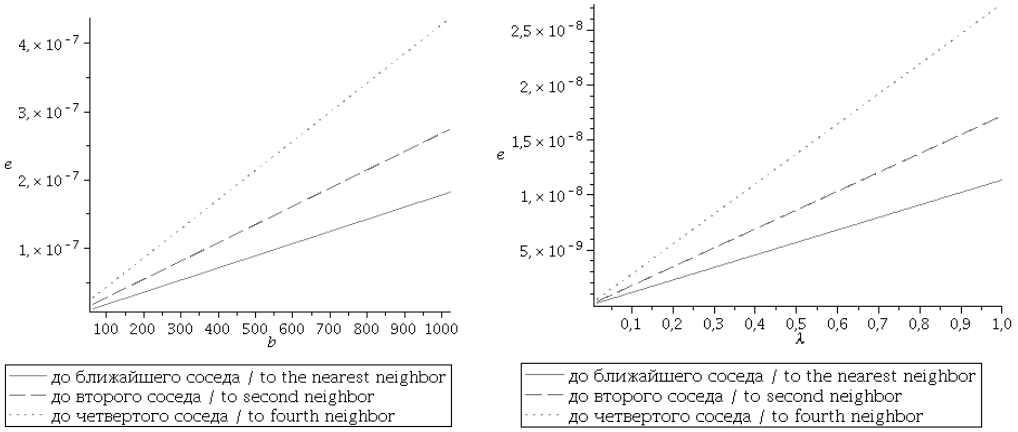


а) б)



в) г)

Рис. 2. Зависимость энергопотребление от плотности умных вещей при значениях частот сигнала: а) f =13,56·10^6 Гц; б) f =40·10^6 Гц; в) f =2,4·10^9 Гц; г) f =5,8·10^9 Гц



а) б)

Рис. 3. Зависимость энергопотребление от: а) длины передаваемых блоков; б) интенсивности появления блоков

Исследование позволило определить взаимную зависимость энергетических и информационных параметров сенсорной сети. Построенная модель позволит оценить время жизни сенсорной сети. Эффективным инструментом энергосбережения сети являются параметры протоколов уровня сети, которые зависят, в частности, от распределения сенсорных устройств в пространстве.

Список используемых источников

1. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions // Future generation computer systems. 2013. Vol. 29. No 7. PP. 1645–1660.

2. Atzori L., Iera A., Morabito G. The internet of things: A survey // Computer networks. 2010. Vol. 54. No 15. PP. 2787–2805.

3. Верзун Н. А., Колбанёв М. О., Шамин А. А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях // Информационные технологии и телекоммуникации. 2017. № 1. С. 88–96.

4. Астахова Т. Н., Колбанев М. О., Шамин А. А. Обеспечение энергоэффективности интернета вещей // Региональная информатика и информационная безопасность. 2018. С. 203–204.

5. Уоллес Р. Максимальная дальность связи по радиоканалу в системе: как этого добиться? // Новости электроники. 2015. № 11. С. 3–13.

УДК 004.852
ГРНТИ 28.23.29

ПОДХОД К ОБНАРУЖЕНИЮ АТАК ТИПА DENIAL-OF-SLEEP В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

А. В. Балуева[1,2], В. А. Десницкий[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В работе анализируются возможные виды атак в области информационной безопасности киберфизических систем и проведен анализ имеющейся литературы в предметной области. Рассматривается проблема уязвимости устройств беспроводных сетей Интернета вещей атакам, направленным на истощение энергоресурсов. Рассмотрено несколько видов трафика и проведен визуальный анализ нормального и атакующего трафика. Предложен подход к обнаружению атак истощения энергоресурсов в киберфизических системах на основе методов машинного обучения. Действенность предлагаемого решения подтверждается на примере задачи выявления атакующего трафика с использованием языка Python и дистрибутива Anaconda.

информационная безопасность, атаки истощения энергоресурсов, анализ, Интернет вещей, киберфизические системы, машинное обучение.

В настоящее время атаки на беспроводные сети Интернета вещей приобретают все большее значение. Атаки истощения энергоресурсов, которые способны в кратчайшее время исчерпать заряд батареи устройства, в особенности представляют значительную угрозу, так как являются достаточно скрытными, как для систем мониторинга защищенности, так и для самого

объекта, а также при исчерпании всех энергоресурсов гарантированно нарушают работоспособность устройства и его доступность.

Атаки истощения энергоресурсов, как правило, довольно легко осуществимы, так как порой нарушителю достаточно обладать минимальными программными и аппаратными средствами, навыками программирования и работы с микроконтроллерами или другим базовым телекоммуникационным оборудованием.

Также основная особенность такого рода атак – сложность их обнаружения, поскольку на атакуемое устройство, как правило, воздействуют через сеть Интернет или дистанционно при помощи серий ложных запросов. Также сложность состоит в том, что не все цепочки ложных запросов можно однозначно идентифицировать как атакующие, поскольку разрядка батареи может быть связана с легитимными действиями пользователя. Помимо этого, чтобы отслеживать атаки истощения энергоресурсов целесообразно фиксировать изменения скорости зарядки, а не только процесса разряда батареи.

В настоящее время выделяются четыре класса атак истощения энергоресурсов [1]. К первому классу относится принудительный вывод устройств из режима пониженного энергопотребления (сна). Атаки второго класса осуществляются путём увеличения объема входящего или исходящего трафика. Третий класс представляет собой создание электромагнитных помех на беспроводных каналах передачи данных, таким образом устройства вынуждены генерировать сигнал повышенной мощности для передачи данных. К последнему, четвертому классу, относится нештатное использование программного обеспечения устройств, множественный запуск приложений и различные нарушения встроенных программно-аппаратных оптимизаций.

В настоящей статье анализируются существующие работы предметной области, предлагается автоматизированное определение атакующего трафика с помощью методов машинного обучения на языке Pythonc помощью дистрибутива Anaconda, а также проводятся эксперименты.

В [2] предлагаются меры профилактики против некоторых видов Denial-of-Sleep атак – описаны несколько возможных видов атак типа Denial-of-Sleep, детально рассматриваются некоторые сценарии атак, а также приведено описание существующих решений борьбы с атаками подобного типа. Также приводятся особенности этих решений и сравнение их ключевых характеристик.

В [3] предлагается простой алгоритм, который обнаруживает и снижает ущерб от Denial-of-Sleep атак. Также проводится моделирование и строится оценка предложенного авторами механизма защиты.

В [4] предлагается более эффективное решение для решения проблемы отказа в спящем режиме путем выделения узлов, которые будут использо-

ваться в иерархической кластеризации. Целью этой исследовательской работы является увеличение времени функционирования сети за счет эффективного сбережения энергоресурса, который потребляется при атаке типа Denial-of-Sleep.

В [5] выявляются уязвимости в современных протоколах управления доступом к среде MAC (*medium access control*), которые делают их восприимчивыми к атакам тип Denial-of-Sleep. Также проводится классификация этих атак с учетом знаний злоумышленником протокола уровня MAC и способности обходить установленные протоколы аутентификации и шифрования. Атаки из каждой категории предложенной классификации смоделированы таким образом, чтобы показать воздействия на четыре текущих разновидностях MAC-протоколов сенсорной сети: S-MAC, T-MAC, B-MAC и G-MAC. Это исследование предоставляет набор механизмов, предназначенных для обнаружения и смягчения последствий атак типа Denial-of-Sleep на сенсорные сети. Набор Clustered Anti-Sleep-Deprivation для сенсорных сетей включает в себя независимый от платформы механизм предотвращения повторного воспроизведения (*anti replay*), адаптивный ограничитель скорости и механизм обнаружения и устранения помех. Эти инструменты предназначены для выборочного или конкретного применения для защиты от атак типа Denial-of-Sleep в зависимости от конкретных уязвимостей в протоколе MAC, используемого в определенной сенсорной сети.

Анализируемый в настоящей работе трафик получен в режиме HIGH и в режиме LOW. Режим LOW характеризуется интервалом между пакетами в 5000 мс с допустимым отклонением +/–500 мс, в то время как режим HIGH – 20000 мс с допустимым отклонением в 2000 мс. Интервал отправления сообщений внутри пакета в режиме LOWсоставляет 500 мс с допустимым отклонением 167 мс, тогда как в режиме HIGH – 2000 мс с допустимым отклонением в 666 мс. Также режим LOW использует в среднем 5 сообщений в пакете с допустимым отклонением +/–2 сообщения, в то время как режим HIGH – 20 сообщений с допустимым отклонением +/–8 сообщений.

Используя оба режима отправления пакетов получается 8 типов трафика, обозначаемого следующим образом: LLL, LLH, LHL, LHH, HLL, HLH, HHL, HHH. В рамках нормального трафика предполагается, что сообщения накапливаются пачками и отправляются через определенные промежутки времени. Трафик нарушителя состоит из исходящего потока сообщений с некоторой фиксированной частотой (то есть без выделения пачек). Таким образом, можно выделить ключевую отличительную характеристику нормального трафика от аномального трафика – сгруппированность его сообщений.

Она выражается в следующих формальных признаках: общее число сообщений (в минуту); отношение максимального интервала между сообщениями и минимального;

Далее представлены графики нормального трафика (рис. 1), атакующего (рис. 2) и случайного (рис. 3), выданные вместе с образцами трафика. По оси *Y* – нормализованное время относительно первого сигнала, по оси *X* – номер сообщения.

Длительность каждого полученного образца трафика – 1 минута. Всего используется 80 образцов трафика. Код для обработки трафика использует нормализованное время (время относительно первого сообщения), рассчитывает количество сообщений в минуту, находит минимальное и максимальное время паузы между передачей пакета и рассчитывает соотношение. На выходе программы – соотношение максимальной и минимальной паузы, количество сообщений в минуту и тип трафика: нормальный или атакующий (рис. 4).

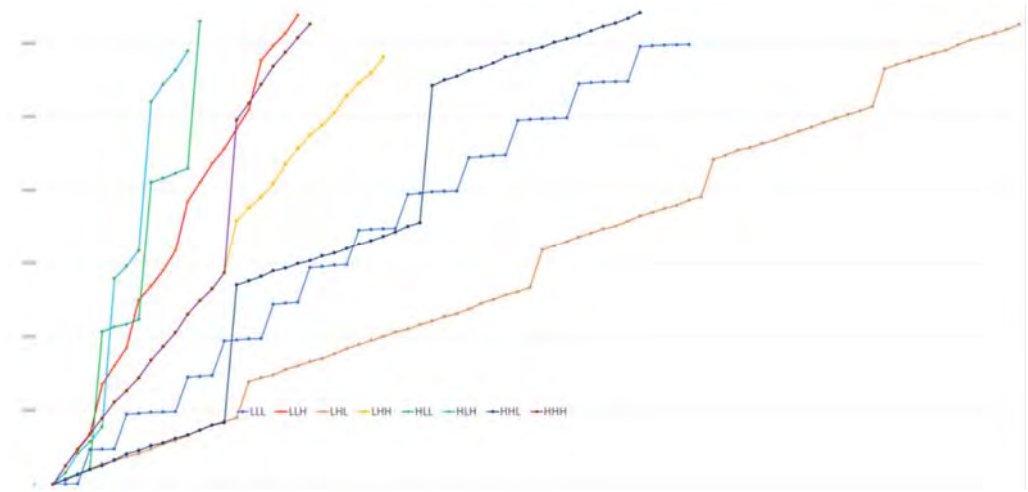


Рис. 1. Нормальный трафик

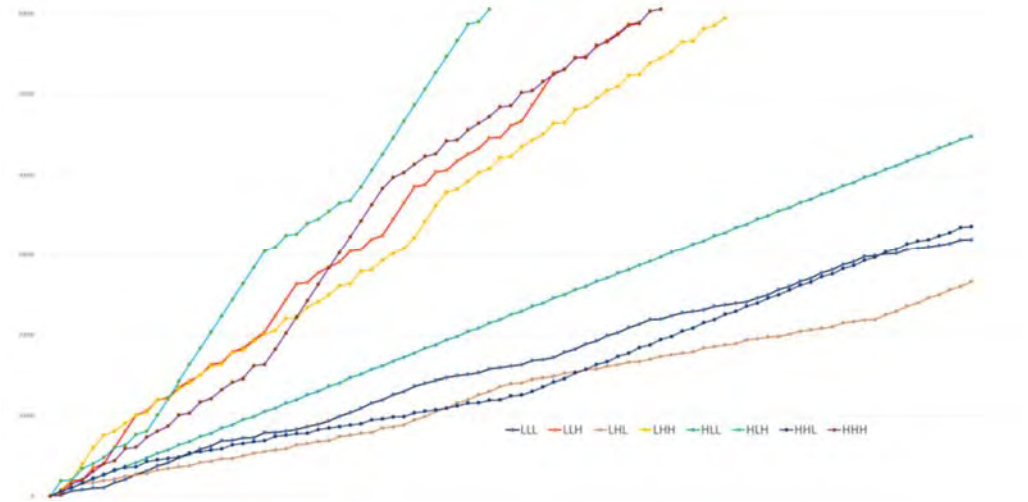


Рис. 2. Атакующий трафик

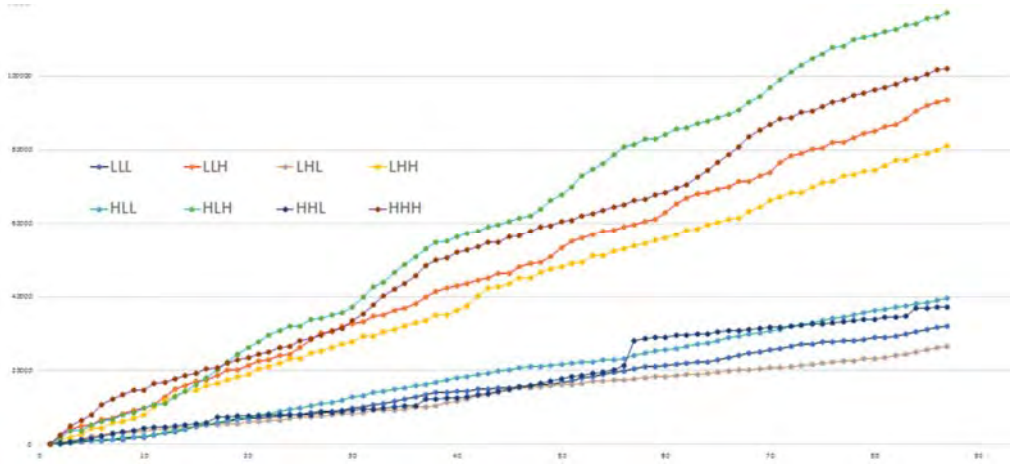


Рис. 3. Случайный трафик

Для обучения был выбран алгоритм KNN (алгоритм ближайших соседей) с параметром K = 10. В качестве обучающей выборки использованы образцы нормального и атакующего трафика, в качестве тестовой – рандомизированный (случайный) трафик (заранее неизвестен). На выходе программа выдаёт результат тестовой выборки (рис. 4). На скриншоте в качестве тестовой выборки был выбран атакующий трафик HHL из образцов случайного трафика (рис. 3), который при визуальном анализе практически не отличается от нормального трафика. По результатам видно, что программа определила тип трафика верно – трафик объявлен атакующим (рис. 5).

```python
import csv
signal = []
_signal = []
curr = 0
# LLL, LLH, LHL, LHH, HLL, HLH, HHL, HHH

filename = 'HHH_random.csv'
raw_data = open(filename, 'rt')
reader = csv.reader(raw_data, delimiter=',', quoting=csv.QUOTE_NONE)
x = list(reader)[1::]
for i in range(len(x)):
    signal = signal + x[i]

_len = int(round(len(signal)/10, 0))
fut = _len
for i in range(0, 10):
    _signal.append(signal[curr:fut])
    curr = curr + _len
    fut = fut + _len

file = open('HHH.csv', 'a')
writer = csv.writer(file)

for i in range(0, len(_signal)):
    _min = int(_signal[i][1]) - int(_signal[i][0])
    _max = int(_signal[i][1]) - int(_signal[i][0])
    for j in range(1, len(_signal[i])):
        m = int(_signal[i][j]) - int(_signal[i][j-1])
        if m < _min:
            _min = m
        elif m > _max:
            _max = m
    corr = round(_max/_min, 1)
    line = str(corr)+','+str(_len)+',\n'
    writer.writerows(line)
file.close()
```

HHH.csv — Блокнот

Файл Правка Формат Вид Справка

```
corr,num,name
16.6,26,normal
17.3,26,normal
15.4,26,normal
16.4,26,normal
16.4,26,normal
16.3,26,normal
16.6,26,normal
17.1,26,normal
16.4,26,normal
16.5,26,normal
60.9,52,attack
64.5,52,attack
62.0,52,attack
32.5,52,attack
44.7,52,attack
48.3,52,attack
66.5,52,attack
44.0,52,attack
27.1,52,attack
47.5,52,attack
63.1,78,
76.2,78,
40.0,78,
28.9,78,
46.3,78,
14.4,78,
```

Рис. 4. Программа для обработки трафика и результат работы

Отметим, что с развитием беспроводных сенсорных сетей датчики приобретают все большее значение в физическом мире. Помимо низкой мощности используемых сенсорных узлов, датчики широко используются для обнаружения температуры, загрязнения, давления и других различных применений. Сенсорные сети с ограниченным энергопотреблением могут подвергаться атакам, которые будут сокращать предполагаемый срок использования устройства и таким образом делать сенсорные сети неработоспособными [6].

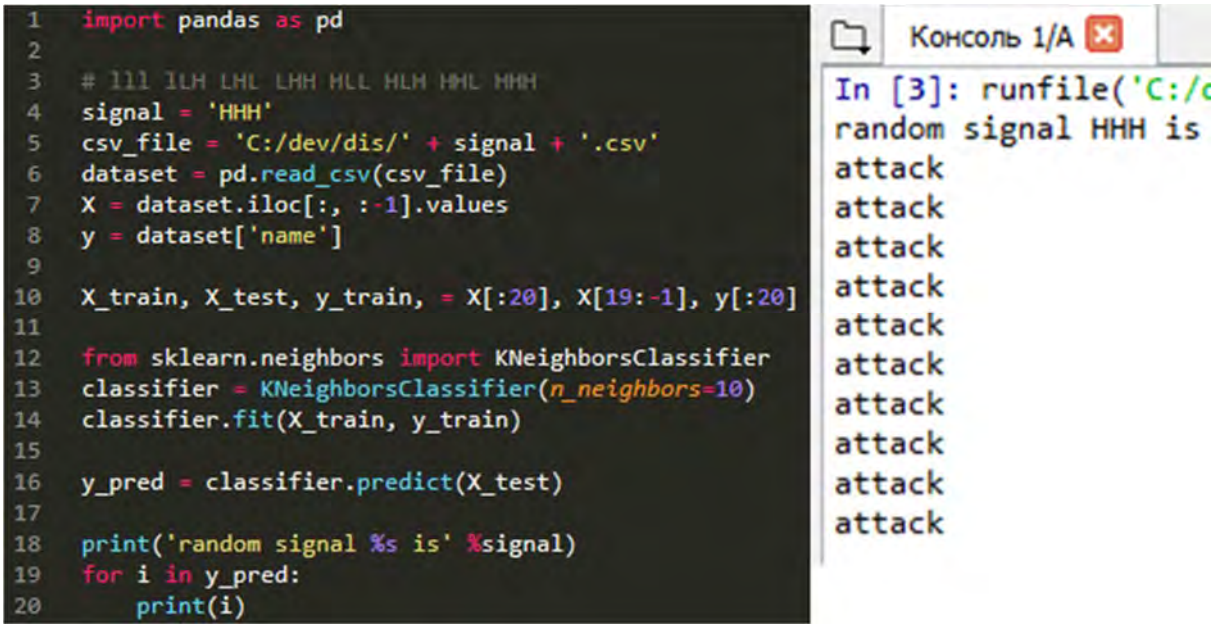


Рис. 5. Программа для определения атакующего трафика и результат работы

Таким образом, в данной статье описывается несколько возможных атак типа Denial-of-Sleep, приводится пример нормального и атакующего трафика, а также приводится фрагмент реализации выявления атакующего трафика на языке Python, где используется метод машинного обучения KNN. По результатам работы, программа верно определяла классификацию сигнала в 70 % случаев.

Работа выполнена при финансовой поддержке Гранта Президента Российской Федерации № МК-5848.2018.9.

Список используемых источников

1. Десницкий В. А., Котенко И. В. Анализ атак истощения энергоресурсов на системы беспроводных устройств // Известия высших учебных заведений. Приборостроение. 2018. Т. 61. № 4. С. 291–297.

2. Kaur S., Ataullah Md., Garg M. Security from Denial of Sleep Attack in Wireless Sensor Network // International Journal of Computers & Technology. 2013. Vol. 4. No. 2. PP. 419–425.

3. Wainis M., Kabalan K., Dandeh R. Denial of Sleep Detection and Mitigation // Latest Trends on Communications. 2014. Vol. 3. No.2. PP. 195–200.

4. Kaur S., Ataullah Md. Securing Wireless Sensor Network from Denial of Sleep Attack by Isolating Nodes // International Journal of Computer Applications. 2014. Vol. 103. No. 1. PP. 29–33.

5. Raymond D. R. Denial-of-Sleep Vulnerabilities and Defenses in Wireless Sensor Network MAC Protocols // Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Engineering. 2008.

6. Десницкий В.А., Котенко И.В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы. 2013. № 1. С. 44–54.

УДК 004.056, 32.019.5
ГРНТИ 81.93.29, 11.25.25

МОНИТОРИНГ ИНФОРМАЦИОННОЙ АКТИВНОСТИ В ПРОСТРАНСТВЕ СОЦИАЛЬНЫХ СЕТЕЙ

Д. Н. Баранова[1], И. Б. Саенко[2], Е В. Смирнов[3]

[1]Информационное агентство GloryStory
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Возможными путями решения задач противодействия вредоносному влиянию в социальных сетях сегодня является конвергенция социогуманитарных и технических наук. Поэтому тогда, когда мы рассматриваем вопросы обнаружения и противодействия противоправной активности, мы исследуем как гуманитарные и технические аспекты. В работе рассматриваются основные методы анализа социальных сетей. Описывается оптимизационный подход муравьиной колонии. Это полиномиальный алгоритм, применимый для нахождения приближенных решений оптимального пути в графе, предложенный еще в 70-х годах XX века американский социологом для анализа сетей.

анализ социальных сетей, социальные графы, муравьиный алгоритм, Ant Colony Optimization, информационная активность, вредоносное влияние.

Введение

Информационной активностью в информационном пространстве социальных сетей является социально-преобразующая деятельность индивида в рамках социальных сетей, которая противостоит социальной пассивности,

характеризуемой полной или частичной утратой интереса к социальной действительности и отказом различных форм участия в ней. В процессе измерения информационной активности, невозможно говорить оценочно об её показателях, так как любые оценки являются субъективными. В связи с этим отсутствует конкретная общепринятая система ее измерения – любая система показателей будет разноплановой для разных видов деятельности, субъектов и социальных групп [1].

Современные социальные сети – не только средство взаимодействия пользователей, но и удобный инструмент для получения данных о субъектах и объектах, присутствующих в них, о том какие связи установлены между пользователями и группами. Используя эти данные и современные возможности анализа, а также системы графического представления данных, можно получить большое количество возможностей для наглядного представления о различных процессах и явлениях. Например, это может быть информация о круге обсуждения определенных тем, о скорости реакции аудитории на те или иные события. Также то, какие темы являются наиболее популярными и охватывающими большее количество пользователей. Это лишь небольшая часть возможностей, которую нам могут представить методы мониторинга информационной активности в информационном пространстве социальных сетей [2, 3].

Главное в социальных сетях – возможность пользователей высказывать свое мнение, и делиться им с окружающими большими группами людей. И это дает основания утверждать, что социальные сети являются не только средством для общения, но и инструментом распространения информации практически любого характера.

Социальные сети могут предоставить возможности для распространения между определенными группами информации, содержащей противозаконный характер. Это происходит благодаря большой популярности социальных сетей и затрудняет отслеживание первоисточников подобной информации.

Одной из основных задач анализа информационных потоков является обнаружение ретрансляторов, каналов распространения и источников информации. Анализ каналов распространения информации в социальных сетях позволяет выявить основные информационные потоки, содержащие нежелательный контент, что, несомненно, относится к актуальным задачам.

Анализ

На настоящий момент существуют различные методики и подходы к анализу социальных сетей. Можно выделить четыре основанных подхода, направленных непосредственно на построения социальных графов. И на то, как они будут выглядеть в зависимости от выбираемого типа объекта:

1) *эгоцентрические сети:* исследование сетей выстраивается вокруг одного объекта. Часто собирается информация о большом количестве подобных сетей, которые в дальнейшем выступают в качестве единиц анализа;

2) *диады:* изучение имеющихся связей между парами объектов;

3) *триады:* рассмотрение петель, состоящих из трех, а в некоторых случаях и большего количества узлов сети. Этот подход применим для изучения степени кластеризации сетей более высокого порядка, то есть для сбора данных, содержащих информацию о выборке объектов, и затем упорядочивание объектов в сравнительно однородные группы;

4) *полные сети:* сети рассматриваются в большом масштабе, то есть изучается вся структура связей социальной сети [4].

Такие методики направлены по большей части на создание самой схемы, построения максимально удобного, для решения конкретной задачи, математического графа социальных связей, для последующего его изучения и составления выводов.

Также можно выделить четыре основных подхода к анализу сетей строящихся на основе анализа социальных графов и зависимостей пользователей: структурный, ресурсный, нормативный и динамический. Рассмотрим их подробнее.

1) *Структурный подход*. Основное внимание уделяется взаимному расположению вершин, а также центральности и транзитивности. Все участники сети здесь анализируются как вершины графа, которые оказывают влияние на других акторов сети, и на общее расположение ребер. Иными словами, основой данного метода является геометрическая форма сети и интенсивность взаимодействий ее вершин. Для формирования выводов на основе графовой модели используются теории сетевого обмена и структурные теории.

2) *Ресурсный подход*. Все участники сетевого взаимодействия рассматриваются с точки зрения индивидуальных и сетевых ресурсов и по ним же и разграничиваются. В качестве индивидуальных ресурсов могут выступать такие позиции как пол, возраст, раса. Сетевыми ресурсами могут быть влияние, уровень образованности и финансовый статус. Суть данного подхода состоит в изучении возможностей акторов по привлечению существующих ресурсов для достижения своих целей.

3) *Нормативный подход*. Рассматривает, какие существуют правила и ограничения, влияющие на взаимодействия участников социальной сети. А также кокой существует уровень доверия между ними. В этом случае существуют разные типы ребер, связывающих вершины графа. Они зависят от того, в каких социальных ролях состоят объекты, связанные с данным ребром сети, например, дружеские или родственные связи, коллеги или деловые партнеры. То, какие задатки имеются для достижения некоторой цели, напрямую зависит от «сетевого капитала» имеющегося у участника

сети в произвольный момент времени. «Сетевой капитал» является сочетанием имеющихся индивидуальных и сетевых ресурсов с нормами и правилами, распространяющимися в рассматриваемой социальной сети. Иными словами, основой данного подхода является изучение того, какого характера отношения имеются между акторами и какими правилами они регулируются.

4) *Динамический подход*. Призван дать ответы на вопросы: как изменяется структура сети при воздействии на неё извне, возможно ли существование стационарной конфигурации сети и какую она имеет структуру, от чего зависит изменение ребер сети. Суть этого подхода состоит в изучении социальной сети с точки зрения изменения ее структуры с течением времени [5].

Один из самых известных примеров анализа сетей был проведен еще в 1970-е гг. американским социологом Марком Грановеттером [6]. Данный эксперимент выявил, что для решения некоторых социальных задач слабые связи могут оказаться эффективнее, чем сильные. Этот эффект был назван «силой слабых связей».

Суть этой идеи основывается на эксперименте, который состоит в следующем. Если существуют несколько путей между муравейником и источником питания, то с течением времени останется только один самый короткий путь, поскольку муравей оставляет за собой след из феромонов, по которому его путь могут повторить другие муравьи. Другие также оставят свои феромоны, укрепляя путь. За одно и то же время по наиболее короткому пути сможет пройти большее количество насекомых, тем самым сделав его более привлекательным, а значит феромоны на менее популярных путях без регулярного обновления испаряться и такие пути со временем станут неиспользуемыми.

Проведя параллели между этим экспериментом и социальной сетью можно прийти к выводу, что для эффективности социальных сетей очень важными являются функциональные роли ее участников. Например, такие как посредники или ретрансляторы. Эти люди могут связывать между собой группы людей, налаживая между ними связи и открывая им доступ к новой информации. Для их идентификации в социальных сетях может быть применен оптимизационный подход муравьиной колонии (ACO = *Ant Colony Optimization*). Это эффективный полиномиальный алгоритм для нахождения приближенных решений оптимального пути в графе.

Суть данного подхода заключается в расположении муравьев в вершинах графа, а затем начинается их движение. С помощью вероятностного метода можно определить направление на основании следующей формулы:

$$P_i = \frac{l_i^q f_i^p}{\sum_{k=0}^{N} l_k^q f_k^p},$$

где P_i – вероятность перехода по пути i; l_i – величина, обратная весу (длине) i-го перехода; f_i – количество феромонов на i-м переходе; q – величина, определяющая «жадность» алгоритма; p – величина, определяющая «стадность» алгоритма и $q + p = 1$.

Данное решение не может быть точным в силу вероятностного характера, однако его многократное повторение должно выдавать достаточно точный результат [7].

Для успешного мониторинга информационной активности в пространстве социальных сетей необходимо изучение закономерностей создания и распространения каналов передачи данных, развитие методов, позволяющих определять характер взаимодействия участников, а также необходимо исследование методов выявления и описания характеристик сетей.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-71-10094) в СПИИРАН.

Список используемых источников

1. Завгородний М. Д. Социальная активность в сети Интернет // Вестник Российского университета дружбы народов. Серия: Социология. 2012. №. 2.

2. Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Том 6. № 3. С. 1–9.

3. 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. Вып. 4. С. 362–377.

4. Пруцкова Е. В. Анализ социальных сетей Social Network Analysis: a Review. 2012.

5. Воронкин А. С. Социальные сети: эволюция, структура, анализ // Образовательные технологии и общество. 2014. Т. 17. №. 1.

6. Granovetter M. S. The Strength of Weak Ties // American Journal of Sociology. 1973. Vol. 78. No. 6. PP. 1360–1380.

7. Батура Т. В. Методы анализа компьютерных социальных сетей // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2012. Т. 10. № 4. С. 13–28.

УДК 519.718:004.722
ГРНТИ 49.33.29

АНАЛИЗ НАДЕЖНОСТИ МНОГОПОЛЮСНЫХ СЕТЕЙ СВЯЗИ НА ОСНОВЕ МЕТОДА МИНИМАЛЬНЫХ СЕЧЕНИЙ

К. А. Батенков

Академия Федеральной службы охраны Российской Федерации

В работе рассмотрен подход к анализу надежности многополюсных сетей связи на основе метода минимальных сечений. Существо данного метода вычисления вероятности несвязности сводится к формированию всех возможных комбинаций из сечений, так что каждая комбинация содержит все элементы графа, входящие в комбинируемые сечения, а также вычислению вероятности существования комбинаций и знакопеременному их суммированию.

сети связи, надежность, коэффициент готовности, метод полного перебора типовых состояний.

Данный метод, по сути, является антиподом метода перебора связных состояний сети связи. Последовательность решения задач сохраняется, но рассматриваются события несвязности. В научной литературе по классической теории надежности он является частным случаем метода минимальных сечений [**Ошибка! Источник ссылки не найден.**]. Необходимо остановиться на случае многосвязных графов сетей связи. В связи с этим событие несвязности для многополюсной сети, наступает в случае отказа всех элементов некоторого сечения. При этом в многополюсной сети сечением будет набор элементов, приводящий к несвязному графу.

Одновременное существование двух и более сечений допустимо, а это означает, что для вычисления вероятности несвязности можно использовать теорему сложения для совместных событий [1, 3], которая трактуется как схема логических высказываний типа «или», т. е. применительно к операндам логического высказывания применима схема «...или то, или другое, или оба вместе». Заметим, что схема «либо» (т. е. «исключающее «или») допускает высказывания «…либо то, либо другое».

Существо данного метода вычисления вероятности несвязности сводится к формированию всех возможных комбинаций из сечений n, так что каждая комбинация содержит все элементы графа, входящие в комбинируемые сечения, а также вычислению вероятности существования ком-

бинаций и знакопеременному их суммированию [4]. Метод достаточно трудоемкий, так как требуется рассмотреть 2^n всех возможных комбинаций из n сечений, что не всегда реализуемо на реальных сложно разветвленных сетях связи даже с использованием современных процессоров. Существенным достоинством метода является то, что нет необходимости определять функцию связности для любого подграфа исходного графа сети [5, 6].

Пусть G_i', $i = 1, 2, \dots, n$ – множество всех сечений (многополюсной или двухполюсной сети) исходного графа G. Событие, состоящее в том, что все элементы сечения G_i' неисправны, будем также обозначать G_i'. Аналогично вычислению вероятности связности, объединение событий G_i' совпадает с множеством всех неисправных состояний сети связи $\bigcup_{i=1}^{n} G_i'$, поэтому для вероятности несвязности сети справедливо равенство

$$q_G = P\left(\bigcup_{i=1}^{n} G_i'\right) = \sum_{i=1}^{n} P(G_i') - \sum_{i<j} P\left(G_i' G_j'\right) + \\ + \sum_{i<j<k} P\left(G_i' G_j' G_k'\right) - \dots + (-1)^{n-1} P(G_1' G_2' \dots G_n').$$

Учитывая, что вероятность совместного события несвязности сразу нескольких сечений рассчитывается на основе соответствующих условных вероятностей, формулу вероятности несвязности сети целесообразно представить в виде:

$$q_G = \sum_{i=1}^{n} q_i - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} q_i \circ q_j + \\ + \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} q_i \circ q_j \circ q_k - \dots + (-1)^{n-1} q_1 \circ q_2 \circ \dots \circ q_n ,$$

где $q_i = 1 - p_i = P(G_i')$ – вероятность несвязности сечения G_i', $i = 1, 2, \dots, n$; $\circ$ – символ логического умножения сечений, предполагающего, что элементы перемноженных сечений в итоге должны включаться только один раз [1].

Отсюда видно, что процедура накопления точного значения вероятности несвязности q_G является, также как и вероятности связности, аддитивной и знакопеременной. Аналогично результаты суммирований при количестве сумм, меньших числа связных подграфов, в общем случае могут выходить за пределы допустимых значений вероятности, т. е. за интервал $[0, 1]$. При этом значения нечетных слагаемых всегда будут больше значений четных. Следует также отметить особенность данного метода, которая

заключается в том, что чем больше значения вероятностей неисправного состояния элементов графа, тем «точнее» слагаемые повторяют поведение огибающих биномиальных коэффициентов.

Пример

Граф исследуемой сети связи приведен на рис. 1. Все узлы сети являются абсолютно надежными, а вероятность исправности любой линии связи равна 0,9. Определить надежность сети связи в целом и в направлении 1–5 методом полного перебора несвязных состояний.

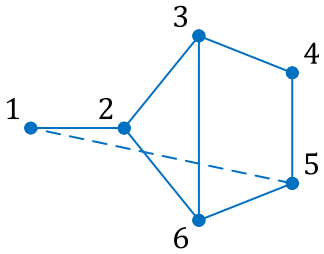


Рис. 1. Граф исследуемой сети связи

Дано: $G, p = 0{,}9$.

Найти: p_G, p'_G.

Первоначально определим набор сечений многополюсной сети на основе графа G. Сечений в графе целых одиннадцать (рис. 2):

$$G_1 = \{12\}, G_2 = \{23, 26\}, G_3 = \{34, 45\}, G_4 = \{34, 56\}, G_5 = \{45, 56\},$$

$$G_6 = \{23, 34, 36\}, G_7 = \{23, 36, 45\}, G_8 = \{23, 36, 56\}, G_9 = \{26, 34, 36\},$$

$$G_{10} = \{26, 36, 45\}, G_{11} = \{26, 36, 56\}.$$

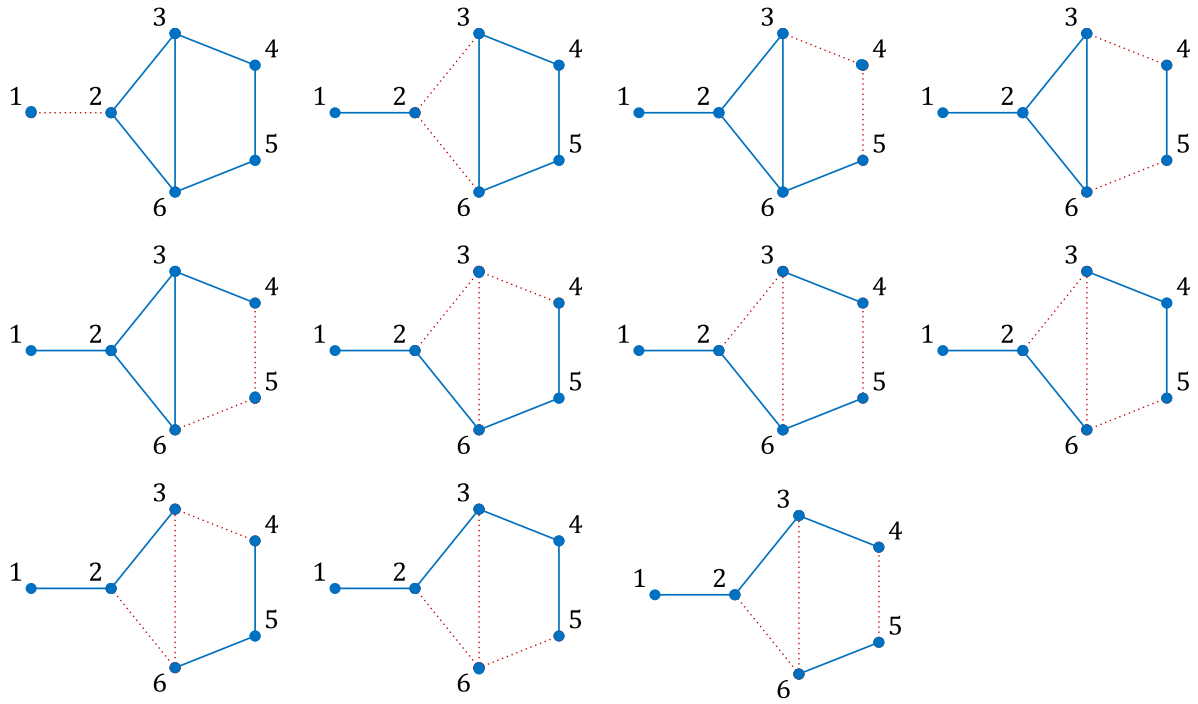


Рис. 2. Сечения графа, представленного на рис. 1

Для вычисления вероятности связности сети приведем лишь несколько промежуточных (табл. 1, 2) и конечные результаты расчета (табл. 3).

ТАБЛИЦА 1. Сечения графа в целом для первой группы слагаемых

Номер слагаемого в группе	Слагаемое	Конституента	Вероятность связности слагаемого	Номер слагаемого в группе	Слагаемое	Конституента	Вероятность связности слагаемого	Номер слагаемого в группе	Слагаемое	Конституента	Вероятность связности слагаемого
1	G_1	q^1	0,1	5	G_5	q^2	0,01	9	G_9	q^3	0,001
2	G_2	q^2	0,01	6	G_6	q^3	0,001	10	G_{10}	q^3	0,001
3	G_3	q^2	0,01	7	G_7	q^3	0,001	11	G_{11}	q^3	0,001
4	G_4	q^2	0,01	8	G_8	q^3	0,001	Сумма			0,146

ТАБЛИЦА 2. Сечения графа в целом для второй группы слагаемых

Номер Слагаемого в группе	Слагаемое	Конституента	Вероятность Связности слагаемого	Номер Слагаемого в группе	Слагаемое	Конституента	Вероятность связности слагаемого	Номер Слагаемого в группе	Слагаемое	Конституента	Вероятность связности слагаемого
1	G_1G_2	q^3	10^{-3}	20	G_3G_4	q^3	10^{-3}	39	G_5G_{10}	q^4	10^{-4}
2	G_1G_3	q^3	10^{-3}	21	G_3G_5	q^3	10^{-3}	40	G_5G_{11}	q^4	10^{-4}
3	G_1G_4	q^3	10^{-3}	22	G_3G_6	q^4	10^{-4}	41	G_6G_7	q^4	10^{-4}
4	G_1G_5	q^3	10^{-3}	23	G_3G_7	q^4	10^{-4}	42	G_6G_8	q^4	10^{-4}
5	G_1G_6	q^4	10^{-4}	24	G_3G_8	q^5	10^{-5}	43	G_6G_9	q^4	10^{-4}
6	G_1G_7	q^4	10^{-4}	25	G_3G_9	q^4	10^{-4}	44	G_6G_{10}	q^5	10^{-5}
7	G_1G_8	q^4	10^{-4}	26	G_3G_{10}	q^4	10^{-4}	45	G_6G_{11}	q^5	10^{-5}
8	G_1G_9	q^4	10^{-4}	27	G_3G_{11}	q^5	10^{-5}	46	G_7G_8	q^4	10^{-4}
9	G_1G_{10}	q^4	10^{-4}	28	G_4G_5	q^3	10^{-3}	47	G_7G_9	q^5	10^{-5}
10	G_1G_{11}	q^4	10^{-4}	29	G_4G_6	q^4	10^{-4}	48	G_7G_{10}	q^4	10^{-4}
11	G_2G_3	q^4	10^{-4}	30	G_4G_7	q^5	10^{-5}	49	G_7G_{11}	q^5	10^{-5}
12	G_2G_4	q^4	10^{-4}	31	G_4G_8	q^4	10^{-4}	50	G_8G_9	q^5	10^{-5}
13	G_2G_5	q^4	10^{-4}	32	G_4G_9	q^4	10^{-4}	51	G_8G_{10}	q^5	10^{-5}
14	G_2G_6	q^4	10^{-4}	33	G_4G_{10}	q^5	10^{-5}	52	G_8G_{11}	q^4	10^{-4}
15	G_2G_7	q^4	10^{-4}	34	G_4G_{11}	q^4	10^{-4}	53	G_9G_{10}	q^4	10^{-4}
16	G_2G_8	q^4	10^{-4}	35	G_5G_6	q^5	10^{-5}	54	G_9G_{11}	q^4	10^{-4}
17	G_2G_9	q^4	10^{-4}	36	G_5G_7	q^4	10^{-4}	55	$G_{10}G_{11}$	q^4	10^{-4}
18	G_2G_{10}	q^4	10^{-4}	37	G_5G_8	q^4	10^{-4}				
19	G_2G_{11}	q^4	10^{-4}	38	G_5G_9	q^5	10^{-5}	Сумма		0,011	

В результате вероятность несвязности:

$$q_G = 0{,}146 - 0{,}011 + 3{,}369 \cdot 10^{-3} - 1{,}17 \cdot 10^{-3} + 6{,}114 \cdot 10^{-4} - \\ -3{,}072 \cdot 10^{-4} + 1{,}445 \cdot 10^{-4} - 5{,}7 \cdot 10^{-5} + 1{,}45 \cdot 10^{-5} - \\ -2 \cdot 10^{-6} + 10^{-11} = 0{,}138,$$

а вероятность связности:

$$p_G = 1 - q_G = 1 - 0{,}138 = 0{,}862.$$

ТАБЛИЦА 3. Связные состояния (остовы) сети связи в целом для оставшихся групп слагаемых

Номер группы слагаемых	Число слагаемых в группе	Вероятность связности слагаемого	Номер группы слагаемых	Число слагаемых в группе	Вероятность связности слагаемого
1	11	0,146	7	330	$1{,}445 \cdot 10^{-4}$
2	55	0,011	8	165	$5{,}7 \cdot 10^{-5}$
3	165	$3{,}369 \cdot 10^{-3}$	9	55	$1{,}45 \cdot 10^{-5}$
4	330	$1{,}17 \cdot 10^{-3}$	10	11	$2 \cdot 10^{-6}$
5	462	$6{,}114 \cdot 10^{-4}$	11	1	10^{-11}
6	462	$3{,}072 \cdot 10^{-4}$			

В данном примере хорошо видно, что трудоемкость рассматриваемого метода определяется количеством сечений исходного графа. Причем номер группы слагаемых, на котором наступает эффект насыщения (увеличения числа рассматриваемых сечений не приводит к изменению конституент), оказывается лишь на единицу меньше числа сечений, что связано с низким значением вероятности неработоспособности ребер графа [5].

Список используемых источников

1. Половко А. М., Гуров С. В. Основы теории надежности. СПб. : БХВ-Петербург, 2006. 704 с.

1. Филин Б. П. Методы анализа структурной надежности сетей связи. М. : Радио и связь, 1988. 208 с.

2. Батенков К. А. Общие подходы к анализу и синтезу структур сетей связи // Современные проблемы телекоммуникаций: материалы Российской научно-технической конференции. 2017. С. 19–23.

3. Батенков К. А. Числовые характеристики структур сетей связи // Труды СПИИРАН. 2017. № 4 (53). С. 5–28.

4. Батенков К. А. Устойчивость сетей связи. Орел : Академия ФСО России, 2017. 277 с.

6. Батенков К. А. К вопросу оценки надежности двухполюсных и многополюсных сетей связи // Современные проблемы радиоэлектроники: сб. науч. тр. Красноярск : Сиб. федер. ун-т. 2017. С. 604–608.

УДК 004.722
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПОЛНОДОСТУПНОГО ЗВЕНА МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ, РЕАЛИЗУЮЩЕГО РАВНОПРАВНУЮ СТРАТЕГИЮ ДОСТУПА К КАНАЛЬНОМУ РЕСУРСУ ЛИНИИ

К. А. Батенков, А. В. Королев, А. Е. Миронов

Академия Федеральной службы охраны Российской Федерации

Подчеркивается, что необходимо обеспечить известный компромисс между максимальной точностью математического описания функционирования МСС, что ведет к усложнению аппарата анализа и доступностью его использования инженерно-техническим составом. Иллюстрируется, что при реализации полнодоступным звеном МСС равноправной стратегии доступа к обслуживанию ресурсоёмкие и малоресурсные заявки обслуживаются с разным качеством (вероятность потерь заявок у первого потока требований ниже, чем у второго ресурсоёмкого).

мультисервисная сеть связи, гетерогенный трафик, аналитическая модель, метод Кауфмана–Робертса.

Высокая сложность систем и сетей связи [1, 2] существенно ограничило область применения аналитических методов расчёта вероятностно-временных характеристик однопотоковых систем обслуживания с гомогенным трафиком, составляющих основу классической теории телетрафика. Причина этого в том, что в классических моделях телетрафика предполагается, что каждая заявка на всех этапах своего обслуживания использует не более одного канального ресурса систем телекоммуникации. В мультисервисных сетях связи данное предположение не выполняется. МСС, являясь универсальной транспортной средой, обеспечивает обслуживание как трафика данных (передача файлов, сообщений электронной почты, передача текста), так и трафика реального времени (передача голосовых сообщений, обеспечение видеоконференцсвязи, видеосвязи и телевизионного вещания), требующих как было показано выше различный канальный ресурс (скоростей передачи).

Очевидно, что при анализе и синтезе МСС использование классического математического аппарата для описания гомогенных сетей, не позволит создать адекватных математических моделей.

Здесь уместно привести цитату из [3] доктора технических наук, профессора Шнепса М. А. «…телекоммуникации сегодня стали столь сложными, что даже алгоритмы работы сетей умом не охватить, куда там еще математическую модель построить, которая сохранила черты еще не существующей сети...».

Однако, несмотря на сложности, связанные с анализом перспективных систем обслуживания, такие модели строят и используют для решения задач анализа и синтеза телекоммуникаций. При этом необходимо обеспечить известный компромисс между максимальной точностью математического описания функционирования МСС, что ведет к усложнению аппарата анализа и доступностью его использования инженерно-техническим составом.

Основная трудность при аналитическом моделировании МСС заключается в непомерном возрастании числа состояний системы, что приводит к необозримости модели. Например, при числе потоков $(k = 1,\ 2,\ 3,\ ...,\ n)$, поступающих на звено МСС, емкость V ЕКР при требуемом ресурсе для обслуживания каждого сервиса $b_k = 1\ EKP$. общее число состояний в пространстве, определяемом неравенством $\sum_{k=1}^{n} i_k \times b_k \le V$, можно найти, применяя комбинаторику $C_V^n = \frac{V!}{n!\cdot(V-n)!}$.

Используя формулу Стирлинга для вычисления числа сочетаний для случая n = 10 и V = 1000 можно определить число состояний системы:

$$C_V^n \approx \frac{e^n}{\sqrt{2\cdot\pi\cdot n}}\cdot\left(\frac{V}{n}\right)^n = \frac{e^{10}}{\sqrt{2\cdot\pi\cdot 10}}\cdot\left(\frac{100}{10}\right)^{10} = 2{,}78\cdot 10^{13}.$$

Для случая n = 10 и V = 1000 число таких состояний уже превосходит значение 2×10^{23}.

В этих условиях особую актуальность приобретает разработка эффективных численных методов исследования.

Для упрощения процесса вычисления вероятностей потерь обслуживания сервисов и величины обслуженной нагрузки используют метод Кауфмана–Робертса. Данный метод основан на разбиении пространства состояний модели по числу занятых единиц канальной емкости и вычислении вероятности потерь заявок k-го сервиса через нормированные вероятности состояний ресурса звена МСС:

$$\pi_k = \sum_{i=V-b_k+1}^{V} p(i). \qquad (1)$$

При этом в (1) соответствующие вероятности занятости единиц канального ресурса связаны между собой рекуррентным соотношением [4]:

$$p(i) = \frac{1}{i} \cdot \sum_{k=1}^{n} Z_k \cdot b_k \cdot p\left(i - b_k\right) \cdot I\left(i - b_k \geq 0\right),\ i = 1,\ 2,\ ...,\ V.$$

где n – общее число сервисов; Z_k – интенсивность поступающей нагрузки k-го сервиса.

Анализ данного алгоритма позволяет сделать следующие выводы:

– вычислительная сложность предложенного рекурсивного алгоритма определяется усилиями, затрачиваемыми на вычисление ненормированных вероятностей $p(i)$;

– при n = const время счёта увеличивается линейно с ростом объёма канального ресурса V (ЕКР).

На основе данного алгоритма было проведено исследование полнодоступного звена МСС, реализующего равноправную стратегию доступа к канальному ресурсу линии при следующих структурных и нагрузочных характеристиках:

– число сервисов реального времени $k = 2$;

– интенсивность поступающей нагрузки первого сервиса $Z_1 = 20$ Эрл;

– интенсивность поступающей нагрузки первого сервиса $Z_2 = 3$ Эрл;

– требуемый канальный ресурс для обслуживания каждой заявки первого потока $b_1 = 1$ единиц канального ресурса (ЕКР);

– требуемый канальный ресурс для обслуживания каждой заявки второго потока $b_2 = 20$ ЕКР;

– канальный ресурс звена МСС изменяется в пределах V = 10, …, 100 ЕКР.

На основе представленных данных построим графики зависимости вероятности потерь заявок различных сервисов от величины объема канального ресурса $\pi_k = f(V)$.

Используя разработанную программы расчета на ЭВМ для звена МСС получили данные, на основе которых построены графики зависимости (рис.).

Анализ зависимостей (рис.) показывает, что:

– с увеличением передаточных возможностей линии V (скорости, пересчитанной в число единиц канального ресурса (ЕКР)) вероятности потерь заявок различных сервисов снижаются, но снижение носит волнообразный характер [5, 6]. Другими словами, с увеличением значения V возможно, как снижение, так и возрастание значений вероятностей потерь заявок различных сервисов. Это обстоятельство в отличие от анализа моносервисных сетей исключает возможность на интуитивном уровне добиться требуемого качества обслуживания за счёт увеличения канальной емкости линии, а требует использования соответствующего математического аппарата;

– возрастание потерь малоресурсных заявок и снижение потерь требований ресурсоёмких заявок происходит при значениях канального ресурса V кратных b_2 единиц канального ресурса.

– из графика видно, что при реализации полнодоступным звеном МСС равноправной стратегии доступа к обслуживанию ресурсоёмкие и малоресурсные заявки обслуживаются с разным качеством (вероятность потерь заявок у первого потока требований ниже, чем у второго ресурсоёмкого). Это обстоятельство обусловлено тем, что для малоресусных требований в системе больше состояний, при которых они обслуживаются. Для широкополосных заявок состояний, при которых достаточно передаточных возможностей линии для их обслуживания меньше.

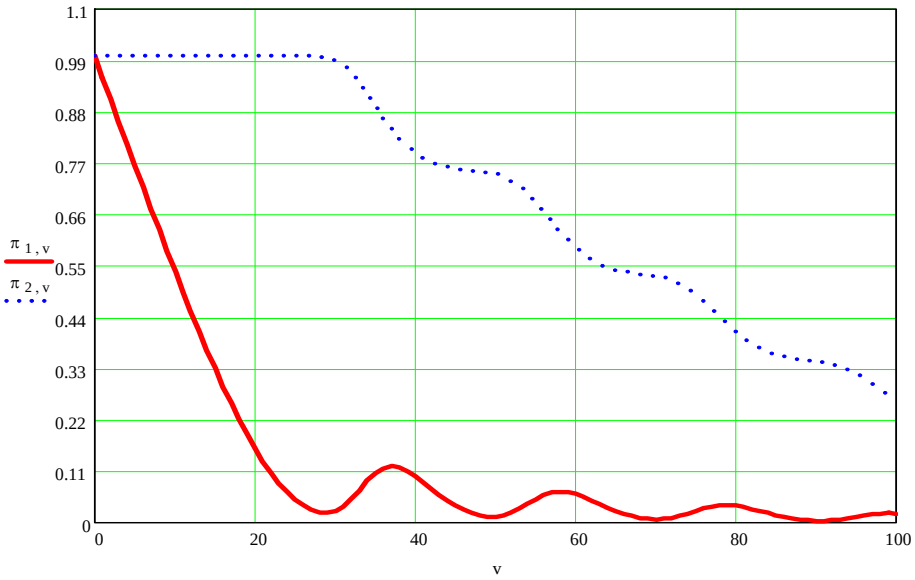


Рисунок. Зависимости вероятностей потерь заявок малоресусного и ресурсоемкого сервисов от передаточных возможностей звена МСС

Список используемых источников

1. Батенков К. А. Числовые характеристики структур сетей связи // Труды СПИИРАН. 2017. № 4 (53). С. 5–28.

2. Батенков К. А. Анализ и синтез структур сетей связи по детерминированным показателям устойчивости // Труды СПИИРАН. 2018. № 3 (58). С. 128–159.

3. Шнепс-Шнеппе М. А. Лекции по сетям нового поколения. М.: МАКС Пресс, 2005. 232 с.

4. Степанов С. Н. Теория телетрафика: концепции, модели, приложения. М.: Горячая линия – Телеком, 2015. 868 с.

5. Батенков К. А., Королев А. В., Миронов А. Е., Орешин А. Н. Анализ статистики голосового трафика сети Ethernet с помощью программы Wireshark // Телекоммуникации. 2018. № 10. С. 39–48.

6. Батенков К. А., Королев А. В., Миронов А. Е., Орешин А. Н. Оценка параметров алгоритмов диспетчеризации на основе имитационного моделирования в программной среде Riverbed // Телекоммуникации. 2018. № 8. С. 17–23.

УДК 004.056.57
ГРНТИ 20.15.05

МОДЕЛЬ ЗАЩИТЫ ОТ БЭКДОРОВ С ПОСЛЕДУЮЩИМ АНАЛИЗОМ И ОЦЕНКОЙ ИНЦИДЕНТОВ

Д. В. Бахтин, В. Н. Волкогонов, В. В. Стасюк

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

В современных распределенных информационных системах преобладают различного вида и характера угрозы, связанные с несанкционированным доступом и утечкой данных. В качестве примера следует упомянуть такие вредоносные эффекты как атаки типа “черных ход” (бэкдор) и атаки типа эксплоит. В данной статье речь идет о модели защиты от бэкдоров с последующим анализом и оценкой инцидентов. Предлагается разработать и внедрить данную модель в распределенные информационные системы.

Backdoor, бэкдор, эксплоит, несанкционированный доступ, распределенные информационные системы, информ. безопасность.

Большинство предприятий располагаются во множестве офисов и промышленных зданий, находящихся на расстоянии друг от друга и не соединенных единой вычислительной сетью. Связь между объектами компаний осуществляется механизмами виртуальных частных сетей.

Для организации взаимодействия между электронно-вычислительными машинами (ЭВМ) внедряется информационная система, позволяющая взаимодействовать независимым, но связанным между собой электронно-вычислительным машинам. Такие информационные системы называются распределенными [1].

Связь между объектами распределенной информационной системы осуществляется с помощью коммуникационной подсистемы, показанной на рис. 1, состоящей из:

– коммуникационных модулей;
– каналов связи;
– концентраторов;
– межсетевых шлюзов и мостов.

Коммуникационные модули (КМ) предназначены для передачи полученных пакетов к другим коммуникационным модулям или абоненту, в соответствии с маршрутизацией.

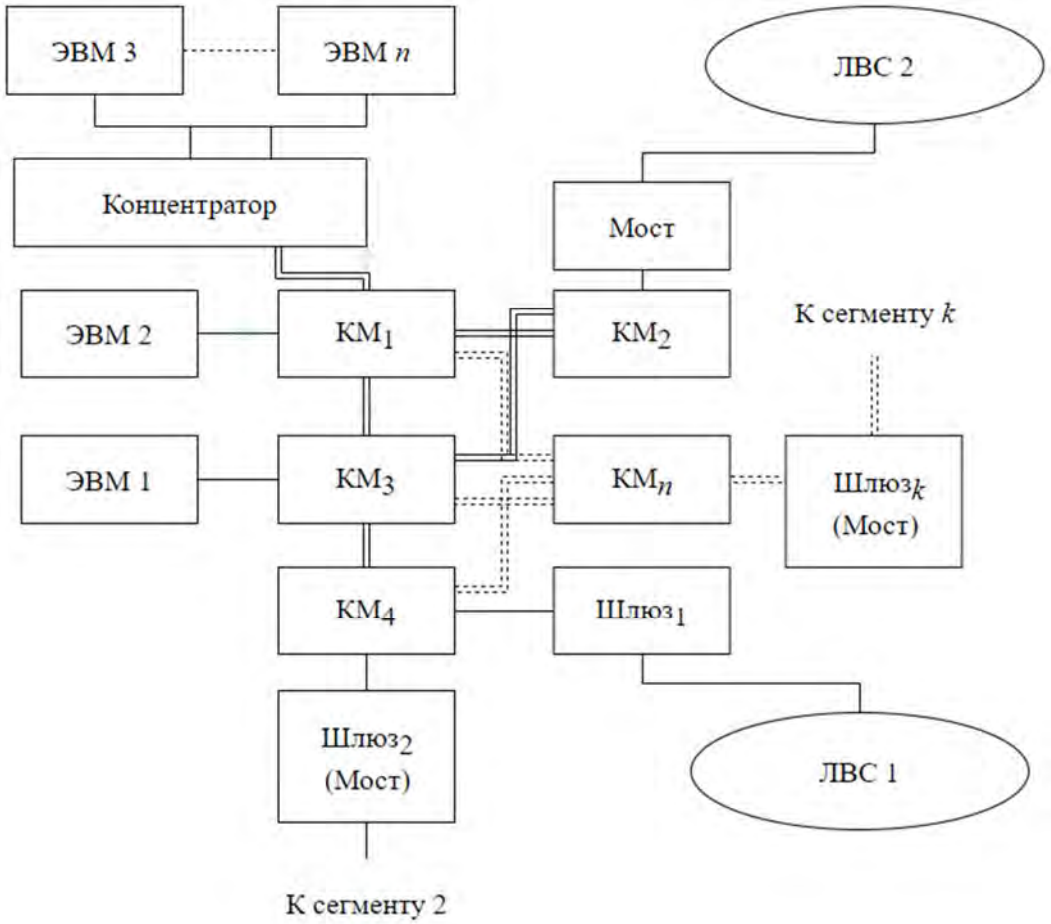


Рис. 1.Фрагмент распределенной информационной системы

Каналы связи выполняют функцию объединения элементов сети в единую сеть.

Концентраторы выполняют функцию уплотнения передаваемой информации, перед отправкой ее по каналам связи.

Межсетевые шлюзы и мосты необходимы для установления связи сегментов глобальной сети или связи внешней сети с локально вычислительной сетью (ЛВС).

Несмотря на то, что распределенные информационные системы удобны, в них есть и недостатки, в частности связанные с информационной безопасностью предприятия [2].

1. Возможность несанкционированного доступа.
2. Чтение остаточной информации с запоминающих устройств.
3. Вывод из строя подсистем.
4. Несанкционированное использование электронных вычислительных машин, имеющих уникальные физические характеристики.
5. Снятие информации с внутренней сети предприятия.

Данные уязвимости позволяют злоумышленникам используя бэкдоры и эксплойты, собирать конфиденциальную информацию и выводить

из строя объекты распределенных информационных систем. Учитывая количество проприетарного программного обеспечения, которое используют компании и открытость его кода, использование бэкдоров и эксплойтов сейчас упрощается.

Наиболее частым и опасным за последнее время стал эксплоит-кит Angler. Angler помогает распространять такое ПО, как Cryptowall, AlphaCrypt, Necurs, и Bedep. Потенциальная жертва перенаправляется на фишнговый сайт. В это время Anlger в фоновом режиме начинает обфускацию вредоносных скриптов. Также на этом сайте есть несколько зашифрованных строк, содержащих URL разных эксплойтов (*Flash, Silverlight, Internet Explorer*), включенных в атаку [3].

Второй слой обфускации используют и другие эксплойт-киты, чтобы затруднить детектирование. Кроме того, что Angler имеет способность распознавать антивирусное ПО, он умеет также определять, когда исследователь пытается выполнить его код в песочнице или на виртуальных машинах, а также через прокси-отладчик Fiddler, популярный среди аудиторов информационной безопасности. Все эти механизмы самозащиты сильно затрудняют анализ Angler исследователями [3].

Исходя из модели защиты от бэкдоров с последующим анализом и оценкой инцидентов делается количественная оценка угроз информационной безопасности по следующим критериям, характерным для бэкдоров и эксплоитов. Причем, следует принимать вредоносный файл эксплоита как предстартовую загрузки перед получением доступа. Таким образом были получены статистические данные в следующей таблице.

ТАБЛИЦА. Зависимость вероятности устойчивости функционирования распределенных информационных системах (РИС)

Угроза безопасности РИС	Вероятность реализуемости угрозы (%)	Угроза безопасности РИС	Вероятность реализуемости угрозы (%)
угроза перехвата управления загрузкой	0,25	угроза обхода системы идентификации и аутентификации данных	0,25
угроза НСД с применением стандартных функций операционной системы	0,35	угроза обхода системы идентификации и сетевых объектов	0,35
угроза НСД с помощью прикладной программы	0,35	угроза внедрения ложного объекта сети	0,35

Угроза безопасности РИС	Вероятность реализуемости угрозы (%)	Угроза безопасности РИС	Вероятность реализуемости угрозы (%)
угроза НСД с применением специально созданных для этого программ	0,25	угроза навязывания ложного маршрута	0,35
угроза НСД при передаче информации по внешним каналам	0,25	угроза перехвата и взлома паролей	0,35
угроза утечки информации при удаленном доступе к информационным ресурсам	0,25	угроза подбора паролей доступа	0,35
угроза утечки информации за счет её несанкционированной передачи по каналам связи	0,35	угроза типа «Отказ в обслуживании»	0,35
угроза «Анализ сетевого трафика»	0,35	угроза внедрения троянских программ	0,35
угроза сканирования открытых портов, служб и соединений	0,35	угроза атаки типа «Переполнение буфера»	0,35

При построении модели обработки данных в распределенных информационных системах предложен принцип объединения пакетной и потоковой обработки на ведущих и ведомых узлах (рис. 1).

В отличие от известных параметров взаимодействия с распределенными информационными системами, центр управления сетью (ЦУС) имеет две параллельные ветви управления системой Больших данных [4].

Модель обработки данных использует дополнительные сервисы и системы, которые расширяют множество механизмов защиты (рис. 2) при выявлении новых угроз безопасности.

Для модели обработки данных определена связь между оценкой защищенности и выбором защитных мер, а также построен идентификатор риска для беспрепятственной работы с системой [5].

Полученные на каждом этапе выходные данные используются как входные данные следующего этапа.

Ниже приведена спроектированная модель обработки данных.

Благодаря модели защиты от бэкдоров с последующим анализом и оценкой инцидентов по исходящей зависимости стало возможным определение конечных потерь до и после внедрения в распределенные информационные системы получается можно определить необходимые данные для оценки защищенности РИС (рис. 2).

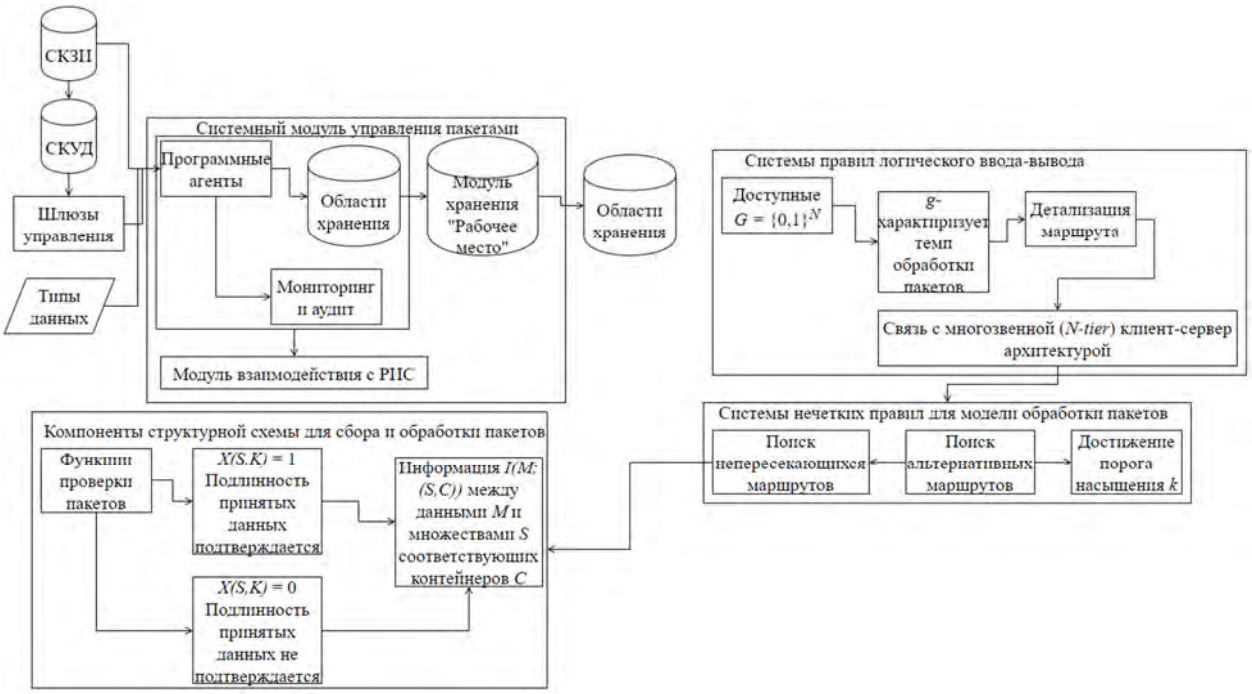


Рис. 2. Модель обработки данных

Проведен эксперимент, состоящий из 11 этапов (отличаются типами атак и скоростью обработки пакетов), которые одновременно запускались в РИС [6].

На рис. 3 (см. ниже) представлены три графика, на которых показаны результаты экспериментов. График с опорными пунктами «точка» описывают порог устойчивости функционирования РИС, с опорными точками «квадрат» потери пакетов при бэкдоре, с опорными пунктами «треугольник» потери пакетов при эксплоите.

Модель защиты от бэкдоров с последующим анализом и оценкой инцидентов спроектированная на кафедре защищенных систем связи при помощи программно-аппаратных средств защиты информации позволяет выявить статистику вероятности угроз безопасности РИС (табл.) и получить сведения по реализации атак бэкдора и эксплоитов рис. 3. Из 11 смоделированных атак возможно сделать замечание, что в процессе реализации данной модели защиты от бэкдоров с последующим анализом и оценкой инцидентов удалось устранить следующие уязвимости:

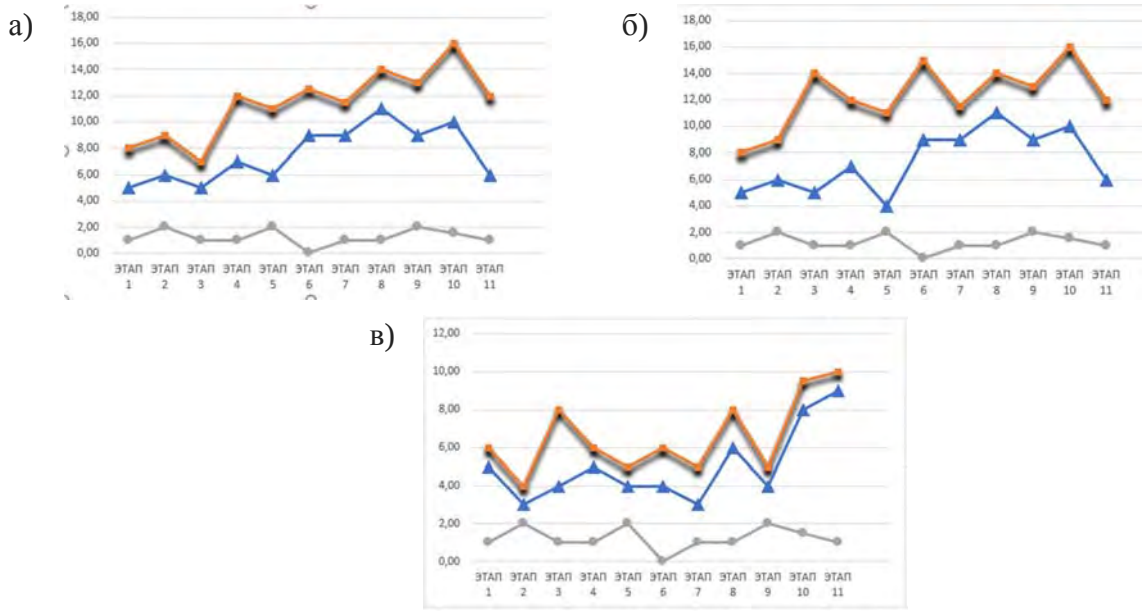


Рис. 3. Анализ экспериментов по определению потерь и временных в случае реализации бэкдора и эксплоита: а) результаты экспериментов с 50 % мощностью атаки, б) результаты экспериментов с 80 % мощностью атаки, в) результаты экспериментов с 100 % мощностью атаки

Угроза перехвата управления загрузкой; угроза НСД с применением стандартных функций операционной системы; угроза НСД с помощью прикладной программы; угроза НСД с применением специально созданных для этого программ; угроза НСД при передаче информации по внешним каналам; угроза утечки информации при удаленном доступе к информационным ресурсам; угроза утечки информации за счет её несанкционированной передачи по каналам связи; угроза «Анализ сетевого трафика»; угроза сканирования открытых портов, служб и соединений; угроза обхода системы идентификации и аутентификации данных; угроза обхода системы идентификации и сетевых объектов; угроза внедрения ложного объекта сети; угроза навязывания ложного маршрута; угроза перехвата и взлома паролей; угроза подбора паролей доступа; угроза типа «Отказ в обслуживании»; угроза внедрения троянских программ; угроза атаки типа «Переполнение буфера» в целом на 32 %

Список используемых источников

1. Андрианов В. И., Романов Г. Г., Штеренберг С. И. Экспертные системы в области информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2-х т. 2015. С. 193–197.

2. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

3. Красов А. В., Сурмина М. С. Использование и разработка методов обнаружения вредоносной активности автоматизированного построения ботнет-сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сборник научных статей в 4-х т. 2018. С. 513–517.

4. Штеренберг С. И. Корреляционный и эвристический анализ действий самомодифицирующегося кода для защиты информации в исполнимых файлах // Актуальные проблемы инфотелекоммуникаций в науке и образовании сборник научных статей. V Международная научно-техническая и научно-методическая конференция. 2016. С. 545–550.

5. Штеренберг С. И. Разработка модели программно-аппаратного комплекса охраны объектов ssp_ai_3.0 // Молодежь. Техника. Космос. Труды X Общероссийской молодежной научно-технической конференции. Сер. «Библиотека журнала «Военмех. Вестник БГТУ» № 50». 2018. С. 145–149.

6. 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. № 3. С. 70–77.

УДК 004.056
ГРНТИ 81.93.29

АЛГОРИТМЫ ЧЕЛОВЕКО-МАШИННОГО ВЗАИМОДЕЙСТВИЯ ДЛЯ СЕНСОРНЫХ ЭКРАНОВ В СИСТЕМЕ ВИЗУАЛИЗАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Ю. Е. Бахтин[1], С. Н. Бушуев[2], М. В. Коломеец[1], Н. А. Комашинский[1], И. В. Котенко[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]АО «Научно производственное предприятие ТЕЛДА»

В работе рассматривается реализация алгоритмов человеко-машинного взаимодействия на основе сенсорных экранов для управления системами анализа состояния компьютерной сети. Предложенные алгоритмы позволяют при помощи жестов управлять режимами отрисовки компьютерной сети, перемещениями между уровнями модели OSI, а также управлять процессами фильтрации и масштабирования информации.

сенсорные экраны, человеко-машинное взаимодействие, информационная безопасности, визуальная аналитика.

В современных системах мониторинга компьютерных сетей крайне быстро растет количество видов информационных источников, которыми становится сложно управлять. Таким образом, возникает необходимость разработки новых методов управления данными в рамках систем поддержки и принятия решений и, в частности, в рамках систем визуальной аналитики мониторинга сетевой безопасности [1, 2, 3].

Для управления данными визуализации с использованием сенсорных экранов необходимо иметь библиотеку жестов, которая позволит реализовать модель человеко-машинного взаимодействия для управления информацией.

В данной работе представляется методика реализации алгоритмов распознавания жестов для модели управления компьютерной сети в виде силовой отрисовки графа.

Данная модель подробно описана в [4] и состоит из следующий категорий жестов:

1 Касания:
- 1.1 касание одним пальцем;
- 1.2 касание тремя пальцами;
- 1.3 касание четырьмя пальцами.

2 Перемещения и повороты:
- 2.1 перемещение пальца по экрану;
- 2.2 перемещение двумя пальцами;
- 2.3 перемещение тремя пальцами;
- 2.4 перемещение четырьмя пальцами;
- 2.5 сведение разведение пяти пальцев;
- 2.6 перемещение пяти пальцев влево или вправо;
- 2.7 перемещение пяти пальцев снизу-вверх.
- 2.8 поворот тремя пальцами.

3 Комбинированные:
- 3.1 касание одним пальцем и прорисовка четверти окружности втором вокруг первого;
- 3.2 касание двумя пальцами и сведение разведение третьего;
- 3.3 долгое касание тремя пальцами и последующее нажатие четвертым;
- 3.4 долгое касание четырьмя пальцами и последующее нажатие пятым;
- 3.5 касание четырьмя пальцами и сведение разведение пятого.

Обработка жестов основывается на данных, получаемых от сенсорного экрана. Для получения данных от сенсорного экрана используется библиотека Hammer.js [5].

Для всех пальцев создается структура со следующими полями:

1. Как много пальцев на экране (переменная *n_of_fing*).

2. Как много пальцев совершили движение (переменная *n_of_mov*).
3. Совершено движение по оси x (переменная *mov_x*).
4. Совершено движение по оси y (переменная *mov_y*).
5. Количество пальцев, совершивших поворот (переменная *rotate*).
6. Между появлением пальцев была задержка (переменная *was_delay*).

Для каждого пальца создается обработчик, который работает в цикле до тех пор, пока палец прислонен к экрану.

Обработчик имеет следующие параметры:

1. Координаты x и y пальца на экране при инициализации (переменная *init_xy*) – передаются в обработчик при касании пальца к экрану.

2. Координаты x и y пальца на текущий момент (переменная *current_xy*) – передаются в обработчик в режиме реального времени пока палец прислонен к экрану.

Обработчик при инициализации инкрементирует переменную *n_of_fing*. Таким образом, переменная *n_of_fing* равняется количеству пальцев на экране.

В цикле обработчик высчитывает собственный параметр *distance_xy* (расстояние между координатами *xy* пальца на экране при инициализации и координатами *xy* пальца на текущий момент). В случае, если *distance_xy* > 50, это интерпретируется как не случайное движение и переменная *n_of_mov* инкрементируется. Обработчик может инкрементировать *distance_xy* один раз за цикл жизни.

Также в цикле обработчик высчитывает направление движения по оси *x distance_x*, по оси *y distance_y*, а также совершение поворота *rotate_xy* вокруг общего центра, который образуют все пальцы. В случае, если *distance_x* > 50, переменная *mov_x* инкриментируется в случае, если *distance_y* > 50, переменная *mov_y* инкриментируется, если *rotate_xy* > 50, переменная *rotate* инкрементируется. Таким образом можно установить характер движения.

Также при инициализации обработчик записывает время касания пальца в переменную *was_delay*. Если переменная уже записана (уже был прислонен другой палец), и разница во времени меньше секунды, то переменная обновляется, а если больше, то переменная записывается как *true*. Если переменная уже *true*, то переменная не перезаписывается.

Переменные структуры проверяются на ряд условий, выполнение которых позволяет распознать жест (табл., см. ниже).

Данная методика может применяться для распознавания жестов в системах человеко-машинного взаимодействия для управления данными состояния компьютерной сети в виде графа [6, 7]. В последующих исследованиях методика будет оценена на робастность и эффективность использования в сравнении с обычными не сенсорными дисплеями.

ТАБЛИЦА. Условия для распознавания жестов

Жест	Условие
касание одним пальцем	n_of_fing = 1 & n_of_mov = 0
касание тремя пальцами	n_of_fing = 3 & n_of_mov = 0
касание четырьмя пальцами	n_of_fing = 4 & n_of_mov = 0
перемещение пальца по экрану	n_of_fing = 1 & n_of_mov = 1
перемещение двумя пальцами	n_of_fing = 2 & n_of_mov = 2
перемещение тремя пальцами	n_of_fing = 3 & n_of_mov = 3
перемещение четырьмя пальцами	n_of_fing = 4 & n_of_mov = 4
сведение разведение пяти пальцев	n_of_fing = 5 & n_of_mov = 5 & mov_x = 1 & mov_y = 4
перемещение пяти пальцев влево или вправо	n_of_fing = 5 & mov_x = 5 & mov_y = 0
перемещение пяти пальцев снизу-вверх	n_of_fing = 5 & mov_x = 0 & mov_y = 5
поворот тремя пальцами	n_of_fing = 3 & rotate = 3
касание одним пальцем и прорисовка четверти окружности вторым вокруг первого	n_of_fing = 2 & mov_x = 1 & mov_y = 1 & rotate = 1
касание двумя пальцами и сведение разведение третьего	n_of_fing = 3 & n_of_mov = 1
долгое касание тремя пальцами и последующее нажатие четвертым	n_of_fing = 4 & was_delay = true
долгое касание четырьмя пальцами и последующее нажатие пятым	n_of_fing = 5 & was_delay = true
касание четырьмя пальцами и сведение разведение пятого	n_of_fing = 5 & n_of_mov = 1

Работа выполнена при финансовой поддержке РФФИ (проект № 18-07-01488-а).

Список используемых источников.

1. Kotenko I., Novikova E. Visualization of Security Metrics for Cyber Situation Awareness // Proceedings 9th International Conference on Availability, Reliability and Security, ARES 2014, 2014. PP. 506–513.

2. Новикова Е. С., Котенко И. В. Анализ механизмов визуализации для обеспечения защиты информации в компьютерных сетях // Труды СПИИРАН. 2012. № 4 (23). С. 7–29.

3. Коломеец М. В., Чечулин А. А., Котенко И. В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. № 5 (42). С. 232–257.

4. Котенко И. В., Коломеец М. В., Комашинский В. И., Бушуев С. Н., Гельфанд А. М. Модель человеко-машинного взаимодействия на основе сенсорных экранов

для мониторинга безопасности компьютерных сетей // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция. Санкт-Петербург, 24–26 октября 2018 г.: материалы конференции. СПб. : СПОИСУ. 2018. С. 143–144.

5. Библиотека Hammer.js [Электронный ресурс]. URL: https://hammerjs.github.io

6. Котенко И. В., Коломеец М. В., Бушуев С. Н., Гельфанд А. М. Методы человеко-машинного взаимодействия на основе сенсорных экранов в ситуационных центрах безопасности // Информационные технологии в управлении (ИТУ-2018). Санкт-Петербург. 2-4 октября 2018 г. : материалы конференции. СПб. : АО «Концерн «ЦНИИ «Электроприбор», 2018. С. 660–664.

7. Чечулин А. А., Коломеец М. В., Котенко И. В., Бушуев С. Н. Архитектура прототипа системы визуализации неформализованных данных // Математические методы в технике и технологиях – ММТТ-29. XXIX Международная научная конференция. Санкт-Петербург, 31 мая – 3 июня 2016 года. СПб. : Санкт-Петербургский государственный технологический институт, 2016. Т. 4. С. 142–144.

УДК004.75
ГРНТИ49.34.01, 49.33.01

ВЛИЯНИЕ ТЕХНОЛОГИИ BLOCKCHAIN НА ВЕРОЯТНОСТНО-ВРЕМЕННЫЕ ХАРАКТЕРИСТИКИ СЕТИ

И. А. Белозерцев, В. С. Елагин, А. В. Онуфриенко

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

В связи с развитием популярности приложений технологии распределенного реестра, возникает задача рассмотреть её влияние на характеристики сети и влияние самой сети на технологию. Авторы указывают ключевые показатели сетевых характеристик, необходимых для обеспечения заданного качества обслуживания при предоставлении и передаче трафика разного вида, определяют схему сети при работе с транзакциями blockchain и зависимость характеристик сети от параметров приложений.

QoS, Quality of service, distributed registry, blockchain.

В связи с появлением передовых технологий и разнообразных приложений, в настоящее время можно наблюдать появление множества представителей blockchain.

Blockchain – это распределенная база данных, которая содержит постоянно растущий список организованных записей, и у которой устройства хранения данных не подключены к общему серверу [1].

Blockchain-сервисы и связанные с ними приложения полагаются на Интернет общего пользования. В данном случае Интернет-провайдер не несет ответственности за содержимое пакетов, а также не обязан гарантировать качественную доставку, как и в случае с OTT-сервисами [2].

Технологияblockchain предлагает взять на себя все три важные роли, которые традиционно играет сектор услуг: регистрация сделок, подтверждение подлинности личности и заключение контрактов.

Перевод хотя бы части услуг на технологию blockchain приведёт к разрыву большого числа связей в сфере традиционных услуг, но одновременно позволит значительно повысить эффективность работы.

Практичность blockchain неоспорима во всем, что касается хранения данных и подтверждения подлинности. В перспективе это может помочь в борьбе с разного рода мошенничеством.

В настоящий момент принято выделять два типа blockchain: публичный – доступный для любого человека в мире, и приватный – с ограниченным членством.

Представим преимущества и недостатки, которые существуют на данном этапе развития в blockchain в таблице 1 [1].

ТАБЛИЦА 1. Преимущества и недостатки blockchain

Преимущества	Недостатки
Децентрализация	Масштабируемость
Надежность	Мошенничество и ошибки
Прозрачность	Открытость финансов в контексте внутренних рабочих процессов крупной компании
Теоретическая неограниченность	Низкая скорость обработки транзакций
Конфиденциальность	Возможность проведения незаконных операций

Безопасность в технологии blockchain обеспечивается через децентрализованный сервер, который устанавливает одноранговые сетевые соединения. После синхронизации с другими узлами сети сохраняются все записи транзакций. Целостность и хронологический порядок транзакций реализуются с помощью криптографических правил [3].

Структура блока представлена в таблице 2 (см. ниже).

Заголовок блока состоит из трех наборов метаданных. Во-первых, это ссылка на предыдущий хеш блока, который соединяет этот блок с предыдущим блоком в цепочке блоков. Второй набор метаданных, а именно сложность, временная метка и некое случайное число. Третьей частью метаданных является корень дерева Меркла – структура данных, используемая для эффективного суммирования всех транзакций в блок.

ТАБЛИЦА 2. Структура блока

Длина поля	Описание	Тип данных	Примечание
4	version	int32_t	Информация о версии блока
32	previousblockhash	char[32]	Значение хеша предыдущего блока (родительский блок), на который ссылается данный блок
32	merkle_root	char[32]	Ссылка на корень дерева Merkle, которая является хешем всех транзакций, связанных с этим блоком
4	timestamp	uint32_t	Запись метки времени и даты, создания этого блока, для предотвращения многократного изменения одной и той же информации (внесения информации в один блок несколько раз)
4	bits	uint32_t	Расчетное значение сложности, используемое для этого блока
4	nonce	uint32_t	Одноразовое значение, используемый для генерации этого блока и чтобы разрешить вариации заголовка и вычислить разные хэши
?	txn_count	var_int	Количество записей транзакции
?	txns	tx[]	Транзакции блока в формате "tx"

Каждый узел всегда «знает» хеш и структуру блока генезиса, фиксированное время его создания и даже одну транзакцию внутри. Таким образом, каждый узел имеет начальную точку для блок-цепи – защищенный «корень», из которого создается надежная блок-цепочка.

Обмен сообщениями Blockchain определяет логику взаимодействия между узлами, а также формат перевода какой-либо структуры данных в последовательность бит для обмена сообщениями по сети.

Алгоритм действий Blockchain технологии при работе с транзакциями представлен на рис. 1 (см. ниже).

Блок передается в сеть по традиционной TCP/IP технологии. Блок представляет собой некий контейнер, который объединяет транзакции для включения в публичный реестр.

Также необходимо рассмотреть влияние на сеть, так как в процессе обмена blockchain генерирует дополнительный трафик для обновления реестров на всех задействованных узлах, и увеличенного объёма служебного трафика, который появляется при шифровании данных и заметно снижает долю полезного трафика (рис. 2). То, что происходило раньше на одном устройстве теперь дублируется на все узлы, в связи с чем увеличивается

количество передаваемых сообщений в *n* раз (где *n* – количество задействованных узлов). Такие данные передаются небольшими порциями, но за короткий промежуток времени, что приводит к резким всплескам передаваемых сообщений и при больших объёмах может нарушить работу сети.

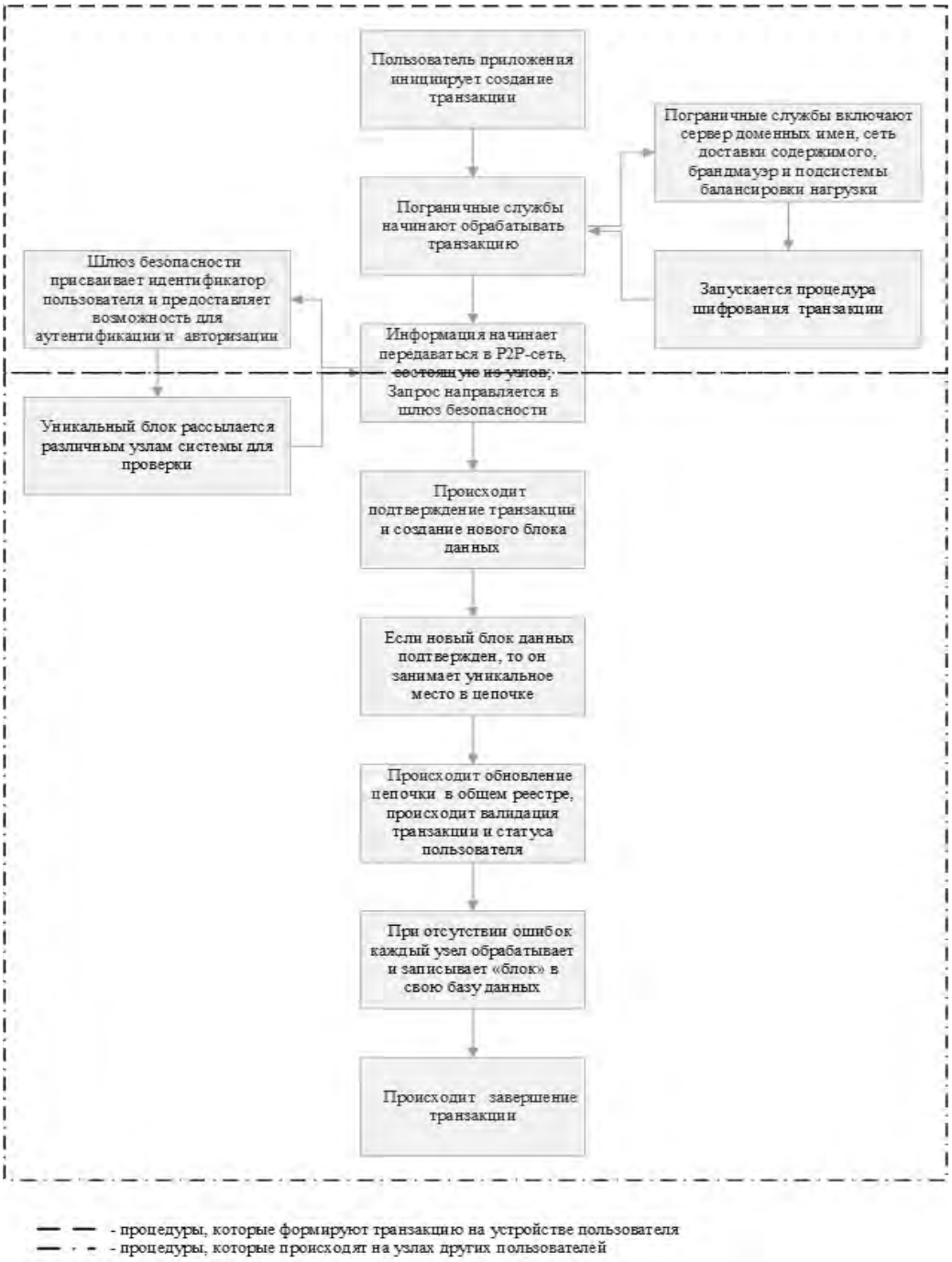


Рис. 1. Алгоритм действий Blockchain технологии при работе с транзакциями

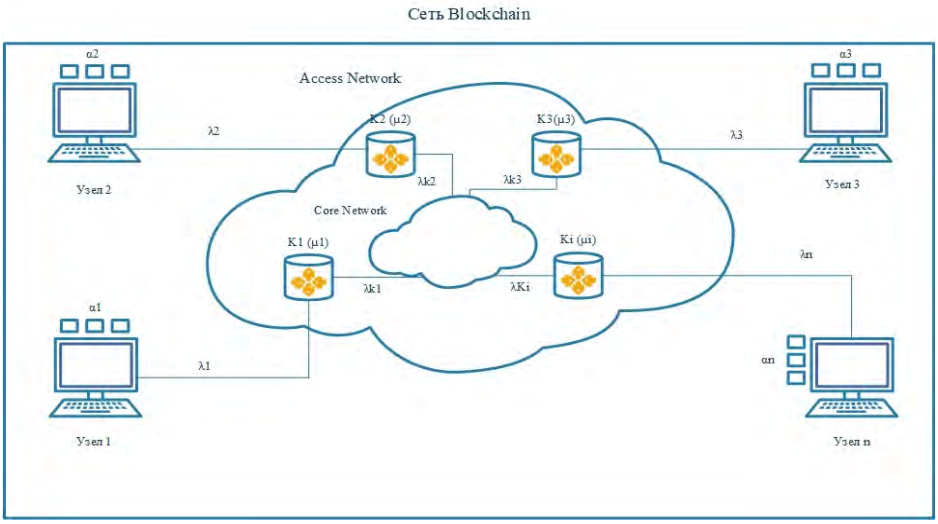


Рис. 2. Схема распределения потоков трафика blockchain

Загрузка сети (ρ) при этом будет зависеть от:

$$\rho \sim F(n, a_n, d, \lambda_n, \mu, k_i), \quad (1)$$

где: n – количество узлов в сетиblockchain (единиц); a_n – интенсивность формирования транзакций (транзакций в секунду); k_i – количество задействованных маршрутизаторов (единиц); μ – интенсивность обработки пакетов маршрутизаторами (пакетов в секунду); λ_n – интенсивность формирования пакетов (пакетов в секунду); d – размер блоков (байт).

Следовательно, при формировании и подтверждении транзакции, blockchain провоцирует лавинообразную загрузку сети.

Появляется задача рассмотреть, как blockchain повлияет на работу сети и как отразится его дальнейший рост на другие технологии, так как это может способствовать появлению недостатка ресурсов, который приведет к увеличению вероятности потерь пакетов и росту задержек, вследствие чего необходимые показатели качества для приложений реального времени не могут быть обеспечены, что может привести к повторной передаче пакета и изменению порядка формирования транзакций.

Определение класса обслуживания для трафика blockchain зависит от типа услуг, для которых он применяется. Необходимо исследовать какой класс будет достаточен для обеспечения приложений с трафиком критичным к задержкам, однако для ряда приложений, которые менее критичны к задержкам можно варьировать класс исходя из других значений данной услуги.

При этом рост числа узлов blockchain будет значительно влиять на характеристики сети. Детальное исследование представленной в формуле (1) зависимости позволит оценить, насколько каждый узел будет загружать сеть и как скажется определенный рост на характеристиках сети, которые

необходимы для качественной работы сети. Предварительные расчеты помогут подготовить сеть к работе с необходимым количеством устройств.

При рассмотрении нашего вопроса о качестве обслуживания трафика, необходимо чётко и однозначно дифференцировать трафик blockchain и трафик других приложений, что можно сделать с использованием DPI-системы, а для улучшения качества распознавания предлагаем добавлять различные метки в блоки от приложений, требующих разного уровня обслуживания [4, 5].

Технология blockchain предполагает взаимное влияние с сетью, качество услуг зависит от качества передачи и обработки данных, а работоспособность сети зависит от определенных параметров, появляющихся в результате работы приложений blockchain.

Список используемых источников

1. Mougayar W. The business blockchain. M. : John Wiley & Sons, Inc., Hoboken, New Jersey, 2016. 169 p.

2. Елагин В. С., Онуфриенко А. В. Как оператору заработать на OTT-сервисах и причем тут SDN? // T-COMM – Телекоммуникации и Транспорт. 2017. № 1. С. 17–21.

3. Kotenko V., A. Kuleshov and I. Ushakov, Aggregation of elastic stack instruments for collecting, storing and processing of security information and events // 2017 IEEE Smart World, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, San Francisco, CA, 2017, PP. 1–8.

4. Elagin V. S., Goldshtein A. B., Onufrienko A. V., Zarubin A.A., Belozertsev I. A. Synchronization of delay for OTT services in LTE // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, 2018, PP. 1–4

5. Elagin V. S., Goldshtein B. S., Onufrienko A. V., Zarubin A. A., Savelieva A. A. The efficiency of the DPI system for identifying traffic and providing the quality of OTT services // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2018, PP. 1–5.

УДК 004.942
ГРНТИ 49.33.29

МОДЕЛИ ОБЕСПЕЧЕНИЯ QOE ДЛЯ OTT СЕРВИСОВ

И. А. Белозерцев, В. С. Елагин, А. В. Онуфриенко

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

В данной статье рассмотрены основные модели, которые способствуют улучшению качества для OTT сервисов. Основной параметр для оценки качества был выбран

QoE – Quality of Experience. Был произведен анализ ряда факторов, которые непосредственно влияют на оценку QoE. Во второй частит статьи рассматривались модели, которые могут обеспечить необходимый уровень качества для OTT сервисов. Данные модели были поделены на три группы: модели на основе трафика, модели на основе приложения и модели на основе скоростных характеристик. Главная задача исследования – найти оптимальные решения для обеспечения качества OTT сервисов.

OTT сервисы, QoE, MOS.

На сегодняшний день традиционные услуги связи, которые предоставляет оператор, устаревают и на их место приходят OTT сервисы [1], которые предоставляют широкой спектр услуг: потоковые и интерактивные сервисы, сервисы обмена сообщениями и данными. Потоковые сервисы OTT, такие как You Tube, Netflix, Hulu, требуют обеспечения качества режимах ультравысокой четкости, 3D, которые нуждаются в большом потреблении трафика и предлагают более высокое требование для скорости сети. То есть, для OTT сервисов с их требованиями к ресурсам необходимо гарантировать качество передачи для отдельных видов сервисов. И поэтому по сравнению с основными телекоммуникационными услугами, OTT сервисы нуждаются в дополнительной поддержке со стороны сетевых операторов. Поэтому необходимо применять математические модели при работе с OTT сервисами, что поможет обеспечить качество, необходимое для этих сервисов.

QoE для OTT сервисов

QoE (*Quality of Experience*) – это общая удовлетворенность пользователей обслуживанием, которое они испытывали, на что может повлиять множество факторов в цепочке обслуживания. Рассматривая ключевые факторы, мы можем разработать соответствующие алгоритмы и модели для получения QoE.

Затем, основываясь на значении QoE, различные решения и оптимизация, включая классификацию трафика, управление пропускной способностью и алгоритмы переключения, могут использоваться для повышения удобства пользователей и повышения эффективности сети (рис. 1).

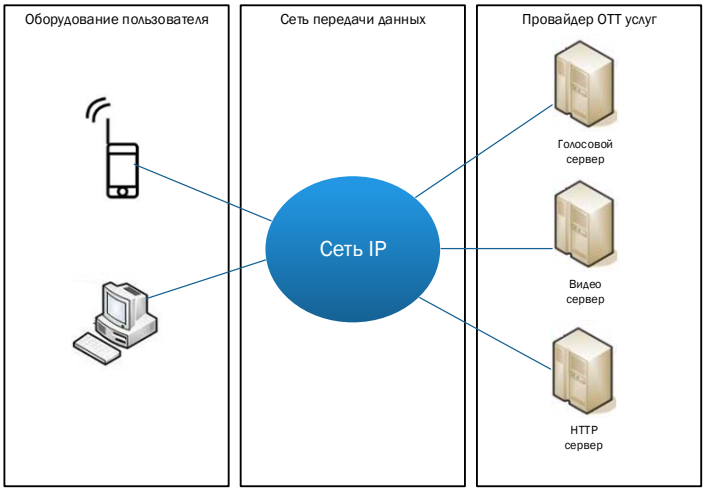


Рис. 1. Схематическое представление передачи OTT сервисов

Модели для оценки QoE

Существующие методы оценки QoE можно разделить на субъективный метод оценки, объективный и субъективно-объективный метод оценки, в зависимости от того, участвует ли пользователь в оценке и существует ли корреляция модели QoE и ее влияющих факторов. Помимо этого, необходимо учитывать количественный метод, суть которого заключается так называемой «средней оценке» (MOS – *Mean Opinion Score*) [4].

Модель на основе трафика

Ricky K. P. Mok в [2] установил сопоставление между метриками сетевого уровня, метриками уровня приложения и пользовательской оценкой MOS. Он смог получить взаимосвязь между метриками прикладного уровня (начальное время буферизации, задержку повторной буферизации и частоту повторной буферизации) и метриками сетевого уровня (пропускная способность, джиттер, потеря пакетов) (рис. 2).

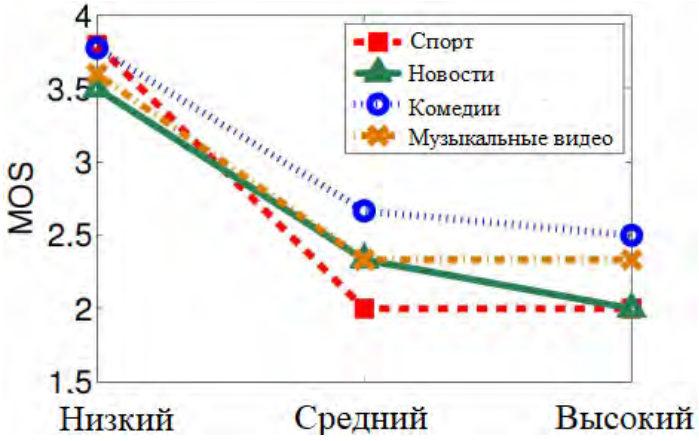


Рис. 2. MOS в зависимости от f_{rebuf} для четырех видов видео

$$MOS = 4{,}23 - 0{,}0672Lti - 0{,}742Lfr - 0{,}106Ltr,$$

где *Lti* – начальное время буферизации, *Lfr* – частота повторной буферизации, *Ltr* – время повторной буферизации.

Также он классифицировал видео на низкий, средний и высокий уровени в соответствии с метриками QoS прикладного уровня (табл.).

ТАБЛИЦА. Три уровня производительности приложения

Уровень	T_{ini}, с	f_{rebuf}, с	T_{rebuf}, с
Низкий	0–1	0–0,02	0–5
Средний	1–5	0,02–0,15	5–10
Высокий	> 5	> 0,15	> 10

Модель предсказания в [2] была оптимизирована в [3], принимая во внимание время просмотра пользователем, время паузы и другие фак-

торы. Однако в документе не получена конкретная формула, просто доказано, что учет факторов поведения пользователя может повысить точность моделей прогнозирования QoE.

На основе алгоритма Q-обучения в [6] был предложен клиент HAS, который может динамически настраиваться в соответствии с состоянием сети. Учитывая необходимую скорость для видео, емкость сети, и повторную буферизацию, было предложено уравнение для получения MOS в [5]:

$$eMOS = \max(5{,}67 * \mu - 6{,}72 * \sigma - 4{,}95 * \varphi + 0.17, 0),$$

где μ и σ представляют собой математическое ожидание и среднеквадратическое отклонение, а φ – определяет влияние частоты и задержки на оценку пользователей (MOS).

В ходе эксперимента была проведена оценка MOS и эффективности данной методики обучения для различных видео длинной 10 минут. Данные видео отрезки делились на 800 кадров, где оценивался определенный уровень MOS. Наилучший прирост наблюдался в последних 50 кадрах. В качестве сравнения выбирались RL (*Reinforcement Learning*) клиент, основанный на HAS, и традиционный MSS (*Microsoft ISS Smooth Streaming*) клиент (рис. 3).

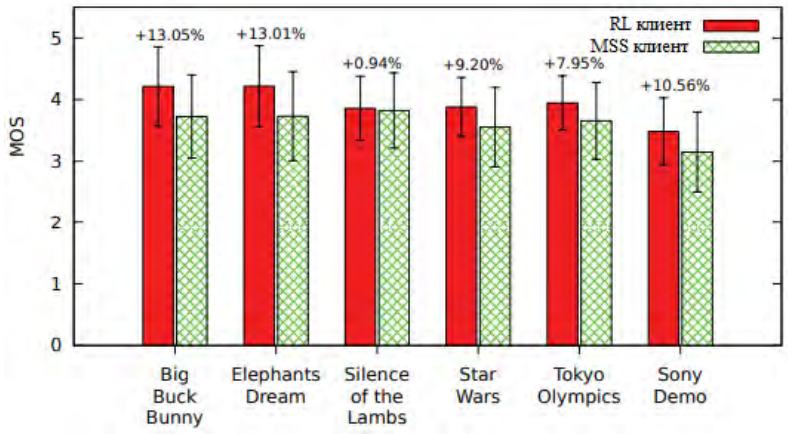


Рис. 3. Оценка эффективности RL клиент для нескольких видео последовательности в последних 50 кадрах.

Модель на основе приложения

В [6] был описан инструмент YoMo для мониторинга YouTube. Инструмент взял пользовательские оценки как «хорошо» или «плохо», где оценка «хорошо» – видео воспроизводилось, а «плохо» – видео буферизировалось. Эта модель в основном зависела от двух пороговых значений: одна была значением, вызвавшим повторную буферизацию, другое – минимальным значением, которое могло бы возобновить воспроизведение видео. Сравнивая два порога, можно вычислить время повторной буферизации.

Модели на основе скорости

В традиционных моделях видео необходимо декодировать и обрабатывать и в зависимости от того, какая часть исходной видеопоследовательности обработана, необходимо на основе этого сделать предсказание MOS. Подобно традиционным моделям, модели, работающие в домене с битовой скоростью для HAS, имеют индикацию качества, связанную с сегментом, и ей необходимо обеспечить QoE последовательности фрагментов с функцией скорости данных приложения R:

$$U = MOS(R).$$

Исходя из предположения о том, что существует простое линейное отображение между MOS и PSNR (*Peak Signal to Noise Ratio*) в [7], и учитывая длину профиля и уровень воспроизводимого качества видео, в [8] был представлен предсказанный MOS (*Mpred*), который высчитывался по формуле:

$$Mpred = \alpha \cdot \mu - \beta \cdot \sigma - \gamma \cdot \varphi + \delta,$$

где α, β, γ и δ являются настраиваемыми параметрами, μ – информация о качестве (например, скорость в определенный момент времени), σ –отклонение при измерении параметра μ, φ – частота переключения между моментами времени.

В данном случае ссылаемся на HAS профиль, где P определяется как последовательность чисел (l_1, ..., l_k, ..., l_K), где $l_k \in \{1, 2, ..., L\}$ указывает, что в сегменте k видео было воспроизведено по качеству значением l_k ($l = 1$ указывает наименьшее качество и $l = L$ самое высокое), а K – длину профиля ($k = 1$ указывает самый последний сегмент). И каждый такой профиль имеет собственную оценку MOS.

Заключение

При обслуживании OTT сервисов ряд сторонних факторов, которые не всегда зависят от среды передачи, влияют на обеспечение качества. Поэтому и для анализа необходимо учитывать не только показатели качества на сети, относящихся к оборудованию, но и учитывать восприятие самого пользователя. Для этого и производится оценка QoE.

Для грамотной же оценки необходимо связывать параметры, относящиеся к оборудованию, с факторами, которые связаны с пользовательским восприятием. Для этого был разработан моделей, которые пытаются связать данные параметры, но все упирается либо в несовершенность описанной модели, что не учитывает ряд факторов, либо в сложность самой модели.

Поэтому существующие модели оценки QoE, представленные в данной статье, недостаточно точны, поскольку редко учитывают факторы эмоцио-

нальной состояния пользователя, а также корреляцию между этими факторами. Важно подбирать для различных сервисов ту модель, которая бы максимально эффективно обеспечивало качество для пользователя.

Список используемых источников

1. Гольдштейн Б. С., Елагин В. С., Белозерцев И. А. О качестве OTT услуг в сетях LTE // Вестник связи. 2018. № 7. С. 9–12.

2. Steven Latré, Nicolas Staelens, Pieter Simoens. On-line estimation of the QoE of progressive download services in multimedia access networks[C] // ICOMP 2008, Las Vegas, Nevada, USA, 2008:14–17.

3. Ricky K. P. Mok, Edmond W. W. Chan, and Rocky K. C. Chang. Inferring the QoE of HTTP Video Streaming from User-Viewing. Activities [C]. W-MUS [16].

4. International Telecommunication Union. Geneva. Methods for subjective determination of transmission quality. Report : ITU TP.800, 1996.

5. A. Balachandran, V. Sekar, A. Akella, S. Seshan et al. A quest for an Internet video Quality-of-Experience, metric. In ACM HotNets, 2012.

6. S. Mohamed and G. Rubino. A Study of Real–time Packet Video Quality Using Random Neural Networks // IEEE Trans. On Circuits and Systems for Video Tech., 200–12, 12(12): 1071–1083.

7. VQEG, “Final report from the video quality experts group on the validation of objective models of video quality assessment”.

8. Johan De Vriendt, Danny De Vleeschauwer, Model for estimating QoE of Video delivered using HTTP Adaptive Streaming [C], IFIP/IEEE IM, 2013.

УДК 004.02
ГРНТИ 49.01.75

ПРИМЕНЕНИЕ ТЕОРИИ ХАОСА ДЛЯ ПРОГНОЗИРОВАНИЯ ОТТОКА АБОНЕНТОВ

А. М. Белозор, А. Б. Гольдштейн

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

Решение проблемы прогнозирования оттока клиентов актуально для всех операторов связи. Отток клиентов можно отнести к хаотическим процессам, т. к. многие из факторов, определяющих отток, не зависят от оператора и не могут быть определены и описаны заранее. В докладе описаны возможности применения математического аппарата теории хаоса для прогнозирования оттока абонентов оператора связи.

отток абонентов, теория хаоса, управление клиентским опытом управление взаимоотношениями с клиентами, OSS/BSS системы.

Управление клиентским опытом (CEM или CXM) представляет собой совокупность процессов, используемых компанией для отслеживания, контроля и организации каждого взаимодействия между клиентом и организацией на протяжении всего жизненного цикла клиента [1].

Целью CEM является оптимизация взаимодействия с точки зрения клиента и повышение лояльности клиентов. С технической точки зрения сбор и обработка численных параметров, характеризующих взаимодействие абонента и оператора связи, является основным инструментом бизнеса. Для оптимизации и автоматизации этих процессов используются специальные CEM-системы, позволяющие собирать и анализировать данные в режиме реального времени. В результате использования инструментов бизнес-анализа оператор получает возможность взаимодействовать с абонентами персонально, делая индивидуальные предложения [2]. На основе собранных данных так же рассчитывается такой важный параметр как отток клиентов.

Отток клиентов в телекоммуникациях – процесс перехода абонента из сети одного оператора в сеть другого оператора, а также частичный или полный его отказ от телекоммуникационных услуг. Он служит показателем того, сколько клиентов покидают компанию в течение определенного периода времени [3, 4].

Используется классификация оттока на следующие типы: с договором или без договора, добровольный или недобровольный. Объем данного доклада не позволяет углубиться в особенности классификации, но она будет рассмотрена более подробно в других работах авторов. Однако важно отметить, что отток абонентов оператора связи совмещает в себе свойства всех типов, тем самым становясь еще более сложным процессом.

Проблема оттока всегда актуальна для операторов связи. Поэтому изучение методов его прогнозирования не стоит на месте. С появлением новых технологий в мире инфокоммуникаций появляются и новые способы прогнозирования [5].

В наши дни основными средствами для предсказания являются в меньшей степени математические классификаторы (логическая регрессия, наивный Байесовский алгоритм), а в большей – методы машинного обучения (случайный лес, градиентный бустинг) [6].

Логистическая регрессия как разновидность множественной регрессии является одним из статистических методов классификации. Основное назначение логической регрессии – анализ связи между несколькими независимыми переменными (называемыми также регрессорами или предикторами) и зависимой переменной. Это происходит с использованием линейного дискриминанта Фишера – метода, определяющего расстояние между распределениями двух разных классов объектов или событий [7].

Наивный Байесовский алгоритм – это классификатор, основанный на теореме Байеса с наивным (очень смелым) предположением о том, что признаки, на которые опирается классификация, независимы. Цель этого метода – определить класс события, поэтому акцент ставится на нахождение наиболее вероятного класса, а не на нахождение самой вероятности [8, 9].

Случайный лес – это алгоритм машинного обучения, применяемый для задач кластеризации, регрессии и классификации, создающий ансамбль деревьев решений, а затем усредняющий полученные результаты. Каждое отдельное дерево дает невысокое качество прогноза, но большое их количество позволяет получить более точный и полный результат [10].

Градиентный бустинг – это метод машинного обучения для решения проблем регрессии и классификации, создающий модель прогнозирования в виде линейной комбинации простых моделей (например, набора деревьев принятия решений). Простые модели строятся поэтапно, причем так, чтобы их обобщение оптимизировало прогнозирование каждой из моделей в отдельности. Каждый следующий этап корректирует недостатки предыдущей модели, используя перевзвешенные данные, что позволяет добиться более точного результата [11].

Однако ни один из этих методов не может верно оценить и учесть параметры, не зависящие от оператора связи. Поэтому разработка новых методов прогнозирования оттока продолжается.

Так как оператор связи может влиять только на некоторые параметры: количество обращений в службу поддержки, количество аварий на сети, изменения в тарифном плане – остаются причины оттока, предсказать которые оператор не может: переезд абонента, изменение состояния его здоровья, изменения в тарифных планах оператора-конкурента и т. д. Соответственно численно описать для использования в прогнозировании оператор может только первую категорию величин. Параметры второй категории возникают неожиданно и, как сказано ранее, не могут быть предсказаны оператором, так как по своей сути являются хаотичными процессами.

Наличие в процессе оттока хаотичных компонентов делает весь процесс хаотичным. Подход к оттоку со стороны теории хаоса позволяет увидеть закономерности, которые невозможно описать без нее.

Теория хаоса – математический аппарат, описывающий поведение систем, характер функционирования которых кажется случайным. На самом деле эти нелинейные системы подчиняются порядку другого уровня – динамическому хаосу. В рамках данного доклада невозможно осветить все аспекты теоретической базы и математических методов теории хаоса, поэтому остановимся лишь на некоторых из них.

Хаос появляется из-за неустойчивости системы, то есть ее высокой чувствительности к начальным условиям. Начальные условия не могут быть за-

даны с абсолютной точностью (например, из-за погрешности измерительных приборов и несовершенства вычислительной техники), поэтому через некоторое время ответ может быть дан в виде вероятности значения или некоторого множества значений. Однако, это множество не бывает бесконечным.

Математические системы, подверженные хаосу, являются детерминированными, то есть подчиняющимися определенной закономерности. И даже кажущиеся самыми нестабильными, оказываются предсказуемыми. Эта предсказуемость выражается в особых графиках – странных аттракторах.

Странный аттрактор – геометрическая структура, к которой стремится динамическая система в процессе развития со сложной и запутанной структурой. Как правило представляет собой незамкнутые кривые. Пример странного аттрактора представлен на рис. 1 [12].

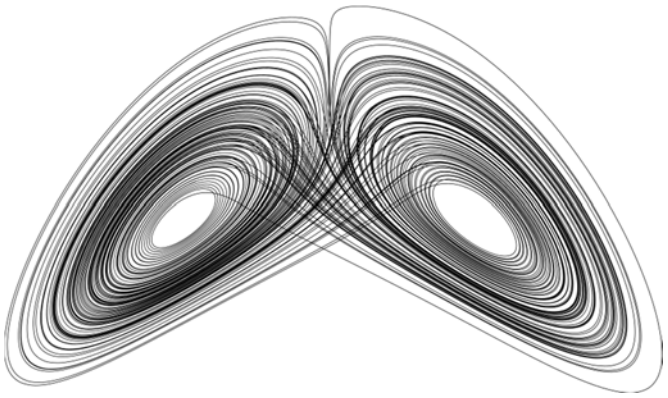


Рис. 1. Странный аттрактор

Аттрактор характеризует поведение исследуемой системы в определенном фазовом пространстве. Под фазовым пространством понимают некое абстрактное пространство, роль координат в котором выполняют те независимые величины, влияние на систему которых принимается во внимание.

Важной частью странного аттрактора является точка бифуркации – это такое соотношение параметров системы, из которого она может перейти в одно из двух состояний. В этом положении на поведение системы влияют даже малейшие изменения параметров окружающей среды [13]. На рис. 1 результатом прохождения точки бифуркации может быть смена «крыла» странного аттрактора или продолжение движения по «крылу»

Чтобы воспользоваться теорией хаоса для прогнозирования оттока, нужно понимать, от каких параметров он зависит. Для этого можно проанализировать уже имеющиеся данные с маркировкой ушедших и оставшихся абонентов. Например, базу данных фирмы Telco, выложенную в свободный доступ.

Анализ различных параметров, прописанных в этой базе данных показал, что наиболее очевидна зависимость оттока абонентов от стоимости обслуживания, от длительности использования услуг и от типа оплаты.

Процент ушедших абонентов с меньшими затратами меньше, чем абонентов с большими затратами. С ростом размера оплаты процент оттока увеличивается, что видно на рис. 2. Но, когда размер оплаты становится выше,

чем определенное значение (в рассматриваемой базе данных это 100 единиц), процент уходящих абонентов становится меньше. Можно объяснить это тем, что тариф становится премиальным и к нему предъявляются другие требования по цене.

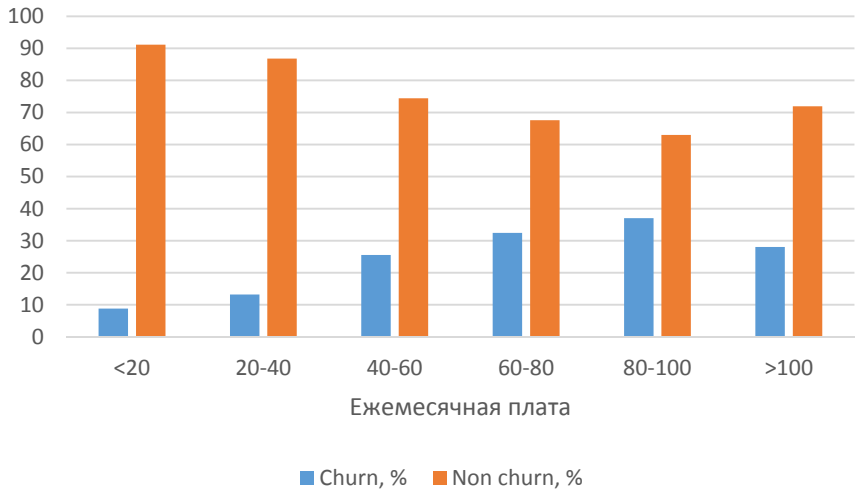


Рис. 2. Зависимость процента оттока от размера ежемесячной оплаты

Чем дольше клиент пользуется услугами оператора, тем меньше вероятность его ухода (рис. 3). В первые месяцы от услуг оператора отказывается больше абонентов, чем в последующие (в рассматриваемой базе данных более 50 % ушедших пользовались услугами меньше года).

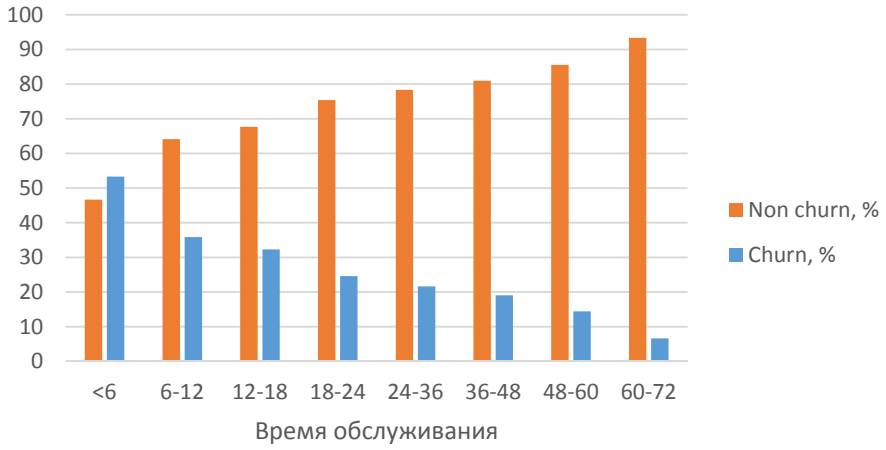


Рис. 3. Зависимость процента оттока от времени обслуживания

Клиенты с помесячной оплатой составляют практически 90 % ушедших (при том, что их доля среди общего числа абонентов около 50 %). На рис.4 видно, что чем больше период оплаты, тем меньше отток абонентов с таким типом оплаты.

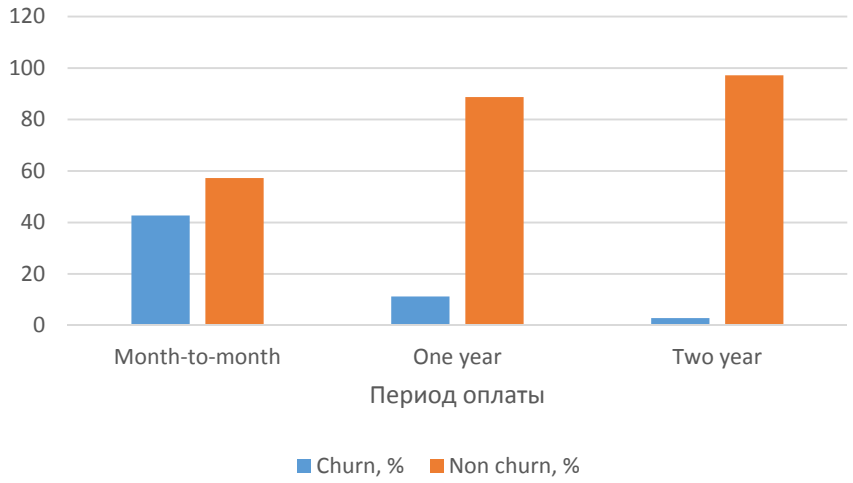


Рис. 4. Зависимость процента оттока от периода оплаты

Описанные выше закономерности позволяют сделать вывод о том, что комбинация таких параметров, как размер ежемесячной оплаты, длительность использования услуг и величина периода оплаты, подходит для описания фазового пространства: это независимые друг от друг переменные, значительно влияющие на отток. Это означает, что на их основании можно будет сделать простейшее прогнозирование оттока абонентов на основе теории хаоса. Имея представление о фазовом пространстве, в котором будет изучаться система, можно приступить к ее математическому описанию, на основе которого будут строиться прогнозы.

Цель дальнейших исследований – сравнение эффективности применения различных методов теории хаоса для прогнозирования оттока на основе имеющейся открытой базы данных Telco.

Список используемых источников

1. Rouse M. Customer Experience Management [Электронный ресурс] // Essential Guide: Build a WCM architecture that supports business needs. February 2018. URL: https://searchcustomerexperience.techtarget.com/definition/customer-experience-management-CEM-or-CXM.

2. Haslam C. Inspire loyalty with customer lifecycle management [Электронный ресурс] // TM Forum Research Report. June, 2018. URL: https://inform.tmforum.org/research-reports/inspire-loyalty-customer-lifecycle-management/ (дата обращения 11.04.2019).

3. Tavsan A. N., Erdem C. Customer Experience Management. Minneapolis, USA : Tasora Books, 2018. 258 с.

4. Рудская Е. Н., Полтавская Ю. Ю. Клиентский опыт (Customer Experience) как инструмент обратной связи в системе интеллектуального анализа данных // Молодой ученый. 2015. № 8. С. 631–639. URL: https://moluch.ru/archive/88/17090/ (дата обращения: 11.04.2019).

5. Hashmi N., Butt N. A., Iqba M. Customer Churn Prediction in Telecommunication. A Decade Review and Classification [Электронный ресурс]. URL: https://www.researchgate.net/publication/257920014_Customer_Churn_Prediction_in_Telecommunication_A_Decade_Review_and_Classification (дата обращения 11.04.2019).

6. Danilina R. Building Customer Churn Models for Business [Электронный ресурс] // Datascience.com Blog. February 20, 2017. URL: https://www.datascience.com/blog/what-is-a-churn-analysis-and-why-is-it-valuable-for-business (дата обращения 11.04.2019).

7. Swaminathan S. Linear Regression–Detailed View [Электронный ресурс] // Towards Data Science. February 26, 2018. URL: https://towardsdatascience.com/linear-regression-detailed-view-ea73175f6e86 (дата обращения 11.04.2019).

8. Soni D. Introduction to Naive Bayes Classification [Электронный ресурс] // Towards Data Science. May 16, 2018. URL: https://towardsdatascience.com/introduction-to-naive-bayes-classification-4cffabb1ae54 (дата обращения 11.04.2019).

9. Баженов Д. Наивный байесовский классификатор [Электронный ресурс] // URL: http://bazhenov.me/blog/2012/06/11/naive-bayes (дата обращения 11.04.2019).

10. Donges N. The Random Forest Algorithm [Электронный ресурс] // Towards Data Science. February 22, 2018. URL: https://towardsdatascience.com/the-random-forest-algorithm-d457d499ffcd (дата обращения 11.04.2019).

11. Литвинов С. Градиентый бустинг — просто о сложном [Электронный ресурс]. URL: https://neurohive.io/ru/osnovy-data-science/gradientyj-busting/ (дата обращения 11.04.2019).

12. Бекман И. Н. Синергетика. Лекция 2. Динамические системы [Электронный ресурс]. URL: https://beckuniver.ucoz.ru/Kurs_Sinerget/Sinerg_Lec2.pdf (дата обращения 11.04.2019).

13. Немцев В. Н. Теоретические основы рискологии: монография. Магнитогорск : Изд-во Магнитогорск. гос. техн. ун-та им. Г. И. Носова, 2015. 207 с.

УДК 004.41/.42
ГРНТИ 81.96

АНАЛИЗ АТАКИ ФАКТОРИЗАЦИИ МОДУЛЯ В КРИПТОСИСТЕМЕ РША НА ОСНОВЕ МОДЕЛИРОВАНИЯ АЛГОРИТМА ШОРА С ИСПОЛЬЗОВАНИЕМ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

Е. О. Березина, В. А. Яковлев

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

Анализируется алгоритм Шора для осуществления атаки факторизации модуля криптосистемы РША. Проводится анализ квантового алгоритма Шора, состоящего из пяти шагов, четыре из которых выполняются на квантовом компьютере. Ускорение

вычислений основано на фундаментальном свойстве квантового параллелизма, позволяющего квантовым компьютерам вычислять функцию для различных значений аргумента одновременно. Приведен пример осуществления атаки факторизации на модуль криптосистемы РША данным методом. Выделены задачи по созданию симулятора квантовых вычислений для алгоритма Шора, который предполагается использовать для изучения атак на криптосистему РША в учебном процессе.

криптосистема РША, алгоритм Шора, квантовый алгоритм Шора, атака факторизации модуля.

Известно, что стойкость алгоритма РША основана на том, что злоумышленник не может решить задачу факторизации модуля M за разумное время [1].

С развитием квантовой технологии стало возможно использование для факторизации модуля алгоритма факторизации Шора [2]. Его суть заключается в сведении задачи факторизации к задаче поиска периода функции – а если он известен, то факторизацию можно осуществить с помощью алгоритма Евклида за полиномиальное время на классическом компьютере [3].

Рассмотрим сначала основные этапы алгоритма Шора [4]. Пусть имеется некоторое известное M, $M = p \cdot q$, где p и q – простые числа. Выберем число a, $a < M$, и определим функцию $f_a(x) = a^x \bmod M$. Без ограничения общности можно считать, что a и M – взаимно простые числа, $\text{НОД}(a, M) = 1$, иначе, определяя $\text{НОД}(a, M)$ с помощью алгоритма Евклида, можно сразу получить множитель в разложении M.

Функция $f_a(x) = a^x \bmod M$ – периодическая, то есть мы можем определить ее период r как порядок числа a в кольце Z_M, т. к. $a < M \equiv a \in Z_M$: $a^r = 1 \bmod M$, причем это число единственное, т. е. для любого $r_1 < r$ $a^{r_1} \neq 1 \bmod N$.

Рассмотрим пример факторизации модуля $M = 21$. Выберем случайное число $a = 2$, $\text{НОД}(2, 21) = 1$. Найдем период функции $f_2(x) = 2^x \bmod 21$ с помощью перебора всех возможных значений x (табл. 1):

ТАБЛИЦА 1. Перебор состояний $a^x \bmod M$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	…
a^x	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	…
$a^x \bmod 35$	1	2	4	8	16	11	1	2	4	8	16	11	1	…

период $r = 6$

Из таблицы видно, что период повторения функции $r = 6$. Поскольку r – четное, то его можно представить как $r = 2k$. Тогда получим

$a^r = a^{2k} = 1 \bmod N$ или $a^{2k} - 1 = 0 \bmod M$. Представим $a^{2k} = (a^k)^2$. Тогда, используя формулу разности квадратов, запишем $(a^k)^2 - 1 = (a^k - 1)(a^k + 1)$ и $(a^k - 1)(a^k + 1) = 0 \bmod M$, что означает наличие общего множителя у M и $(a^k \pm 1)$. Следовательно, с помощью алгоритма Евклида мы можем найти числа p и q как НОД$(a^k + 1, M) = p$ и НОД$(a^k - 1, M) = q$.

Для $r = 6$ из таблицы 1 имеем:

$$\text{НОД}((2^3 + 1), 21) = \text{НОД}(8 + 1, 21) = \text{НОД}(9, 21) = 3,$$

$$\text{НОД}((2^3 - 1), 21) = \text{НОД}(8 - 1, 21) = \text{НОД}(7, 21) = 7.$$

Проверяем: $p \cdot q = 3 \cdot 7 = 21 = M$. Далее на основании известных p и q можно вычислить функцию Эйлера и секретный ключ.

Таким образом, основным по затратам времени в алгоритме Шора является поиск периода функции $f_a(x) = a^x \bmod M$.

Опишем квантовый алгоритм для поиска периода r функции $f_a(x)$ [5]. Для вычисления используем два квантовых регистра: регистр $|x\rangle$, хранящий значения аргументов функции и регистр $|y\rangle$, хранящий значения функции (рис. 1). Введем число N, определяющее количество используемых кубитов n и отвечающее условиям $N = 2^n \geq M^2$ и $r \leq \sqrt{N}$. Например, если $M = 21$, $M^2 = 441$, $N = 2^n \geq M^2 \Rightarrow N = 512 = 2^9$, $\sqrt{N} \approx 22$, то есть $r < 22$.

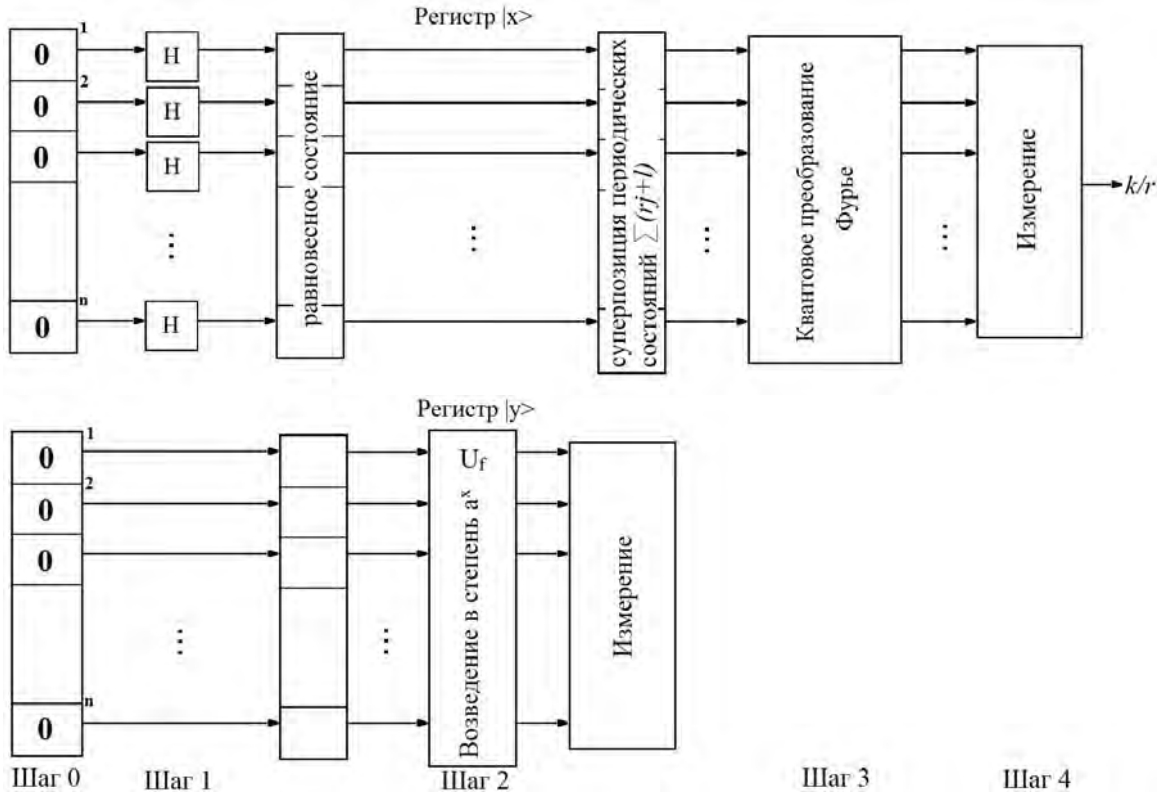


Рис. 1. Шаги реализации алгоритма Шора

Квантовый алгоритм Шора описывается последовательностью следующих шагов (рис. 1):

Шаг 0 (подготовительный этап). Все кубиты квантовых регистров устанавливаются в нулевое состояние вида:

$$\varphi_0 = |0\rangle|0\rangle .$$

Шаг 1 (равновероятное состояние). К каждому кубиту первого регистра применим преобразование Адамара. В результате регистр $|x\rangle$ переводится к равновероятной суперпозиции всех возможных состояний:

$$\varphi_1 = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle .$$

Шаг 2 (возведение в степень). Вычисляются значения функции $a^x \bmod M$ для всех x первого регистра аргументов, результаты записываются во второй регистр. В результате регистры будут в состоянии:

$$\varphi_2 = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle\left|a^x \bmod M\right\rangle .$$

Например, для $M = 21$ и $a = 2$ выберем $N = 512$, $n = 9$. Состояние φ_2 будет иметь вид:

$$\varphi_2 = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle\left|2^x \bmod 21\right\rangle = \frac{1}{2^{n/2}}[|0\rangle|1\rangle + |1\rangle|2\rangle + |2\rangle|4\rangle + |3\rangle|8\rangle + |4\rangle|16\rangle + |5\rangle|11\rangle +$$

$$+ |6\rangle|1\rangle + |7\rangle|2\rangle + |8\rangle|4\rangle + |9\rangle|8\rangle + |10\rangle|16\rangle + |11\rangle|6\rangle + ... + \left|2^n - 1\right\rangle\left|2^{2^x-1} \bmod M\right\rangle] .$$

Тогда каждому фиксированному состоянию регистра $|y\rangle$, соответствует последовательность значений регистра $|x\rangle$ (табл/ 2):

ТАБЛИЦА 2. Состояния регистров $|x\rangle\,|y\rangle$

A	$\|0\rangle\|1\rangle$	$\|1\rangle\|2\rangle$	$\|2\rangle\|4\rangle$	$\|3\rangle\|8\rangle$	$\|4\rangle\|16\rangle$	$\|5\rangle\|11\rangle$
	$\|6\rangle\|1\rangle$	$\|7\rangle\|2\rangle$	$\|8\rangle\|4\rangle$	$\|9\rangle\|8\rangle$	$\|10\rangle\|16\rangle$	$\|11\rangle\|11\rangle$
	…	…	…	…	…	…
	$\|24\rangle\|1\rangle$	$\|25\rangle\|2\rangle$	$\|26\rangle\|4\rangle$	$\|27\rangle\|8\rangle$	$\|28\rangle\|16\rangle$	$\|29\rangle\|11\rangle$
	…	…	…	…	…	…
	$\|504\rangle\|1\rangle$	$\|505\rangle\|2\rangle$	$\|506\rangle\|4\rangle$	$\|507\rangle\|8\rangle$	$\|508\rangle\|16\rangle$	$\|509\rangle\|11\rangle$
	$\|510\rangle\|1\rangle$	$\|511\rangle\|2\rangle$				

Например, фиксированному состоянию $|y\rangle = 4$ соответствует последовательность значений *x* вида:

$$\varphi_2 = \frac{1}{\sqrt{A}}\left(|2\rangle + |8\rangle + |14\rangle + ...\right) \otimes |4\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |r \cdot j + l\rangle |4\rangle,$$

где $A \approx \frac{N}{r}$, $l = 2$.

Таким образом, второй регистр служит для приготовления периодического состояния в первом регистре. Если провести измерение состояния $|y\rangle$, то некоторому конкретному значению $y = a^x \bmod M$ соответствует сумма базисных векторов вида $\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} (r \cdot j + l) = f(l)$. Функция $f(l)$ периодическая и имеет дискретный спектр, но, поскольку l – случайная величина, период можно определить только посредством использования квантового преобразования Фурье (КПФ).

Шаг 3 (квантовое преобразование Фурье). Осуществляется над последовательностью значений *x* в регистре $|x\rangle$, соответствующей фиксированному значению регистра $|y\rangle$. Преобразование Фурье в общем виде переводит состояние квантового регистра $|s\rangle$, где $s \in Z$, $0 \le s < N$ в состояние $\frac{1}{\sqrt{N}} \sum_{u=0}^{N-1} e^{2\pi i \frac{s \bullet u}{N}} |u\rangle$.

На выходе шага 3 получаем в регистре $|x\rangle$ состояние:

$$|x\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |l + j \cdot r\rangle \Rightarrow QFT|x\rangle = \frac{1}{\sqrt{AN}} \sum_{j=0}^{A-1} \sum_{u=0}^{N-1} e^{2\pi i \frac{l \bullet u}{N}} e^{2\pi i \frac{jru}{N}} |y\rangle = \frac{1}{\sqrt{AN}} \sum_{u=0}^{N-1} e^{2\pi i \frac{l \bullet u}{N}} \sum_{j=0}^{A-1} e^{2\pi i \frac{jru}{N}} |u\rangle.$$

Шаг 4 (наблюдение состояния). Для произвольного вектора $|u\rangle$ амплитуда состояний будет равна:

$$\frac{1}{\sqrt{AN}} e^{2\pi i \frac{l \bullet u}{N}} \sum_{j=0}^{A-1} e^{2\pi i \frac{jru}{N}}.$$

Тогда вероятность измерения такого *u* равна:

$$P(u^*) = \frac{1}{AN} \left| e^{2\pi i \frac{l \bullet u}{N}} \right|^2 \left| \sum_{j=0}^{A-1} e^{2\pi i \frac{jru}{N}} \right|^2 = \frac{1}{AN} \left| \sum_{j=0}^{A-1} e^{2\pi i \frac{jru}{N}} \right|^2.$$

Доказывается, что с вероятностью $P(u) = \frac{4}{\pi^2 r} \cdot r = \frac{4}{\pi^2} \approx 0,4$ *u* лежит в диапазоне $\frac{k}{r} - \frac{1}{2N} \le \frac{u}{N} \le \frac{k}{r} + \frac{1}{2N}$.

Таким образом, после выполнения алгоритма Шора имеем некоторое значение $\frac{u}{N}$, в окрестности $\frac{1}{N}$ которого лежит интересующее нас число $\frac{k}{r}$. Поиск этого $\frac{k}{r}$ может осуществляться методом непрерывной дроби.

Например, на выходе алгоритма получено $u = 85$, $\frac{u}{N} = \frac{k}{r}$, тогда при $M = 21$ и $N = 512$:

$$\frac{u}{N} = \frac{85}{512} = \frac{1}{\frac{512}{85}} = \frac{1}{6 + \frac{2}{85}} \Rightarrow \frac{1}{6}.$$

В результате вычислений методом непрерывной дроби мы получили число $r = 6$, которое является периодом функции $f(x)$.

Детальный анализ атаки факторизации позволяет сформулировать основные задачи для разработки симулятора квантового алгоритма Шора:

1. Моделирование квантовых вентилей и разработка алгоритма КПФ на этих вентилях.
2. Разработка алгоритма квантового возведения в степень.
3. Разработка алгоритма вычисления периода по результатам измерения состояния $|x\rangle$.

Симулятор предполагается использовать в учебном процессе кафедры защищенных систем связи СПбГУТ в рамках курса «Основы криптографии с открытым ключом» для анализа атак на криптосистему РША.

Список используемых источников

1. Коржик В. И., Яковлев В. А. Основы криптографии: учебное пособие. СПб. : ИЦ Интермедия, 2016. 296 с.
2. Ян Сонг Й. Криптоанализ RSA. Ижевск : НИЦ «Регулярная и хаотическая динамика», Ижевский институт компьютерных исследований, 2011. 312 с.
3. Босс В. Лекции по математике. Т. 10: Перебор и эффективные алгоритмы: учебное пособие. М. : Издательство ЛКИ, 2008. 216 с.
4. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. arXiv.quant-ph/9508027 v2, 1996.
5. Богданов А. Ю., Кижватов И. С. Квантовые алгоритмы и их влияние на безопасность современных криптографических систем. Обзор. М. : РГГУ, факультет защиты информации, 2005. 18 с.

УДК 621.391
ГРНТИ 49.33.29

АНАЛИЗ ПРОБЛЕМАТИКИ СОЗДАНИЯ АРХИТЕКТУРЫ МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ НА БАЗЕ ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ СЕТЕВЫХ ФУНКЦИЙ

К. Б. Боброва[1], А. К. Канаев[2], М. А. Сахарова[2]

[1]ОАО «Радиоавионика»
[2]Петербургский государственный университет путей сообщения Императора Александра I

Анализ проводимых исследований в направлении развития и возможности применения технологии виртуализации сетевых функций выявить различия и даже противоречия между различными подходами и существующим стандартом ETSI GS NFV-SWA 001 V1.1.1 (2014-12) в части построения архитектуры мультисервисной сети связи на основе предложенной технологии.

В статье представлен сравнительный анализ предлагаемых решений исследователями данной области и основных положений построения NFV, регламентированных стандартом ETSI. А также предложен порядок поэтапного перехода от использования узлов существующей мультисервисной сети передачи данных к новой архитектуре сети связи на базе технологии NFV.

Выявленные противоречия и проблематика построения архитектуры мультисервисной сети связи на базе технологии NFV определяет актуальность дальнейшего исследования и разработки вариантов ее совершенствования и применения в различных отраслях.

мультисервисная сеть связи (МСС), Network Function Virtualization (NFV), Management and Orchestration (MANO), Telecommunication Management Network (TMN).

Обеспечение требований к функционированию мультисервисной сети связи (МСС) для оказания услуг связи заданного качества определяется согласованной работой всех подсистем архитектуры МСС.

Разработка научно обоснованных принципов перехода от МСС к технологии виртуализации сетевых функций (*Network Function Virtualization*, NFV) с предложением по разработке новой (альтернативной) архитектуры с учетом существующих стандартов к качеству сети связи на базе NFV, а также с заменой выделенного сетевого оборудования на специализированное программное обеспечение (ПО), в свою очередь позволила предложить алгоритм достижения поставленной задачи.

Переход от традиционной МСС к технологии NFV позволит выстроить гибкую, стабильно работающую архитектуру сети, которую можно подстраивать при увеличении или уменьшении объема передаваемой нагрузки.

Основная задача управления сетью состоит в обеспечении заданных требований к функционированию МСС. Одним из решений построения и реализации системы управления (СУ) является концепция сети управления электросвязью (*telecommunication management network*, TMN) [1].

Концепция TMN основана на базовых принципах управления открытыми системами и обеспечивает управление, оперативный контроль (мониторинг) и автоматизированную эксплуатацию телекоммуникационного оборудования. Концепция TMN используется для управления услугами сетей связи для администрирования сетевыми устройствами с целью обеспечения качества оказания услуг и безопасности связи (рис. 1) [1, 3].

Рис. 1. Взаимосвязь TMN, eTOM и NGOSS

Для обеспечения функций контроля предоставления сервисов и бизнес-процессов была разработана концепция eTOM.

Модель eTOM предоставляет рекомендации для распределения бизнес-процессов по категориям, управления процессами, заключения соглашений с поставщиками и партнерами и является стартовой точкой при проведении работ по реинжинирингу бизнес-процессов [3].

Модель Next Generation OSS (NGOSS) включает карты операций, архитектуру приложений и информационные модели [3].

Предоставляя многообразие услуг, МСС включает в себя большое количество телекоммуникационного оборудования, для передачи разнородной информации. Решение задач по оперативному контролю и эксплуатации отвечает концепция TMN определяющая принципы создания единой системы управления для сетей разных уровней

Для оптимизации услуг, параметров элементов сети МСС в целом, переход к технологии NFV позволит операторам трансформировать сетевую инфраструктуру за счет виртуализации сетевых функций.

Архитектура NFV представлена в [2].

Инфраструктура сети виртуализации (*Network Function Virtualization Infrastructure*, NFVI) включает аппаратные (*Hardware*) и программные (*Virtual*) ресурсы.

С целью реализации программных ресурсов на разных аппаратных платформах в группе ETSI предложено ввести уровень виртуализации (*Virtualisation Layer*). На этом уровне находится программное обеспечение (ПО гипервизор), позволяющее запускать несколько виртуальных машин. На каждой виртуальной машине устанавливается необходимое ПО.

Непосредственную реализацию (разработку) выделенной сетевой функции (маршрутизация, коммутация и т. д.) позволяет обеспечить блок VNF (*Virtual Network Function*).

Контроль состояния и управление инфраструктурой сети и виртуализацией функций осуществляется с помощью модуля СУ (MANO) [2]. Оказание услуг по передаче информации прочно связано с вопросами комплексного управления сетями связи. Цель управления – обеспечение заданного уровня качества оказания услуг и функционирования сетей связи. При сравнении архитектуры NFV и архитектуры TMN выявлено отсутствие в СУ (MANO) NFV уровня управления сетью, а именно, явно не представлено какая часть архитектуры NFV отвечает за совокупность организационно-технических мероприятий, в том числе регулирование трафика.

Также, согласно архитектуре NVF не ясно, почему класс программных средств OSS/BSS относится к блоку аппаратно-программного комплекса (АПК) NFV, а не выделен в раздел СУ (MANO).

Для подключения нового пользователя или расширения перечня предоставляемых услуг требуется добавление нового соответствующего оборудования, что влечет за собой необходимость поиска свободного места или установка новой стойки, отдельного источника питания, а также специалиста, обладающего необходимыми знаниями и т. д.

Увеличение объема предоставляемых инфокоммуникационных услуг влечет за собой наращивание разнообразного телекоммуникационного оборудования вследствие чего, возрастает потребность в строительстве и эффективном использовании сетевой инфраструктуры, обеспечивающей передачу непрерывно растущего абонентского и интернет трафика.

Используя единый канал для передачи данных, к МСС предъявляются требования [4, 5, 6] определяющие сетевые характеристики и нормы качества обслуживания в сетях.

Все эти особенности привели к развитию новой технологий, позволяющей повысить эффективность капиталовложений и общую гибкость сетевой

архитектуры за счет ухода от аппаратных реализаций в сторону программного внедрения сетевых услуг.

Переход от стандартной архитектуры МСС к архитектуре на основе технологии NFV с обеспечением требований к сетям связи [4, 5, 6], можно выполнить поэтапно.

На первом этапе (рис. 2) сетевые функции второго и третьего уровня модели OSI реализуются программно на сервере, на котором запущено несколько виртуальных машин. Суть виртуализации заключается в замене реальных ресурсов виртуальными с теми же функциями что и у физических прототипов и обеспечение при этом логической изоляции друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.

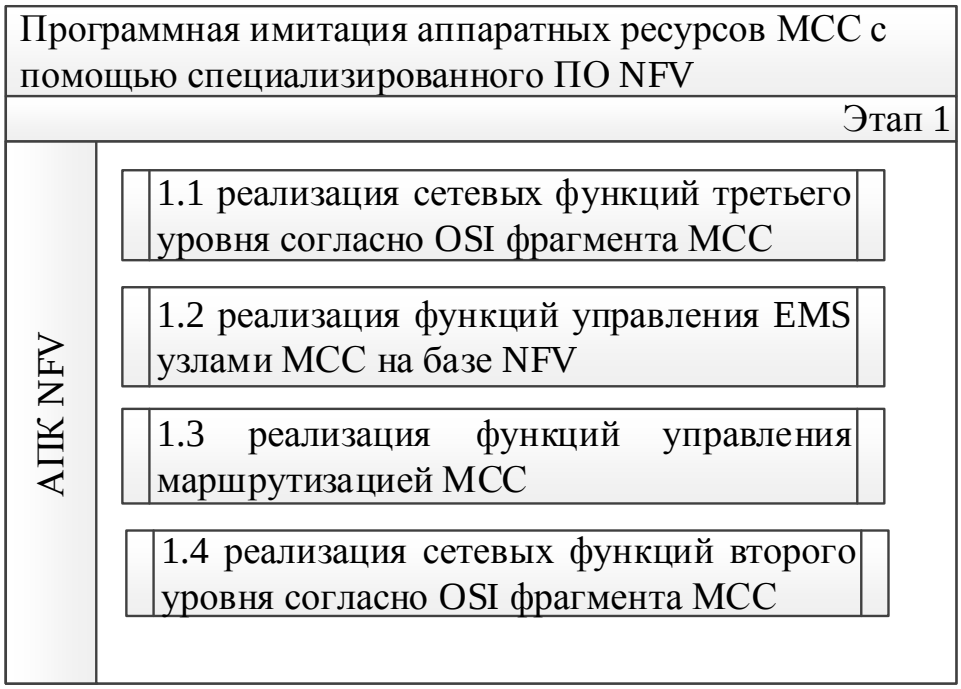


Рис. 2. Структурно-логическая схема 1 этапа реализации процессов управления и функционирования МСС на основе технологии NFV

Управление и контроль работой одной или несколькими VNF, осуществляется за счет сетевых элементов EMS в режиме реального времени.

В основу второго этапа инфраструктуры NFV входят три блока, на которых развертываются и выполняются VNF:

1. Аппаратные ресурсы (серверы).
2. Уровень виртуализации (гипервизор, сопряжения).
3. Программные ресурсы, реализующие задачи на первом этапе.

При реализации инфраструктуры сети NFV организуются логические связи между множеством VNF.

Третий этап (рис. 3) включает в себя создание информационной модели обмена данными в сети с использованием концепции «Менеджер-Агент» для обеспечения контроля виртуальной инфраструктуры и работы элементов сети через открытые протоколы, для получения информации о состоянии ресурсов.

Рис. 3. Структурно-логическая схема 3 этапа реализации процессов управления и функционирования МСС на основе технологии NFV

На четвертом этапе поставщик услуг при внедрении NFV получает механизм администрирования инфраструктуры, обеспечивая простоту в управлении аппаратными и программными ресурсами, гибкость и масштабируемость сети, быстрое решение оперативных задач и развертывание новых сетевых функций, минимизируя работу системного администратора.

Можно выделить следующие преимущества от внедрения NFV:

– предоставление новых услуг с сокращением капитальных затрат на оборудование;

– гибкость управляемости сети;

– переход оборудования на стандартизированные серверы и сетевые компоненты, не привязывая операторов к поставщикам оборудования;

– снижение операционных расходов за счет упрощения системы мониторинга и администрирования;

– быстрое подключение новых пользователей к сети;

– обеспечение безопасности данных за счет разделения и изоляции сегментов сети;

– масштабируемость услуг, организованные не базе ПО позволяют в течении дня увеличивать или уменьшать объем используемых ресурсов одного и того же аппаратного обеспечения в зависимости от нагрузки.

Перевод сетевых функций МСС второго и третьего уровня модели OSI на технологию NFV позволит снизить капитальные затраты и эксплуатационные расходы, обеспечить требования к качеству предоставляемых услуг, а также выполнить предъявляемые требования к функционированию сети (надежность, гибкость, масштабируемость, управляемость) за счет организации кроссплатформенной СУ.

Список используемых источников

1. Гребешков А. Ю. Управление сетями электросвязи по стандарту TMN: учеб. пособие. М. : Радио и связь, 2004. 155 с.
2. Стандарт ETSI (ETSI GS NFV 002 v1.1.1 2013-10).
3. Канаев А. К., Сахарова М. А. Системы управления телекоммуникациями: учеб. пособие. СПб., 2016. 86 с.
4. Рекомендация МСЭ-Е Y.1540.
5. Рекомендация МСЭ-Е Y.1541.
6. Приказ Министерства информационных технологий и связи РФ от 27 сентября 2007 г. № 113 «Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования».

УДК 654.026; 510.334 ***Приглашенный доклад***
ГРНТИ 81.93.29

ПОСТРОЕНИЕ «ЛЁГКИХ» ШИФРОВ С ИСПОЛЬЗОВАНИЕМ ПОДСТАНОВОК С ТРИВИАЛЬНОЙ ГРУППОЙ ИНЕРЦИИ ПО ОТНОШЕНИЮ К АФФИННЫМ ПРЕОБРАЗОВАНИЯМ

Н. П. Борисенко

АО «Региональный центр защиты информации «ФОРТ»

В процессе применения криптографических методов защиты информации возникают проблемы при защите высокоскоростных информационных потоков, а также при необходимости массового применения механизмов защиты, например, обеспечения безопасности «Интернета вещей».

Одним из направлений решения возникающих проблем является применение, «легкой криптографии», т. е. подмножества таких шифров, которые при достижении такой же неопределенности, по отношению к ключу и защищаемой информации, как и в классических шифрах, требуют для своей реализации минимальных ресурсов, энергии и времени.

В работе рассматривается возможность решения данной задачи путем применения в блочных шифрах подстановок с тривиальной группой инерции по отношению к аффинным преобразованиям.

подстановки (S-блоки), координатные булевы функции, аффинная эквивалентность S-блоков, группа инерции, блочные шифры.

В условиях тотальной цифровизации, основную роль в обеспечении информационной безопасности играют криптографические методы. Однако стандартные криптоалгоритмы не в полной мере решают возникающие проблемы обеспечения информационной безопасности, при защите высокоскоростных информационных потоков, а также при необходимости массового применения криптозащиты, например, в «Интернете вещей».

Одним из направлений решения этой проблемы является применение, так называемой, «легкой криптографии» [1], которая определяет подмножество шифров, которые при достижении такой же стойкости, по отношению к ключу и защищаемой информации, как и классические шифры, требуют для своей реализации минимальных ресурсов, энергии и времени.

Рассмотрим два типа шифров: блочные и поточные. В первых, основное внимание уделяется сложности отображения $Y = E(X, K)$ множества сообщений X в множество криптограмм Y с учетом используемого ключа K, при этом сам ключ для различных сообщений не меняется. В поточных, наоборот, основное внимание уделяется сложности отображения используемого ключа K в гамму $\Gamma = E'(K, S)$, где S – случайный вектор инициализации. Затем гамма по простому правилу (часто линейному) накладывается на сообщение $Y = X \oplus E'(K, S)$. Для того, чтобы получить эффект «лёгкой криптографии» можно объединить оба эти подхода в одном шифре. Т. е. сначала, по аналогии с поточным шифром, ключ (возможно дополнительный K_1) должен участвовать в формировании правила шифрования $\tilde{E} = f(E, K_1)$, где функция f выполняет роль правила зашифрования в поточном шифре, а E правило шифрования блочного шифра. Потом, по аналогии с блочным шифром, правило $\tilde{E}$ должно участвовать в отображении $Y = \tilde{E}(X, K)$. Для любого $\tilde{k}_1 \in \tilde{K}_1$ отображения $Y = \tilde{E}(X, K)$ должны быть эквивалентны исходному отображению $Y = E(X, K)$ и обеспечивать выполнение свойств, принятых в стандартах. Поскольку множество ключей

$\tilde{K} = \tilde{K}_1 \cup K$ увеличилось, в необходимых случаях, за счет применения изменяющегося правила $\tilde{E}$ можно достичь сокращения количества раундов шифрования и/или уменьшить размер блока.

Мы предлагаем подход достижения этого требования на основе выполнения следующих условий:

– подстановки, используемые в *S*-преобразовании блочного шифра, должны иметь тривиальную группу инерции по отношению к аффинным преобразованиям;

– правило выбора подстановок аффинно-эквивалентных к заданной подстановке *S* должно обеспечивать равную вероятность для любого из возможных вариантов.

Множество подстановок $\{S_1(x)\}$ аффинно-эквивалентных подстановке $S_2(x)$ определяется выражением [2]:

$$S_1(x) = B^{-1} \cdot (S_2(A \cdot x) \oplus c^T) \oplus d^T, \qquad (1)$$

где S_2 – исходная *n*-битная подстановка; S_1 – производная подстановка; A и B – невырожденные двоичные квадратные матрицы размером $n \times n$; $x, c, d \in V_n$ – *n*-мерные двоичные векторы.

Известно, что существуют подстановки $S_2(x)$, для которых группа инерции по отношению к аффинным преобразованиям (1) тривиальна.

Это означает, что множество всех аффинно-эквивалентных подстановок $\{S_1(x)\}$ попарно несравнимо, т.е. во всех возможных подстановках S_1 нет ни одной повторяющейся. Число таких подстановок определяется выражением $|S_1| = \left(2^n \prod_{i=0}^{n-1} (2^n - 2^i)\right)^2$. Т. о. неопределенность, обусловленная случайным и равновероятным выбором подстановок S_1, может достигать $\tilde{k}_1 \le -\log_2 |S_1|^{-1}$ бит.

В таблице приведены максимально возможные значения мощности множеств: невырожденных двоичных матриц $|\mathrm{M}|$, всех аффинных преобразований $2^n|\mathrm{M}|$, $|S_1|$, а также энтропия множества $\{S_1\}$ – $\tilde{k}_1$ для подстановок размерностью *n*.

ТАБЛИЦА. Значения мощности множеств

n	$\lvert\mathrm{M}\rvert$	$2^n\lvert\mathrm{M}\rvert$	$\lvert\mathrm{M}\rvert^2$	$\lvert S_1\rvert = \left(2^n\lvert\mathrm{M}\rvert\right)^2$	$\tilde{k}_1$-бит
4	20160	322560	406425600	1,04045E+11	36
5	9999360,00	319979520	9,99872E+13	1,02387E+17	56
6	20158709760	1,29016E+12	4,06374E+20	1,66451E+24	80

n	$\lvert\mathrm{M}\rvert$	$2^n\lvert\mathrm{M}\rvert$	$\lvert\mathrm{M}\rvert^2$	$\lvert S_1\rvert=\left(2^n\lvert\mathrm{M}\rvert\right)^2$	$\tilde{k}_1$-бит
7	1,6385E+14	2,09728E+16	2,68468E+28	4,39858E+32	108
8	5,34806E+18	1,3691E+21	2,86018E+37	1,87445E+42	140
16	3,34399E+76	2,19152E+81	1,1182E+153	4,8027E+162	540

Известно [3], что с увеличением размера подстановки n вероятность того, что она окажется с тривиальной группой инерции стремится к 1. Однако, доказательство этого факта является сложной задачей. Один из наиболее эффективных алгоритмов проверки аффинной эквивалентности подстановок изложен в [2], однако его сложность $O\left(n^3 2^{2n}\right)$ такова, что для подтверждения тривиальности группы инерции подстановок размером $n > 8$ его применение нецелесообразно.

Для упрощения решения этой задачи было рассмотрено подмножество аффинно-эквивалентных булевых функций, которое определяется выражением [3, 4]:

$$g(x) = f(D(x) \oplus u^T) \oplus l \cdot x^T \oplus m, \qquad (2)$$

где $g(x)$ *и* $f(x)$– булевы функции от n переменных; D – невырожденная, двоичная матрица размером $n \times n$; $x, u, l \in V_n$ – n-мерные векторы.

Ниже приводится теорема, в которой устанавливается связь между аффинными координатными функциями для множества подстановок S_1, координатными функциями исходной подстановки S_2 и мощностью группы инерции относительно аффинно-эквивалентных преобразований.

Теорема

Если множество координатных функций для аффинно-эквивалентной $n \times n$ подстановки S_1 линейно зависимо, то группа инерции по отношению к аффинным преобразованиям исходной подстановки S_2 не тривиальна.

Доказательство[1] из-за ограниченности объёма статьи не приводится.

Получена оценка сложности проверки аффинной неэквивалентности координатных булевых функций с использованием алгоритма Бирюкова [2] – $O\left(n^2 2^{2n}\right)$, которая с учетом числа пар линейных комбинаций, имеет достаточно большую сложность. Также разработана модификация этого алгоритма на основе поиска «представителя» по минимальному значению координатных функций, представленных в виде числа из 2^{2^n} -ичных цифр. Полученная оценка сложности $O(n2^{2n} + n^2 2^n)$ лучше, чем для алгоритма Бирюкова, но все же остается трудно достижимой.

[1] Получено совместно с Нгуен Ван Лонгом.

Из сравнения (1) и (2), а также приведенных оценок видно, что проверка аффинной неэквивалентности отдельных координатных булевых функций подстановки S_2 значительно проще, чем перебор всего множества $\{S_1\}$. Поэтому необходимо совершенствовать алгоритмы, реализующие проверку координатных булевых функций на аффинную эквивалентность (2). Эту работу целесообразно проводить по следующим направлениям:

– сравнение спектра весов автокорреляционных функций;

– сравнение коэффициентов преобразований Уолша-Адамара координатных булевых функций;

– сравнение таблиц дифференциалов и линейных аналогов для подстановок; … .

Сочетание перечисленных способов позволяет найти подстановки с тривиальной группой инерции, которые также должны удовлетворять и другим требованиям, предъявляемым к подстановкам [6, 7] при построении блочных шифров.

Таким образом, для построения правила $\tilde{E}$, обладающего свойствами не уступающими стандарту, например, «Кузнечику», достаточно:

1. Иметь подстановку S_2 размерностью n бит с тривиальной группой инерции;

2. Иметь алгоритм выбора невырожденных, двоичных матриц A и B размером $n \times n$, с вероятностью близкой к $\frac{1}{|\mathrm{M}|}$.

Решение первой задачи рассмотрено выше.

Способы решения второй задачи известны, однако для того, чтобы шифр был «легким» необходимо их дальнейшее совершенствование.

Одним из вариантов, исследованным в работе, является формирование невырожденной матрицы из «окна» размером $n \times n$, продвигаемого по последовательности максимального периода n-мерного линейного рекуррентного регистра сдвига, являющегося генератором мультипликативной группы поля $GF(2^n)$.

Возвращаясь к началу нашей работы отметим, что применение изменяемого правила подстановки $\tilde{E} = f(E, K_1)$, зависимого от дополнительного ключа $\tilde{k}_1$, создает дополнительный запас стойкости, который может быть использован для повышения быстродействия шифратора, например за счет уменьшения количества раундов или/и применения S блока меньшего размера.

Аналогичным образом можно поступить при необходимости минимизации массогабаритных характеристик или/и энергопотребления.

Заключение

1. Существует возможность построения «легких шифров» с надежностью сравнимой со стандартными шифрами. Общая неопределенность «лёгкого шифра» может достигать $\tilde{k} \le k + \tilde{k}_1$ бит, где k – энтропия ключа блочного шифра, из которого формируются раундовые ключи, $\tilde{k}_1$ – дополнительная неопределенность при выборе преобразования S_1, которая тоже может задаваться ключом.

2. Реализованная на основе описанного способа (правила шифрования) структура, может быть «залита» в ПЛИС и работать значительно быстрее, чем стандартные алгоритмы, поскольку при одинаковой с ними неопределенности будет иметь существенно меньше раундов.

3. Для малогабаритных устройств шифрования, применение концепции «легких шифров», при заданной неопределенности, позволит уменьшить размер блока и тем самым упростить реализацию.

4. Перспективным является направление, когда на объекте (в организации) существует центр распределения ключей, который генерирует кроме традиционных ключей *K*, необходимые правила «легкой криптографии» $\tilde{K}$ и распределяет (доставляет) их на мобильные объекты: смартфоны, планшеты и другие технические средства «Интернета вещей».

Список используемых источников

1. Thomas Peyrin. Lightweight Symmetric-Key Cryptography // CTCRYPT 2018, Suzdal, May 29, 2018.

2. Alex Birykov, Christophe De Cannere, An Braeken, Barn Prenell. A Toolbox for Cryptanalysis: Linear and Affine Equivalent Algorithms* // Advances in Cryptology – EUROCRYPTO 2003. Springer, 2003. Vol. 2656. pp. 33–50.

3. Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В. Булевы функции в теории кодирования и криптологии. М. : ЛЕНАНД, 2015. 576 с.

4. Joanne Fuller and William Millan. Linear redundancy in S-boxes // In Fast Software Encryption. 2003. Springer.

5. Biryukov, A., Perrin, L.: On Reverse-Engineering S-Boxes with Hidden Design Criteria or Structure // In: Advances in Cryptology – CRYPTO 2015. Lecture Notes in Computer Science. Springer Berlin Heidelberg (2015) (to appear).

6. Зензин О. С., Иванов М. А. Стандарт криптографической защиты – AES. Конечные поля. М. : КУДИЦ-ОБРАЗ, 2002. 176 с.

7. G. Leander and A. Poschmann. On the Classification if 4 Bit S-Boxes / In C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547, pp.159–176.

УДК 004.72
ГРНТИ 49.38.49

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕШЕНИЙ SDN ОТ ВЕДУЩИХ ПРОИЗВОДИТЕЛЕЙ

И. В. Бохан, А. В. Красов, И. А. Ушаков

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

В стремительно развивающемся мире сетевых технологий большое внимание на себя обращает такая инновационная сетевая архитектура, как SDN. В статье рассматриваются решения для SDN от ведущих в области сетевых технологий компаний – Cisco Systems и VMWare, а также будут проведены сравнения между этими проектами.

программно-конфигурируемые сети, SDN, Cisco ACI, VMWare NSX.

Программно-конфигурируемые сети (*Software-defined Networking*, SDN) – это современный взгляд на развитие сетевой архитектуры, в которой сетевые устройства перестанут конфигурироваться и обмениваться информацией автономно. Роль управления оборудованием в сетях SDN на себя берет единый элемент – контроллер. Это позволяет значительно сократить затраты на эксплуатацию сетей, а также повысить эффективность сетевых устройств, достигнув таких критериев как масштабируемость, гибкость и отказоустойчивость [1, 2]. Поэтому не вызывает удивления заинтересованность в разработке своих решений для SDN у компаний - лидеров в области сетевых технологий.

В настоящее время Cisco Systems (Cisco ACI) продвигает ACI в качестве своего решения SDN. Контроллер APIC (*Application Policy Infrastructure Controller*) работает независимо от уровня управления и коммутационного уровня данных, не разделяя соответствующие процессы. Его главные функции – управление инфраструктурой и информирование систем вышестоящего уровня о ее состоянии (мониторинг).

ACI, подобно SDN, предусматривает управление программным образом, но в качестве управляемых элементов выступают не тривиальные коммутаторы, а, как и раньше, многофункциональные сетевые устройства. Главная концепция ACI – дать приложениям возможность конфигурировать сеть под свои требования. Для этого создается сетевой профиль приложения Application Network Profile (ANP), где указываются параметры безопасности, качества обслуживания (QoS), балансировки нагрузки и прочее. Данные профили загружаются в контроллер APIC, а тот – программирует коммутаторы Cisco [3, 4, 5].

В основе ACI лежит архитектура Leaf and Spine, минимальная структура которой представлена на рис. 1.

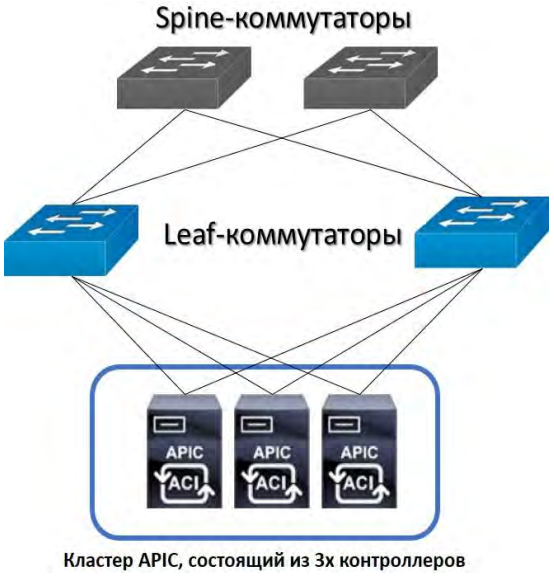


Рис. 1. Минимальная ACI-фабрика

Преимуществами внедрения архитектуры Leaf and Spine являются:

– облегчение устранения отказов оборудования за счет его однородности;

– высокая масштабируемость;

– простота автоматизации управления;

– меньшее падение пропускной способности сети при отказе оборудования;

– схема по умолчанию защищена от появления петель и не требует для этого STP;

– если порт не отвечает – протокол маршрутизации считает его неактивным и не рассматривает возможность его участия в маршрутах, в отличие от STP.

VMWare NSX – overlay-решение, которое следует рассматривать, если владелец не готов пойти на замену всей сети ЦОД. Для передачи данных по существующей аппаратной сети используются VXLAN-туннели. Отличительной особенностью является более плотная интеграция с экосистемой для управления серверной виртуализацией от VMWare (используя программное обеспечение только от VMWare). Результатом является возможность управления всей инфраструктурой ЦОД из единого веб-интерфейса [3].

VMware NSX – это платформа виртуализации сети для программно-определяемого центра обработки данных (*Software-Defined Data Center*, SDDC), предоставляющая рабочую модель виртуальной машины для целых сетей. В NSX сетевые функции, включая коммутацию, маршрутизацию и сетевой экран, встроены в гипервизор и распределены по всей среде. Это эффективно создает «сетевой гипервизор», который выступает в качестве платформы для виртуальных сетей и служб, позволяя управлять ими независимо от физического оборудования. NSX воспроизводит всю модель сети внутри программного обеспечения, позволяя тем самым за секунды создавать и подготавливать любую топологию сети – от самой простой до многоуровневой [6].

Основные преимущества NSX (схема архитектуры приведена на рис. 2):

– к конкретным рабочим нагрузкам применяется микросегментация;

– сокращение времени подготовки сети с нескольких дней до нескольких секунд и повышение эффективности работы за счет автоматизации;

– мобильность рабочей нагрузки не зависит от физической топологии сети внутри и между центрами обработки данных;

– повышенная безопасность и расширенные сетевые услуги благодаря экосистеме ведущих сторонних поставщиков.

Рис. 2. Архитектура VMWare NSX

Сравнивая технические возможности ACI и NSX (табл.) можно прийти к выводу, что NSX наиболее применим в ЦОД, где подавляющее большинство серверов виртуализированы с помощью VMWare. ACI более подходит для ЦОД, инфраструктура которых построена на коммутаторах серии Nexus 9000, однако, с помощью установки виртуального коммутатора AVS, к ACI можно подключать напрямую как виртуальные машины (VMWare ESXi), так и физические серверы [8].

ТАБЛИЦА. Сравнительный анализ ACI и NSX

Предмет сравнения	**Cisco ACI** [3, 7]	**VMWare NSX** [6]
Безопасность	Автоматизация политик безопасности уровня 4–7, микросегментация, открытая экосистема	Микросегментация важных приложений, динамическое добавление сторонних служб безопасности, создание ДМЗ в любой точке
Удаленная связность между серверами ЦОД	Через OTV (*Overlay Transport Virtualization*), который не принадлежит к ACI	Поддерживается (рекомендуется использовать, даже если не требуется соединение через VXLAN)
Поддержка оборудования других производителей	Проприетарное решение (необходимы коммутаторы серии Nexus 9000)	Поддержка возможна, если используется виртуализация от VMWare

Как и в случае любого крупного технологического решения, важно получить четкое представление о том, что предлагают продукты, и каковы их возможности в сфере бизнеса. Не стоит смотреть на ACI и NSX

как на конкурирующие решения, потому что, на самом деле, они ими не являются. Если бизнесу требуется динамически подготавливаемая, масштабируемая и программируемая сеть, ACI является лучшим выбором. Если компании требуется микросегментация на уровне гипервизора для трафика между виртуальными машинами, выбор NSX будет верным решением. Если требуется и то и другое сразу, эти решения могут использоваться совместно [9, 10].

Список используемых источников

1. Hyojoon Kim, Nick Feamster: Improving network management with software defined networking, 2013.

2. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

3. Диалектика виртуальных сетей – Cisco ACI vs Vmware NSX [Электронный ресурс]. URL: http://www.jetinfo.ru/jetinfo_arhiv/tekhnologii-virtualizatsii/ dialektika-virtualnykh-setej-cisco-vs-vmware/2015 (дата обращения 19.12.2018).

4. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Методология управления потоками трафика в программно-определяемой адаптивной сети // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 4. С. 3–8.

5. Котенко И. В., Ушаков И. А. Технологии Больших данных для мониторинга компьютерной безопасности. // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.

6. Микросегментация – система безопасности ЦОД [Электронный ресурс]. URL: https://www.vmware.com/ru/products/nsx/security.html (дата обращения 19.12.2018).

7. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи Multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

8. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

9. Eriksson J., Hedlund R. Cisco ACI and VMware NSX, a comparison between Software Defined Networks – 2016.

10. Алейников А. А., Билятдинов К. З., Красов А. В., Кривчун Е. А., Крысанов А. В. Технические аспекты управления с использованием сети Интернет : монография. СПб., 2016. 305 с.

УДК 159.923
ГРНТИ 15.41.39

ОБЩИЙ ПОДХОД К ВЫЯВЛЕНИЮ ДЕСТРУКТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ И НЕГАТИВНЫХ ЛИЧНОСТНЫХ ТЕНДЕНЦИЙ МОЛОДОГО ПОКОЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ НЕЙРОСЕТЕВОЙ ОБРАБОТКИ ИНТЕРНЕТ-КОНТЕНТА

А. А. Браницкий[1], Н. П. Ванчакова[2], Е. В. Дойникова[1], И. В. Котенко[1,3], Н. В. Красильникова[2], И. Б. Саенко [1], А. В. Тишков[2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Первый Санкт-Петербургский государственный медицинский университет им. И. П. Павлова
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье описывается разработанный общий подход к выявлению деструктивных информационных воздействий и негативных личностных тенденций молодого поколения с использованием методов нейросетевой обработки Интернет-контента. В настоящее время Интернет-пространство является основной средой для распространения деструктивных информационных воздействий. Поэтому актуальным является мониторинг и выявление деструктивных информационных воздействий и негативных личностных тенденций молодого поколения при взаимодействии с Интернет-пространством. Предлагаемый подход включает методику определения признаков и критериев для выявления деструктивного контента и деструктивного воздействия в сети Интернет; методику выявления признаков деструктивности пользователей сети Интернет на основе информации на их персональных страницах в социальных сетях; методику мониторинга и выявления деструктивного информационного воздействия в сети Интернет на основе применения методов нейрокомпьютерной и нейросетевой обработки Интернет-контента.

деструктивное воздействие, деструктивный контент, социальные сети, нейросети.

В современном мире Интернет-пространство является одной из популярных форм взаимодействия молодого поколения. В то же время оно является основной средой для распространения деструктивных информационных воздействий. Целью данного исследования является выявление таких воздействий и мониторинг их влияния на молодое поколение. Важность данной задачи определяется важностью психологического здоровья нации для ее эффективного развития.

Первоначальная гипотеза, которая легла в основу подхода, разрабатываемого в данном исследовании, заключается в том, что информация

на страницах пользователей в социальных сетях может служить для определения склонности пользователя к деструктивности. Поэтому для выявления деструктивных информационных воздействий в Интернет-пространстве предлагается подход, основанный на анализе данных социальных сетей и включающий три основных этапа, а именно:

Этап 1 – определение склонности пользователей социальных сетей к деструктивности.

Этап 2 – классификация сообществ социальной сети по тому, оказывают ли они деструктивное воздействие.

Этап 3 – выявление изменений в склонности пользователей к деструктивности при взаимодействии с сообществами в социальной сети.

Для реализации каждого этапа предлагается соответствующая методика. Методика, реализующая первый этап, предполагает обучение нейросети для ранжирования страниц пользователей по склонности к деструктивности на основе предварительно сформированной выборки и выделенных признаков. В процессе исследования для ручного определения склонности пользователя к деструктивности была выбрана шкала, предложенная Злоказовым К. В. [1], которая включает три основных категории: интраперсональное, интерперсональное и метаперсональное поведение. Каждая из основных категорий, в свою очередь, разделена на две подкатегории. Интраперсональная деструктивность – это деструктивность, направленная на самоизменение и саморазрушение. В качестве подкатегорий выделяются слабая и сильная формы изменений. Интерперсональная деструктивность подразумевает взаимоотношения двух субъектов, один из которых стремится принизить другого (первая подкатегория), а другой является жертвой (вторая подкатегория). Метаперсональная деструктивность подразумевает взаимоотношения субъекта с социальной группой и делится на сопротивление устоям внутри группы и избыточное отстаивание интересов социальной группы.

Отметим, что для последующего обучения нейросети необходимо выделить основные признаки, на основе которых эксперт принимает решение, и сопоставить их с информацией, представляемой в социальной сети. В частности, это может быть характер текстовой информации (эмоциональная и смысловая направленность), характер мультимедийной информации (категории фотографий и видео), активность пользователя в сети, количество открытой/закрытой информации, представление ложной информации, участие в сообществах и прочее. Разработанная методика предполагает итеративную классификацию, то есть корректировку признаков по результатам обучения нейросети.

Помимо шкалы, предложенной Злоказовым К. В., в рамках предлагаемой методики для выявления центральных личностных функций пользователей социальной сети используется тест Аммона, позволяющий выявить

конструктивные, деструктивные и дефицитарные проявления [2]. Результаты данного теста также сопоставляются с информацией в Интернет-пространстве и используются как дополнительные признаки при обучении нейронной сети.

Для практической реализации методики выбрана нейронная сеть word2vec [3], обладающая следующими характеристиками: наличие одного скрытого слоя; возможность выявления семантической схожести слов; и возможность восстановления слова по окружающему его контексту. Ее планируется использовать для обработки текстовых признаков. Для обработки мультимедийной информации планируется использовать нейронную сеть tensorflow-imagenet, являющуюся глубокой сверточной сетью [4]. Также при реализации методики будут использованы стандартные классификаторы, такие как min-max нормализация, метод главных компонент, машина опорных векторов, метод k ближайших соседей, наивный байесовский классификатор, линейная регрессия, дерево решений и метод взвешенного голосования [5].

Методика, реализующая второй этап, предполагает обучение нейросети для классификации сообществ социальной сети по тому, оказывают ли они деструктивное воздействие на пользователей на основе выборки, размеченной вручную экспертами, и выделенных признаков. Отметим, что классификация сообществ реализуется на основе той же шкалы, что и классификация отдельных пользователей, но за основу для ручной разметки и выделения признаков различных категорий берется информация со страницы сообщества.

Методика, реализующая третий этап, предназначена для выявления изменений в склонности пользователей к деструктивности при взаимодействии с сообществами в социальной сети. Она предполагает мониторинг изменений значений признаков, выбранных для классификации, а также состава сообществ, с которыми взаимодействуют пользователи, для которых выявлены изменения. В рамках методики предлагается использовать семиуровневую шкалу перехода к деструктивному состоянию, от «разочарования», к «агрессивному протесту», «демонстративной агрессии», «невербальному призыву к общему протесту», «поиску единомышленников», «призыву к действию в виртуальном мире» и, наконец, «призыву к активному протесту в реальном мире». Предполагается, что данная шкала позволит отслеживать усугубление деструктивности субъектов в динамике.

Отметим, что основная сложность выявления деструктивных воздействий в Интернет-пространстве связана с огромным количеством информации, которую необходимо проанализировать. Предлагаемый подход позволит специалистам сократить количество обрабатываемой информации и сосредоточиться на автоматически ранжированных объектах [6].

Работа выполнена при финансовой поддержке Гранта РФФИ мк 18-29-22034 в СПИИРАН.

Список используемых источников

1. Злоказов К. В. Деструктивное поведение в различных контекстах его проявления // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». 2016. Т. 26. № 4. С. 67–73.

2. Я – структурный тест Гюнтера Аммона. URL: https://www.psychol-ok.ru/statistics/ista/

3. Библиотека “Word2vec-GoogleNews-vectors”. URL: https://github.com/mmihaltz/word2vec-GoogleNews-vectors

4. Библиотека “Tensorflow Models”. URL: https://github.com/tensorflow/models

5. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

6. Комашинский Д. В., Котенко И. В., Чечулин А. А. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности. 2011. № 2. С. 102–106.

УДК 004.056
ГРНТИ 15.41.39

Приглашенный доклад

АНАЛИЗ СИСТЕМЫ МЕТРИК ЗАЩИЩЁННОСТИ CVSS ДЛЯ РАЗРАБОТКИ АЛГОРИТМА ПОСТРОЕНИЯ ГРАФА АТАК

А. А. Браницкий[1], Е. В. Дойникова[1], В. И. Кузьмина[1,2], И. Б. Саенко[1], А. А. Чечулин[1,3]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена разработке алгоритма построения графа атак. Алгоритм разработан с учетом анализа системы метрик защищённости CVSS v.3. Работа алгоритма и итоговый граф рассмотрены на примере тестовой компьютерной сети.

граф атак, CVSS, компьютерные сети, компьютерная безопасность.

Согласно Kaspersky Security Bulletin [1] наиболее значимые угрозы на предстоящий год будут связаны с APT-атаками (*Advanced Persistent Threat*, целевыми кибератаками). Этот тип атак отличается сложностью, наличием четко поставленной цели и обычно включает несколько шагов,

в том числе разведывательных. Возможным способом выявления и прогнозирования развития таких атак является анализ событий, происходящих в системе, и отображение их на предварительно сформированную модель атак.

Шаги злоумышленника, которыми он может скомпрометировать сеть, можно визуализировать и представить в виде графа атак. Под графом атак понимается множество возможных путей компрометации компьютерной сети атакующим, включающих шаги атаки (узлы графа) и переходы между ними (связи). Для определения связей между шагами атаки предлагается использовать показатели общей системы оценки уязвимостей CVSS версии 3 (*Common Vulnerability Scoring System*) [2].

Задача оперативного представления графов атак решалась в работе [3]. Однако оперативность достигалась за счёт исключения ряда связей на графе. Для анализа защищённости, в том числе отображения событий на модель атак, определения предыдущих и прогнозирования будущих шагов атаки, это является существенным ограничением. Поэтому существует необходимость в разработке новых алгоритмов оперативного формирования и анализа графа атак, учитывающего все возможные пути атаки в компьютерной сети.

Описание подхода

Как уже упоминалось выше, граф атак представляет собой множество атакующих действий и связей между ними. На текущем этапе исследования ограничимся атакующими действиями, использующими уязвимости. Возможность перехода от одного атакующего действия к другому будем определять в зависимости от пред- и постусловий эксплуатации уязвимостей. Для определения пред- и постусловий были выбраны показатели CVSS версии 3 [2].

Общая система оценки уязвимостей CVSS версии 3

CVSS является инструментарием для количественной оценки уязвимостей. Целью CVSS является получение интегрального числового показателя по десятибалльной шкале для каждой уязвимости, записанной в базе общеизвестных уязвимостей информационной безопасности CVE (*Common Vulnerabilities and Exposures*), определяющего ее сравнительное влияние на безопасность (чем больше значение показателя, тем более опасна уязвимость с точки зрения информационной безопасности). Интегральный показатель CVSS, в свою очередь, формируется на основе базовых показателей, временных показателей или показателей среды.

Базовые показатели отражают основные характеристики уязвимости, такие как возможность использования уязвимости (показатели возможности

эксплуатации) и последствия её использования для подвергающегося воздействию объекта (показатели воздействия).

Временные показатели отражают характеристики уязвимости, которые могут меняться во времени, но не зависят от пользовательской среды. Показатели среды позволяют учесть требования безопасности конкретной системы при оценивании уязвимостей. На основании показателей среды аналитик, который осуществляет оценку уязвимостей, может предусматривать меры безопасности, которые позволят ослабить последствия эксплуатации уязвимости. Обычно в роли уязвимого компонента выступает прикладная программа, модуль, драйвер и т. д. (или даже устройство), а атакуемым компонентом может быть прикладная программа, устройство или сетевой ресурс [4].

Для построения алгоритма использовались только базовые показатели, поскольку данные показатели позволяют получить необходимую информацию для построения связей между атакующими действиями.

Ключевая особенность CVSS версии 3 заключается в том, что есть возможность измерять воздействие уязвимости на другие объекты, помимо уязвимого компонента [2]. Данная характеристика отражена в показателе «S (*Scope*) – область действия». Поскольку для разработки алгоритма построения связей между хостами нужны не все показатели, в таблице 1 рассмотрены только характеристики базовых показателей, используемых для реализации алгоритма построения графа атак.

ТАБЛИЦА 1. Характеристики базовых показателей, используемых в алгоритме

Показатель	Характеристика	Значение показателя
AV (*Attack Vector*) – вектор атаки	Показатель отражает контекст, в котором возможна эксплуатация уязвимости. Уязвимость, доступную через Интернет, способно эксплуатировать большее число потенциальных злоумышленников, чем уязвимость, требующую физического доступа к устройству.	**N** (*Network*) – сетевой; **A** (*Adjacent*) – соседский; **L** (*Local*) – локальный; **P** (*Physical*) – физический.
PR (*Privileges Required*) – требуемые привилегии	Показатель описывает уровень привилегий, которыми должен обладать злоумышленник. Чем ниже требуемые привилегии, тем большее число потенциальных злоумышленников может использовать уязвимость, соответственно, тем выше оценка CVSS	**N** (*None*) – отсутствует; **L** (*Low*) – низкая; **H** (*High*) – высокая.
Priv. (*Privileges*) – привилегии после эксплуатации уязвимости	Показатель отражает привилегии, которые получит злоумышленник после эксплуатации уязвимости.	**All** – все; **User** – пользователь; **Other** – другие; **None –** нет.

Описание алгоритма построения графа

На рис. 1 представлен алгоритм построения графа. В данном алгоритме рассмотрены все варианты, когда можно осуществить связь между атакующими действиями. Например: *link* $v1$ *with* $v2$ (злоумышленник после эксплуатации уязвимости наделён привилегиями). В обратном случае, когда атакующий не получает привилегии, необходимые для эксплуатации конкретной уязвимости, связь между уязвимостями не строится.

Algorithm 1: Attack Graph

1 **Data:** v1, v2, v3, v4, v5, v6, v7, v8

2 **if** $v1 < -AV = (N|L|A|P)$ & $PR = (N|L)$ & $Priv. = User$ *and*
$v2 <$ −AV= $(N|L|A|P)$ & $PR = (L)$ & Priv. $= All$
link $v1$ *with* $v2$

3 **elif** $v3 <$ −AV= $(N|L|A|P)$ & $PR = (N|L)$ & Priv. = Other *and*
$v4 <$ −AV= $(N|L|A|P)$ & $PR = (L)$ & Priv. = User
link $v3$ *with* $v4$

4 **elif** $v5 <$ −AV= $(N|L|A|P)$ & $PR = (L|H)$ & Priv. = All *and*
$v6 <$ −AV= $(N|L|A|P)$ & $PR = (N)$ & $Priv. = (User|Other|All)$
link $v5$ *with* $v6$

5 **else** $v7 <$ −AV= $(N|L|A|P)$ & $PR = (N)$ & $Priv. = None$ *and*
$v8 <$ −AV= $(N|L|A|P)$ & $PR = \forall$ & $Priv. = \forall$
NOT link $v7$ *with* $v8$ *if* $Priv. = None$ *in* $v7$

Рис. 1. Алгоритм построения графа

Тестовый пример

Для представления того, как формируются связи между атакующими действиями на графе, выполним моделирование компьютерной сети в программе Opnet Modeler. На рис. 2 представлена смоделированная сеть.

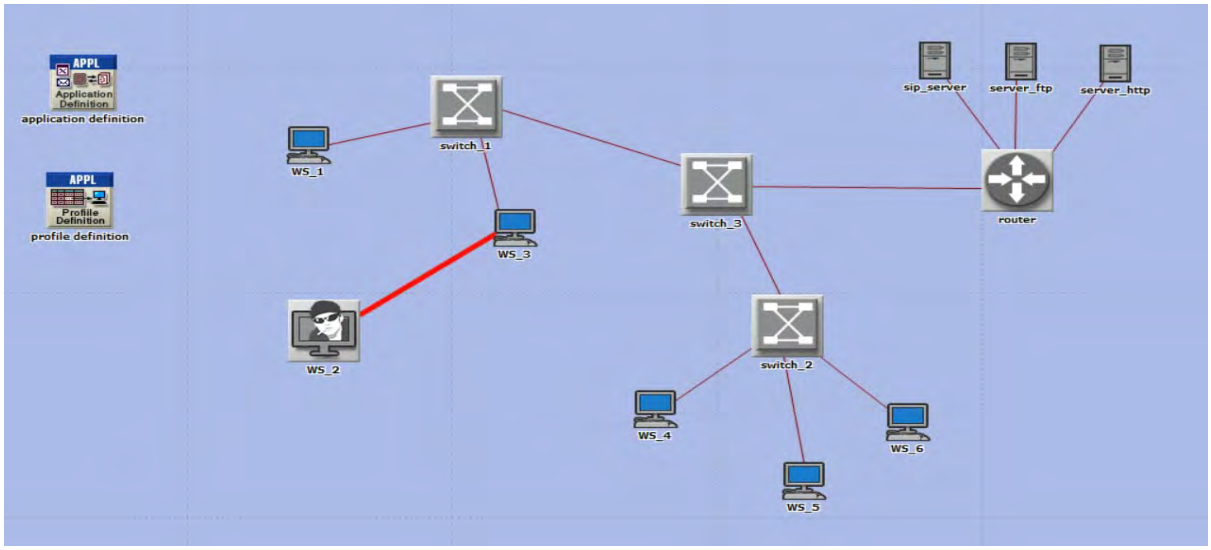


Рис. 2. Смоделированная компьютерная сеть

Для каждого хоста сети в таблице 2 представлено программное обеспечение, на основе которого определяются уязвимости и базовые показатели, которые необходимы для построения графа атак.

ТАБЛИЦА 2. Характеристики используемых хостов сети

	Workstation 1	Workstation 2	Workstation 3	Workstation 4	Switch 1, 2, 3
Программное обеспечение	Apple mac OS v. 10.11.0	Linux Kernel Realease 2.6	Windows 10 Version 1709	Windows 10 Version 1511	Cisco NX_OS
Базовые показатели	AV: Local PR: Low Priv: All	AV: Adjacent PR: None Priv: All	AV: Network PR: None Priv: All	AV: Network PR: None Priv: False	AV: Network PR: None Priv: User
Уязвимость	CVE-2015-6980	CVE-2017-1000251	CVE-2018-0775	CVE-2018-0993	CVE-2016-1341

Граф атак, который представлен на рис. 3 для конкретного участка компьютерной сети, построен с использованием алгоритма, представленного на рис. 1, и языка Python. Предположим, что злоумышленник начинает атаку с хоста WS_2. В случае если эксплуатация уязвимости позволяет злоумышленнику получить привилегии All, User или Other на атакованном хосте, связи между соответствующими узлами (последовательными шагами атаки, описанными с помощью использованной уязвимости и атакованного объекта) обозначены красным цветом. Если атакующее действие не позволяет злоумышленнику получить привилегии, то соответствующий узел на графе атак окрашивается в синий цвет, а связь с данным узлом – в черный.

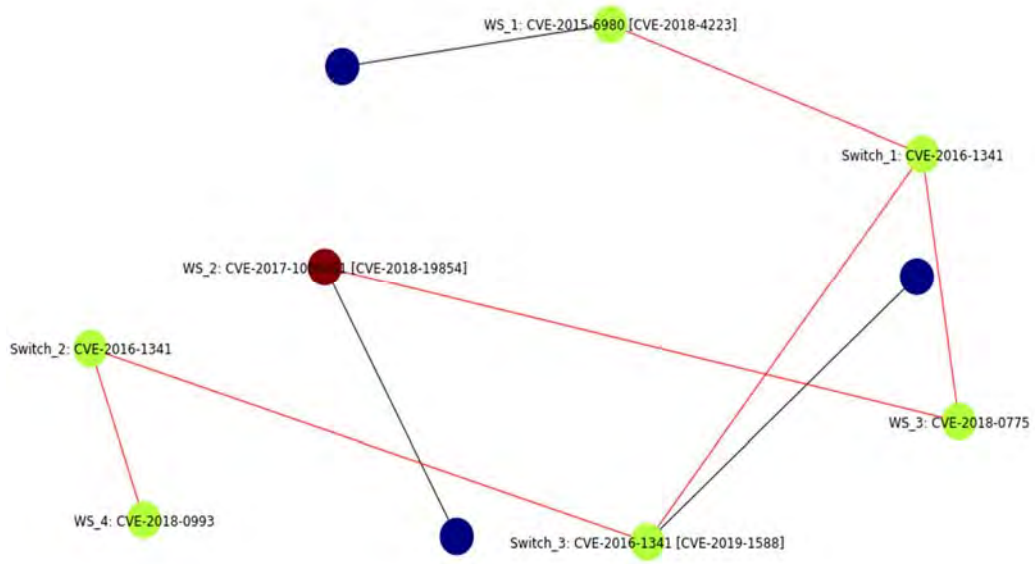


Рис. 3. Граф атак

Выводы

В статье были рассмотрены метрики CVSS версии 3 и их возможные значения для построения графа атак. Данные метрики были использованы для определения пред- и постусловий атакующих действий, являющихся узлами предлагаемого графа. В работе был описан разработанный алгоритм формирования графа атак. Алгоритм и итоговый граф были рассмотрены на примере тестовой компьютерной сети.

Работа выполнена при поддержке гранта РФФИ 19-07-01246.

Список используемых источников

1. Kaspersky Security Bulletin: 2017. Развитие угроз [Электронный ресурс]. URL: https://securelist.ru/ksb-review-of-the-year-2017/88142/

2. Common Vulnerability Scoring System v.3.0: Specification Document [Электронный ресурс]. URL: https://www.first.org/cvss/specification-document

3. Чечулин А. А. Построение и анализ деревьев атак на компьютерные сети с учетом требования оперативности : дисс. … наук : 05.13.19 / Чечулин Андрей Алексеевич; С.-Петерб. ин-т информатики и автоматизации РАН. Санкт-Петербург, 2013. 152 с.

4. Recommendation X.1521: Common vulnerability scoring system (03/2016). ITU. URL: https://www.itu.int/rec/T-REC-X.1521/en

УДК 681.7.06; 621.372
ГРНТИ 49.44.31; 49.44.29

МОДЕЛИРОВАНИЕ РАСПРОСТРАНЕНИЯ ОПТИЧЕСКИХ СИГНАЛОВ СИСТЕМ 10GBASE-LX ПО МНОГОМОДОВЫМ ОПТИЧЕСКИМ ВОЛОКНАМ С УВЕЛИЧЕННЫМ ДИАМЕТРОМ СЕРДЦЕВИНЫ 100 МКМ И УМЕНЬШЕННОЙ ДИФФЕРЕНЦИАЛЬНОЙ МОДОВОЙ ЗАДЕРЖКОЙ

А. В. Бурдин, В. А. Бурдин, А. Е. Жуков

Поволжский государственный университет телекоммуникаций и информатики

В работе представлены результаты моделирования процесса распространения оптических сигналов системы передачи спецификации IEEE 802.3ba 10GBase-LX в нерегулярных кварцевых многомодовых оптических волокнах с экстремально увеличенным до 100 мкм диаметром сердцевины. Рассматривались кварцевые нерегулярные ММ ОВ

с ранее полученным, оптимизированным для совместной работы с когерентными источниками оптического излучения градиентным профилем показателя преломления специализированной формы, обеспечивающей снижение дифференциальной модовой задержки до 256 пс/км на оптической несущей λ = 1310 нм.

многомодовые оптические волокна, дифференциальная модовоя задержка.

В работе представлены результаты моделирования процесса распространения сигналов волоконно-оптической системы передачи (ВОСП) стандарта IEEE 802.3ba спецификации 10GBase-LX в нерегулярных кварцевых многомодовых оптических волокнах (ММ ОВ) с экстремально увеличенным до 100 мкм диаметром сердцевины. Для этой цели было предложено воспользоваться ранее разработанной моделью кусочно-регулярной волоконно-оптической линии передачи (ВОЛП), функционирующей в маломодовом режиме [1], адаптированной на рассматриваемый случай. В отличие от известных решений, данная модель, в общем случае, ориентированная на одиночные кварцевые слабонаправляющие ОВ с увеличенным, относительно стандартных одномодовых ОВ, диаметром сердцевины (нормированная частота $V >> 1$), совместно учитывает исходный модовый состав оптического излучения на выходе когерентного источника, вводимого в ОВ линии, условия ввода сигнала, дифференциальную модовую задержку (ДМЗ), дифференциальные модовые потери, хроматическую дисперсию основной и высших направляемых мод, а также процессы взаимодействия и смешения модовых компонентов оптического сигнала, обусловленные нерегулярной структурой реальных промышленных ОВ, а также наличием микро- и макроизгибов волокон в оптических кабелях, неизбежно возникающих при инсталляции ВОЛП. Сама модель базируется на кусочно-регулярном представлении и использует общий подход метода расщепления по физическим процессам [2].

Рассматривались кварцевые нерегулярные ММ ОВ со специализированной, ранее полученной [3, 4], формой градиентного профиля показателя преломления, оптимизированной для совместной работы с когерентными источниками оптического излучения, представленной на рис. 1 (см. ниже). Данный профиль обеспечивает снижение ДМЗ до 256 пс/км на оптической несущей λ = 1310 нм, при этом указанный параметр не превышает 380 пс/км во всем «O»-диапазоне длин волн (рис. 2, см. ниже).

С помощью указанной модели кусочно-регулярной многомодовой ВОЛП, функционирующей в маломодовом режиме [1], был проведен расчет динамики оптического импульса гауссовой формы длительностью τ_{05} = 90,91 пс ВОСП 10GBase-LX (λ = 1310 нм, скорость 10 Гбит/с), распространяющегося по исследуемому ОВ общей протяженностью 2 км. Здесь нерегулярная структура ОВ была представлена в виде флуктуаций диаметра сердцевины, которые задавались непосредственно из протокола датчика

контроля внешнего диаметра ОВ, измеряемого в процессе вытяжки строительной длины ММ ОВ 50/125 с разрешающей способностью Δz = 8 м [5]. Фрагмент этого протокола, масштабированный на номинальный диаметр сердцевины 100 мкм, и статистика распределения значений разброса диаметра сердцевины на исследуемую 2 км длину ОВ приведена на рис. 3.

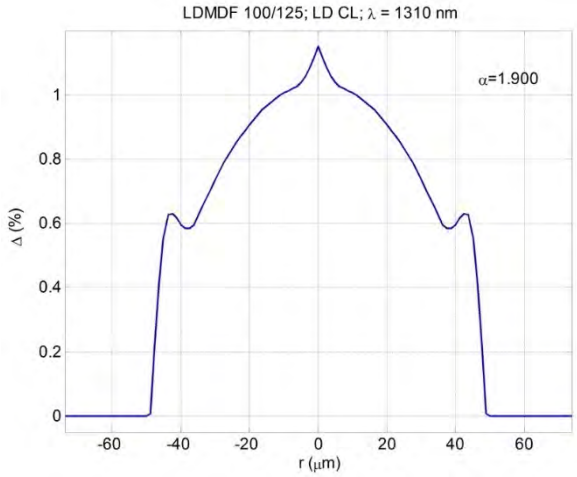


Рис. 1. Профиль показателя преломления ОВ с диаметром сердцевины 100 мкм, оптимизированный для совместной работы с когерентными источниками излучения

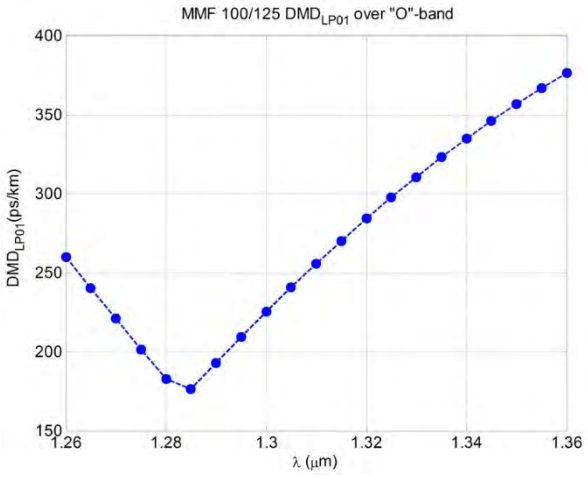


Рис. 2. Спектральная характеристика ДМ ММ ОВ с диаметром сердцевины 100 мкм и оптимизированным профилем в «O»-диапазоне длин волн

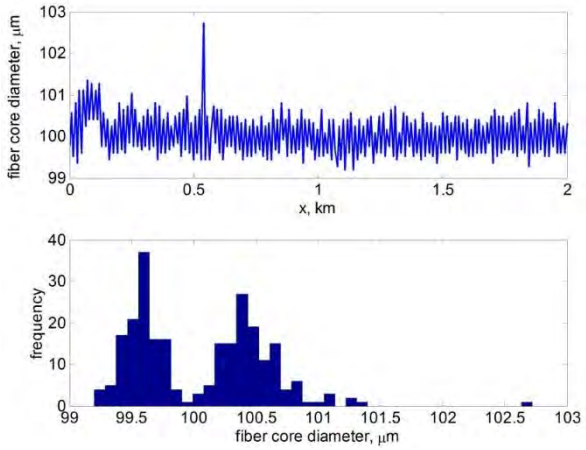


Рис. 3. Фрагмент протокола на выходе датчика контроля диаметра ОВ длиной 2 км, масштабированный на номинальный диаметр сердцевины 100 мкм, и гистограмма распределения его значений [5]

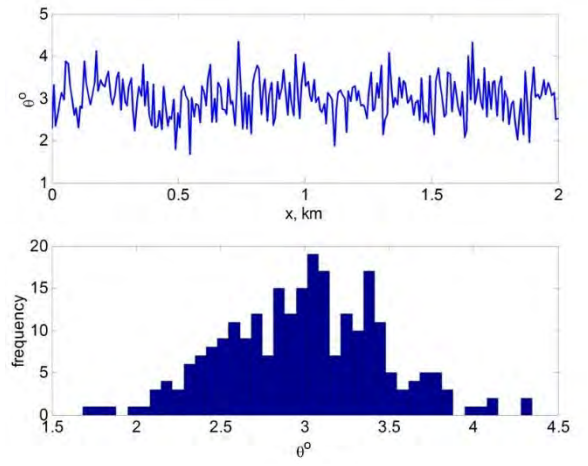
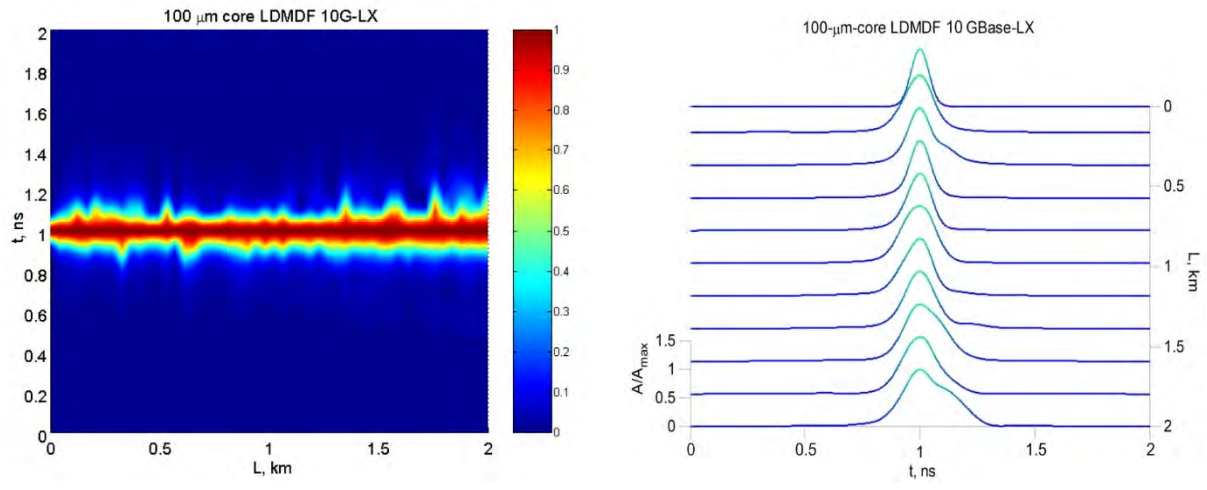


Рис. 4. Распределение значений углового рассогласования стыков регулярных участков представления исследуемого ОВ и гистограмма статистики распределения данного параметра

В свою очередь, согласно [1], микро- и макро-изгибы ОВ, а также кручение и тяжение световода, которые неизбежно возникают на практике при

инсталляции оптического кабеля и являются дополнительными факторами взаимодействия и смешения модовых компонентов оптического сигнала, представлены в данной модели в виде стыков регулярных участков линии, выполненные с некоторым малым угловым рассогласованием. В данном случае использовался нормальный закон распределения случайной величины, при этом математическое ожидание было выбрано равным 3,0°, а дисперсии – 0,5°. Распределение значений углового рассогласования стыков регулярных участков представления исследуемого ОВ и гистограмма статистики этого распределения приведены на рис. 4 (см. выше).

В данной работе исследуется «наихудший вариант» реализации ввода сигнала с выхода лазерного диода (ЛД) передающего модуля ВОСП в торец ОВ линии – без применения каких-либо дополнительных устройств согласования или согласующих волоконных световодов, а непосредственно через типовой волоконно-оптический адаптер (проходную оптическую розетку) на корпусе трансивера / патч-панели, которая в данном случае моделируется как выполненное с угловым раасогласованием $\theta = 4{,}20^{o}$ [6] соединение между упомянутым одномодовым ОВ рек. ITU-T G.652, пигтелирующим ЛД, и ОВ линии. Результаты расчета динамики распространения оптического импульса ВОСП 10GBase-LX по исследуемому ОВ при указанных условиях ввода в виде 3D-диаграммы и ее отдельных фрагментов представлены на рис. 5а и 5б, соответственно. Анализ полученных данных показывает, что на протяжении всех 2 км сильного проявления эффекта ДМЗ не наблюдается, сигнал сохраняет свою огибающую, при этом дисперсия на выходе 2 км линии составляет D = 92,11 пс.

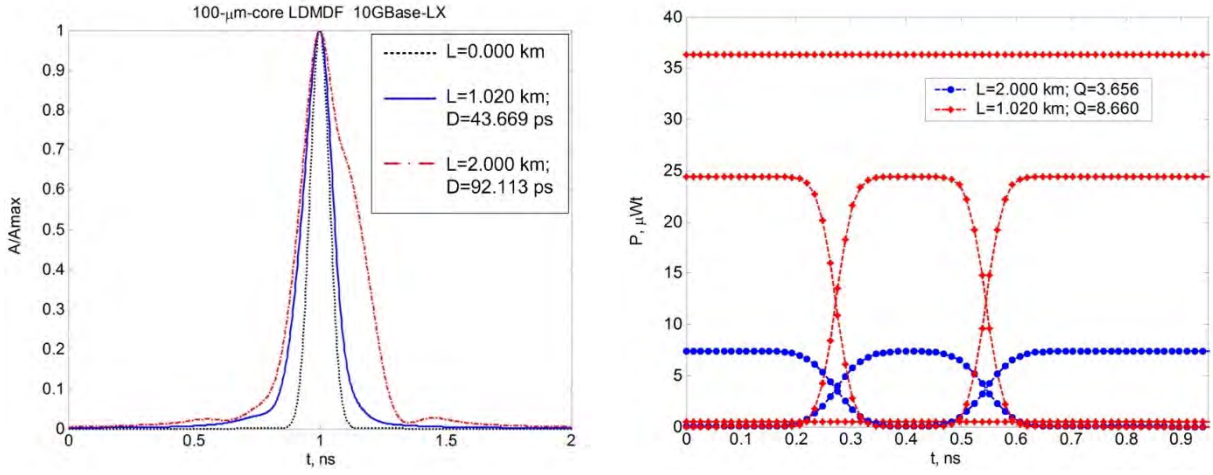


а) б)

Рис. 5. Результаты расчета динамики оптического импульса системы 10GBase-LX (B = 10 Гбит/с, λ = 1310 нм), распространяющегося по ОВ с диаметром сердцевины 100 мкм (профиль показателя преломления рис. 1) протяженностью 2 км с вводом сигнала ЛД, пигтелированного стандартным одномодовым ОВ рек. ITU-T G.652 через типовую оптическую розетку: а) 3D-диаграмма; б) динамика оптического импульса

На следующем этапе для оценки эффективности применения рассматриваемого ОВ при совместной работе с ВОСП 10GBase-LX был проведен расчет огибающей глаз-диаграммы с последующей оценкой Q-фактора/*BER*. Для этой цели использовалась простая приближенная методика, разработанная непосредственно коллективом авторов ратифицированного стандарта IEEE 802.3z, которая подробно изложена в оригинальных работах [7, 8]. В качестве исходных данных использовались спецификации коммерческих трансиверов Cisco SFP-10G-LR-S [9]: уровень мощности на выходе источника оптического излучения p_0 = –8,2 дБм, чувствительность фотоприемника p_R= –14,4 дБм, что обеспечивает типовой бюджет мощности 6,2 дБ. Результаты расчета представлены на рис. 6.

Как было отмечено выше, на выходе 2 км линии с исследуемым ОВ дисперсия сигнала достигает 92,11 пс что приводит к неприемлемо низкому, с точки зрения нормы *BER* = 10^{-12} [10], значения Q-фактора Q = 3,66 при искомом номинальном $Q_{ном}$ = 7,04 [7, 8, 10]. Поэтому на следующем этапе был сделан повторный перерасчет огибающей глаз-диаграммы, Q-фактора и *BER* для уменьшенной протяженности ОВ 100/125 с целью подбора порогового значения этого параметра.



а) б)

Рис. 6. ВОЛП с исследуемым ОВ (диаметр сердцевины 100 мкм, профиль рис. 1), ВОСП 10GBase-LX: а) формы импульсных откликов на передающей стороне, а также расстояниях 1 км и 2 км от ЛД; б) огибающие глаз-диаграммы

Согласно полученным результатам, канал передачи данных со скоростью 10 Гбит/с может быть организован путем совместного использования типового активного оборудования ВОСП 10GBase-LX и исследуемого протяженностью до 1 км без специализированных устройств согласования «ЛД – ОВ», при этом обеспечивается искомое номинальное значение коэффициента ошибок *BER* = 10^{-12}: дисперсия составляет 43,67 пс, в то время как значение Q-фактора превышает искомое номинальное и достигает Q = 8,66.

Таким образом, эффективная модовая полоса пропускания исследуемого ОВ, несмотря на экстремально увеличенный диаметр сердцевины, в маломодовом режиме не менее 10000 МГц·км для каналов передачи данных без проведения дополнительных мероприятий по компенсации дисперсии.

Список используемых источников

1. Bourdine A. V. Modeling and simulation of piecewise regular multimode fiber links operating in a few-mode regime // Advances in Optical Technologies. 2013. vol. 2013. PP. 469389-1–469389-18.

2. Агравал Г. Нелинейная волоконная оптика. М. : Мир, 1996. 323 с.

3. Bourdine A. V., Zhukov A. E. Design of graded refractive index profile for silica multimode optical fibers with improved effective modal bandwidth for short-distance laser-based multi-Gigabit data transmission over “O”-band // Proceedings of SPIE. 2017. vol. 10342. – PP. 1034202-1–1034202-11.

4. Zhukov A. E., Burdin V. A., Bourdine A. V. Design of silica optical fibers with enlarged core diameter for a few-mode fiber optic links of onboard and industrial multi-Gigabit networks // Procedia Engineering. 2017. vol 201. PP. 105–106.

5. Demidov V. V., Ter-Nersesyants E. V., Bourdine A. V., Burdin V. A., Minaeva A. Yu., Matrosova A. S., Khokhlov A. V., Komarov A. V., Ustinov S. V., Golyeva E. V., Dukelskii K. V. Methods and technique of manufacturing silica graded-index fibers with a large central defect of the refractive index profile for fiber-optic sensors based on few-mode effects // Proceedings of SPIE. 2017. vol. 10342. PH. 103420X-1–103420X.

6. Raddatz L., White I. H., Cunningham D. G., Nowell M. C. An experimental and theoretical study of the offset launch technique for the enhancement of the bandwidth of multimode fiber links // IEEE Journal of Lightwave Technology. 998. vol. 16(3). PP. 324–331.

7. Cunningham D., Nowell M., Hanson D. Proposed worst case link model for optical physical media dependent specification development [Электронный ресурс] // IEEE 802.3z Task Force. Presentation materials. January 1997 meeting. 1997. URL: http://www.ieee802.org/3/z/public/presentations/ (дата обращения 30.01.2019).

8. Cunningham D. G., Nowell M., Hanson D. C., Kazovsky L. The IEEE 802.3z worst case link model for optical physical media dependent specification [Электронный ресурс] // IEEE 802.3z Task Force. Presentation materials. March 1997 meeting. 1997. URL: http://www.ieee802.org/3/z/public/presentations/mar1997/ (дата обращения 30.01.2019).

9. Cisco GBase SFP+Modules. Data Sheet. Cisco Public Information. 2012. 9 p.

10. ITU-T Recommendations G.957 (06/99) Optical interfaces for equipments and systems relating to the synchronous digital hierarchy. 1999.

УДК 621.395
ГРНТИ 49.34.06

ОРГАНИЗАЦИЯ И ОЦЕНКА КАЧЕСТВА ПЕРЕДАЧИ РЕЧИ ПО IP ПРОТОКОЛУ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ С ОПЕРАЦИОННОЙ СИСТЕМОЙ ANDROID

М. А. Буценко

Военная академия связи им. Маршала Советского Союза С. М. Будённого

В статье рассматривается пример разработки программного телефона на базе операционной системы Android и открытой библиотеки LibLinphone. Мобильное приложение предоставляет услуги соединения пользователей для последующего обмена информацией по протоколу SIP. Проведено испытание качества передачи речи по стандарту PESQ. Проведен расчет полосы пропускания, требуемой для разрабатываемого программного телефона.

ip-телефония, sip, android, VoIP.

SIP *(Session Initiation Protocol)* – протокол контроля и сигнализации уровня приложения для создания, изменения и завершения сеансов с одним или несколькими участниками [1]. Сеансы могут включать в себя как телефонные вызовы через сеть Интернет, так и презентацию мультимедийных данных.

По данным статистики, в настоящее время насчитывается более 3-х миллиардов пользователей сети интернет. В период с 2000 по 2018 год удельный вес пользователей сети интернет вырос практически в восемь раз – с 6,5 до 51 % мирового населения [2]. Анализируя динамику проникновения интернета во все сферы человеческой жизни, становится понятно, что в скором времени будет происходить коренной перелом подходов к построению сетей связи. Если раньше традиционные сети передачи данных основывались на коммутации каналов, используемых для передачи телефонного трафика, то в наше время телефония будет надстраиваться над инфраструктурой сети передачи данных.

Популярность IP заключается в его восприимчивости к требованиям со стороны не только услуг передачи данных, но также и приложений реального времени. Яркий тому пример – технология передачи речевой информации по сетям с маршрутизацией пакетов IP – Voice over IP (VoIP).

VoIP подразумевает не только использование Интернет в качестве среды передачи, но и протокол IP в совокупности с технологиями, обеспечивающими надежную и качественную передачу речевого трафика в сетях с пакетной коммутацией [3]. По каналам связи передаются пакеты, ячейки, кадры. Каждый пакет имеет заголовок, в котором содержится информация о пункте назначения. Передача осуществляется через маршрутизаторы и коммутаторы. В пункте назначения все пакеты собираются в единое целое в правильной последовательности. Между абонентами обеспечивается виртуальное соединение, при этом создание выделенного соединения не требуется. Благодаря этому сети с коммутацией пакетов являются более гибкими и эффективными, в отличие от традиционной телефонии, которая использует принцип коммутации каналов.

Эффективность использования сети с коммутацией пакетов обеспечивает достаточное сокращение расходов на капитальные затраты на приобретение, установку оборудования и затрат на его содержание. Если направить речевой трафик через корпоративную магистральную сеть передачи данных, то можно заметно сократить финансовые затраты на стандартные телефонные услуги.

Разработанное приложение предназначено для совершения вызовов с использованием технологии VoIP, при этом все звонки являются бесплатными. Для организации связи между абонентами, входящими в сеть достаточно знать IP адрес. Помимо звонков присутствует возможность обмена текстовыми сообщениями. Приложение позволяет организовать работу сотрудников и обеспечить большую мобильность по сравнению с обычными телефонами.

Установление соединения между пользователями осуществляется по пиринговой сети «peer-to-peer». На рис. 1 представлен алгоритм установления соединения без участия прокси-сервера.

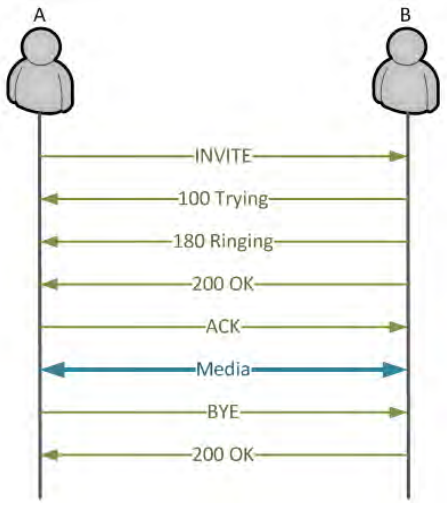


Рис. 1. Алгоритм установления соединения без участия прокси-сервера

Пользователь А отправляет сообщение INVITE на SIP-адрес пользователя В. Содержимое сообщения – сообщение в протоколе SDP, в котором описывается ожидаемый обмен данными. После получения запроса и его обработки оборудование вызываемого пользователя сообщает пользователю о том, что поступил входящий вызов, а встречной стороне передает ответ «180 Ringing». После поднятия трубки удаленной стороне отправляется сообщение «200 OK». UA вызывающего пользователя отправляет второму подтверждение ответа «ASK»

и далее начинается передача мультимедийного трафика. Пользователь А кладет трубку, его UA отправляет запрос BYE. UA второго пользователя отправляет сообщение «200 ОК» [3].

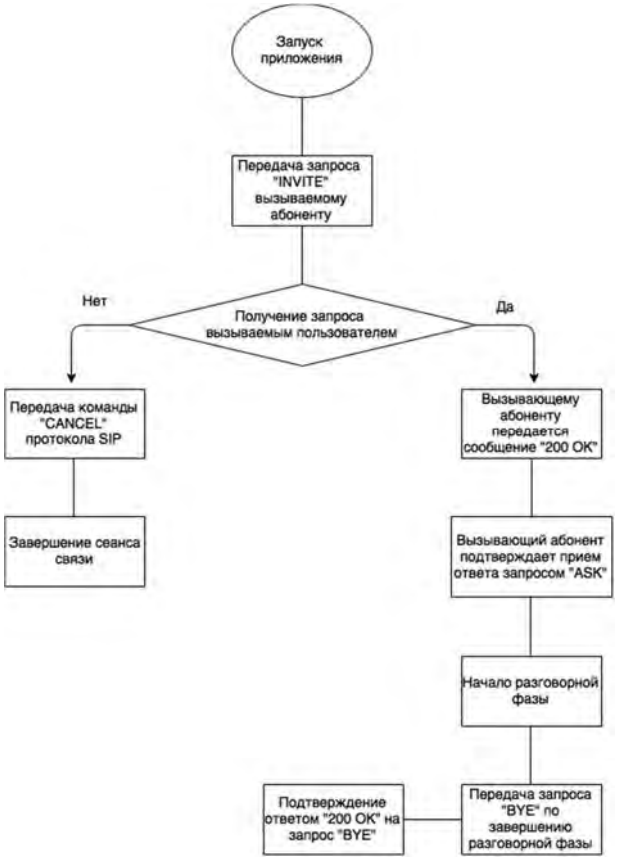


Рис. 2. Блок-схема работы приложения

На рис. 2 представлена блок-схема работы приложения.

Таким образом, практическая реализация телефона заключается в разработке клиентской части и пользовательского интерфейса.

Для разработки мобильного приложения под операционную систему Android использовалась открытая библиотека Liblinphone, которая позволяет создавать собственный пользовательский интерфейс, используя при этом все функциональные возможности программного ядра [4].

На рис. 3 изображен графический интерфейс разработанного программного телефона.

Главный экран приложения содержит информацию о собственном IP-адресе и окно ввода IP-адреса пользователя, с которым необходимо установить сеанс связи. Для быстрого набора можно использовать контактный лист. При вводе IP-адреса осуществляется проверка на правильность ввода.

Как только пользователь вводит адрес вызываемого абонента ему предоставляется возможность осуществления вызова, отправки сообщения или добавление в контактный лист.

Значение PESQ *(Perceptual Evaluation of Speech Quality)* является интегральным показателем качества и включает в себя широкий круг параметров, влияющих на качество, в том числе – деградацию голоса из-за использования кодеков. На рис. 4 представлена схема измерения PESQ, а в таблице – результат измерения для разных кодеков.

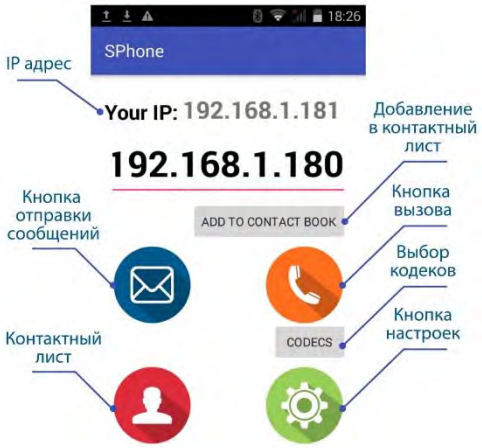


Рис. 3. Графический интерфейс мобильного приложения

Рис. 4. Схема измерения PESQ

ТАБЛИЦА. Результат измерения PESQ

Кодек	Результат измерения
PCMA (G.711 a)	3,361
PCMU (G.711 u)	3,097
Speex	2,942
G.722	2,899

PCMA (G.711 a) обеспечивает наилучшее качество передачи голоса.

Один из важных факторов, который необходимо учесть при создании сети пакетной передачи данных – планирование пропускной способности. Занимаемая VoIP трафиком полоса пропускания складывается из полезной нагрузки – голосовых данных, сжатых аудиокодеком и дополнительных расходов, определяемых стеком протоколов RTP, UDP, IP, канальным и физическим уровнем сети. В зависимости от кодека, в VOIP пакет входит либо 20, либо 30 миллисекунд аудиоданных [5]. Каждый пакет содержит дополнительные расходы стека протоколов.

Таким образом, чем меньше продолжительность аудиоданных, тем больше пакетов будет отослано за 1 секунду и тем больше будут относительные дополнительные расходы стека протоколов RTP, UDP, IP, канального и сетевого уровня сети.

Пример расчета для кодека G.711 до канального уровня сети.

Размер VoIP данных = 160 байт.

$$\text{Дополнительные расходы} =$$

$$= RTP + UDP + IP + L2 = 12 + 8 + 20 + 18 = 58 \text{ байт}$$

$$\text{Количество пакетов в секунду} = \frac{1000 \text{ мс}}{\text{длина пакета в мс}} = \frac{1000}{20} = 50 \text{ пакетов}$$

$$\text{Полоса пропускания} = \left(\frac{\text{аудиоданные}}{1000} + \frac{\text{доп. нагрузка стека протоколов}}{1000}\right) \times$$

$$\times \frac{\text{количество пакетов за секунду} \times 8}{1000} = \frac{(160 + 58) \times 50 \times 8}{1000} = 87{,}2 \text{ кбит/с}$$

Список используемых источников

1. Гольдштейн А. Б., Гольдштейн Б. С. SOFTSWITCH. СПб. : БХВ Санкт-Петербург, 2014.

2. Интернет-доступ (мировой рынок) [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Интернет-доступ_(мировой_рынок) (дата обращения: 28.02.2019).

3. Гольдштейн Б. С., Зарубин А. В., Саморезов В. В. Протокол SIP. Справочник. СПб. : БХВ Санкт-Петербург, 2005.

4. Официальный сайт для Android разработчиков [Электронный ресурс]. URL: https://developer.android.com/ (дата обращения 11.12.2018).

5. Voice Over IP – Потребление пропускной способности на один вызов [Электронный ресурс]. URL: http://www.cisco.com/cisco/web/support/RU/9/92/92059_bwidth_consume.html (дата обращения 22.02.2019).

Статья представлена доцентом ВАС, кандидатом военных наук В. Г. Ивановым.

УДК 621.315
ГРНТИ 47.61, 49.29.17, 59.29

ОБЗОР И СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕФЛЕКТОМЕТРИЧЕСКИХ МЕТОДОВ ИЗМЕРЕНИЯ ПАРАМЕТРОВ КАБЕЛЬНЫХ ЛИНИЙ СВЯЗИ

М. С. Былина

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

Приведена классификация рефлектометрических методов по типу используемого зондирующего сигнала. Проведен сравнительный анализ различных методов по сложности реализации, области применения и информативности. Выявлены преимущества и недостатки каждого рассмотренного метода. Сформулированы рекомендации по применению различных рефлектометрических методов для решения конкретных измерительных задач.

двухпроводная цепь, рефлектометрический метод измерений, рефлектометр, рефлектометрия во временной области, рефлектометрия в частотной области, рефлектометрия во время-частотной области.

Метод рефлектометрических измерений или метод рефлектометрии [1, 2, 3] основан на зондировании двухпроводной цепи (ДЦ) специальными зондирующими сигналами с последующей регистрацией, обработкой и анализом совокупности отраженных от неоднородностей сигналов, называемой сигналом обратного потока (СОП). Приборы, реализующие этот метод, называют рефлектометрами.

По типу используемого зондирующего сигнала различные модификации метода рефлектометрических измерений можно разделить на три основных семейства [4, 5]: рефлектометрия во временной области (*Time Domain*

Reflectometry – TDR), рефлектометрия в частотной области (*Frequency Domain Reflectometry* – FDR) и рефлектометрия во время-частотной области (*Time-Frequency Domain Reflectometry* – TFDR).

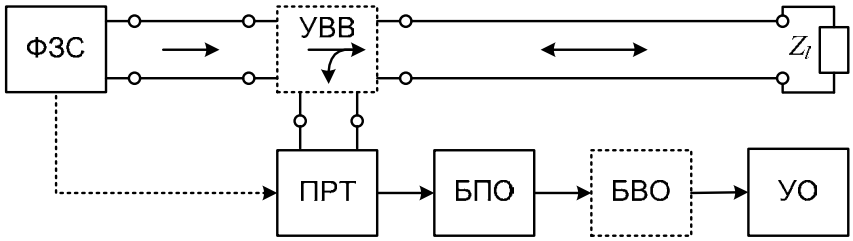


Рисунок. Упрощенная структурная схема рефлектометра

Обобщенная схема рефлектометра (рис.) содержит: формирователь зондирующих сигналов (ФЗС), устройство ввода/вывода сигналов (УВВ), приемно-регистрирующий тракт (ПРТ), блок первичной обработки СОП (БПО), блок вторичной обработки СОП (БВО) и устройство отображения (УО). ФЗС генерирует зондирующие сигналы, которые поступают в исследуемую ДЦ напрямую или через УВВ и распространяются по ней. СОП из ДЦ напрямую или через УВВ, основной функцией которого является направление зондирующего сигнала в ДЦ, а пришедшего из ДЦ СОП к ПРТ, а также согласование выходного сопротивления ФЗС с волновым сопротивлением исследуемой ДЦ. ПРТ обеспечивает усиление СОП и его аналого-цифровое преобразование. С выхода ПРТ СОП поступает на БПО, осуществляющий при необходимости его цифровую фильтрацию, накопление, логарифмирование и хранение. БВО может осуществлять дополнительную математическую обработку СОП, необходимую для рефлектометров, работающих в частотной и время-частотной областях, а также для рефлектометров, работающих во временной области и использующих сложные зондирующие сигналы. БВО может выполнять также различные алгоритмы обработки, направленные на повышение разрешающей и обнаружительной способности, точности и информативности рефлектометрических измерений. После обработки СОП выводится на УО в виде рефлектограммы.

К семейству FDR относятся методы рефлектометрии, использующие гармонические сигналы в качестве зондирующих. Наибольшее распространение получили следующие разновидности этого метода:

1) Phase Detection Frequency Domain Reflectometry (PDFDR) – FDR с регистрацией фазы [4, 5]. В данном методе для последовательного зондирования ДЦ используется N гармонических сигналов, частота $f_i = f_0 + i\Delta f$ ($i = 0 \ldots N–1$) которых ступенчато изменяется в интервале от f_0 до $f_{N–1}$ с шагом $\Delta f = (f_{N–1} – f_0) / N$. Метод основан на измерении на каждой частоте амплитуды и фазового сдвига отраженных от неоднородностей сигналов относительно

зондирующего сигнала. Измеренные величины зависят от параметров неоднородностей и расстояния до них. Известны также модификации данного метода:

1. Standing Wave Reflectometry (SWR) – рефлектометрия стоячей волны, основанная на измерении фазы стоячей волны, которая возникает в ЛС в результате интерференции зондирующей и отраженной волн;

2. Multicarrier reflectometry (MCR) – многочастотная рефлектометрия, в которой зондирование ДЦ осуществляется одновременно суммой N сигналов.

Результатом измерения является зависимость амплитуды и фазы отраженного сигнала от частоты, которая в результате математической обработки в БВО позволяет получить информацию о коэффициентах отражения неоднородностей и расстоянии до них.

2) Frequency Modulated Continuous Wave (FMCW) system (система с частотно модулированным непрерывным сигналом) [4, 5]. В данном методе в качестве зондирующего сигнала используется гармонический сигнал с возрастающей во времени (обычно по линейному закону) частотой. Отраженный сигнал подвергается многократной корреляционной обработке с копиями зондирующего сигнала, сдвинутыми на различные интервалы времени τ. Целью обработки является выявление экстремумов корреляционной функции определение их амплитуд и временных сдвигов τ_i. Количество экстремумов соответствует числу неоднородностей ДЦ, а величина τ_i равна удвоенному времени распространения зондирующего сигнала до неоднородности.

Общими недостатками всех методов FDR являются:

1. Отсутствие наглядности результатов измерения и, как следствие, необходимость их математической обработки.

2. Трудоемкость анализа результатов измерения ДЦ со многими неоднородностями.

3. Сложность в определении параметров искажающих неоднородностей, коэффициенты отражения от которых являются частотнозависимыми. В целом методы FDR существенно уступают в информативности методам TDR и TFDR.

Основными методами, относящимися к семейству TDR являются:

1) Time Domain Reflectometry (TDR) – классический метод рефлектометрии во временной области, использующий в качестве зондирующего сигнала короткий одиночный импульс или перепад напряжения [1, 2, 3]. Рефлектограмма такого прибора представляет собой зависимость СОП от времени или расстояния. Импульсный TDR – единственный прибор, позволяющий получить наглядную рефлектограмму неоднородной ДЦ, по которой в принципе можно определить коэффициенты отражения от неоднородно-

стей и расстояния до них. Возможность отдельной регистрации близко расположенных неоднородностей называется разрешающей способностью, которая улучшается при уменьшении длительности зондирующего импульса. Динамический диапазон импульсного TDR возрастает с увеличением энергии зондирующего импульса, т.е. при увеличении длительности зондирующего импульса.

Математическая обработка СОП импульсного TDR позволяет количественно оценить неоднородность и повысить точность ее локализации.

Рефлектограммы приборов, реализующих перечисленные ниже методы семейства TDR, представляют собой результат корреляции СОП с зондирующим сигналом. Расстояния до неоднородностей определяются по расположению экстремумов корреляционной функции.

2) Sequence Time Domain Reflectometry (STDR) – рефлектометрия во временной области, использующая в качестве зондирующего сигнала псевдослучайные последовательности импульсов (ПСП) [4, 5]. Достоинством метода является увеличение энергии зондирующего сигнала и, следовательно, динамического диапазона при сохранении его разрешающей способности.

3) Spread Spectrum Time Domain Reflectometry (SSTDR) – рефлектометрия во временной области [4, 5] с гармоническим фазоманипулированным зондирующим сигналом, для модуляции которого используется ПСП. Достоинством метода является удаление из спектра зондирующего сигнала низкочастотных составляющих.

4) Noise Time Domain Reflectometry – рефлектометрия без зондирующего сигнала. В качестве такового используется рабочий сигнал. Корреляционная функция имеет пик шириной 1 такт.

5) Chaos Time Domain Reflectometry (CTDR) – рефлектометрия во временной области шумоподобным зондирующим сигналом [6]. Данный метод рекомендован авторами для мониторинга – контроля состояния ДЦ без перерыва связи. Шумоподобный сигнал в этом случае аддитивно складывается с передаваемым по работающей ДЦ сигналом. Шум более высокочастотный, поэтому имеет более узкий пик.

6) Orthogonal Multi-Tone TDR (OMTDR) – рефлектометрия во временной области ортогональными тонами [4, 5], использующая в качестве зондирующего сигнала сумму N гармонических составляющих с разными частотами (тонов), каждая из которых предварительно подвергнута преобразованию с помощью M-QAM модулятора.

К TFDR относятся методы рефлектометрии, работающие одновременно и во временной и в частотной области благодаря использованию специальных зондирующих сигналов:

1) Joint Time-Frequency Domain Reflectometry (JTFDR) – рефлектометрия во время-частотной области [4, 7], использующая в качестве зондирующего сигнала импульс с линейной частотной модуляцией, имеющий гауссову огибающую. Для анализа результатов измерения вычисляются преобразования Вигнера зондирующего сигнала и СОП во время-частотной области. Рефлектограмма представляет собой время-частотную корреляционную функцию двух полученных преобразований.

2) Wavelet Time-Frequency Domain Reflectometry (WTFDR) – вейвлет-рефлектометрия, использующая в качестве зондирующих сигналов вейвлеты (ограниченные и по времени и по спектру) [8, 9]. Для получения рефлектограммы, традиционного для TDR-рефлектометров вида, зарегистрированный сигнал подвергается специальной обработке на основе вейвлет-преобразования.

Отметим, что к WTFDR иногда ошибочно относят рефлектометры класса TDR, в которых осуществляется цифровая фильтрацию СОП с использованием время-частотного вейвлет-преобразования [9, 10]. Такая фильтрация позволяет повысить разрешающую и обнаружительную способность метода.

Основным достоинством методов TFDR является возможность локализации и измерения параметров нестационарных неоднородностей, для которых значимыми параметрами являются не только место расположения и коэффициент отражения, но и время возникновения. Для профилактических и аварийных измерений кабельных ЛС, в которых неоднородности, как правило, стационарны, эти методы пригодны, но не имеют существенных преимуществ по точности и информативности по сравнению с методами TDR.

Учитывая сложность аппаратной и программной реализации методов TFDR, для профилактических и аварийных измерений кабельных ЛС можно рекомендовать методы TDR. Данный вывод косвенно подтверждается и тем, что именно рефлектометры, реализующие метод TDR, наиболее широко представлены на рынке.

Список используемых источников

1. Воронцов А. С., Фролов П. А. Импульсные измерения коаксиальных кабелей связи. М. : Радио и связь, 1985. 96 с.

2. Былина М. С., Глаголев С. Ф. Рефлектометрия кабелей связи : монография, СПбГУТ. СПб., 2015. 228 с.

3. Андреев В. А., Попов Б. В., Попов В. Б. [и др.] Измерения на кабельных линиях связи : учебное пособие для вузов / Под ред. В. А. Андреева. Самара : СРТТЦ ПГАТИ, 2008. 158 с.

4. Furse Cynthia, You Chung Chung, Chet Lo, Praveen Pendayala. A critical comparison of reflectometry methods for location on wiring faults // Smart Structures and Systems. 2006. Vol. 2, No. 1. PP. 25–46.

5. Auzanneau, Fabrice. Wire Troubleshooting and Diagnosis: Review and Perspectives // Progress In Electromagnetics Research. 2013. Vol. 49. PP. 253–279.

6. Auzanneau, Fabrice, Ravot Nicolas, Incarbone Luca. Chaos Time Domain Reflectometry for Online Defect Detection in Noisy Wired Networks // IEEE Sensors Journal. 2016. Vol. 16, No. 22. PP. 8037–8044.

7. Jingjiang Wang, P.E.C. Stone, Yong-June Shin, and Roger A. Dougal. Application of Joint Time–Frequency Domain Reflectometry for Electric Power Cable Diagnostics // IET Signal Processing 2010. Vol. 1, Iss. 4. PP. 395–405.

8. Горохов В. М., Сергеев Д. В. Цифровой вейвлет-рефлектометр. Рефлектометрия во временной области [Электронный ресурс] // ООО «Связьприбор». URL: http://www.svpribor.ru/vestnik.php?id=070302015011.

9. Lima V. D., Klautau A., Costa J. [et all]. A Wavelet-Based Expert System for Digital Subscriber Line Topology Identification // International Journal of Communication Systems. 2014. Vol. 29, Iss. 1. PP. 46–53.

10. Иванов А. Б., Котляр С. С., Левченко А. С., Ташоян А. Ф. Применение вейвлет-преобразования и нейронных сетей для локализации и идентификации сигналов в условиях шумов // Спецтехника и связь. 2010. № 2–3. С. 52–57.

УДК 621.372.2, 621.3.011.4
ГРНТИ 49.29

НОВАЯ МЕТОДИКА И РЕЗУЛЬТАТЫ РАСЧЕТА ПОГОННОЙ ЕМКОСТИ ДВУХПРОВОДНЫХ ЦЕПЕЙ

М. С. Былина[1], С. Ф. Глаголев[1], А. Б. Семенов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[2]Национальный исследовательский Московский государственный строительный университет

Проанализирован известный метод Г. Хоу для расчета погонной емкости двухпроводных цепей. Показано, что его применение приводит к заниженному результату. Предложена новая методика расчета погонной емкости, основанная на учете реального распределения линейной плотности заряда по поверхности проводников. Представлены результаты расчета погонной емкости различных двухпроводных цепей, подтверждающие эффективность предложенной методики.

двухпроводная цепь, симметричная цепь, погонная емкость, метод Г. Хоу, линейная плотность заряда.

Для двухпроводной цепи (ДЦ), состоящей из двух протяженных проводников, вводят понятие погонной емкости c (Ф/м), которая определяется отношением линейной плотности заряда Q_l одного из проводников цепи (Кл/м) к напряжению U между ними [1]:

$$c = \left| Q_l / U \right|. \quad (1)$$

Предполагается, что проводники имеют одинаковые по значению, но противоположные по знаку заряды и расположены в однородной бесконечно протяженной диэлектрической среде с относительной диэлектрической проницаемостью ε.

Известны выражения для расчета погонной емкости симметричной ДЦ, состоящей из двух проводников цилиндрической формы радиуса r_a, находящихся на расстоянии a друг от друга [2, 3, 4].

$$c = \frac{\pi \cdot \varepsilon \cdot \varepsilon_0}{\ln\left((a - r_a)/r_a\right)},\ c = \frac{\pi \cdot \varepsilon \cdot \varepsilon_0}{\ln\left(\left(0{,}5a + \sqrt{(0{,}5a)^2 + r_a^2}\right)\Big/ r_a\right)},\ c = \frac{\pi \cdot \varepsilon \cdot \varepsilon_0}{\ln\left(a/r_a\right)}, \quad (2)$$

где $\varepsilon_0 = 8{,}85 \cdot 10^{-12}$ Ф/м – электрическая постоянная. Значения емкости, наиболее близкие к значениям, полученным в результате измерений, можно получить, используя выражение (2б). Расчет по выражению (2а) дает завышенное значение емкости, а по (2в) – заниженное.

Для ДЦ более сложной конструкции необходимо использовать численные методы расчета погонной емкости, из которых наиболее известным является метод Г. Хоу, основанный на предположении о равномерном распределении зарядов по поверхности проводников. Известно, что метод Г. Хоу приводит к заниженным значениям емкости во всех случаях, когда истинное распределение зарядов отличается от равномерного [1].

Для определения истинного распределения зарядов и последующего расчета емкости нами предлагается следующая методика, которую мы рассмотрим на примере симметричной цепи с проводниками, имеющими эллиптическую форму поперечного сечения (рис. 1). Такой проводник будем характеризовать размерами двух полуосей эллипса r_a и r_b.

Представим поверхности проводников совокупностями N бесконечно тонких заряженных нитей. Линейную плотность заряда нити обозначим q_{li}, где $i = 0, 2, \ldots N - 1$ – номер нити. Для удобства последующего изложения и без потери общности будем считать N четным числом, а левый проводник – положительно заряженным. Общая линейная плотность заряда одного проводника может быть определена по формуле:

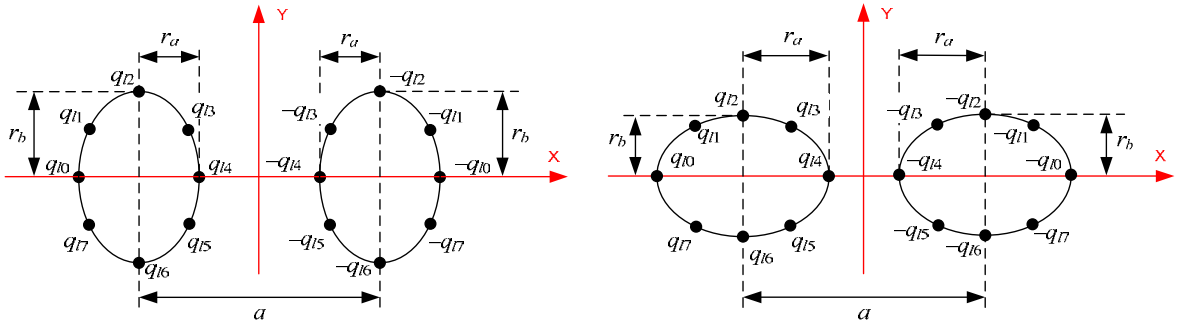
$$Q_l = \sum_{i=0}^{N-1} q_{li}. \quad (4)$$

Потенциал поля заряженной нити в точке, расположенной от нее на расстоянии r, можно определить по известному выражению [5]:

$$\varphi(i, r) = -\left[q_{li} / \left(2\pi \cdot \varepsilon \cdot \varepsilon_0\right)\right] \cdot \ln\left(r/r_0\right), \quad (5)$$

где r_0 – расстояние от заряженной нити до точки, потенциал которой принят равным 0.

На рис. 1 представлено поперечное сечение рассматриваемой цепи. Точками на рисунке показаны места расположения нитей. Введем систему координат X, Y, как показано на рис. 1. В силу симметрии задачи можно утверждать, что: 1) нити, расположенные на поверхностях разных проводников на одинаковых расстояниях от оси Y, имеют одинаковые по абсолютной величине и противоположные по знаку линейные плотности зарядов, 2) нити, расположенные на поверхности одного проводника на одинаковых расстояниях от оси Y, имеют одинаковые линейные плотности зарядов. Будем нумеровать точки расположения нитей следующим образом: на левом проводнике – от 0 до $N-1$, на правом – от N до $2N-1$.



а) б)

Рис. 1. Поперечное сечение симметричной цепи с эллиптическими проводниками при $r_a < r_b$ (а) и $r_a > r_b$ (б)

Определим координаты каждой точки j, в которой расположена заряженная нить. Тогда для координат x_j, y_j точки j можно записать:

$$x_j = \begin{cases} -0{,}5a - B_j \cos\left(j \cdot 2\pi/N\right) \text{ при } i < N \\ 0{,}5a + B_j \cos\left(j \cdot 2\pi/N\right) \text{ при } i \geq N \end{cases}, \quad y_j = B_j \sin\left(j \cdot 2\pi/N\right), \tag{6}$$

где

$$B_j = r_a \cdot r_b \Big/ \sqrt{r_a^2 \sin^2\left(j \cdot 2\pi/N\right) + r_b^2 \cos^2\left(j \cdot 2\pi/N\right)}\,. \tag{7}$$

Выражения, подобные (6) и (7), можно записать для проводников с любой формой поперечного сечения.

Расстояние между любыми двумя точками $j1$ и $j2$ определяется по известному выражению:

$$r_{j1,j2} = \sqrt{\left(x_{j1} - x_{j2}\right)^2 + \left(y_{j1} - y_{j2}\right)^2}\,. \tag{8}$$

Для потенциала точки j, расположенной на поверхности одного из проводников, справедливы выражения:

$$\varphi_j = -\frac{1}{2\pi\cdot\varepsilon\cdot\varepsilon_0}\sum_{i=0}^{N-1} q_{li}\cdot A_{j,i}\,,\ A_{j,i} = \begin{cases} \ln\left(r_{j,i}/r_{j,i+N}\right) \text{ при } j\neq i \\ -\ln\left(r_{j,i+N}/r_0\right) \text{ при } j=i \end{cases}. \quad (9)$$

Составим систему из N уравнений для расчета q_{li}. Первым уравнением системы будет уравнение (4). Остальные уравнения получим, исходя из требования, чтобы разность потенциалов между любыми двумя точками $j1$ и $j2$, расположенными на поверхности левого (положительно заряженного) проводника была равна 0, так как поверхности проводников должны быть эквипотенциальными:

$$U_{j1,j2} = \varphi_{j1} - \varphi_{j2} = -\left[1/\left(2\pi\cdot\varepsilon\cdot\varepsilon_0\right)\right]\cdot\sum\nolimits_{i=0}^{N-1} q_{li}\cdot\left(A_{j1,i} - A_{j2,i}\right) = 0\,. \quad (10)$$

Для формализации задачи уравнения со 2 по (N/2+1) запишем для $j1 = 0$, $j2 = 1, 2, \ldots N/2$, а уравнения с (N/2+2) по N – для $j1 = 1$, $j2 = N/2+1, N/2+2, \ldots N-1$. В матричном виде система будет иметь вид:

$$\mathbf{M}\cdot\vec{q} = \vec{b}\,, \quad (11)$$

где $\vec{q}$ – вектор неизвестных линейных плотностей, **M** – матрица размером N x N, $\vec{b}$ – вектор свободных членов. Элементы **M** и $\vec{b}$ имеют вид:

$$M_{k,i} = \begin{cases} 1 & \text{при } k = 0 \\ A_{0,i} - A_{k,i} & \text{при } 0 < k \le 0{,}5N \\ A_{1,i} - A_{k,i} & \text{при } 0{,}5N < k \le N-1 \end{cases},\ b_k = \begin{cases} Q_l & \text{при } k = 0 \\ 0 & \text{при } k \neq 0 \end{cases}, \quad (12)$$

где k – номер уравнения. Решение (11) имеет вид:

$$\vec{q} = \mathbf{M}^{-1}\cdot\vec{b}\,. \quad (13)$$

Разность потенциалов проводников можно определить по выражениям (9). Для расчета можно выбрать любые две точки, расположенные на поверхностях разных проводников, например:

$$U = \varphi_j - \varphi_{j+N}\,. \quad (14)$$

Результат расчета U по выражению (14) не зависит от выбора номера j, так как мы потребовали равенства потенциалов во всех точках расположения заряженных нитей, и от выбора точки с нулевым потенциалом (расстояния r_0). Погонная емкость может быть рассчитана по выражению (1).

Используя соотношения (4)–(9) можно провести аналогичные расчеты методом Г. Хоу. Для этого необходимо принять все q_{li} одинаковыми и равными Q / N, рассчитать все потенциалы φ_j для точек на поверхности проводников, определить средние потенциалы φ_l и φ_r поверхностей левого и правого проводников по выражениям:

$$\varphi_l = \frac{1}{N}\sum_{i=0}^{N-1}\varphi_i\,,\ \varphi_r = \frac{1}{N}\sum_{i=N}^{2N-1}\varphi_i\,, \qquad (15)$$

рассчитать разность потенциалов проводников и определить погонную емкость по выражению (1).

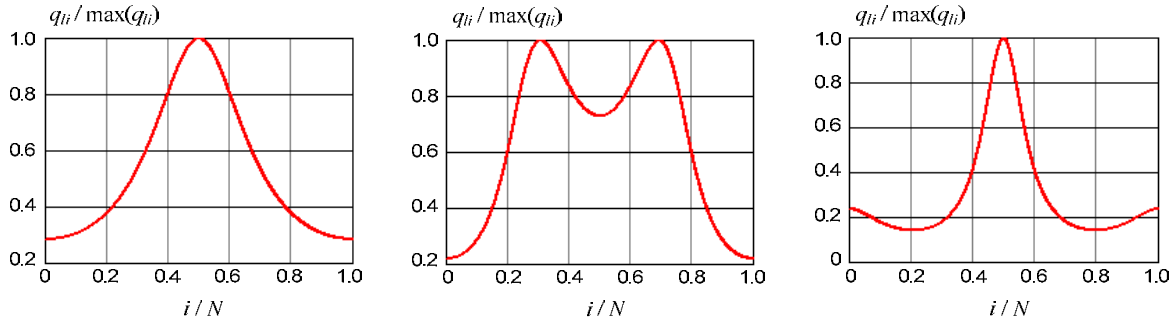
В таблице представлены результаты расчета погонной емкости ДЦ со следующими параметрами: расстояние между проводниками a = 0,95 мм, площадь поперечного сечения проводника 0,212 мм^2, относительная диэлектрическая проницаемость изоляции ε = 2,2. В случае $r_a = r_b$ (цилиндрические проводники) параметры ДЦ соответствуют параметрам симметричного кабеля UTP категории 5E, имеющего погонную емкость около 50 нФ/км. Из таблицы видно, что предлагаемая методика позволяет рассчитать погонную емкость значительно точнее, чем метод Г. Хоу. В таблице представлены также результаты расчета погонной емкости цепей с эллиптическими проводниками.

ТАБЛИЦА. Результаты расчета погонной емкости симметричных цепей

Метод расчета	Погонная емкость (нФ/км)		
	цилиндрич. проводники $r_a = r_b$ = 0,26 мм	эллиптические проводники	
		r_a = 0,208 мм r_b = 0,325 мм	r_a = 0,325 мм r_b = 0,208 мм
Выражение (2а)	56,0	не применимо	не применимо
Выражение (2б)	50,5	не применимо	не применимо
Выражение (2в)	47,2	не применимо	не применимо
Метод Г. Хоу	47,3	46,7	47,9
Предлагаемая методика	50,7	49,5	55,8

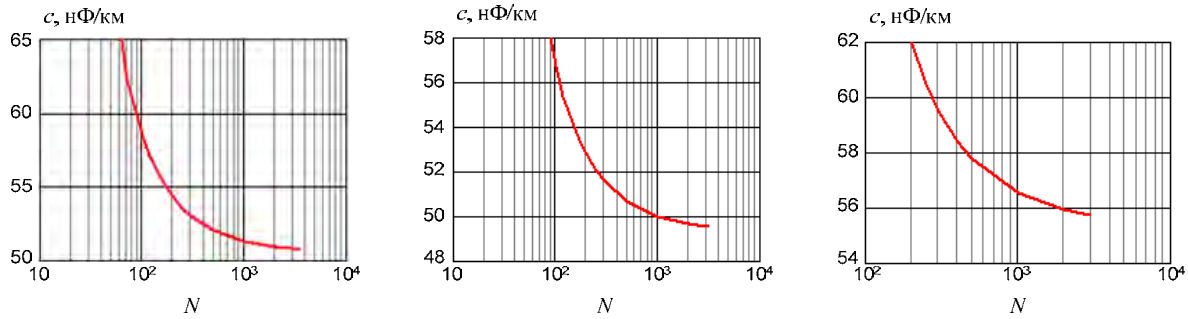
На рис. 2 представлена зависимость нормированной линейной плотности заряда нити q_{li} / max(q_{li}) на поверхности левого проводника от ее относительного номера i / N. Принцип нумерации нитей показан на рис. 1. Из рис. 2 видно, что распределение линейной плотности заряда сильно зависит от формы и взаимного расположения проводников.

Расчеты проводились при разных значениях N. На рис. 3 (см. ниже) представлены зависимости рассчитанной по предложенной методике погонной емкости от числа нитей N. Видно, что при увеличении N погонная емкость уменьшается, стремясь к постоянному значению, которое и принимается за результат расчета.



а) б) в)

Рис. 2. Зависимость нормированной линейной плотности заряда нити от ее относительного номера: а) для ДЦ с цилиндрическими проводниками; б) для ДЦ на рис. 1а; в) для ДЦ на рис. 1б



а) б) в)

Рис. 3. Зависимость погонной емкости, рассчитанной по предложенной методике, от числа нитей: а) для ДЦ с цилиндрическими проводниками; б) для ДЦ на рис. 1а; в) для ДЦ на рис. 1б

Список используемых источников

1. Иоссель Ю. Я., Кочанов Э. С., Струнский М. С. Расчет электрической емкости. Л. : Энергоиздат, 1981. 288 с.

2. Андреев В. А., Портнов Э. Л., Кочановский Л. Н. Направляющие системы электросвязи: учеб. для вузов в 2-х томах. Том 1 – Теория передачи и влияния / Под ред. В. А. Андреева, 7-е изд., перераб. и доп. М. : Горячая линия–Телеком, 2011. 424 с.

3. Чостковский Б. К., Смородинов Д. А. Математическая модель витой пары радиочастотного кабеля объекта управления // Вестник СГТУ. Серия Физико-математические науки. 2008. № 1 (16). С. 113–118.

4. Брискер А. С., Руга А. Д., Шарле Д. Л. Городские телефонные кабели: справочник / Под ред. Д. Л. Шарле, 2-е изд., перераб. и доп. М. : Радио и связь, 1984. 304 с.

5. Кошкин Н. И., Ширкевич М. Г. Справочник по элементарной физике. М. : Наука, 1972.

УДК 681.7.064.43
ГРНТИ 29.31.15

МЕТОДИКА И РЕЗУЛЬТАТЫ РАСЧЕТА ИНТЕРФЕРЕНЦИОННЫХ ФИЛЬТРОВ

М. С. Былина, Б. К. Резников

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

В работе рассматривается матричный метод расчета многослойных структур, лежащий в основе оптических интерференционных фильтров. Предлагается методика расчета структур на основе матриц передачи и матриц рассеяния. Приведены результаты расчета фильтра, представляющего собой двухслойную структуру.

фильтры оптические интерференционные, фильтрация излучения, слоистые среды, многослойные структуры, частотные характеристики.

По принципу работы интерференционные фильтры можно разделить на две группы – пропускательные и отражательные. К первой группе относятся фильтры, в качестве выходного параметра которого используются характеристики проходящей многослойную структуру фильтра волны, а ко второй – характеристики отраженной от структуры волны.

Слои в многослойных средах (рис. 1) [1], используемые в конструкциях оптических фильтров изготавливаются из выращиваемых оптических кристаллов. Широкий набор выращенных материалов позволяет получить излучение в диапазоне от ультрафиолетового (170 нм) до инфракрасного (18 мкм).

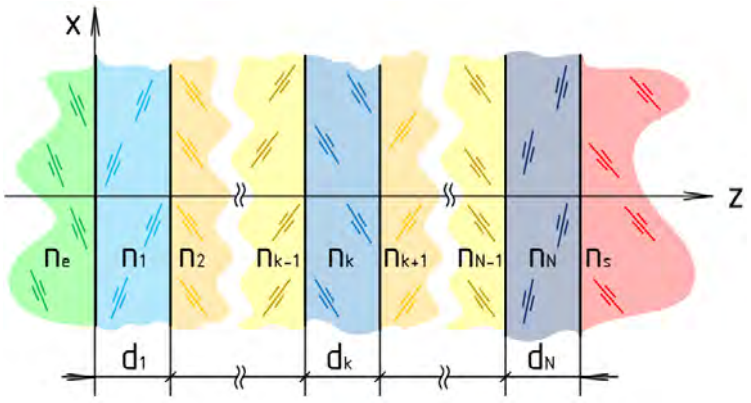


Рис. 1. Поперечное сечение многослойной структуры

Матричный метод расчета многослойной структуры [2] основан на факте, что в каждом слое существует только два типа волн: сонаправленные с падающей волной и направленные противоположно падающей волне. Интерферируя, эти волны в каждой точке структуры образуют одну волну

ξ_t, направленную вперед (прямую), и одну волну ξ_r, направленную назад (обратную). В этом случае описание волн сводится к определению амплитуд напряженностей электрического поля [3].

В [4] определяется следующая *процедура расчета спектральных характеристик многослойной структуры* с заданными показателями преломления и толщинами:

1. Многослойная структура условно делится на однородные слои.
2. Для каждой границы двух соседних слоев с использованием формул Френеля определяются амплитудные коэффициенты пропускания и отражения, строится матрица рассеяния, из которой путем преобразования (4) определяется соответствующая матрица передачи.
3. Для каждого однородного слоя определяется матрица передачи.
4. Матрица передачи многослойной структуры определяется по формуле (2).
5. Матрица рассеяния многослойной структуры определяется путем преобразования (5).
6. Используя коэффициенты матрицы рассеяния, рассчитываются амплитуды напряженностей электрического поля в отраженной от структуры и прошедшей структуру волнах по формуле (3).

Спектральные характеристики многослойной структуры определяются по найденным амплитудам напряженностей электрических полей проходящей и обратной волн.

Расчет спектральных характеристик двухслойной структуры в проходящем свете. В качестве примера рассмотрим процесс расчета спектральных характеристик двухслойной структуры (рис. 2), находящейся в воздухе (n_e = n_s = 1). Свет падает на структуру нормально.

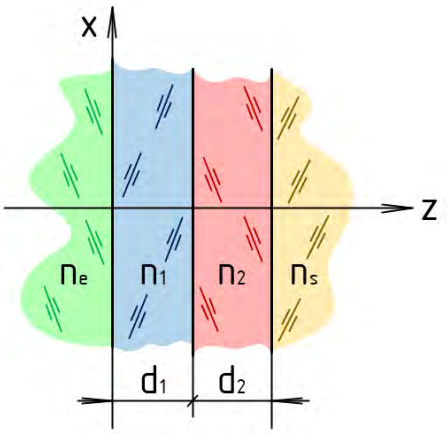


Рис. 2. Поперечное сечение многослойной структуры

n_1 = 1,74 – показатель преломления среды 1; d_1 = 220 нм – толщина среды 1; n_2 = 1,76 – показатель преломления среды 2; d_2 = 220 нм – толщина среды 2.

Определим матрицу передачи для структуры [4]:

$$\mathbb{M}_{es}(\lambda_0) = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix} = \mathbb{M}_{2s}\mathbb{M}_2(\lambda_0)\mathbb{M}_{12}\mathbb{M}_1(\lambda_0)\mathbb{M}_{e1}.$$

Найдем матрицу рассеяния структуры:

$$\mathbb{S}_{es}(\lambda_0) = \begin{bmatrix} t_{es} & r_{se} \\ r_{es} & t_{se} \end{bmatrix} = \frac{1}{m_{22}} \begin{bmatrix} m_{11}m_{22} - m_{12}m_{21} & m_{12} \\ -m_{21} & 1 \end{bmatrix}.$$

И, наконец, приняв за 1 амплитуду прямой волны в среде *e*, за 0 – амплитуду обратной волны в среде *s*, вычислим амплитуды прямой волны в среде *s* и обратной в среде *e*:

$$\mathbb{E}'_{es} = \begin{bmatrix} E_{ts} \\ E_{re} \end{bmatrix} = \begin{bmatrix} t_{es} & r_{se} \\ r_{es} & t_{se} \end{bmatrix} \begin{bmatrix} E_{te} \\ E_{rs} \end{bmatrix} = \begin{bmatrix} t_{es} & r_{se} \\ r_{es} & t_{se} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Амплитудная характеристика (рис. 3) пропускания структуры определяется выражением:

$$\mathrm{A}_t(\lambda) = \left| \frac{E_{ts}(\lambda)}{E_{te}(\lambda)} \right|.$$

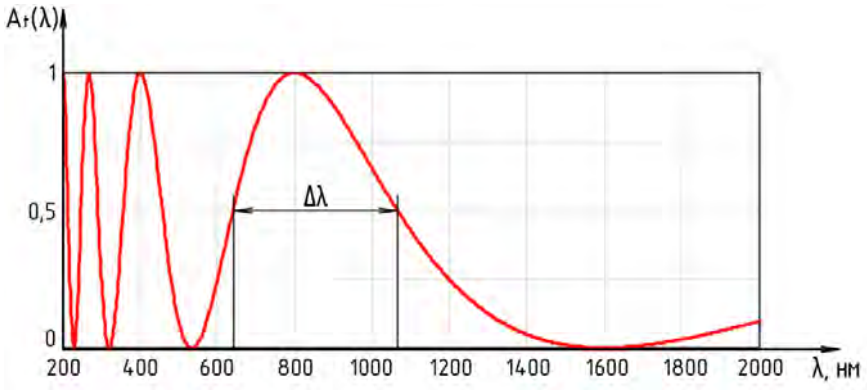


Рис. 3. Амплитудная спектральная характеристика пропускания двухслойной структуры

Ее фазовая спектральная характеристика (рис. 4) определяется выражением:

$$\Phi_t(\lambda) = \arg\left(\frac{E_{ts}(\lambda)}{E_{te}(\lambda)} \right).$$

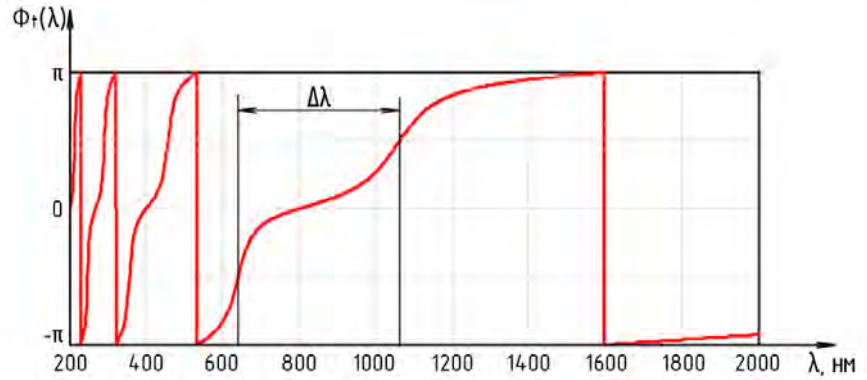


Рис. 4. Фазовая спектральная характеристика пропускания двухслойной структуры

Используя переход от длины волны к частоте, рассмотрим частотные характеристики (рис. 5, 6) фильтра:

$$\lambda = \frac{c}{f}.$$

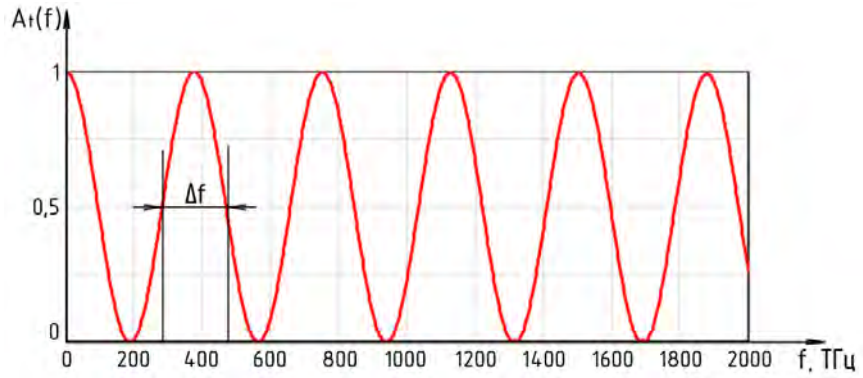


Рис. 5. Амплитудно-частотная характеристика пропускания двухслойной структуры

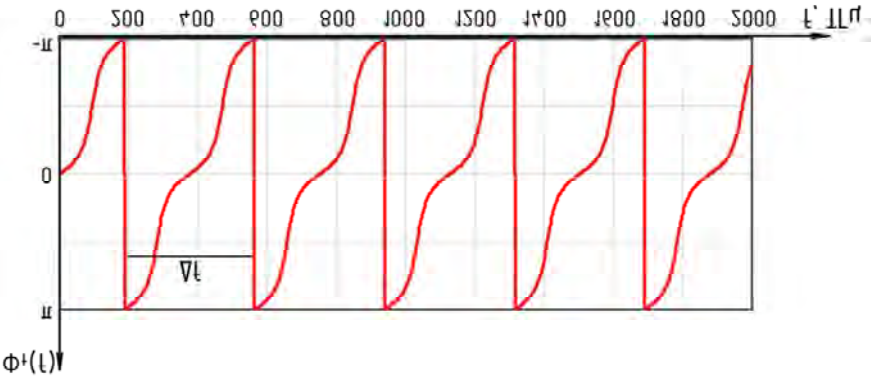


Рис. 6. Фазочастотная характеристика пропускания двухслойной структуры

Из рис. 5–6 видно, что амплитудно- и фазочастотные характеристики двухслойной структуры являются периодическими. Частоты, на которых фильтр со слоями равной толщины d имеет максимальное пропускание, могут быть приближенно определены по выражению:

$$f_{pj} \approx j\frac{c}{2\tilde{n}d}, j \in \{0, \mathbb{N}\},$$

где $\tilde{n}$ – среднее арифметическое значений показателей преломления двух сред, составляющих структуру.

Частоты, которые фильтр со слоями равной толщины d задерживает, могут быть приближенно определены по выражению:

$$f_{sj} \approx (2j-1)\frac{c}{4\tilde{n}d}, j \in \{\mathbb{N}\}.$$

В результате исследования предложена методика анализа спектральных характеристик оптических фильтров, основанных на многослойных структурах. Установлено, что при увеличении количества слоев в многослойной структуре улучшается избирательность фильтра. Приведен пример анализа двухслойной периодической структуры.

Список используемых источников

1. Борн М., Вольф Э. Основы оптики. М. : Наука, 1973.

2. Джеррард А., Берч Дж. М. Введение в матричную оптику. М. : Мир, 1978.

3. Салех Б., Тейх М. Оптика и фотоника. Принципы и применения. Т. 1. Долгопрудный : Издательский дом «Интеллект», 2012. 784 с.

4. Резников Б. К. Исследование оптических интерференционных фильтров // 72-я региональная научно-техническая конференция студентов, аспирантов и молодых ученых «Студенческая весна – 2018»: сб. науч. ст. в 2-х т. / Под ред. К. В. Дукельского. Т. 1. СПб.: СПбГУТ, 2018. С. 169–174.

УДК 004.056 ***Приглашенный доклад***
ГРНТИ 81.93.29

ПРЕДВАРИТЕЛЬНАЯ ОБРАБОТКА ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В СИСТЕМАХ МОНИТОРИНГА СЕТИ ИНТЕРНЕТ

К. А. Валиева[1], Л. А. Виткова[1,2], А. А. Чечулин[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Сегодня основные информационные потоки данных на человека направлены из сети Интернет. Общество погружено в информационную сферу, процесс цифровизации имеет устойчивую тенденцию к развитию. В современных системах мониторинга используются методы сбора, разработанные в тот период, когда потоков и объемов данных было гораздо меньше. Авторы исследуют современные подходы, методы и алгоритмы, ищут пути улучшения. Основной целью исследования является поиск характеристик и оценивание параметров информационных объектов, что позволило бы ввести приоритезацию задач для систем мониторинга сети Интернет.

мониторинг, большие данные, информационный объект, класс информационных объектов, модель данных.

Анализ современных исследований в области мониторинга, методов сбора и хранения данных показывает, что, прежде всего ученые решают технические вопросы оптимизации систем хранения, повышения производительности и разработки алгоритмов работы с большими данными [1, 2, 3]. Данная работа является продолжением предыдущих исследований авторов. Ранее рассматривались методы выявления нежелательной информации на отдельных веб-страницах сети Интернет и вопросы их классификации [4, 5].

Классификация информации основана на базовом представлении информационного объекта (IO) в сети Интернет. IO – это логически цельный блок информации, представленный в определенной фиксированной форме, созданный и используемый в ходе информационной составляющей деятельности человека.

Для формализации представления всех IO необходимо ввести понятие «класс информационных объектов (CIO)». CIO определяется формой представления, которая задает следующие возможные компоненты макроструктуры:

1. Большие информационные объекты (BIO):
   - информационная система;
   - социальная сеть;
   - мессенджер;
   - игровой портал;
   - медиа-портал;
   - веб-сайт;
   - форум.
2. Средние информационные объекты (MIO):
   - веб-страница;
   - группа;
   - блог;
   - канал;
   - статья.
3. Малые информационные объекты (LIO):
   - пост;
   - сообщение;
   - комментарий;
   - текст статьи;
   - заголовок;
   - медиаконтент (картинка, видео, музыка).

Формально можно записать следующее соотношение:

$$(CIO = LIO \in MIO \in BIO).$$

К числу основных особенностей сети Интернет и социальных сетей, влияющих на предварительную обработку информационных объектов, относятся следующие факторы:

1) огромный объем данных, доступных пользователям;

2) сложная, многокомпонентная структура *IO*;

3) большое количество связей между отдельными объектами в сети Интернет.

Все три фактора определяют выбор подхода к сбору и предобработки объектов. Одновременно на него влияют и доступные способы хранения собранного материала, типы базы данных. Возможно использовать технологию связок в БД, но это может привести к потере места. Также, работа со связками в базе не всегда эффективна. Часть решений сегодня просто сохраняет файл в выбранное поле, и при необходимости анализирует. Для вывода результатов анализа и оценки есть средства, которые показывают вложенности (зависимости) между элементами.

В качестве примера рассмотрим модель данных с новостного агрегатора, связанность между сюжетами и алгоритм ранжирования (рис.).

Рисунок. Модель данных новостного агрегатора

Модель данных помогает сделать выбор между возможными вариантами БД. Согласно графику трендов [6], отраженному в таблице (см. ниже), сегодня лидирует 10 систем управления БД.

В таблице выделены 6 систем управления БД, исходный код которых открыт. В дальнейшей работе авторы планируют исследовать 3 из них: (1) MySQL, (2) PostgreSQL, (3) MongoDB. К СУБД предъявляются следующие требования:

1. Совместимость с платформой Hadoop.

2. Совместимость с БД OrientDB, в которой анализируются графы связей между информационными объектами.

В рамках исследования авторы настраивают сбор данных из новостных агрегаторов, зарегистрированных в реестре [7]. Проводят тестирование модели данных и анализируют полученные выгрузки с целью выявления различных характеристик, оценивания их параметров и разработки подхода к приоритетизации задач мониторинга информационных объектов в сети Интернет.

ТАБЛИЦА. Рейтинг систем управления БД

Ранжирование			Название БД	Модель данных	Рейтинг		
03.2019	02.2019	03.2018			03.2019	02.2019	03.2018
1	1	1	Oracle	Реляционная и мультимодельная	1279,14	+15,12	–10,47
2	2	2	**MySQL**		1198,25	+30,96	–30,62
3	3	3	Microsoft SQL		1047,85	+7,79	–56,94
4	4	4	**PostgreSQL**		469,81	–3,75	+70,46
5	5	5	**MongoDB**	**Документная**	401,34	+6,24	+60,82
5	5	5	IBM Db2	Реляционная и мультимодельная	177,20	–2,23	–9,47
7	9	7	Microsoft Access	Реляционная	146,20	+2,18	+14,26
8	7	8	**Redis**	Ключ–значение (*Key-value*), мультимодельная	146,12	–3,32	+14,90
9	8	9	**Elasticsearch**	Поисковая система (*Search engine*), мультимодельная	142,79	–2,46	+14,25
10	10	11	**SQLite**	Реляционная	124,87	–1,29	+10,06

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-11-00302) в СПИИРАН.

Список используемых источников

1. Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Т. 6. № 3. С. 1–9.

2. Котенко И. В., Ушаков И. А. Модели NOSQL баз данных для мониторинга кибербезопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. В 4-х томах. 2018. С. 498–501.

3. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). IEEE, 2017. С. 1–8.

4. 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, Вып. 4. С. 362–377.

5. Kotenko, I., Chechulin, A., Komashinsky, D.: Categorisation of web pages for protection against in-appropriate content in the internet. International Journal of Internet Protocol Technology 10(1), 61–71 (2017).

6. DB-Engines Ranking. URL: https://db-engines.com/en/ranking (дата обращения 22.03.2019)

7. Федеральный закон от 23 июня 2016 г. N 208-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Кодекс Российской Федерации об административных правонарушениях».

УДК 654.1
ГРНТИ 49.34.06

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ ПРИМЕНИТЕЛЬНО К ЗАДАЧЕ ПРОГНОЗИРОВАНИЯ НАГРУЗКИ КОНТАКТ-ЦЕНТРА

Н. И. Васылив[1], К. Э. Есалов[1], С. В. Кисляков[1,2], Р. И. Пупцев[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Научно-технический центр «АРГУС»

Работа посвящена исследованию нейросетевой модели прогнозирования количества поступающих вызовов в колл-центр. Для расчета параметров модели применён метод машинного обучения с применением реальных входных нагрузок контакт-центра. Актуальность задачи, поставленной в докладе, обуславливается пониманием того, какое количество операторов должно быть «на своих местах», для обеспечения должного качества обслуживания колл-центра. Для этого нам нужно заранее предсказывать число входящих вызовов. В работе приводится сравнительный анализ различных моделей предсказания входящих вызовов, основанных на различных математических методах.

колл-центр, оператор, нейронные сети, LSTM, прогнозирование.

Введение

При создании контакт-центра всегда необходимо знать предполагаемую нагрузку в виде количества поступающих вызовов за единицу времени. Это поможет грамотно распределить ресурсы, как сетевые, так и человеческие, в смысле количество операторов, обслуживающих вызовы. Исходя из нагрузки, можнр знать сколько операторов должно быть нанято в контакт-центр и выведено в работу. Чем точнее будет известна какая нагрузка поступает на контакт-центр, тем большая вероятность задействовать необходимое количество операторов соответственно нагрузке, следовательно,

обслужить вызовы с заданным качеством и грамотно распределить денежные ресурсы на оплату труда. Это значит, что экономия денежного ресурса зависит от того, как точно предсказана нагрузка за определенный промежуток времени. Причем чем меньший промежуток времени и точней прогноз, тем точнее будет информация сколько нужно операторов и сколько нужно заплатить за часы их работы.

Сейчас существует большое количество методов решения задач предсказания. Помимо моделей для решения задач предсказания временных рядов [1] применяются также и регрессионные модели [2]. Среди предсказательных методов того и иного типа для предсказания нагрузки могут быть использованы, например, модели типа Holt-Winters' Method, учитывающие тренд и сезонную составляющую, и ARIMA [3].

Современной теоретической альтернативой таким методам прогнозирования могут быть Deep Learning (глубокое обучение) методы прогнозирования, в частности LSTM [4] нейронные сети, такие модели могут давать результаты лучше, чем обычные регрессионные и предсказательные методы [1].

Постановка задачи

Исходный набор данных выглядит как представлено на рис. 1. Требуется по известным данным, предсказать будущую нагрузку на контакт-центр.

В нейронную сеть будут поступать последовательно только значения нагрузки, то есть временные интервалы, представленные в виде каждых пятнадцати минут работы контакт-центра. Нейронная сеть будет настраивать веса исходя из подаваемой обучающей выборки, а на тестовой выборке можно выяснить насколько хорошо работает модель. В качестве критерия оценки обучения нейросети возьмем такие показатели как среднеквадратическая ошибка (*Mean Squared Error*, MSE) и коэффициент детерминации (R^2):

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)^2,$$

$$R^2 = 1 - \frac{MSE*n}{\sum_{i=1}^{n}(\hat{y}_i - \bar{y})},$$

	Начало временного интервала	Количество поступивших вызовов в очередь
01.01.16	00:00 - 00:15	39
01.01.16	00:15 - 00:30	39
01.01.16	00:30 - 00:45	56
01.01.16	00:45 - 01:00	56
01.01.16	01:00 - 01:15	46
01.01.16	01:15 - 01:30	46
01.01.16	01:30 - 01:45	36
01.01.16	01:45 - 02:00	36
01.01.16	02:00 - 02:15	31
01.01.16	02:15 - 02:30	31
01.01.16	02:30 - 02:45	27
01.01.16	02:45 - 03:00	27
01.01.16	03:00 - 03:15	17
01.01.16	03:15 - 03:30	17
01.01.16	03:30 - 03:45	16
01.01.16	03:45 - 04:00	16
01.01.16	04:00 - 04:15	21
01.01.16	04:15 - 04:30	21
01.01.16	04:30 - 04:45	23
01.01.16	04:45 - 05:00	23
01.01.16	05:00 - 05:15	17
01.01.16	05:15 - 05:30	17
01.01.16	05:30 - 05:45	20
01.01.16	05:45 - 06:00	20
01.01.16	06:00 - 06:15	22
01.01.16	06:15 - 06:30	22

Рис. 1. Количество поступивших вызовов за первые 7 часов

где y_i – i-ое значение из выборки, $\hat{y}_i$ – i-ое значение, возвращенное моделью, $\bar{y}$ – среднее арифметическое, n – количество значений.

Первый показывает, как отличается выходное значение нейронной сети от реального, а второй на сколько хорошо работает модель, где отрицательное значение будет показывать неправильность работы сети. Нулевое значение отображать эталонную модель. А единица – идеальную модель. Для написания кода нейронной сети используется библиотека Keras, средой проектирования выбрана платформа Colaboratory от Google.

Модели

Эксперимент был проведен на четырех моделях, различающихся архитектурами. Здесь под архитектурой понимается совокупность слоев нейронной сети и количество нейронов или ячеек памяти в слоях. Общее между ними то, что в каждой используются LSTM слои, полносвязные слои из обыкновенных нейронов, для свертки в одно значение на выходе, активационной функциях ReLu и сигмоидальной активационной функции.

Первая модель для сравнения – модель с единичным LSTM слоем и двумя полносвязными слоями, нужными для сведения выхода к единичному значению. Вторая аналогична первой, однако добавлен Dropout слой. Третья модель состоит из двух LSTM слоев и одного слоя Dropout. А особенность четвертой не только в двух LSTM слоях, полносвязных слоях и Dropout между каждым слоем, но и в том, что LSTM слои находятся в состоянии stateful.

Методы Dropout и Stateful

После результатов работы первой модели можно видеть, что значения среднеквадратической ошибки и коэффициента дифференциации (рис. 2, см. ниже) недостаточно достоверны. На основании низких показателей среднеквадратической ошибки было сделано предположение о том, что модель переобучается. Чтобы бороться с явлением переобучения используют различные методы регуляризации. Самым распространенным и эффективным методом на данный момент является метод прореживания (*dropout*) [5]. Прореживание применяется к слою и выражается в обнулении некой доли случайно выбранных выходов нейрона.

При практическом построении нейронной сети вводится понятие batch (батч) – набор из n образцов, подаваемых в нейронную сеть за одну итерацию обучения. Понятие батч тесно связано с архитектурой последней модели LSTM с состоянием stateful. Можно подавать значения единично, но и можно сгруппировать их в батчи, чтобы ускорить процесс обучения, а также дать понять LSTM нейронной сети, что в сгруппированных данных

существует тренд, который нужно запомнить. Суть состояния stateful заключается в том, что LSTM нейронная сеть запоминает зависимость исключительно в конкретном батче, но не между ними [6]. Dropout реализуется добавлением между слоями нейросети слоя dropout:

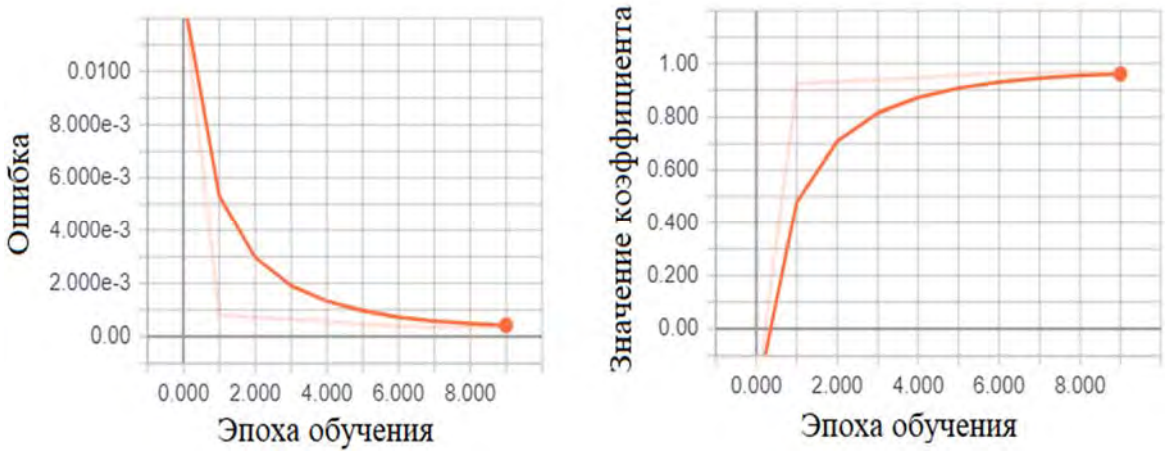


Рис. 1. Изменение среднеквадратической ошибки (слева)
и коэффициента дифференциации (справа) относительно итерации обучения

Сравнение результатов

На рис. 3 показаны значения корня среднеквадратической ошибки (RMSE):

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)^2}.$$

Рисунок отражает значение корня среднеквадратической ошибки на обучении (синим) и на тесте(оранжевым) по итогу работы каждой из моделей. Из рисунка видно, что значения ошибки на тесте не сильно выше значений ошибки на обучении, следовательно, модели не переобучены. Несмотря на то, что ошибка на обучении и тесте выше в результатах последней модели, наиболее достоверными могут быть именно они, если учитывать описанное выше stateful состояние.

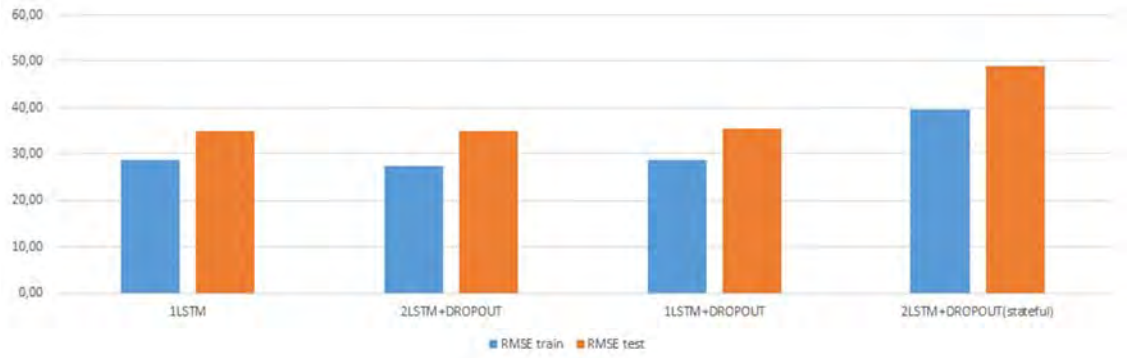


Рис. 2. Значения корня среднеквадратической ошибки

Выводы

На данном этапе можно сказать о том, что при решении поставленной задачи более целесообразно использовать несколько LSTM слоев рекуррентной нейронной сети с stateful состоянием и dropout слоями (четвертая модель). Стоит учесть такой важный момент работы с библиотекой Keras, как построение предсказаний. В ходе проведения эксперимента для получения предсказанных значений использовалась функция predict, которая требовала подачу в нее тестовой выборки. Следовательно, для дальнейших экспериментов следует решить проблему предсказания без заранее известных значений для сравнения. Тем не менее на данный момент известно от какой архитектуры нейронной сети нужно отталкиваться, какую методику оптимизации решения использовать и факт того, что нейронная сеть хорошо справляется с задачей регрессии. Следующим этапом исследования планируется использовать более глубокие модели нейронных сетей с использованием различных слоёв, а также сбор более объемной статистики call-центра.

Список используемых источников

1. [cs.LG] 9 Nov 2018 Youru Li, Zhenfeng Zhu , Deqiang Kong, Hua Han , Yao Zhao. EA-LSTM: Evolutionary Attention-based LSTM for Time Series Prediction. arXiv:1811.03760v1, 2018.

2. Фёрстер Э., Рёнц Б. Методы корреляционного и регрессионного анализа. Руководство для экономистов: пер. с нем. и предисловие В. М. Ивановой. М. : Финансы и статистика, 1983. 304 с.

3. [Jansen, 2010] Mathijs Jansen. Call Centre Forecasting A comprehensive analysis of missing data, extreme values, holiday influences and different forecasting methods. Tilburg University 1 April 2010.

4. Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory". Neural computation 9.8 (1997): 1735–1780.

5. Brownlee, Jason. December 3, 2018. “A Gentle Introduction to Dropout for Regularizing Deep Neural Networks”. URL: www.machinelearningmastery.com

6. Brownlee, Jason. July 28, 2016. “Understanding Stateful LSTM Recurrent Neural Networks in Python with Keras”. URL: www.machinelearningmastery.com

УДК 004.72
ГРНТИ 49.33.35

ОСНОВНЫЕ ВИДЫ УГРОЗ ПРИ КОМПРОМЕТАЦИИ OPENFLOW КАНАЛОВ В SDN

А. Д. Венедиктов, В. Н. Волкогонов

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

В архитектуре, предлагаемой SDN сетями, плоскость управления и плоскость данных для устройств передачи данных разделены, что приводит к преобразованию исходной закрытой архитектуры сети в более открытую. Из этого следует, что предлагаемая архитектура подвержена различным специфичным видам атак. Реализация угроз в программно-конфигурируемой сети может привести к компрометации различных компонентов, таких как контроллеры OpenFlow, физические или виртуальные коммутаторы, системы управления и приложения. В данной статье представлен анализ основных видов угроз при компрометации канала Openflow и меры, способствующие их противодействию.

SDN, архитектура SDN, программно-конфигурируемые сети, Openflow.

Современный интернет представляет собой комбинацию сетей различных размеров и топологий, поддерживающих широкий спектр приложений, которые могут различаться требованиями к качеству обслуживания (QoS) [1]. Производительность любой сети зависит от многих факторов, включая структуру сети, механизмы управления перегрузками и т. д. Современные сети, несут большой объем трафика, который предъявляет динамические требования к пропускной способности и задержкам, что усложняет процесс их управления. Постоянно увеличивающиеся размеры и сложность существующих сетей и служб требуют наличие эффективного, но в то же время упрощенного управления, которое сводит к минимуму взаимодействие с человеком и ввод команд вручную. В связи с этим в качестве перспективных решений была разработана архитектура программно-определяемой сети (*Software-Defined Networking*, SDN). Данная архитектура обладает большими возможностями для автоматического и динамического управления сетевыми потоками.

В SDN контроллер управляет всеми коммутаторами через каналы «OpenFlow» [2]. Команды и запросы от контроллера, а также состояние и статистика от коммутаторов передаются по этому протоколу, поэтому безопасность и надежность каналов OpenFlow между контроллером и коммутаторами имеют решающее значение для надёжной работы SDN сети,

её конфигурации и управления. Если злоумышленник имеет возможность перехватить и/или изменить сообщения на этих каналах, он может отправить ложные сообщения на коммутаторы и контроллеры, а также осуществить широкий спектр атак, таких как отказ в обслуживании (DoS) или атака «человек посередине» (MitM) [3].

Для защиты управляющего канала Openflow можно использовать методы шифрования и аутентификации канала, например, Transport Layer Security [4, 5]. TLS, как и его предшественник, Secure Sockets Layer (SSL), являются криптографическими сетевыми протоколами для защиты передачи данных. TLS обеспечивает конфиденциальность и целостность, а также аутентификацию сервера и клиента. Он основан на асимметричном шифровании. Однако одна только аутентификация и шифрование не могут гарантировать безопасность каналов OpenFlow. Использование TLS для шифрования канала не обеспечивает полной защиты из-за известных уязвимостей данного протокола. Так, например, протокол TLS не сможет противостоять ситуации, в которой атакующий имеет возможность извлечь криптографический ключ из заранее скомпрометированного коммутатора. Для защиты от подобных атак используется метод out-of-band передачи управляющего трафика.

В рамках данной работы был собран стенд (рис.) на основе виртуальных коммутаторов Open vSwitch и контроллера OpenDaylight для экспериментальной проверки методов компрометации и защиты каналов Openflow.

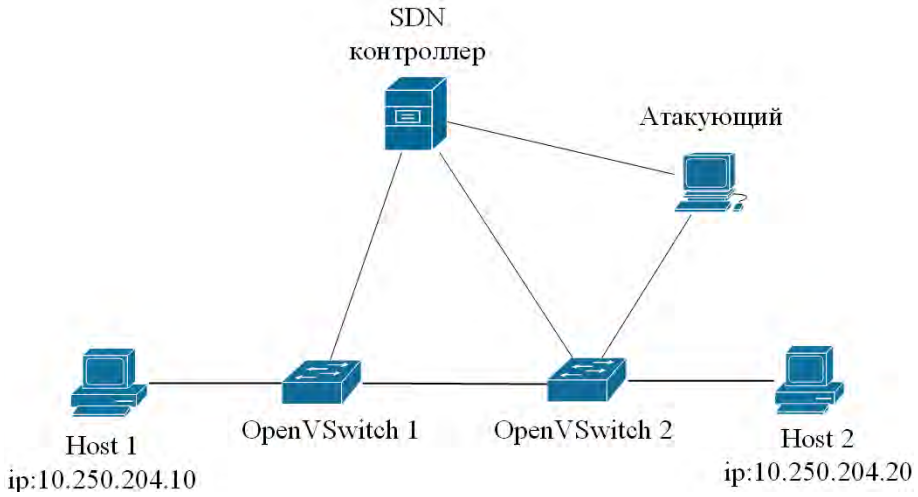


Рисунок. Схема архитектуры SDN-сети экспериментального стенда

Из-за перехвата каналов OpenFlow могут возникнуть катастрофические последствия, как для сетевых провайдеров, так и для их клиентов. Например, злоумышленник может собирать конфиденциальную информацию о клиентах, путем передачи команды коммутаторам отправлять копии пакетов, содержащих данную информацию, злоумышленнику. Таким образом,

сетевая архитектура SDN имеет присущие ей проблемы с безопасностью, связанные с компрометацией Openflow-канала [6], рассмотрим основные и них.

Модификация Flow-таблиц

Самая очевидная атака - незаметное изменение таблицы переадресации атакуемого коммутатора. К примеру, злоумышленник может заблокировать поток трафика, идущий к определенному клиенту, и перенаправить этот поток на адрес другого хоста. Для этого атакующему необходимо вставить в канал управления OpenFlow два пакета, которые содержат команды изменения таблицы потоков.

Сбор информации

Атакующий может скрытно собирать информацию, изменяя таблицу переадресации коммутатора. Для этого злоумышленнику нужно подделать пакет OpenFlow, содержащий команды изменения таблицы потоков, и отправить его коммутатору. В этом случае атакующий дает указание коммутатору отправить копию каждого пакета с адресом требуемого ему хоста устройству, которое подконтрольно злоумышленнику. Как только атакуемый коммутатор обновит свою таблицу пересылки, злоумышленник получит все пакеты, изначально предназначенные для атакуемого хоста.

Атака на изменение топологии

В SDN контроллер изучает глобальную топологию через LLDP пакеты. Предположим, что контроллер приказывает первому коммутатору отправлять пакеты LLDP через порт eth1. Второй коммутатор получает этот пакет через порт eth2. Затем второй коммутатор включает и этот пакет, и номер порта eth2 в сообщение типа packet_in и отправляет его контроллеру. Из этого сообщения контроллер узнает, что порт eth1 на первом коммутаторе соединяется с портом eth2 на втором. В том случае, если злоумышленник изменит пакеты LLDP, у контроллера будет неправильное представление о предоставленной ему топологии.

Схема аутентификации в случае использования протокола TLS должна включать аутентификацию и контроллера, и коммутатора, поскольку без проверки последнего может быть осуществлена данная атака на изменение топологии.

В программно-определяемой сети контроллер выступает в качестве центральной точки отказа. Поскольку по каналам управления передаются различные команды и запросы, а также состояние и статистика, их компрометация может привести к потере доступности и конфиденциальности данных, передающихся по сети. Наличие таких атак как модификация Flow-

таблиц, «человек посередине» и атака на изменение топологии позволяют злоумышленнику собрать достаточно информации, чтобы скомпрометировать контроллер и другие устройства, чтобы манипулировать потоками данных. Наличие аутентификации, контроля доступа и безопасного зашифрованного канала по протоколу OpenFlow позволяет обеспечить его безопасность.

Список используемых источников

1. Левин М. В., Ушаков И. А., Цветков А. Ю., Исаченков П. А. Основы построения компьютерных сетей. СПб. : СПбГУТ, 2016. 56 с.

2. Openflow switch specification: Version 1.5.1 [Электронный ресурс]. URL: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf (дата обращения 15.01.2019).

3. Kreutz D., Ramos F. M. V., Verissimo P. Towards Secure and Dependable Software-Defined Networks, Hot Topics in Software Defined Networking // HotSDN. ACM, 2013, pp. 55–60.

4. Киррилов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем : учебное пособие. Часть 1. СПб. : СПбГУТ, 2012. 64 с.

5. Киррилов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем: учебное пособие. Часть 2. СПб. : СПбГУТ, 2012. 64 с.

6. Cheng Li, Zhengrui Qin, Ed Novak, Qun Li Securing SDN Infrastructure of IoT-Fog Networks from MitM Attacks, Software Architecture // IEEE Internet of Things Journal, 2017, pp. 1156–1164.

УДК 004.056
ГРНТИ 81.93.29

МЕСТО И РОЛЬ МОНИТОРИНГА И ПРОТИВОДЕЙСТВИЯ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Л. А. Виткова[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

При высоком уровне распространения социальных сетей и отсутствия четких правовых механизмов контроля за ними, политические оппоненты, международные террористические и экстремистские организации, криминальные структуры осознают те возможности, которые они могут использовать для воздействия на пользователя.

Современные подходы к обнаружению противоправной информации в сети Интернет в общем и в социальных сетях в частности требуют доработки с учетом смены «модели коммуникации» современного пользователя. В работе представлена модель коммуникации пользователя. Описаны возможные пути улучшения системы мониторинга и противодействия с учетом представленной модели.

мониторинг, противодействие, нежелательная информации, анализ социальных сетей, модель коммуникации.

Вопрос информационной безопасности в социальных сетях стоит достаточно остро и является дискуссионным. Исследуя современные направления государственной политики в сфере мониторинга и противодействия информации, необходимо отметить, что государство стремиться обеспечить безопасность в сети Интернет.

Одним из наиболее проработанных правовых актов в этой области является ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ [1]. В статье 9 говориться об ограничении доступа к информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. В статье 10 описаны требования и ограничения к распространению информации в сети Интернет и в Средствах массовой информации (далее СМИ).

В первом квартале 2019 года в реестре Роскомнадзора числилось 145165 СМИ [2]. Такое количество несравнимо с объёмом зарегистрированных веб сайтов. Согласно отчету [3] в феврале 2019 года в доменной зоне «.RU» зарегистрировано 5015756 домена верхнего уровня, из них 62,3 % являются веб-сайтами или одностраничными сайтами. То есть в доменной зоне «.RU» находится более 3 млн. информационных сайтов.

Однако, все без исключения социальные сети располагаются на доменах верхнего уровня «.COM», как и многие зарегистрированные СМИ. Ни одно сетевое СМИ не зарегистрировано на домене второго уровня социальной сети и согласно требованиям ООО «В Контакте» регистрировать аккаунт в целях использования группой лиц или организацией запрещено [4].

И все же, множество публичных и открытых страниц в социальных сетях являются информационными каналами. На рис. (см. ниже) представлена модель коммуникации современного пользователя сети Интернет.

Модель демонстрирует передачу информации пользователю через множество каналов. Так, например, сообщение о событии может прозвучать в новостях на телевидении и одновременно на радио. Часть сюжета будет включено в периодические издания, освещено со стороны информационных агентств. Каждый канал, так или иначе, передаст некоторую тональность, эмоциональный окрас. И если первые 4 канала чаще всего попадают

под действие «Закона о СМИ» [5], включены в реестр Роскомнадзора, ограничены определенными правовыми, этическими и моральными нормами. То 5 информационный канал, то есть социальные платформы (Вконтакте, Telegram, Viber и др.) менее подконтрольны.

Рисунок. Модель коммуникации пользователя

По данным исследований, современный пользователь больше времени проводит в социальных сетях [6], чем смотрит ТВ или слушает радио. Возможность комментирования сообщений, выражения одобрения или поддержки со стороны других участников делает такие сети наиболее значимыми информационными каналами в современной модели коммуникации.

Отметим, что сегодня на уровне «Контроль и надзор» различные государственные ведомства занимаются обнаружением противоправного сообщения, блокировкой его или страницы в целом. В процессе могут не учитываться источники такого сообщения, множество его «репостов», копии в сети. По сути, из множества одинаковых информационных объектов блокируется доступ только к одному из них.

Возможным решением является совершенствование систем мониторинга и противодействия, направленное на выявление каналов распространения, выявления инициаторов и ферм ботов [7].

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-71-10094) в СПИИРАН.

Список используемых источников

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 31.07.2006. N 31 (1 ч.), ст. 3448.

2. Перечень наименований, зарегистрированных СМИ. URL: https://rkn.gov.ru/mass-communications/reestr/media/ (дата обращения 03.04.2019).

3. Отчет АНО «Координационного центра национального домена сети Интернет». Февраль 2019. URL https://cctld.ru/files/stats/2019_feb_RU.pdf (дата обращения 03.04.2019).

4. Лицензионное соглашение ООО «ВКОНТАКТЕ». URL https://vk.com/licence (дата обращения 03.04.2019).

5. Закон РФ от 27.12.1991 N 2124-1 (ред. от 18.04.2018, с изм. от 17.01.2019) «О средствах массовой информации» // Ведомости СНД и ВС РФ. 13.02.1992. N 7, ст. 300.

6. Виткова Л. А., Проноза А. А., Сахаров Д. В., Чечулин А. А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х томах. 2018. С. 191–195.

7. Левкин И. М., Науменко К. А., Виткова Л. А. Особенности информационно-психологического воздействия в интернете // Информационная безопасность регионов России (ИБРР-2017): материалы конференции. 2017. С. 365–367.

Статья представлена доцентом кафедры, кандидатом технических наук А. А. Чечулиным.

УДК 004.056
ГРНТИ 81.96.00

АНАЛИЗ ОСОБЕННОСТЕЙ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ ДЛЯ ФОРМИРОВАНИЯ СИСТЕМЫ МЕТРИК ЕГО ЗАЩИЩЕННОСТИ

Л. А. Виткова[1], Т. О. Гамидов[2], Е. В. Дойникова[1], О. С. Дудкина[2], А. Г. Кушнеревич[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Статья посвящена анализу особенностей индустриального Интернета вещей, существующих методик и стандартов информационной безопасности, с целью формирования системы метрик защищенности системы индустриального Интернета вещей.

интернет вещей, оценка рисков, уязвимости, информационная безопасность, методики оценки защищенности.

В настоящее время активно развивается Интернет вещей (*Internet of Things*, IoT), стремительно растет число подключенных устройств, что ведет к прямо пропорциональному росту числа рисков как физической, так и информационной безопасности (ИБ). Поэтому во избежание разного рода потерь, необходимо обеспечивать защиту «умных» устройств и каналов передачи данных. Еще большее значение имеет обеспечение безопасности индустриального Интернета вещей (*Industrial Internet of Things*, IIoT), напрямую связанного с критичными технологиями. Поэтому в данном исследовании рассматривается понятие IIoT и смежные понятия, описываются различные виды систем IIoT, выделяются его основные компоненты и особенности. В результате проведенного анализа предлагается модель IIoT и первичные группы метрик защищенности для последующей оценки защищенности.

Понятие IIoT тесно связано с такими понятиями, как киберфизические системы (*Cyber-physical system*, CPS), диспетчерский контроль и сбор данных (*Supervisory Control And Data Acquisition*, SCADA) и IoT. Киберфизическая система – это система, включающая набор взаимодействующих физических и цифровых компонентов, которые могут быть централизованными или распределенными. SCADA – это программное обеспечение (ПО), используемое для мониторинга и управления производственными процессами в широком спектре отраслей, в реальном времени. IoT – это система объединенных в сеть подключенных устройств («вещей»). Каждое устройство представляет собой узел в виртуальной сети, непрерывно передающий данные о себе и своем окружении благодаря встроенным датчикам и ПО [1]. IIoT – это система, состоящая из сетевых интеллектуальных объектов, киберфизических активов, связанных посредством информационных технологий, которые обеспечивают интеллектуальный и автономный доступ в режиме реального времени, сбор, анализ, обмен данными и обмен информацией о процессах, продуктах и/или услугах в промышленной среде [2]. Применяется в различных отраслях, таких как электроэнергетика, транспорт, финансы, сельское хозяйство, водоснабжение и другие.

Поскольку в системах CPS и SCADA не требуется обязательное подключение к сети Интернет в отличие от IoT и IIoT, сравнивать будем последние две системы. Сравнительный анализ систем IoT и IIoT представлен в таблице 1 (см. ниже).

На данный момент существует довольно много методик оценки защищенности систем SCADA, однако методики оценки защищенности IoT и IIoT только начинают появляться. Оценка защищенности систем напрямую связана с оценкой рисков. Хороший обзор методик оценки рисков

для SCADA представлен в [3]. Он охватывает 24 методики. Их можно разделить на:

– методики, основанные на модели, в которых риск рассчитывается по формулам с использованием математической модели риска. Такие методики представляют информацию в табличной или текстовой форме;

– методики, основанные на графической модели процесса оценки защищенности, которые дают качественную или количественную оценку риска. В частности, используются модели в виде графа.

ТАБЛИЦА 1. Сравнение IoT и IIoT

	IoT	IIoT
Цель появления	Повысить комфорт в быту	Повысить рентабельность производства
Цена выхода из строя	Средняя, или скорее низкая	Высокая, или очень высокая
Скорость внедрения	Высокая	Низкая
Влияние стоимости обслуживания	Низкое	Высокое
Объем данных	Небольшой или средний	Большой или очень большой
Риски ИБ	Высокие	Критически высокие

Также методики можно классифицировать по уровню детализации и охвату:

– методики с низким уровнем детализации и широким охватом. Представляют собой порядок действий, которые должен выполнить пользователь, без их подробного описания;

– методики, с высоким уровнем детализации и узким охватом. Представляют собой подробное описание конкретного этапа;

– методики, объединяющие в себе два предыдущих типа, то есть с высоким уровнем детализации и широким охватом. Представляют собой подробные руководства, охватывающие множество этапов процесса управления рисками.

Подавляющее большинство методик, описанных в [2], относятся к классу методик, основанных на моделях, по первой классификации, и к классу методик с высоким уровнем детализации и узким охватом по второй классификации. Однако предпочтительной представляется методика, основанная на модели, дающая количественную оценку риска, и отличающаяся высоким уровнем детализации и широким охватом. Отметим, что такая классификация подойдет для методик, применимых к разным видам систем. Таким образом, в данном исследовании предполагается разработать

методику для IIoT, основанную на модели, дающую количественную оценку риска и с широким охватом и высоким уровнем детализации.

Поскольку обеспечение безопасности IoT и IIoT достаточно актуальная на сегодняшний день проблема, начали появляться стандарты обеспечения их безопасности. С целью усиления безопасности промышленного IoT-оборудования ИСО представила новый технический стандарт ISO/TR 22100-4 «Безопасность производственного оборудования – Связь с ISO 12100 – Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов информационной безопасности (кибербезопасности)». Данный стандарт дополняет стандарт безопасности промышленного оборудования ISO 12100 «Безопасность производственного оборудования – Основные принципы проектирования – Оценка и снижение рисков».

Однако на текущий момент данные стандарты поддерживаются не везде, так как их внедрение является непростой задачей ввиду особенностей систем IIoT (таких как распределённость, разнородность, множество источников и большие объемы собираемой информации). Поэтому одной из важных задач является мониторинг защищенности таких систем и постоянная переоценка защищенности. Это необходимо учитывать при разработке методики оценки защищенности.

Поскольку в исследовании предполагается разработать методику оценки защищенности, основанную на модели, рассмотрим основные компоненты IIoT и взаимодействие между ними, внешние факторы, влияющие на них, а также актуальные угроз и уязвимости.

Для успешной работы IIoT на производстве в любой отрасли требуется специальное оборудование. Основными устройствами являются различные web-программируемые контролеры, модули удаленного ввода/вывода с поддержкой протоколов TCP/IP, UDP, HTTP, DHCP, ARP, также необходимы шлюзы и IIoT платформы для сбора данных с конечных устройств и передачи их для дальнейшего мониторинга и анализа. Помимо этого, используются различные датчики и сенсоры, собирающие необходимые сведения об устройствах и среде, в которой они находятся, это могут быть датчики температуры, давления, влажности, содержания в воздухе различных примесей и т. д.

Наибольшее распространение в системе IIoT получил протокол MQTT или Message Queue Telemetry Transport, благодаря применимости в нестабильных сетях, низкому энергопотреблению и небольшим пакетам данных. MQTT – это протокол обмена данными между удаленными устройствами, работающий поверх TCP/IP на прикладном уровне.

В качестве модели предлагается использовать модель в виде графа, как, например, в [4]. В качестве узлов данного графа будут выступать уязвимости системы IIoT, а в качестве связей – переход от одной уязвимости

к другой за счет получения необходимых привилегий для эксплуатации следующей уязвимости. Состояние системы будем определять наличием связей между уязвимостями в каждый момент времени, а также оценкой риска, которая будет определяться для каждого узла графа. Основной проблемой при этом является определение уязвимостей систем IIoT, для этого можно использовать базы NVD [5] и ФСТЭК [6]. В частности, в таблице 2 представлены некоторые уязвимости, характерные для подобных систем.

ТАБЛИЦА 1. Пример уязвимостей для систем IIoT

Идентификатор	Описание	Продукт, содержащий уязвимость
CVE-2018-7839	Уязвимость связана с ошибками при использовании криптографии. Эксплуатация уязвимости может позволить нарушителю раскрыть защищаемую информацию.	Платформа мониторинга IIoT Monitor
CVE-2018-7837	Уязвимость связана с некорректным контролем внешних XML-ссылок. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, внедрять некорректные документы в выходные данные.	Платформа мониторинга IIoT Monitor
CVE-2018-7836	Уязвимость связана с отсутствием ограничений при загрузке файлов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, загружать и запускать вредоносные файлы, которые могут быть автоматически обработаны в рамках среды продукта.	Платформа мониторинга IIoT Monitor
CVE-2018-7835	Уязвимость связана с отсутствием фильтрации специальных символов. Эксплуатация уязвимости может позволить злоумышленнику выйти за пределы каталога с ограниченным доступом.	Платформа мониторинга IIoT Monitor

Для оценки защищенности с использованием разрабатываемой модели могут применяться разные метрики. Категории метрик (показателей), применяемых для оценки защищенности, представлены на рис. (см. ниже) [7]. Для оценки защищенности IIoT, комплекс метрик необходимо расширить, учитывая особенности его состава. Таким образом, основные изменения будут касаться категории «Показатели топологического уровня».

Промышленный Интернет вещей позволяет повысить эффективность разного рода систем и активно развивается. Однако, одновременно с этим, появляется все больше проблем с его защитой, что указывает на необходимость создания новых методик оценки его защищенности и обеспечения безопасности. В результате сравнительного анализа и изучения особенностей индустриального Интернета вещей, была получена необходимая база

знаний для формирования метрик защищенности, учитывая особенности состава IIoT, и выбрана модель IIoT, которая ляжет в основу методики его защищенности.

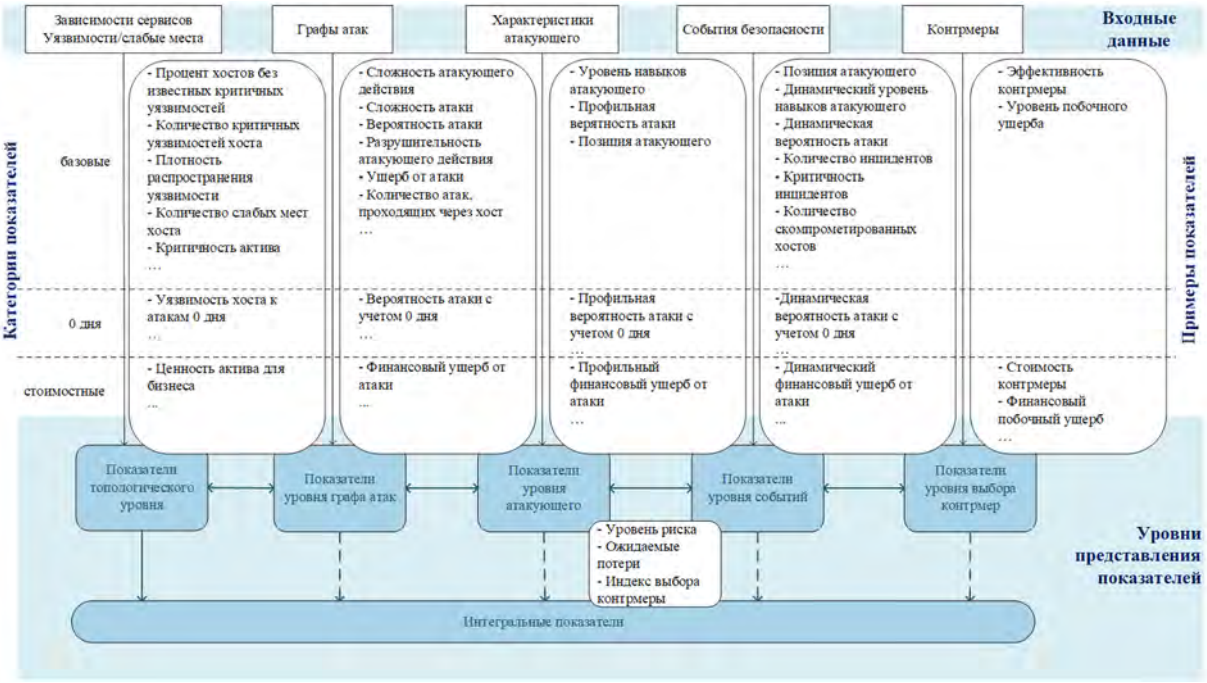


Рисунок. Комплекс метрик защищенности

Работа выполнена при поддержке гранта РФФИ 19-07-01246.

Список используемых источников

1. Российская ассоциация электронных коммуникаций (РАЭК). Исследование IIoT 2017.

2. Hugh Boyes, Bil Hallaq, Joe Cunningham, Tim Watson. The industrial internet of things (IIoT): An analysis framework // Cyber Security Centre, WMG, University of Warwick, Coventry, CV4 7AL, UK.

3. Cherdantseva, Y., Burnap P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K.: "A Review of cyber security risk assessment methods for SCADA systems" . Computers & Security. Volume 56, February 2016, pp. 1–27.

4. Дойникова Е. В., Котенко И. В. Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер // Труды СПИИРАН, 2018, Вып. 2 (57). С. 211–240. DOI: 10.15622/sp.57.9

5. National Vulnerability Database [Электронный ресурс]/ URL: https://nvd.nist.gov/

6. Банк данных угроз безопасности информации [Электронный ресурс]/ URL: https://bdu.fstec.ru/vul

7. Дойникова Е. В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Труды СПИИРАН. 2013. Вып. 3 (26). С. 54–68.

УДК 004.51
ГРНТИ 81.93.29

ОБЗОР СПОСОБОВ ЧЕЛОВЕКО-КОМПЬЮТЕРНОГО ВЗАИМОДЕЙСТВИЯ ДЛЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Л. А. Виткова, В. А. Десницкий, К. Н. Жернова, А. А. Чечулин

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В статье представлен анализ способов человеко-компьютерного взаимодействия в современных программных средствах обеспечения сетевой безопасности. В качестве примера рассматриваются несколько систем управления информацией и событиями безопасности и анализаторов трафика с точки зрения взаимодействия пользователя и программы как со стороны пользователя, так и со стороны программы. Способы реализации человеко-компьютерного взаимодействия в данных программных средствах сравниваются между собой, определяются их достоинства и недостатки. На основе проведённого анализа даётся оценка эффективности человеко-компьютерного взаимодействия в современных программных средствах обеспечения сетевой безопасности.

человеко-компьютерное взаимодействие, информационная безопасность, SIEM-системы, пользовательские интерфейсы, графический пользовательский интерфейс, текстовый пользовательский интерфейс.

Информационная безопасность в настоящие дни достаточно автоматизирована, однако окончательное решение при обнаружении проблем в безопасности всё ещё принимается человеком. По этой причине разработка методов человеко-компьютерного взаимодействия (далее ЧКВ) является важной частью при создании программного обеспечения (далее ПО) информационной безопасности.

Одним из основных направлений ЧКВ является переход к графическим интерфейсам. Текстовый интерфейс постепенно вытесняется графическим, в том числе и в ПО информационной безопасности. Данный факт объясняется тем, что увеличение количества обрабатываемых данных требует грамотного подбора модели визуализации [1], а также тем, что возникает необходимость увеличения скорости обработки данных [2].

Программы по сетевой аналитике чаще всего предоставляют следующие способы взаимодействия с ними: графические элементы в виде кнопок, выпадающих списков, чекбоксов, всплывающих подсказок. Вывод информации происходит в текстовом виде, либо в виде графиков и диаграмм.

В качестве примеров ЧКВ в сфере сетевой безопасности ниже рассмотрены следующие программы, относящиеся к разным классам: Wireshark (пассивный анализ сетевого трафика), ZenMap (активный анализ

хостов со стороны сети), OSSIM (система управления информацией и событиями безопасности, объединяющая множество источников данных в единый интерфейс). Показаны достоинства и недостатки их интерфейсов.

WireShark

WireShark – программа для анализа сетевого трафика, которая захватывает все проходящие по сети пакеты в режиме реального времени вне зависимости от того, кому они были адресованы.

Возможности визуализации информации в данной программе реализованы слабо и сводятся к построению линейных графиков, например, графика зависимости количества пакетов от времени, а также цветовой фильтрации разных типов пакетов (рис. 1). На рис. 1 также представлена оперативная панель управления ПО Wireshark, в которой отображаются необработанные данные о пакетах в трафике.

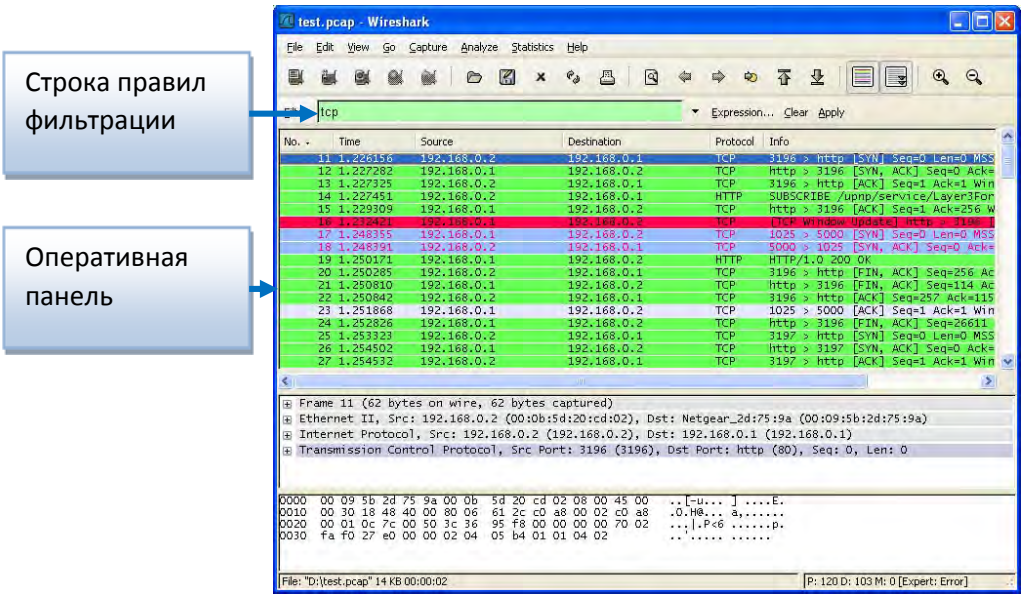


Рис. 1. Фильтрация TCP пакетов в WireShark [3]

ЧКВ с программой происходит при помощи кнопок и ввода правил фильтрации отображаемого трафика в текстовом виде в соответствующую строку. Таким образом, здесь реализовано комбинирование графического и текстового интерфейсов.

Достоинством ПО Wireshark является гибкость интерфейса: данные о пакетах представлены в сокращённом виде с возможностью выбирать определённый тип пакетов и просмотреть более подробную информацию о каждом перехваченном пакете в соответствующем окне.

Недостатками интерфейса ПО Wireshark являются: необходимость помнить команду для её ввода, наличие большого количества элементов

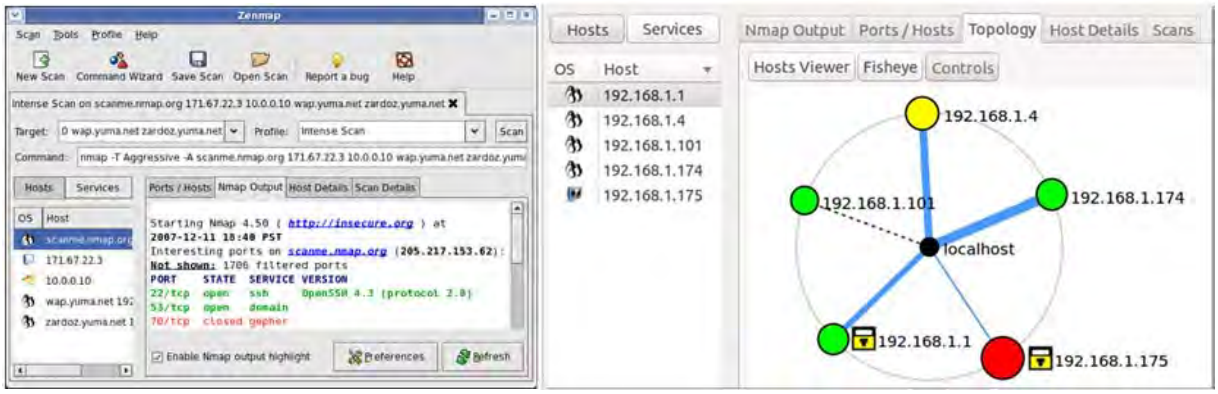
текстового интерфейса, который не естественен для пользователя, необходимость визуального поиска, т. е. просмотра пользователем большого количества текста в поисках нужных данных.

ZenMap

Zenmap предоставляет графический пользовательский интерфейс для Nmap Security Scanner. Nmap – программа для активного сбора информации о сетевой инфраструктуре, которая поддерживает набор различных видов сканирования (например, UDP, TCP-SYN, TCP-FIN, TCP-ACK и др.).

Первоначально ПО Nmap предполагало взаимодействие пользователя с ПО через текстовый интерфейс (командную строку). ПО ZenMap является расширением (графической оболочкой) для ПО Nmap и позволяет пользователю использовать графический интерфейс вместо командной строки. Данный интерфейс позволяет выбирать тип сканирования, цели сканирования и прочие параметры, а команда в командную строку вводится автоматически с возможностью редактирования (рис. 2а).

Визуализация обработанных данных Zenmap представлена интерактивной диаграммой топологии сети (рис. 2б). Информация, касающаяся каждого рассматриваемого хоста, просматривается и обрабатывается пользователем вручную.



а) б)

Рис. 2. Интерфейс Zenmap [4]: оперативная панель (а), интерактивная диаграмма сети (б)

Достоинством интерфейса ПО ZenMap также является гибкость, т. е. возможность выбора удобных для пользователя правил фильтрации. Также существует возможность сохранить результаты сканирования для последующего сравнения с другими результатами, при этом различия выделяются с помощью цвета. Результаты можно записать в поисковую базу данных.

Основной *недостаток интерфейса* ПО ZenMap, так же, как и Wireshark, состоит в необходимости визуального поиска нужной информации, что затрудняет процесс обучения использованию программы.

OSSIM

OSSIM – система управления информацией и событиями безопасности, которая сопоставляет логи событий с информацией, полученной от специализированных средств защиты информации и систем обнаружения, таким образом получая информацию, которую нельзя получить при использовании только одного источника.

OSSIM располагает панелью управления, содержащей результаты обработки и анализа данных о событиях. При этом для анализа трафика программа использует другие приложения-анализаторы с открытым кодом. Пользователь может сортировать события при помощи выпадающего списка, либо отмечая необходимый фильтр в соответствующих чекбоксах. Обработанные данные могут быть представлены графически (рис. 3).

Рис. 3. Примеры основных моделей визуализации в OSSIM [5]

Достоинством интерфейса ПО OSSIM служит наличие инструментов для графического анализа собранной информации. Обработанные данные представлены в виде графиков (рис. 3).

Недостатком интерфейса ПО OSSIM является отсутствие фокусировки внимания пользователя на значимой текстовой информации в обработанных данных. Кроме того, набор графических моделей недостаточно разнообразен, представляя собой в основном линейные графики, гистограммы и круговые диаграммы.

На основе проведённого выше анализа можно представить таблицу сравнения трёх рассматриваемых приложений для безопасности сети. Из таблицы видно, что интерфейс WireShark и Zenmap можно отнести к ком-

бинированным, поскольку в них есть свойства как текстового, так и графического интерфейсов, при этом способы ЧКВ довольно ограничены. В то же время интерфейс OSSIM полностью графический и демонстрирует большое разнообразие инструментов графического интерфейса. Визуализация данных в WireShark и Zenmap крайне слабая, OSSIM же обладает визуальными моделями для представления различных данных. Однако количество этих моделей в OSSIM сравнительно мало. Отсюда следует, что OSSIM является наиболее развитой программной средой сетевой безопасности с точки зрения ЧКВ.

ТАБЛИЦА. Сравнение характеристик ЧКВ в программных средствах WireShark, Zenmap и OSSIM

Характеристики ЧКВ	WireShark	Zenmap	OSSIM
Тип интерфейса	Комбинированный (текстовый + графический)	Комбинированный (текстовый + графический)	Графический
Визуализация обработанных данных	Крайне слабая	Крайне слабая	Присутствуют различные визуальные модели
Взаимодействие пользователя с приложением	Кнопки, всплывающие списки, командная строка	Кнопки, всплывающие списки, командная строка	Широкий набор инструментов графического интерфейса

Таким образом, с точки зрения восприятия информации человеком, OSSIM является наилучшим вариантом из описанных выше. Однако, можно улучшить взаимодействие между человеком и программой путём добавления графических моделей, поддерживаемых OSSIM. Можно видеть, что в области информационной безопасности ЧКВ только встало на путь своего развития.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 18-07-01488) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Коломеец М. В., Чечулин А. А., Котенко И. В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Т. 5. №. 42. С. 232–257.

2. Виткова Л. А. К вопросу безопасности современных пользователей ПК // Naučno-issledovatel'skij žurnal. 2015. № 1 (32) Ч. 3. С. 10.

3. Filtering Packets While Viewing [Электронный ресурс]: Wireshark, 2019. URL: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html (дата обращения 20.11.2018).

4. Zenmap [Электронный ресурс]: Nmap.org, 2017. URL: https://nmap.org/zenmap/ (дата обращения 29.11.2018).

5. How to test OTX within OSSIM [Электронный ресурс]: AlienVault, 2019. URL: https://www.alienvault.com/forums/discussion/17252/how-to-test-otx-within-ossim (дата обращения 10.12.2018).

УДК 004.056
ГРНТИ 81.93.25

МОДЕЛЬ МЕР ПРОТИВОДЕЙСТВИЯ НЕЖЕЛАТЕЛЬНОЙ, СОМНИТЕЛЬНОЙ И ВРЕДОНОСНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Л. А. Виткова[1,2], Е. В. Дойникова[1], И. В. Котенко[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Целью работы является разработка модели мер противодействия нежелательной, сомнительной и вредоносной информации в сети Интернет. В статье рассматриваются различные меры противодействия нежелательной, сомнительной и вредоносной информации и выделяются их виды. Определяется классификация мер противодействия по различным признакам, в том числе, по виду информации, против которой направлены меры, по каналу распространения информации, по целевой аудитории данной информации, по оперативности и способу противодействия. Также определяется набор метрик, характеризующих меры противодействия. С учетом выделенных классов и их признаков, то есть качественных характеристик мер противодействия, а также выделенных метрик, то есть количественных характеристик мер, формируется их модель. В работе также описано применение данной модели в общем процессе противодействия нежелательной, вредоносной и сомнительной информации.

нежелательная, вредоносная и сомнительная информация, меры противодействия, модель, сеть Интернет.

В последнее время все актуальнее становится проблема материального и информационно-психологического ущерба от нежелательной, сомнительной и вредоносной информации, то есть информации, представляющей угрозу для сознания, духовной жизни и информационной деятельности гражданина, и общества в целом. В рамках разработки методики противодействия такой информации в статье предлагается модель мер противодействия нежелательной, сомнительной и вредоносной информации в сети Интернет.

Для защиты от нежелательной информации применимы следующие способы: управление, препятствие, регламентация, принуждение и побуждение. Управление охватывает и описывает применение всех остальных способов (препятствие, регламентация, принуждение и побуждение). Для описания видов, способов распространения и противодействия нежелательной информации используются способы регламентации и принуждения. Средствами, реализующими данные способы, являются акты, принятые в различных организациях и определенные на основе законов Российской Федерации (РФ).

Методы защиты от нежелательной информации на самом верхнем уровне можно разделить на технические (соответствуют физическим, аппаратным, программным средствам защиты), такие как блокировка источников нежелательной информации, и организационные (соответствуют организационным, законодательным, морально-этическим средствам защиты), такие как информирование пользователей.

В настоящее время в РФ существует несколько механизмов защиты от нежелательной информации [1]. К ним относится:

1) ручная классификация информационной продукции по категориям доступа к просмотру, при этом механизм защиты предполагает выдачу предупреждения о категории доступа [2];

2) ручная блокировка ресурсов, содержащих нежелательную информацию, с использованием реестра блокировок;

3) автоматизированные системы защиты от информации в виде отдельных опций в операционной системе (ОС).

Ограничение доступа к нежелательной информации, определенное законами РФ, осуществляется методами препятствия, и зависит от способа распространения нежелательной информации. Методы препятствия подразумевают автоматизированное применение программных и аппаратных средств, ограничивающих доступ к нежелательной информации. В настоящее время основными способам препятствия распространению нежелательной информации является блокировка соответствующих ресурсов [3], а также системы родительского контроля.

Кроме способов препятствия для ограничения доступа к нежелательной информации также применим способ побуждения. В данном случае используются морально-этические средства, в том числе побуждающие родителей не допускать детей к веб-сайтам, содержащим нежелательную информацию. Также необходимо повышать информированность населения об ущербе от распространения такой информации, наказании за ее распространение и средствах защиты.

В таблице 1 конкретные средства защиты от информации разделены на классы. Эти классы могут пересекаться. Класс методов защиты от неже-

лательной информации зависит от вида нежелательной информации, способа и скорости ее распространения (в частности, информация может выкладываться на сайтах или вбрасываться для последующего лавинного распространения), целевой аудитории, влияния средств защиты на права граждан.

ТАБЛИЦА 1. Соответствие между способами и средствами защиты от информации

Классы способов защиты от информации	Классы средств защиты от информации	Средства защиты от информации
препятствие (физическая защита)	физические, аппаратные и программные	фильтрация сообщений, блокировка источников нежелательной информации, автоматизированные системы защиты от информации в виде отдельных опций в ОС, системы родительского контроля
маскировка (шифрование данных)	программные, аппаратные	блокировка источников нежелательной информации
регламентация (определение процедур манипуляции данными)	организационные, законодательные	акты, принятые в различных организациях и определенные на основе законов РФ
управление (выделение основных компонентов информационной системы и управление ими)	организационные, физические, программные и аппаратные	системы мониторинга нежелательной информации и выбора мер по противодействию
принуждение (введение средств защиты для выполнения регламента)	организационные, законодательные, программные, аппаратные, физические	фильтрация сообщений, блокировка источников нежелательной информации, автоматизированные системы защиты от информации в виде отдельных опций в ОС, системы родительского контроля
побуждение (использование Этических и личностных соображений для выполнения регламента)	морально-этические	информирование пользователей, предупреждение о категории доступа информации, побуждение родителей не допускать детей к веб-сайтам, содержащим нежелательную информацию, повышение информированности населения об ущербе от распространения нежелательной информации, наказании за ее распространение и средствах защиты

Класс способа защиты от информации, как и класс средств защиты от информации, являются параметрами предлагаемой модели мер противодействия. Разработанная модель описывается следующими параметрами: класс способа защиты от информации; класс средства защиты от информации; вид информации (нежелательная, вредоносная, сомнительная); тип информационного объекта (сообщение, рисунок); канал распространения информации (новости, социальные сети, веб-сайты); целевая аудитория (дети, взрослые); влияние на модель распространения информации (поскольку модель распространения информации в общем подходе представляется в виде графа, влияние может заключаться в удалении связей/узлов графа, либо изменении значений метрик для узлов/связей); метрики (эффективность меры, побочный ущерб при реализации меры, стоимость меры, степень ущерба от нежелательной информации).

Данные параметры являются основой для выбора меры противодействия и позволяют сопоставить модель меры противодействия и другие модели в рамках общей методики защиты от информации (такие как модель распространения информации, модель источника нежелательной информации, модель объект воздействия информации и другие). В таблице 2 приведены примеры значений параметров мер противодействия разных классов.

ТАБЛИЦА 2. Примеры значений параметров мер противодействия разных классов

Класс информационного объекта	Канал распространения	Целевая аудитория	Класс способа защиты от информации
Большие информационные объекты: информационная система, социальная сеть, мессенджер, микроблог, форум, игровой портал, медиа-портал, веб-сайт, и т. д.	Большие информационные объекты: информационная система, социальная сеть, мессенджер, микроблог, форум, игровой портал, медиа-портал, веб-сайт, и т. д.	Взрослые Дети	препятствие (физическая защита)
Средние информационные объекты: веб-страница, группа, публичная страница, канал, статья, страница форума, и т. д.	Большие информационные объекты: веб-сайт, социальная сеть, мессенджер	Взрослые Дети	маскировка (шифрование данных)
Малые информационные объекты: пост, сообщение, комментарий, заголовок, текст статьи, медиа-объект (изображение, аудио, видео), и т. д.	Большие информационные объекты: веб-сайт, социальная сеть, мессенджер	Взрослые Дети	регламентация (определение процедур манипуляции данными)

Общий подход противодействия нежелательной, вредоносной и сомнительной информации включает определение класса информации, определение класса мер противодействия и выбор оптимальных мер.

Выбор класса мер осуществляется на основе класса информации, канала ее распространения, типа, и целевой аудитории (рис.). Разным совокупностям классов данных объектов и субъектов ставятся в соответствие разные классы контрмер (табл. 2). Затем из выбранного класса (классов) выбираются оптимальные меры с учетом метрик, включенных в модель.

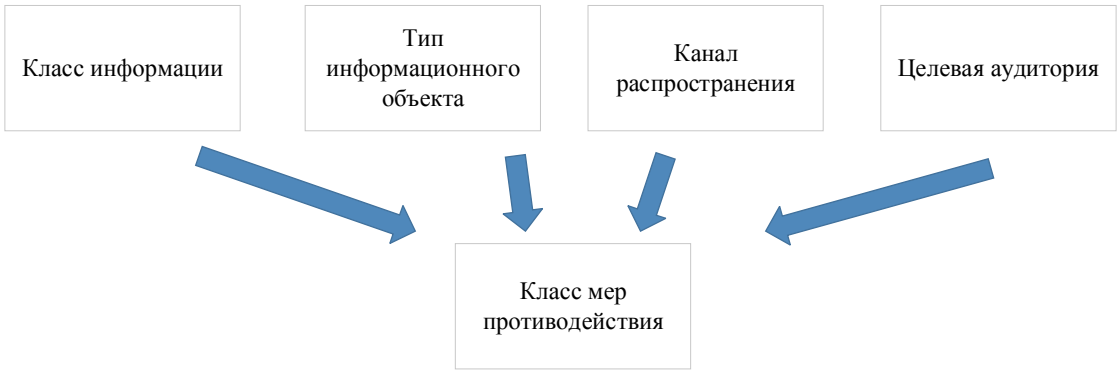


Рисунок. Концепция второго этапа подхода к противодействию

Таким образом, в статье описана модель мер противодействия и принцип ее применения в общем подходе противодействия нежелательной, вредоносной и сомнительной информации. В дальнейшей работе предполагается формализовать модель, разработать конкретные методики выбора мер противодействия в рамках предложенного подхода и провести эксперименты по оценке эффективности подхода.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-11-00302) в СПИИРАН.

Список используемых источников

1. Тумбинская М. В. Системный подход к обеспечению защиты от нежелательной информации в социальных сетях // Вопросы кибербезопасности. 2017. № 2 (20). С. 30–44.

2. Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Собрание законодательства РФ, 03.01.2011, N 1, ст. 48.

3. Котенко И. В., Саенко И. Б., Чечулин А. А. Защита от нежелательной и вредоносной информации в глобальных информационных сетях // Информационно-психологическая и когнитивная безопасность: состояние и задачи: коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. СПб. : Изд-во «Аврора», 2017. С. 207–229.

УДК 004.056
ГРНТИ 81.93.29

РАСПРЕДЕЛЕННЫЙ СБОР И ОБРАБОТКА ДАННЫХ В СИСТЕМАХ МОНИТОРИНГА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СОЦИАЛЬНЫХ СЕТЕЙ

Л. А. Виткова[1,2], И. В. Котенко[1,2], А. В. Федорченко[1,2], А. В. Хинензон[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Одним из важнейших направлений, качественно меняющих структуру информационной безопасности государства, в последние годы является вовлеченность населения в социальные сети. При этом постоянный рост объема и изменчивость данных, полученных из социальных сетей, требует новых подходов к построению архитектуры системы мониторинга и поддержки принятия решений о противодействии распространению противоправной информации. В данной работе авторами предлагается общий подход и концептуальная схема архитектуры такой системы с учетом динамики социальных сетей. Предполагается, что использование предложенной архитектуры позволит повысить эффективность защиты от нежелательной информации.

мониторинг социальных сетей, архитектура системы мониторинга, анализ социальных сетей, распределенные алгоритмы и системы.

Социальные сети – это источник данных, которые обновляются в режиме реального времени. Пользователь может взаимодействовать с сетью посредством веб-интерфейса или специального приложения. Информационная система социальных сетей не предполагает автоматического сбора и анализа данных, построения графа взаимосвязи пользователей или информационных объектов. Таким образом, в условиях большого многообразия типов данных и их гетерогенности при построении архитектуры системы мониторинга социальных сетей центральными становятся вопросы распределенного сбора и обработки информации. Целью моделирования архитектуры является повышение оперативности по защите и выявлении вредоносной информации.

Так, например, при обнаружении одного информационного объекта (поста) с нежелательным контентом возможно провести анализ всех связанных с ним объектов и выявить канал распространения, источник публикации. Таким образом, при реализации требований законодательства по информационной безопасности [1], по противодействию экстремизму [2] или по защите детей [3], можно оказывать противодействие распространению нежелательной информации в социальных сетях.

Существует ряд ограничений при реализации сбора данных из социальных сетей, перечисленных ниже.

1) Приватность страниц пользователей и групп.

Тогда, когда доступ к странице разрешён только зарегистрированным пользователям социальных сетей, требуется эмуляция пользовательской сессии с помощью специальных учётных записей (аккаунтов). Однако и на данном этапе сбора в информационной системе существуют ограничения и правила, отсекающие искусственную активность специальных учетных записей.

2) Слабая структурированность данных.

Данные, получаемые из социальных сетей требуют разработки специальных автоматизированных подходов к анализу. Так, например, получив все сведения по участникам группы, по всем постам и лайкам невозможно с точностью определить потенциал угрозы распространения информации в таком сообществе. Для анализа слабоструктурированных данных потребуется сетевой анализ [4, 5, 6].

3) *Размерность данных.*

Количество пользователей, сообщений, постов и т. д. в социальных сетях приводит к тому, что при попытке проанализировать, например, малый мир пользователя на графе, аналитик не может отделить его от сотни тысяч других вершин на графе. Размерность данных в социальных сетях обуславливает необходимость в параллельном и распределенном методе сбора данных. А также в применении метода сэмплирования.

Для обхода данных ограничений в [7] предлагается использовать методы формирования выборки пользователей для сбора информации через веб-интерфейс. Алгоритм Markov Chain Monte Carlo (MCMC) представляет собой случайное блуждание и множество запросов к информационной системе. В связи с ограничением количества таких запросов от одного источника авторы [7] предлагают улучшенный вариант. Это модифицированная схема выборки топологии (MTO-Sampling), которая, использует входные параметры ограничения от социальной сети на частоту и количество запросов и создает на лету «виртуальную» топологию, по которой и распределяются требуемые запросы.

В работе [8] предлагается масштабируемый алгоритм выборки подграфов с помощью случайного блуждания (SSRW) для подсчетов малых связных неизоморфных индуцированных подграфов большой сети (графлетов) и их концентрации. Такой подход позволяет оптимизировать процесс сбора информации об объектах социальной сети, но, как и в случае с [7], авторы рассматривают алгоритм сбора информации через веб-интерфейс, а не через API.

Отличительной чертой самой популярной в России сети «ВКонтакте» является большая доступность информации в ней. Так, например, пользователь Facebook не может получить доступ к API сети и создать свое приложение без определенных административных проверок. Facebook и Twitter стараются максимально исключить возможность сбора через специальные учётные записи. Хотя они предоставляют доступ на возмездной основе к информации из социальной сети через аккредитованные сервисы сбора.

При разработке системы мониторинга социальной сети с условно открытым API сбор информации может быть поделенным на 3 уровня:

1) уровень сбора сведений через веб-интерфейс;
2) уровень сбора через специально созданный аккаунт;
3) уровень сбора через специально созданное приложение.

Страницы в социальной сети могут быть публичными (МИД России, страница аффилированная к официальному СМИ). Доступными пользователю, зарегистрированному в сети или приложению, которому пользователь дал разрешение на сбор данных со страниц его друзей, и из закрытых групп.

Однако, для выявления каналов распространения или источников особой необходимости в доступе к закрытым группам или полностью закрытым страницам нет. Для противодействия вредоносному влиянию, нежелательной информации большую опасность представляют публичные страницы.

Рассмотрим концептуальную схему архитектуры распределенного сбора и обработки данных из социальных сетей (рис., см. ниже).

Процесс сбора и обработки происходит в несколько этапов, представленных ниже.

1. На первом уровне реализуется распределенный сбор из социальной сети путем атомарных запросов. Программное обеспечение Docer используется для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации. При этом каждый запущенный контейнер (Docker) – атомарный сервис со своим ядром ОС, ip-адресом и т. д. Такой подход позволит системе делать множественные обращения к социальной сети одновременно и собирать сведения частями.

2. На втором уровне в архитектуре используются алгоритмы парсинга топологии (АПТ) страниц для сбора информации через веб-интерфейс о графе.

3. На третьем уровне в полученной топологии определяются слепые зоны и формируется множество запросов через API от пользователя к публичным страницам или от приложения к закрытым страницам. Запросы запускаются через свободные контейнеры.

4. На четвертом уровне в архитектуре системы распределенного сбора и предобработки формируются информационные каналы в базе данных Redis, множество разрозненных запросов собираются в необходимую последовательность и передается на следующий уровень для анализа.

5. На последнем, пятом уровне происходит предварительная оценка сведений. Так, например, полученная информация может иметь признаки информационной операции. Аудитория наблюдаемого объекта может быть очень большой и активной, следовательно, потребуется срочный глубокий анализ. На уровне предобработки в системе устанавливается приоритет, формируются дополнительные задачи.

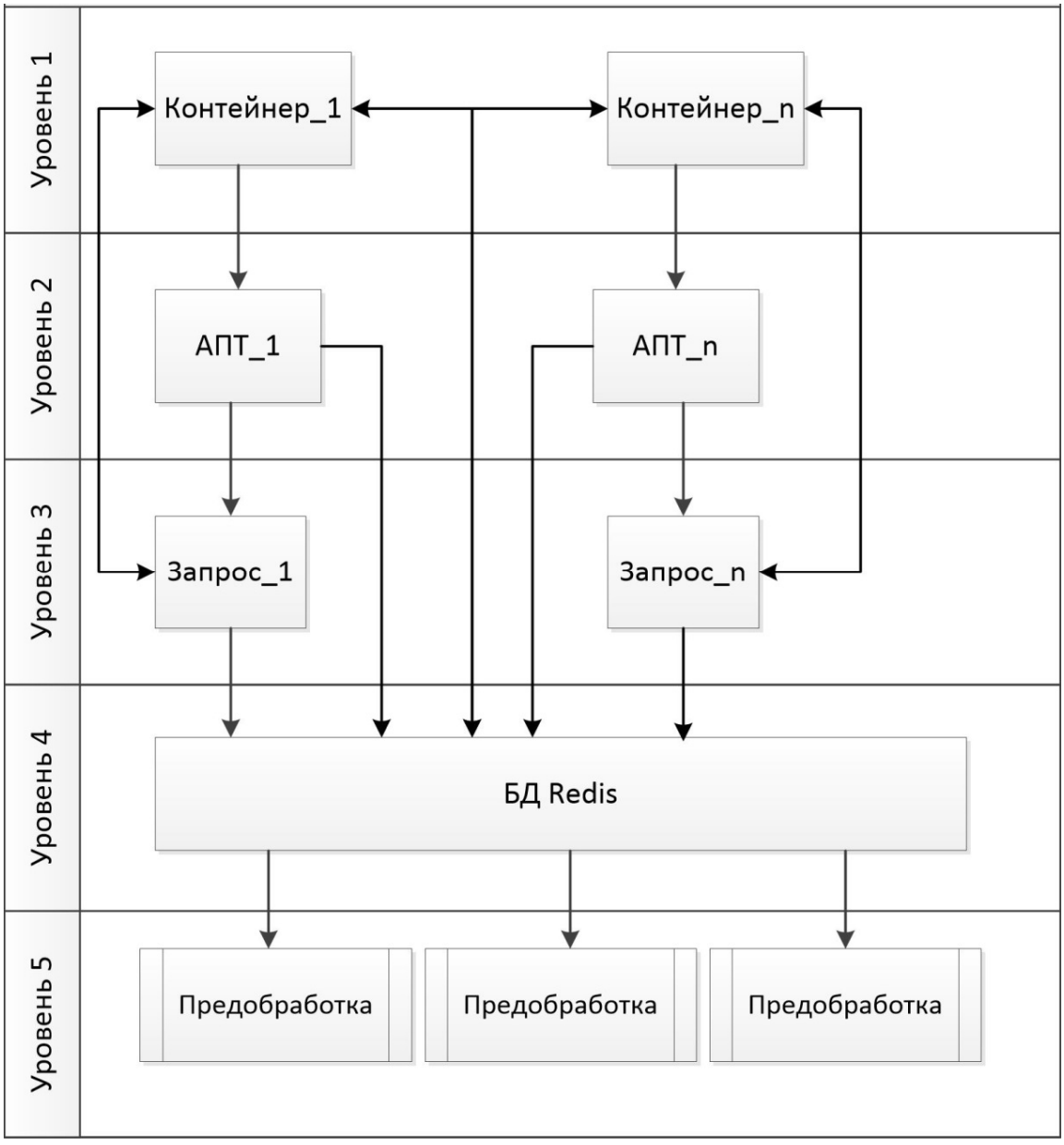


Рисунок. Концептуальная архитектура распределенного сбора и обработки данных из социальных сетей

Предполагается, что при мониторинге социальных сетей происходит выделение потенциально опасной информации. Сам процесс, в свою очередь, разбивается на компонент отслеживания информации и компонент выявления вредоносного влияния. Отслеживание информации предполагает постоянный контроль над группами риска, «пабликами» и публичными страницами. То есть под наблюдение попадают сообщества со специфическими участниками (радикальные группировки, экстремисты, несовершеннолетние и т. д.), и площадки с большой аудиторией. При этом ведется как контроль за передаваемой информацией, так и за изменением связей между участниками одного сообщества или между группами сообществ (создание сообществ сходной тематики, «резервов» на случай блокировки и т. п.). Факт выявления опасного влияния в социальной сети устанавливается при обнаружении источника атаки, целевой аудитории, каналов распространения информации и ее характера.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-71-10094) в СПИИРАН.

Список используемых источников

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, N 31 (1 ч.), ст. 3448.

2. Федеральный закон от 25 июля 2002 г. N 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства Российской Федерации, 29.07.2002, N 30 ст. 3031.

3. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 18.12.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию» // Собрание законодательства РФ, 03.01.2011, N 1, ст. 48

4. Коршунов А., Белобородов И., Бузун Н., Аванесов В., Пастухов Р., Чихрадзе К., Козлов И., Гомзин А., Андрианов И., Сысоев А., Ипатов С., Филоненко И., Чуприна К., Турдаков Д., Кузнецов С. Анализ социальных сетей: методы и приложения // Труды Института системного программирования РАН. 2014. Т. 26. №. 1. С. 439–456.

5. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Monitoring and counteraction to malicious influences in the information space of social networks // 10th International Conference on Social Informatics (SocInfo) 2018. PP. 159–167.

6. Barabási A. L. et al. Network science. Cambridge university press, 2016. 456 p. ISBN 978-1107076266.

7. Zhou Z. et al. Faster random walks by rewiring online social networks on-the-fly // ACM Transactions on Database Systems (TODS). 2016. Т. 40. №. 4. P. 26.

8. Yang C. et al. SSRW: A Scalable Algorithm for Estimating Graphlet Statistics Based on Random Walk // International Conference on Database Systems for Advanced Applications. Springer, Cham, 2018. PP. 272–288.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ ВЫЯВЛЕНИЯ И ОЦЕНКИ СТРАНИЦ ЛИДЕРОВ МНЕНИЙ В СОЦИАЛЬНЫХ СЕТЯХ

Л. А. Виткова[1,2], А. М. Кураева[1], А. А. Проноза[2], А. А. Чечулин[1,2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Целью исследования является анализ доступных способов и методик для обнаружения лидеров мнений в пространстве социальных сетей. За основу эксперимента, результаты которого описываются в работе, были взяты индикаторы вовлеченности пользователей сети «ВКонтакте», такие как «просмотр», «комментарий» и «лайк». Одновременно с этим авторы предлагают делить лидеров мнений и увлеченных ими пользователей на кластеры. Сегодня механизмы контроля за информационным пространством социальных сетей, еще не вполне соответствуют тем критериям, которые возложены на них. Предполагается, что выделение таких кластеров позволит повысить эффективность системы мониторинга и противодействия нежелательной информации.

лидеры мнений, анализ социальных сетей, распространение информации, аудитория социальных сетей.

Введение

Анализ социальных сетей позволяет исследовать взаимодействия между участниками сети, прогнозировать их поведения в социальных сетях. Формально социальную сеть можно представить графом, где существует конечное множество вершин – агентов (индивидуумов) и множество рёбер – отношений между ними. Наиболее эффективным способом влияния на целевую аудиторию (агентов) является воздействие на лидеров мнения, которые, в свою очередь, оказывают влияние на широкие массы пользователей [1, 2, 3].

Губанов Д. А. в одной из своих работ [4] выделяет несколько моделей исследования социальных сетей (распространения влияния). Например, модели с диффузией информации и информационными каскадами, в основе которых лежит некая фиксированная сеть и локальные правила взаимодействия её членов. Также две базовые модели: модель с линейным порогом (*Linear Threshold Model*) и модель независимых каскадов (*Independent Cascade Model*). Согласно данным моделям узел в сети может находится

в двух состояниях: активном и неактивном. Если в первой модели агент испытывает влияние своих соседей и становится активным в зависимости от выбранного им порога, то во второй модели агент получает единственный шанс активировать только на следующем шаге каждого из своих соседей с определённой вероятностью.

Реализация алгоритма линейных порогов подробно рассматривается в работе К. В. Козловской [5]. Стоит отметить, что так же существуют теоретико-игровые модели противоборства, которые были затронуты в совместной работе Губанова Д. А и Калашникова А. О. [6]. В том числе в книге Альберта Барабаши [7] можно найти модели исследования, например, модели просачивания и заражения, которые предполагают, что каждый агент может находится в одном из нескольких состояний. Например, быть восприимчивым к информации или являться носителем нежелательной информации и переходить из одного состояния в другое.

Эксперимент

За основу эксперимента была взята социальная сеть «ВКонтакте», исходные данные собирались из трёх групп: «Кудрово 24», «Кудрово здесь», «Жизнь в Кудрово». Были рассмотрены такие индикаторы вовлеченности отдельных пользователей всех трёх групп, как:

1) количество поставленных «лайков» к постам;
2) количество полученных «лайков» к постам;
3) количество поставленных «лайков» к комментариям;
4) количество полученных «лайков» к комментариям;
5) количество написанных «комментариев»;
6) количество постов;
7) дата последнего входа в социальную сеть.

Для начала был проведён анализ активности всех трёх групп на основе полученных и поставленных отдельным пользователем «лайков», в следствие которой аудитория была поделена на:

– пользователи, которые не заходили более 30 дней или были удалены, которые не проявили активность в группе – неактивные пользователи;

– пользователи, которые проявили активность хотя бы один раз – пассивные;

– пользователи, которые больше всего проявляют заинтересованность: активные или лидеры.

На основе собранных данных была проведена сегментация аудитории по следующим показателям: «Количество поставленных лайков» и «Количество полученных лайков». Данная сегментация наглядно показывает оценку аудитории групп.

На рис. 1 представлены данные, собранные из трёх групп по показателю «количество полученных лайков». Данный показатель позволяет выделить группу людей, у которой степень активности наиболее высокая. Также можно выделить «потенциал» участника группы на основе полученных им «лайков» на комментарии и посты в группах.

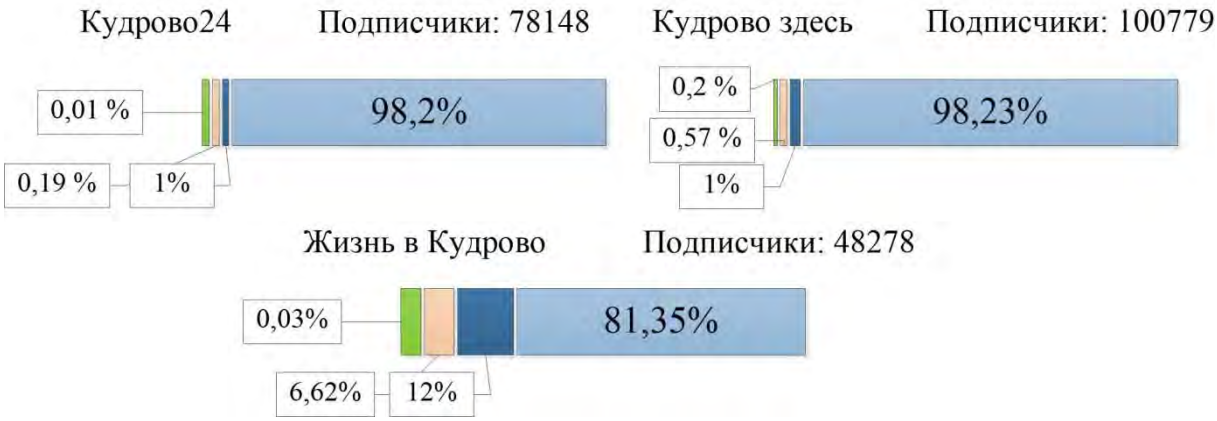


Рис. 1. Показатели активности аудиторий

Из диаграмм на рис. 1 видно процентное соотношение неактивных, пассивных и активных пользователей групп. Одновременно можно выделить наиболее влиятельных агентов в группе.

Таблица 1 показывает, что показатели активности пользователей группы «Жизнь в Кудрово», где количество подписчиков в два раза меньше двух других групп, выше. В таблице показаны «Лидеры» – пользователи, которые больше всех пишут и одновременно больше всех получают «лайков» на свои сообщения. «Активные» – те, кто пишут или ставят «лайки». «Пассивные» – не пишут, не ставят лайки». «Неактивные» – не входили в социальную сеть более месяца.

ТАБЛИЦА 1. Процентное соотношение групп и пользователей по потенциалу (%)

Статус/Группа	Кудрово 24	Кудрово здесь	**Жизнь в Кудрово**
Лидеры	0,01	0,02	**0,03**
Активные	0,19	0,57	**6,62**
Пассивные	1	1	**12**
Неактивные	98,2%	98,23	**81,35**

Для наглядности, аудитории поделены на три сегмента: неактивные, пассивные и активные. Данная сегментация выделяет именно ту группу людей, которая по всем показателям вовлеченности подходит под «лидеров мнений». На рис. 2 представлены процентные соотношения групп.

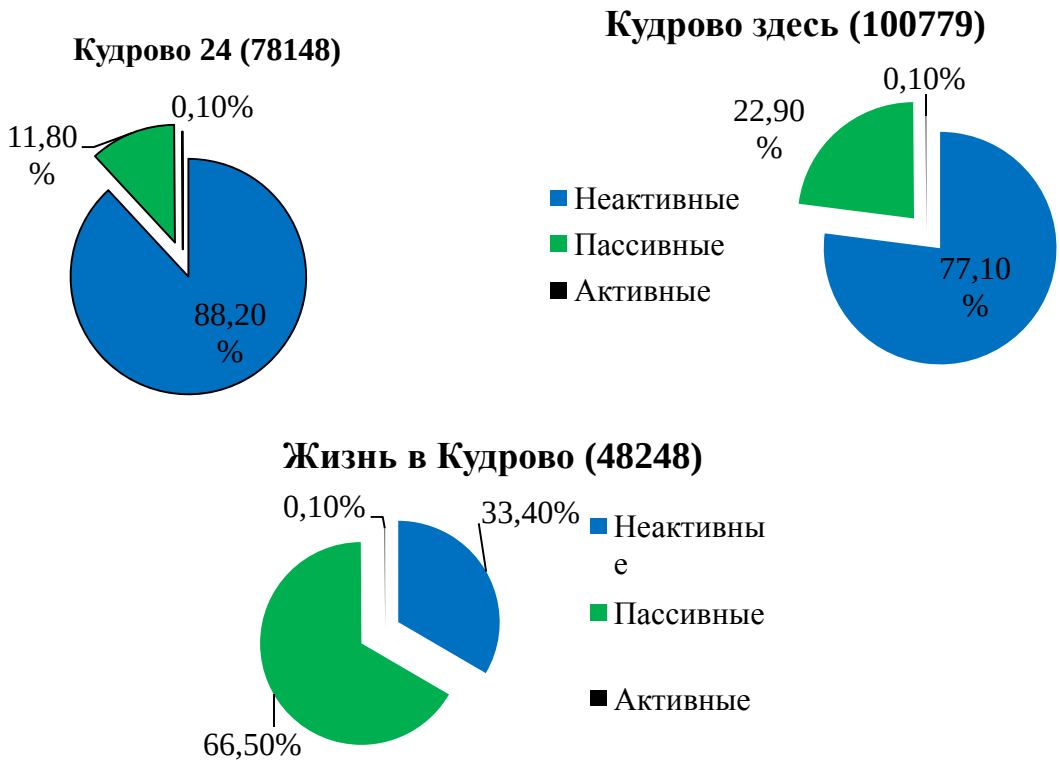


Рис. 2. Диаграммы процентных соотношений аудиторий групп

В таблице 2 представлены статистические данные из диаграмм на рис. 2.

ТАБЛИЦА 2. Процентное соотношение аудитории по трем сегментам (%)

Статус/Группа	Кудрово 24	Кудрово здесь	**Жизнь в Кудрово**
Неактивные	88,2	77,1	**33,4**
Пассивные	11,8	22,9	**66,5**
Активные	0,1	0,1	**0,1**

Таким образом, в группе «Жизнь в Кудрово» намного большее высокие показатели активности, по сравнению с «Кудрово 24» и «Кудрово здесь». Такой анализ позволяет не только выявлять каналы распространения, потенциальных агентов влияния в социальных сетях. Прежде всего, при планировании контрмер и для поддержки принятия решений о противодействии нежелательной информации такой анализ может быть базовым и эффективным.

Подводя итоги, в работе представлены методы исследования социальных сетей и выявления лидеров мнений. Данное исследование позволило количественно оценить влиятельность агентов и их групп, выявить шаб-

лоны группового поведения. Собранные данные могут в дальнейшем послужить базовым материалом для мониторинга и противодействия нежелательной информации. В дальнейшем авторы планируют провести кластерный анализ участников групп, выявить общие связи и провести сравнительный анализ с другими группами.

Работа выполнена при финансовой поддержке Гранта РНФ 18-71-10094 в СПИИРАН.

Список используемых источников

1. Левкин И. М., Науменко К. А., Виткова Л. А. Особенности информационно-психологического воздействия в интернете // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 365–367.

2. Левкин И. М., Науменко К. А. Роль информационно-психологического воздействия при реализации европейской арктической политики // Организационно-правовое регулирование безопасности жизнедеятельности в современном мире : сб. материалов II МНК / Под ред. Э. Н. Чижикова. 2018. С. 328–332.

3. Вильчинская Э. А., Виткова Л. А., Парсон И. М. Актуальные проблемы правового регулирования средств массовой информации // Право и информация: вопросы теории и практики : сб. материалов МНПК. Сер. «Электронное законодательство» ФГБУ «Президентская библиотека имени Б. Н. Ельцина». 2017. С. 102–108.

4. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д. А. Новикова. М. : Издательство физико-математической литературы, 2010. 228 с. ISBN 9785-94052-194-5.

5. Козловская К. В. Реализация алгоритма выявления наиболее влиятельных пользователей в социальных сетях [Электронный ресурс] // Научный альманах: электрон. научн. журн. 2016. N 5–3. С. 95–98. URL: http://ucom.ru/doc/na.2016.05.03.095.pdf (дата обращения 20.03.2019)

6. Губанов Д. А., Калашников А. О., Новиков Д. А. Теоретико-игровые модели информационного противоборства в социальных сетях // УБС. 2010. № 31. URL: https://cyberleninka.ru/article/n/teoretiko-igrovye-modeli-informatsionnogo-protivoborstva-v-sotsialnyh-setyah (дата обращения: 20.03.2019).

7. Barabási A. L. et al. Network science // Cambridge university press, 2016. 456 p. ISBN 978-1107076266.

УДК 621.396
ГРНТИ 49.03.03

ДЕКОДИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ГОРДОНА–МИЛЛСА–ВЕЛЧА С ИСПОЛЬЗОВАНИЕМ ДВОЙСТВЕННОГО БАЗИСА

С. С. Владимиров, О. С. Когновицкий

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

В работе представлен алгоритм определения начальных состояний регистров сдвига, формирующих составные широкополосные псевдослучайные последовательности Гордона–Миллса–Велча, с использованием двойственного базиса поля Галуа. Предложенный алгоритм позволяет определять произвольные начальные состояния регистров сдвига, что расширяет возможности применения составных широкополосных последовательностей ГМВ для решения различных задач при передаче информации по каналам связи с шумами.

последовательности Гордона–Миллса–Велча, регистр сдвига, двойственный базис, вероятность ошибки.

Псевдослучайные последовательности Гордона–Миллса–Велча (ГМВП) относятся к классу составных последовательностей, формируемых на основе М-последовательности $\{s\}$ периода N над полем GF(2^n), из которой посредством децимаций формируются две новые последовательности – $\{u\}$ с периодом N и $\{v\}$ с периодом $N_1 < N$, являющимся делителем N. Искомая ГМВП $\{t\}$ периода N будет равна линейной сумме $\{u\}$ и $\{v\}$ [1, 2].

Для формирования $\{u\}$ и $\{v\}$ удобно использовать n-элементные рекуррентные регистры сдвига с линейными обратными связями (РСЛОС). Последовательности $\{u\}$ и $\{v\}$ поступающие с выхода регистров, поэлементно складываются по модулю 2, образуя ГМВП $\{t\}$. Для построения РСЛОС используются неприводимые многочлены $h_1(x)$ и $h_2(x)$ степени n. Корни этих многочленов являются p-сопряженными ($p = 2$) элементами поля GF(2^n), образованного полиномом $g(x)$. Первообразный элемент поля будем обозначать ε. Степени корней многочленов $h_1(x)$ и $h_2(x)$ будут представлять собой циклоклассы $\{q_1, 2q_1, 4q_1, ..., 2^{n-1}q_1\}$ и $\{q_2, 2q_2, 4q_2, ..., 2^{n-1}q_2\}$ соответственно, где q_1 и q_2 — индексы децимаций, выбранных для построения ГМВП. Результирующая ГМВП будет являться рекуррентной последовательностью $\{t\}$ периода $N = 2^n-1$ с характеристическим многочленом $h(x) = h_1(x)h_2(x)$ степени $2n$ [1, 2, 3].

Рассмотрим процедуру формирования ГМВП и ее последующего декодирования на примере ГМВП периода $N = 63$, вычисляемой из M-последовательности $\{s\}$ над полем $GF(2^6)$ с образующим полиномом $g(x) = 1 + x + x^6$. Зададим индексы децимации $q_1 = 5$ и $q_2 = 3$ для вычисления последовательности $\{u\}$ с периодом $N_1 = 63$ и последовательности $\{v\}$ с периодом $N_2 = 21$ соответственно. Исходя из выбранных индексов децимации, вычислим значения неприводимых полиномов $h_1(x)$ и $h_2(x)$ через значения их корней, младшие степени которых равны, соответственно, $\mu = \varepsilon^5$ для $h_1(x)$ и $\gamma = \varepsilon^3$ для $h_2(x)$:

$$h_1(x) = 1 + x + x^2 + x^5 + x^6; \quad h_2(x) = 1 + x + x^2 + x^4 + x^6. \qquad (1)$$

Далее согласно полученным полиномам (1) необходимо построить два регистра сдвига из $n = 6$ ячеек каждый. Исходно в ячейки регистров записываются начальные фазы $C(\mu)$ и $D(\gamma)$ последовательностей $\{u\}$ и $\{v\}$, записываемые в общем виде как элементы полей, образованных полиномами $h_1(x)$ и $h_2(x)$:

$$C(\mu) = a_0 + a_1\mu + a_2\mu^2 + a_3\mu^3 + a_4\mu^4 + a_5\mu^5 \equiv (a_0\, a_1\, a_2\, a_3\, a_4\, a_5);$$

$$D(\gamma) = b_0 + b_1\gamma + b_2\gamma^2 + b_3\gamma^3 + b_4\gamma^4 + b_5\gamma^5 \equiv (b_0\, b_1\, b_2\, b_3\, b_4\, b_5).$$

Фактически начальные фазы $C(\mu)$ и $D(\gamma)$ являются полезной информацией, которая будет содержаться в кодовом слове ГМВП.

Далее в течение $2^n - 1 = 63$ тактов на выходе регистров формируются последовательности $\{u\}$ и $\{v\}$ как значения функции-след:

$$\{u\} = (u_0, u_1, u_2, ..., u_{62}) = (T[C(\mu)], T[\mu C(\mu)], T[\mu^2 C(\mu)], ..., T[\mu^{62} C(\mu)]); \qquad (2)$$

$$\{v\} = (v_0, v_1, v_2, ..., v_{62}) = (T[D(\gamma)], T[\gamma D(\gamma)], T[\gamma^2 D(\gamma)], ..., T[\gamma^{62} D(\gamma)]), \qquad (3)$$

где функция-след для произвольного элемента поля $\mu^i = (a_0\, a_1\, a_2\, a_3\, a_4\, a_5)$ равна $T[\mu^i] = a_1+a_2+a_3+a_4+a_5$, а функция-след для элемента $\gamma^j = (b_0\, b_1\, b_2\, b_3\, b_4\, b_5)$ равна $T[\gamma^j] = b_5$.

При этом период последовательности $\{v\}$ равен 21, т. е. она состоит из трех одинаковых последовательностей $(v_0\, v_1\, v_2\, ...\, v_{20})$. То есть $v_0 = v_{21} = v_{42}$, $v_1 = v_{22} = v_{43}$, ..., $v_{20} = v_{41} = v_{62}$.

Исходя из вида многочленов (1) и формул (2) и (3), построим схемы РСЛОС, для формирования последовательностей $\{u\}$ и $\{v\}$, которые вместе образуют схему формирования искомой последовательности ГМВ $\{t\}$, представленную на рис. 1.

В результате работы генератора (рис. 1) будет получена ГМВП {t}, которая затем передается в канал связи.

$$\{t\} = (t_0, t_1, t_2, ..., t_{62}) = (u_0 + v_0, u_1 + v_1, u_2 + v_2, ..., u_{62} + v_{62}) \qquad (4)$$

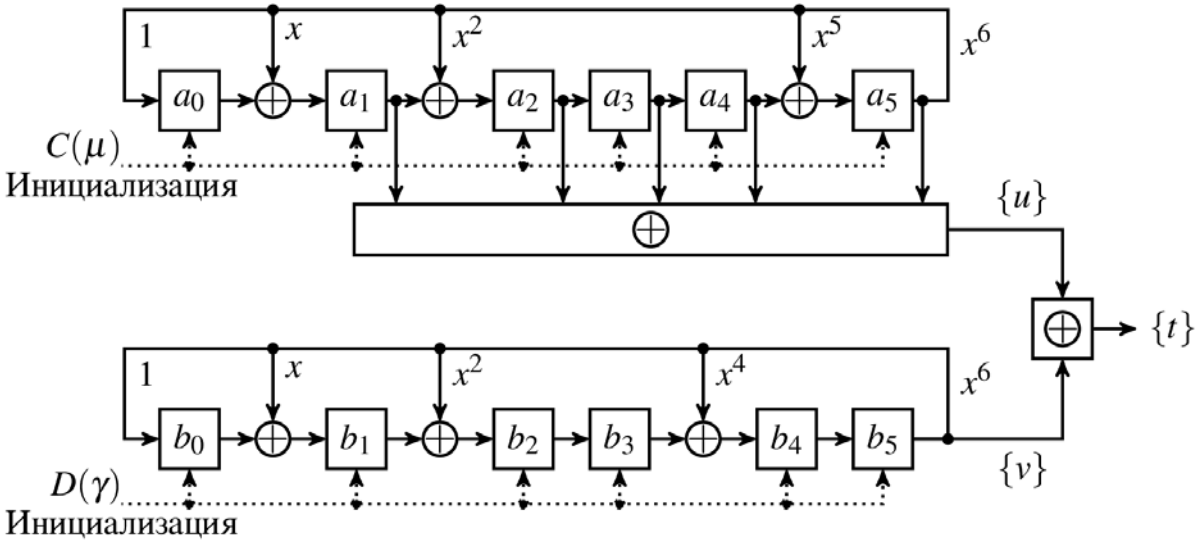


Рис. 1. Генератор последовательности $\{t\}$ как линейной суммы $\{u\}$ и $\{v\}$ по mod 2

На приемной стороне необходимо, в предположении синхронной системы передачи, определить начальные фазы (информационные элементы) $C(\mu)$ и $D(\gamma)$, т. е. произвести процедуру декодирования ГМВП.

Для этого используем коэффициенты двойственного базиса [α] и [β] для последовательностей $\{u\}$ и $\{v\}$ соответственно [4]. Матрицы коэффициентов базисов [α] и [β] для выбранных многочленов $h_1(x)$ и $h_2(x)$ показаны в формуле (5).

$$[\alpha]=\begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\\ \alpha_5\\ \alpha_6\\ \alpha_7\\ \alpha_8\\ \alpha_9\\ \alpha_{10}\\ \alpha_{11}\\ \alpha_{12}\end{bmatrix}=\begin{bmatrix}1&1&1&0&1&1\\ 1&1&0&1&1&0\\ 1&0&1&0&0&1\\ 1&1&1&0&0&0\\ 1&1&0&1&1&1\\ 1&1&0&0&1&0\\ 1&1&0&0&0&1\\ 0&0&1&0&1&1\\ 1&0&0&1&1&0\\ 0&0&0&1&1&0\\ 1&1&1&0&0&1\\ 1&0&1&1&0&0\end{bmatrix};\quad [\beta]=\begin{bmatrix}\beta_1\\ \beta_2\\ \beta_3\\ \beta_4\\ \beta_5\\ \beta_6\\ \beta_7\\ \beta_8\\ \beta_9\\ \beta_{10}\\ \beta_{11}\\ \beta_{12}\end{bmatrix}=\begin{bmatrix}1&1&0&0&1&0\\ 0&1&0&1&0&0\\ 1&1&0&0&0&1\\ 0&0&1&1&0&0\\ 0&0&0&0&0&1\\ 0&0&1&0&0&0\\ 1&0&0&0&0&1\\ 0&1&1&1&0&1\\ 1&0&1&0&1&0\\ 1&0&0&1&0&0\\ 1&1&0&1&0&1\\ 0&1&1&1&1&0\end{bmatrix}. \quad (5)$$

Используя двойственные базисы (5), по любому участку $\{t_j\} = (t_j, t_{j+1}, t_{j+2}, t_{j+3}, t_{j+4}, t_{j+5}, t_{j+6}, t_{j+7}, t_{j+8}, t_{j+9}, t_{j+10}, t_{j+11})$, $j = 1, 2, ..., 63$, состоящему из $2k = 12$

последовательных элементов замкнутой в кольцо ГМВП $\{t\}$, можно по формулам (6) определить начальные фазы $C(\mu)$ и $D(\gamma)$.

$$C(\mu) = \mu^{-j} \sum_{k=0}^{11} t_{j+k} \alpha_{k+1}, \bmod h_1(\mu); \quad D(\gamma) = \gamma^{-j} \sum_{k=0}^{11} t_{j+k} \beta_{k+1}, \bmod h_2(\gamma). \quad (6)$$

В случае, когда принятая последовательность $\{t\}$ содержит ошибки, вычисления по участкам $\{t_j\}$, содержащим ошибочные разряды, в результате дадут значения $C_j(\mu)$ и $D_j(\gamma)$, отличающиеся от искомых $C(\mu)$ и $D(\gamma)$. Для того, чтобы осуществить исправление ошибок, необходимо использовать мажоритарный принцип декодирования. Для этого необходимо перебрать все $N = 63$ 12-элементных участка $\{t_j\}$, вычислить для них по формулам (6) значения $C_j(\mu)$ и $D_j(\gamma)$ и по мажоритарному принципу выбрать значения начальных фаз $C(\mu)$ и $D(\gamma)$.

В зависимости от количества и расположения ошибочных разрядов, в результате декодирования может получиться три возможных исхода: правильное декодирование (результат декодирования совпадает с начальными фазами), неправильное декодирование (несовпадение хотя бы одной начальной фазы) и отказ от декодирования (невозможность однозначно выделить хотя бы одну из начальных фаз).

Для оценки вероятностных характеристик метода декодирования с использованием двойственного базиса при синхронной передаче данных было проведено моделирование по методу Монте-Карло в системе математических вычислений GNU/Octave. При моделировании использовались модель двоично-симметричного канала (ДСК) и модель канала АБГШ совместно с двоичной фазовой манипуляцией. Схема модели системы передачи приведена на рис. 2.

Рис. 2. Блок-схема модели системы передачи для определения вероятностных характеристик синхронного декодирования ГМВП по методу двойственного базиса

При моделировании передавалось по 50000 ГМВП для каждого значения битовой ошибки в канале ДСК и каждого значения нормированного отношения сигнал/шум в канале АБГШ. В результате были получены оценочные значения вероятностей правильного декодирования $P_{ПД}$, неправильного

декодирования $P_{НД}$ и отказа в декодировании $P_{ОД}$, графики которых приведены на рис. 3.

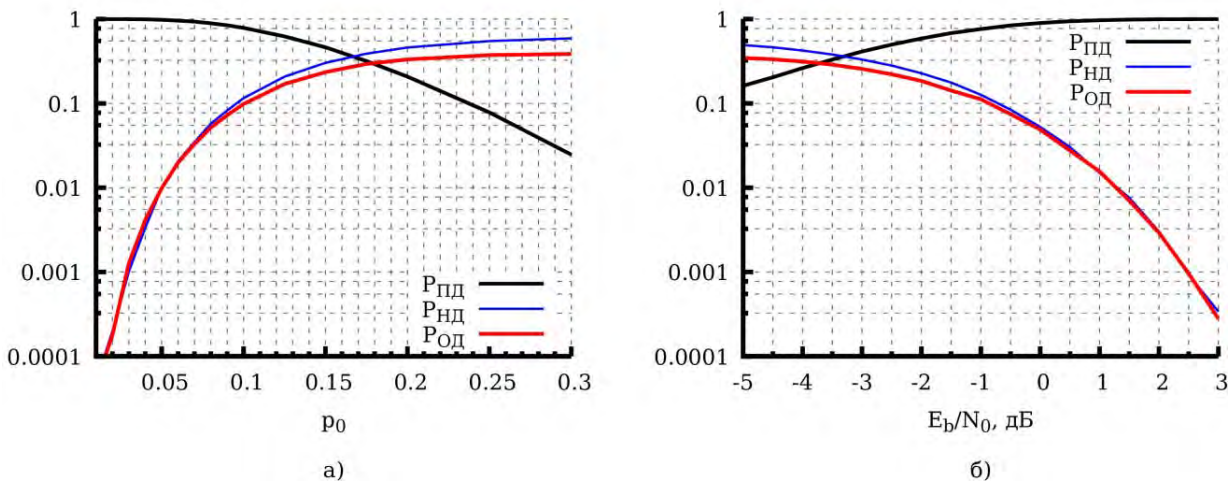


Рис. 3. Вероятностные характеристики декодера ГМВП на основе двойственного базиса при синхронном декодировании: а) для канала ДСК; б) для канала АБГШ с манипуляцией ФМ-2

Результаты моделирования показали, что предложенный метод декодирования обеспечивает вероятность правильного определения начальных фаз ГМВП более 0,99 при вероятности ошибки в канале ДСК не более 0,05 и нормированном отношении сигнал/шум в канале АБГШ не менее 1,5 дБ. При отношении сигнал/шум, равном 0 Дб, вероятность правильного определения начальных фаз приблизительно равна 0,9, что позволяет использовать рассмотренный метод в зашумленных каналах.

Список используемых источников

1. Стародубцев В. Г. Алгоритм формирования последовательностей Гордона–Миллса–Велча // Изв. вузов. Приборостроение. 2012. Т. 55, № 7. С. 5–9.

2. Стародубцев В. Г. Формирование последовательностей Гордона–Миллса–Велча на основе регистров сдвига // Изв. вузов. Приборостроение. 2015. Т. 53, № 6. С. 451–457.

3. Диксон Р. К. Широкополосные системы, пер. с англ. Под ред. В. И. Журавлева. М. : Связь, 1979. 304 с.

4. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях. СПб. : Линк, 2009. 424 с. ISBN 978-5-98595-020-5.

УДК 004.94
ГРНТИ 49.03.03

РАЗРАБОТКА АППАРАТНОЙ МОДЕЛИ РАДИОКАНАЛА С ПОМЕХАМИ ДЛЯ ИССЛЕДОВАНИЯ ПОМЕХОУСТОЙЧИВЫХ КОДОВ

С. С. Владимиров, В. В. Малашерифов

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

Статья рассматривает реализацию аппаратной модели радиоканала с помехами для исследования помехоустойчивых кодов в рамках разрабатываемой на кафедре сетей связи и передачи данных СПбГУТ системы имитационного численного моделирования процессов ПД DTSMS. Приведены требования к разрабатываемой модели радиоканала, выбрана аппаратная конфигурация приемопередатчика и управляющих модулей и проработан интерфейс взаимодействия с ядром системы DTSMS.

имитационное моделирование, система моделирования DTSMS, радиоканал, радиочастотный приемопередатчик, помехоустойчивое кодирование.

Помехоустойчивое кодирование является важной составной частью современных систем передачи информации, позволяя передавать данные в условиях внешних помех и взаимного влияния каналов. Выбор методов помехоустойчивого кодирования при разработке аппаратного и программного обеспечения систем передачи данных (СПД) требует проведения предварительного численного моделирования, которое позволяет оценить, насколько тот или иной метод кодирования удовлетворяет требованиям технического задания на разработку системы передачи. Для решения этой задачи существуют разнообразные системы моделирования, как например системы компьютерной алгебры Matlab, Scilab и GNU/Octave, включающие в свой состав модели многих элементов типичной СПД – модуляторов и демодуляторов, основных кодеров/декодеров ряда широко используемых помехоустойчивых кодов, моделей цифровых и аналоговых каналов передачи данных [1]. Широко используются библиотеки функций и моделей, такие как IT++ в C++ или SciPy в Python, позволяющие создавать собственные быстродействующие модели на соответствующих языках программирования. На кафедре Сетей связи и передачи данных разрабатывается собственная система имитационного численного моделирования систем передачи данных Data Transmission System Modeling Software (DTSMS), обеспечивающая параллельную работу моделей, имитирующих взаимодействие отдельных элементов СПД в трактах приема-передачи [2, 3].

Поскольку помехоустойчивое кодирование наиболее важно в системах радиосвязи, принято решение разработать для системы DTSMS аппаратную модель радиоканала с помехами, которая позволит проводить оценку методов помехоустойчивого кодирования в условиях реального радиоканала. Данную модель предполагается применять на кафедре Сетей связи и передачи данных для обучения в рамках профильных дисциплин, посвященных помехоустойчивому кодированию и передаче данных с использованием радиотехнологий и радиосетей.

Для обеспечения необходимого функционала к разрабатываемой модели были предъявлены следующие требования: максимальная гибкость с точки зрения используемых методов кодирования и модуляции при минимальной стоимости аппаратной базы; возможность работы в различных диапазонах частот; наличие или возможность создания удобного интерфейса взаимодействия аппаратной части модели и программных модулей системы DTSMS в рамках стандартных стыков.

В качестве аппаратной части модели радиоканала были выбраны приемопередатчики SI4432 и SI4463 компании Silicon Labs. Технические характеристики этих устройств приведены в таблице.

ТАБЛИЦА. Технические характеристики приемопередатчиков SI4432 и SI4463

Параметр	SI4432	SI4463
Рабочие частоты, МГц	240–930	433,4–473
Модуляция	(G)FSK, OOK	(G)FSK, OOK, (G)MSK
Чувствительность, дБм	до −121	до −126
Максимальный уровень выходного сигнала, дБм	20	20
Дальность передачи, км	≈1	≈1
Управление	SPI, GPIO	UART/TTL (AT команды)
Стоимость, руб.	≈150	≈300

Выбор этих приемопередатчиков обусловлен сочетанием их низкой стоимости с широкими возможностями. Они поддерживают различные методы модуляции и позволяют работать в достаточно широком диапазоне частот.

Для управления приемопередатчиками и сопряжения их с персональными ЭВМ используется модуль ESP8266/ESP32 компании Espressif Sysmems на основе 32-разрядного микроконтроллера с тактовой частотой 240 МГц, поддерживающий аппаратные интерфейсы, необходимые для работы с выбранными приемопередатчиками. Взаимодействие с ЭВМ предполагается через стандартные стыки интерфейсов UART и USB. Управление

модулем ESP8266/ESP32 производится по беспроводной сети Wi-Fi в частотном диапазоне 2,4 ГГц с использованием веб-интерфейса.

Работа системы имитационного моделирования DTSMS и модели радиоканала в качестве мобильного источника преднамеренной помехи обеспечивается применением микрокомпьютера RaspberryPi, который содержит необходимые аппаратные интерфейсы управления приемопередатчиками и способен запускать систему моделирования DTSMS.

Схема лабораторной установки аппаратной модели радиоканала для исследования помехоустойчивых кодов в системе DTSMS приведена на рис.

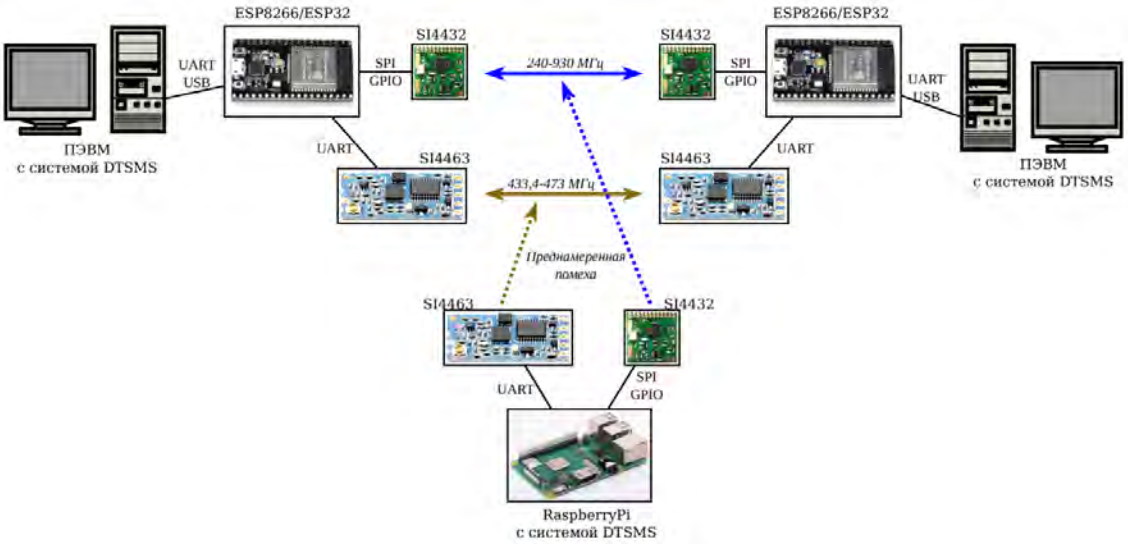


Рисунок. Схема лабораторной установки аппаратной модели радиоканала для исследования помехоустойчивых кодов в системе DTSMS

Использование приемопередатчиков под управлением микрокомпьютера RaspberryPi в качестве источника преднамеренной помехи позволяет быстро изменять положение источника помехи для удобного проведения измерений и экспериментов.

Кроме использования в качестве модели для исследования помехоустойчивых кодов, данная лабораторная установка может быть использована в целях оценки методов защиты данных в радиоканалах от перехвата их третьими лицами. В этом случае мобильный блок лабораторной установки под управлением RaspberryPi будет играть роль злоумышленника/криптоаналитика.

Список используемых источников

1. Prabhu P., Jablin T.B., Raman A., Zhang Y. и др. A survey of the practice of computational science // Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis. August 2011. DOI: https://doi.org/10.1145/2063348.2063374.

2. Владимиров С. С., Самайданов А. А. Исследование методов построения модульной системы имитационного моделирования систем передачи данных с помехоустойчивым кодированием // Информационные технологии и телекоммуникации. 2016. Т. 4. № 1. С. 9–16.

3. Владимиров С. С., Когновицкий О. С. Модульный комплекс параллельного имитационного моделирования для исследования систем передачи данных с помехоустойчивым кодированием // Электросвязь. 2017. № 11. С. 48–53.

УДК 621.396
ГРНТИ 49.03.03

МЕТОД ДЕКОДИРОВАНИЯ ЦИКЛИЧЕСКИХ КОДОВ МАКСИМАЛЬНОЙ ДЛИНЫ НА ОСНОВЕ ОБРАТНОЙ МАТРИЦЫ С ИСПОЛЬЗОВАНИЕМ МЯГКИХ РЕШЕНИЙ

С. С. Владимиров, Д. Ф. Мухаметшина

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

В статье представлен метод декодирования кодов максимальной длины на основе метода декодирования по k-элементным линейно-независимым комбинациям с использованием мягких решений на основе весовых шаблонов. Проведен анализ декодирования ошибок различных кратностей. Получена таблица весовых шаблонов для кода максимальной длины (7, 3). Приведен сценарий использования предлагаемого метода декодирования.

код максимальной длины, мягкое декодирование, М-последовательность, декодирование по линейно-независимым комбинациям.

Циклические коды максимальной длины (КМД) представляют собой блочные эквидистантные (n, k)-коды, кодовые кодовые слова $\{w\}$ которых рассчитываются как рекуррентные псевдослучайные последовательности максимальной длины над полем Галуа GF(2^k), через функцию-след $T(x)$ по формуле [1, 2, 3]:

$$\{w\} = \{w_0; w_1; \ldots; w_{2^k-2}\} = \left[T(c);\ T(c\varepsilon);\ \ldots;\ T(c\varepsilon^{2^k-2})\right],$$

где c – элемент поля Галуа GF(2^k), который является начальной фазой последовательности максимальной длины, соответствующей кодовому слову КМД; ε^i – элементы поля Галуа GF(2^k), i = 0, 1, ..., 2^k–2. Для несистематического КМД начальная фаза c является информационной частью кодового

слова $\{w\}$, а в случае систематического кода она позволяет однозначно определить информационные элементы этого кодового слова [1, 3].

Для декодирования КМД можно использовать различные алгоритмы декодирования, которые условно разделяются на две группы: методы жесткого декодирования, в которых каждый символ принятого декодером кодового слова равен 1 либо 0, и методы мягкого декодирования, когда каждому разряду принятого из канала передачи данных кодового слова присваивается вероятностный критерий неопределенности символа, так называемая верность или вероятность приема [4]. Вероятность приема определяется демодулятором согласно параметрам модуляции входного сигнала, таким как амплитуда, частота, фаза или форма импульса. Далее полученные вероятностные значения передаются в декодер, который использует их при декодировании.

Представленный в статье метод декодирования позволяет оценивать вероятности приема символов кодового слова на уровне декодера. Для этого используется метод декодирования КМД по k-элементным линейно-независимым комбинациям $\{s_i\}$ элементов кодового слова $\{w\}$ [1, 3]. Согласно этому методу начальная фаза c кодового слова $\{w\}$ рассчитывается по формуле [1, 3]:

$$C = \Theta^{-1} S = \begin{bmatrix} \left(F^{i1}\theta_0\right)^T \\ \left(F^{i2}\theta_0\right)^T \\ \vdots \\ \left(F^{ik}\theta_0\right)^T \end{bmatrix}^{-1} \cdot S, \qquad (1)$$

где $C = [c_0, c_1, ..., c_{k-1}]^T$ – вектор коэффициентов начальной фазы c; $S = [s_{i1}, s_{i2}, ..., s_{ik}]^T$ – вектор-столбец из k элементов линейно-независимой комбинации $\{s_i\}$; Θ^{-1} – обратная квадратная матрица размера $k \times k$; F_{ij} – сопровождающая матрица $k \times k$ элемента поля ε_{ij}, соответствующего элементу s_{ij} линейно-независимой комбинации $\{s_i\}$; θ_0 – первый столбец матрицы $\theta = E + X_2 + X_4 + \ldots + X_{2^{k-1}}$, равной сумме единичной матрицы E и матриц возведения в степень 2^z, где $z = 1..k-1$ [1, 3].

Для определения начальной фазы c по мажоритарному принципу декодирования выполняется перебор всех возможных для выбранного КМД k-элементных линейно-независимых комбинаций $\{s_i\}$ и вычисление для каждой из них начальной фазы c по формуле (2). После перебора всех k-элементных комбинаций получится набор начальных фаз c_i, каждой из которых будет соответствовать некоторое количество k-элементных комбинаций – вес начальной фазы. Правильной начальной фазой будет считаться фаза c_i, имеющая наибольший вес [1, 3].

При декодировании принятого на вход декодера кодового слова данным методом возможны 3 исхода: правильное декодирование (получена начальная фаза, соответствующая исходному кодовому слову); неправильное декодирование (получена неверная начальная фаза); отказ от декодирования или обнаруженная неисправляемая ошибка (однозначно выделить начальную фазу по мажоритарному принципу невозможно – получено 2 возможных значения начальной фазы с одинаковым весом) [1, 3].

Для КМД (7, 3) существует 28 *k*-элементных линейно-независимых комбинаций. Исправляющая способность метода декодирования по *k*-элементным линейно-независимым комбинациям для кода (7, 3) вплоть до 3-кратных ошибок приведена в таблице 1.

ТАБЛИЦА 1. Исправляющая способность метода декодирования кода максимальной длины (7,3) по *k*-элементным линейно-независимым комбинациям

Кратность ошибки	Кол-во ошибок	Правильное декодирование		Неправильное декодирование		Отказ от декодирования	
		Кол-во	Доля	Кол-во	Доля	Кол-во	Доля
1	7	7	1,0	0	0	0	0
2	21	0	0	0	0	21	1,0
3	35	0	0	28	0,8	7	0,2

Из таблицы видно, что данный алгоритм позволяет правильно декодировать ошибки первой кратности. Все ошибки кратности 2 приводят к отказу от декодирования, а ошибки больших кратностей или неверно исправляются, или приводят к отказу от декодирования.

Рассмотрим принцип оценки вероятности символа принятого кодового слова на примере КМД (7, 3), построенного над полем Галуа $GF(2^3)$ с образующим полиномом $p(x) = x^3 + x + 1$. В каждом кодовом слове этого кода содержится 28 линейно-независимых 3-элементных комбинаций, по каждой из которых вычисляется начальная фаза *c*. Эти комбинации распределены равномерно и каждому из 7 символов кодового слова соответствует 12 линейно-независимых комбинаций из 28. Анализ результатов, полученных по каждой из этих комбинаций, позволяет присвоить вероятность правильного приема каждому символу.

Проанализируем результаты декодирования кодового слова с начальной фазой $c = 1_{10} = 001_2 = \varepsilon$.

Рассмотрим ситуацию с декодированием 2-кратной ошибки {0110000}, которая приводит к отказу от декодирования. Результаты декодирования сведены в таблицу 2, а соответствующие шаблоны вынесены в сводные таблицы 3 и 4. Оранжевым отмечены разряды, содержащие ошибку.

ТАБЛИЦА 2. Анализ обработки 2-кратной ошибки {0110000}, приводящей к отказу от декодирования

Общий результат декодирования									
c	0	1	2	3	4	5	6	7	Σ
Вес	24	24	3	3	3	3	0	24	84
Результат по каждому разряду кодового слова в отдельности									
Разряд	Веса по *k*-элементным комбинациям для каждого из разрядов кодового слова								
1	0	5	1	0	1	0	0	5	12
2	5	0	0	1	1	0	0	5	12
3	5	0	1	0	0	1	0	5	12
4	5	5	0	0	1	1	0	0	12
5	0	5	0	1	0	1	0	5	12
6	5	5	1	1	0	0	0	0	12
7	4	4	0	0	0	0	0	4	12

Как видно из таблицы 2, в распределении весов, соответствующих отдельным разрядам кодового слова, можно выделить несколько характерных шаблонов, которые отличаются расположением значений весов. Вынесем эти шаблоны в сводную таблицу 3 и отсортируем веса по убыванию.

ТАБЛИЦА 3. Шаблоны весов, выделяемые при обработке 2-кратной ошибки {0110000}, приводящей к отказу от декодирования

Разряды	Шаблон	Шаблон в сокращенном виде
1,2,3,4,5,6	5,5,1,1,0,0,0,0	2×5,2×1
7	4,4,4,0,0,0,0,0	3×4

Анализ показал, что шаблоны весов разных разрядов кодовой комбинации для каждой из ошибок в первую очередь отличаются количеством повторений максимального и второго по величине весов. Поэтому шаблоны весов, соответствующие отдельным разрядам кодового слова можно представить так, как показано в таблице 4.

ТАБЛИЦА 4. Шаблоны весов, выделяемые при обработке 2-кратной ошибки {0110000}, в сокращённом виде

Разряд	1	2	3	4	5	6	7
Шаблон весов	2/2	2/2	2/2	2/2	2/2	2/2	3

Анализ статистических данных показал, что в шаблонах весов, содержащих единственную 3, эта 3 указывает на гарантированно безошибочный разряд.

Для кода (7, 3) авторами был проведен полный перебор всех возможных комбинаций ошибок и определен полный набор возможных весовых шаблонов с указанием соответствия значений шаблона ошибочным и безошибочным битам. Для примера в таблице 5 приведены полученные весовые шаблоны для ошибок вплоть до кратности 3. Для удобства шаблоны в таблице отсортированы по убыванию количества повторений максимального веса. Буквами ПД, НД и ОД отмечены весовые шаблоны, соответствующие правильному декодированию кодового слова, неправильному декодированию и отказу от декодирования.

ТАБЛИЦА 5. Весовые шаблоны для КМД (7, 3)
для ошибок до кратности 3 включительно

Кратн. ошибки	Результат	Весовой шаблон	Вес	Кол-во	Доля	
					ош.	б/ош.
1	ПД	4,1/2,1/2,1/2,1/2,1/2,1/2	1/2	42	0,00	1,00
			4	7	1,00	0,00
2	ОД	3,2/2,2/2,2/2,2/2,2/2,2/2	2/2	126	0,33	0,67
			3	21	0,00	1,00
3	ОД	4,4,4,4,4,4,4	4	49	0,43	0,57
		4,1/2,1/2,1/2,1/2,1/2,1/2	4	4	0,00	1,00
			1/2	24	0,50	0,50
	НД	4,1/2,1/2,1/2,1/2,1/2,1/2	1/2	144	0,50	0,50
			4	24	0,00	1,00

Из-за малой избыточности кода (7,3) невозможно исправлять ошибки кратности больше 2. Однако, для получения лучших результатов, можно использовать мягкое декодирование совместно с демодулятором. При этом вероятности ошибки разряда, полученные от демодулятора, складываются с вероятностями (долями) ошибки, согласно полученному весовому шаблону. Затем производится исправление разрядов кодового слова, наиболее вероятно пораженных ошибкой. Учитывая, что одинаковые шаблоны при разных кратностях ошибки могут соответствовать как ошибочным, так и безошибочным разрядам, приоритет отдается той кратности ошибки, которая наиболее вероятна для известного качества канала.

Список использованных источников

1. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях. СПб. : Линк, 2009. 424 с. ISBN 978-5-98595-020-5
2. Кларк Д. К., Кейн Д. Б. Кодирование и исправление ошибок в системах цифровой связи. Статистическая теория связи. М. : Радио и Связь, 1987. 392 с.
3. Владимиров С. С. Моделирование процессов мажоритарного декодирования комбинации эквидистантного кода по К линейно-независимым элементам // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2010. Т. 3. № 101. С. 149–156.
4. Proakis J. Digital Communications. McGraw-Hill, 2001. 1002 p. ISBN 978-0070509375.

УДК 621.391.64
ГРНТИ 49.29.14

ОБ ОЦЕНКЕ ДИСПЕРСИОННОЙ ДЛИНЫ РЕГЕНЕРАЦИОННОЙ СЕКЦИИ В СИСТЕМАХ SDH

И. В. Власова, Б. К. Никитин, А. Н. Сергеев

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

При проектировании ВОЛС в современной нормативно-технической литературе существует несколько подходов оценки дисперсионных длин элементарных кабельных участков. Каждый из них определяет максимальную протяженность ВОЛС и накладывает ограничения на скорость передачи оптической информации. В связи с увеличением скорости и стремлением увеличить протяженность кабельной линии, возникают новые влияющие факторы, которые нельзя не учитывать в инженерных расчетах проектируемой или реконструируемой линии связи. Кроме того, при выполнении расчётов нужно учитывать, как тип источника оптического излучения, так и его спектральные характеристики, которые даже в случае их доступности приводятся в виде, требующем некоторого пересчёта.

дисперсия, компенсация дисперсии, групповое время задержки, совместимость оборудования, параметры ЛЧМ, накопленная дисперсия, общая дисперсия, длина ВОЛС, максимально допустимая дисперсия.

Оценка дисперсионной длины регенерационной секции в системах SDH

Длина регенерационного участка (или элементарного кабельного участка) зависит от типа выбранного волокна и технических характеристик приемопередающей аппаратуры для необходимого стыкового кода.

Эту длину можно рассчитать по затуханию и дисперсии. При проектировании ВОЛС в современной нормативно-технической литературе существует несколько подходов оценки длин ЭКУ. В более ранних документах расчет длины ЭКУ по дисперсии приводится, но в крайне неудобном для расчётов виде. Например, если расчёты для уровней STM-1 и STM-4 ещё можно выполнить с большой степенью достоверности [1], то расчёт для уровня *STM*-16 может дать в некоторых случаях неверный результат. Кроме того, при выполнении расчётов нужно учитывать, как тип источника оптического излучения, так и его спектральные характеристики, которые даже в случае их доступности приводятся в виде, требующем некоторого пересчёта.

В рекомендациях МСЭ с целью облегчения проектирования и технической эксплуатации приводятся нормы для оценки соответствия отдельных частей проектируемой ВОЛП требованиям, предъявляемым приёмопередающему оборудованию и волоконно-оптическому тракту. Эти нормы приводятся как для разных скоростей передачи, так и для разных диапазонов рабочих длин волн в каждом стыковом коде.

Для того чтобы снизить стоимость проектируемой ВОЛП и сделать её оптимальной по критериям протяжённости и быстродействия необходимо выполнять достаточно сложные расчёты [2].

Какие же расчёты надо проводить при проектировании ВОЛП?

1. Самые простые расчёты – это расчёты длины ЭКУ по затуханию. Здесь оценивается минимальная длина волоконно-оптической линии, и максимальное её значение со всеми запасами на строительные работы и последующую эксплуатацию.

2. Необходимо рассчитать максимально допустимую дисперсию на участке регенерации. Такой расчет даст возможность оценить запас линии на последующее увеличение скорости передачи или изменение стыкового кода по другим причинам. По результатам расчёта можно оценить необходимость применения компенсаторов дисперсии.

На сегодня существуют следующие методы компенсации дисперсии:

a) DA – пассивная компенсация дисперсии (PDC);

b) компенсация с помощью фазовой самомодуляции;

c) компенсация с помощью предварительной линейной частотной модуляции (PCH);

d) передача при наличии дисперсии (DST).

Методика выбора метода компенсации дисперсии пока не отработана.

Все предложенные на сегодняшний день схемы пассивной компенсации (DA) компенсируют дисперсию на ограниченном расстоянии и не способны работать во всем диапазоне от нулевой длины до полной длины линии. Эти системы могут зависеть от некоторой минимальной дисперсии, которая должна быть представлена в линии [3]. Вследствие этого введён параметр «минимальная хроматическая дисперсия».

3. Надо рассчитать бюджет ВОЛП по времени нарастания импульса, поскольку в некоторых случаях время нарастания в оптическом волокне может оказаться больше, чем в передатчике и приёмнике мультиплексора. Такой расчёт может стать очень важным при изменении линейного кода, особенно, в случае применения кода RZ с разным отношением длительности логической единицы к длине битового интервала;

4. Надо знать максимально допустимую мощность, вводимую в волокно. Это особенно важно для стандартного одномодового волокна, если в будущем планируется повышать скорость и мощность передачи, особенно при переходе к работе с системами со спектральным разделением каналов.

5. Нужна оценка максимально допустимого отношения «сигнал-шум» на входе мультиплексора, которое сильно влияет на коэффициент ошибок в приёмнике, особенно в случае применения регенерации 1R на длине кабельной секции регенерации.

6. Оценку характеристик волоконно-оптической линии передачи не выполнить без знания максимальной дифференциальной групповой времени задержки (ДГВЗ)[1], то есть разницы во времени между двумя частями импульса, которые передаются в двух основных состояниях поляризации оптического сигнала [4]. Для расстояния свыше нескольких километров, в предположении случайного (сильного) взаимодействия мод, ДГВЗ в волокне можно статистически смоделировать с использованием распределения Максвелла. Для уровня STM-4 (коды применения V-4.1 – V-4.3, а также U-4.2 и U-4.3) величина ДГВЗ может достигать 480 пс, STM-16 120 пс. Номинальные значения затухания и искажений из-за группового времени задержки приведены в таблице 1 (см. ниже).

7. Кроме этого рассчитывается минимально допустимая мощность при вводе оптического излучения в волокно. Роль этого фактора, видимо, пояснений не требует.

8. И, наконец, оценивается возможность трансверсальной (поперечной) совместимости активного и пассивного оборудования, поскольку её отсутствие может стать причиной возникновения сбоев при работе сложной сети.

Вышеперечисленные расчёты необходимы при проектировании одноканальных систем. В случае многоканальных систем они должны быть дополнены расчётами, свойственными системам со спектральным уплотнением, учитывающими нелинейные процессы в оптическом волокне и влиянием отдельных каналов друг на друга.

[1] Дифференциальное групповое время задержки, определяемое как значение ДГВЗ, которое должно допускаться в системе с максимальным ухудшением чувствительности на 1 дБ.

ТАБЛИЦА 1. Номинальные значения затухания и искажения из-за группового времени задержки

f/f_0	Затухание (дБ)	Искажение из-за группового запаздывания (UI)
0,15	0,1	0
0,3	0,4	0
0,45	1,0	0
0,6	1,9	0,002
0,75	2,0	0,008
0,9	4,5	0,025
1,0	5,7	0,044
1,05	6,4	0,055
1,2	8,5	0,10
1,35	10,9	0,14
1,5	13,4	0,19
2,0	21,5	0,30

Входящая в расчетную формулу для STM-16 ширина спектра источника оптического излучения определяется на уровне –3 дБ, в то время, как в справочных материалах она приводится для уровня –20 дБ. В таких системах и в системах более высокого уровня SDH используются лазеры с внешней модуляцией. Например, система STM-64, работающая с волокном типа Rec.ITU-T G.652 на дисперсионном пределе[2] требует идеального спектра мощности. При этом важность максимальной ширины спектра, начиная с уровня STM-16, вытесняется ещё более важным параметром линейной частотной модуляции, более известным как параметр α, определяемый, в свою очередь, как:

$$\propto = \frac{\frac{d\varphi}{dt}}{\frac{1}{2P}\frac{dP}{dt}},$$

где φ – оптическая фаза сигнала, а P – его мощность. Параметр линейной частотной модуляции требуется для регулирования и описания изменения фазы сигнала, которая не определяется в расчётах для спектра мощности. Отсюда уже происходит неопределённость расчёта длины регенерационного участка, выполненного по предлагаемым нормативно-техническими

[2] Типовой дисперсионный предел для систем STM-64, работающих в волокне G.652, составляет примерно 60 км при использовании идеального спектра источника

документами расчётным формулам, применяемым для расчёта длины регенерационного участка по дисперсии.

Изменение фазы сигнала может использоваться для получения «пикового качества» системы, например, за счет компрессии импульса в ходе линейной частотной модуляции. Оно также может использоваться для изменения поведения нелинейности из-за изменения мощности. Это взаимовлияние очень сложно, а допустимые пределы параметра ЛЧМ (1–10 рад) могут изменяться с изменением кода приложения и других параметров системы и достигать значения от 10 до 100 рад.

Приведённая в РД45.047 формула для расчета длины регенерационного участка выглядит следующим образом:

$$L_B = \frac{4{,}4 \cdot 10^5}{\sigma \cdot \Delta\lambda \cdot B},$$

где L_B – длина участка в километрах; σ – суммарная дисперсия одномодового оптического волокна; Δλ – ширина спектра источника излучения; B – широкополосность цифровых сигналов, передаваемых по оптическому тракту. Коэффициент $4{,}4\times10^5$ отражает тип источника оптического излучения. Приведённое в формуле значение этого коэффициента относится к одномодовому лазерному диоду с рабочей длиной волны 1550 нм. В случае применения других источников вместо него нужно применять иные значения данного коэффициента.

В международных рекомендациях предлагается оценивать длину участка по накопленной дисперсии. При этом расчет накопленной хроматической дисперсии ведётся по следующей формуле:

$$DL = \frac{\varepsilon c}{\lambda^2 B \sqrt{\left(\frac{B}{\pi f}\right)^2 + \sigma_\nu^2}},$$

где D – коэффициент дисперсии данного оптического волокна, пс/нм*км; L – длина рассматриваемого участка, км; f – рабочий цикл (отношение длительности оптической цифровой единицы к длительности битового интервала; для кода *RZ* $f < 1$, для кода NRZ $f = 1$); B – битовая скорость в Гбит/с; λ – средняя длина волны источника в мкм (не в нм); c – скорость света, км/с; ε – эпсилон-параметр, его значение при заданном коэффициенте ошибок $1*10^{-10}$ равно 0,115, а при $К_{ош} = 1*10^{-12}$ равно 0,109 для MLM. Для SLM значение ε приведено в таблице 2 (см. ниже).

Для широкого спектра и малой битовой скорости: $\lambda^2 BDL\sigma_\nu = \varepsilon c$ или $\varepsilon \approx BDL\sigma_\lambda$, а для узкого спектра и высокой битовой скорости: $\pi\varepsilon cf \approx \lambda^2 B^2 DL$.

ТАБЛИЦА 2. Зависимость эпсилон-значения от ухудшения сигнала по мощности

Ухудшение по мощности, дБ	Эпсилон-значение
0,5	0,203 = 0,2
1	0,305 = 0,3
2	0,491 =0,49

Длину, ограниченную дисперсией, можно получить путём деления этой дисперсии на коэффициент дисперсии волокна [5, 6]. Ниже на рис. приведена номограмма для определения длины линии по накопленной дисперсии в зависимости от скорости передачи и ширины спектра источника сигнала.

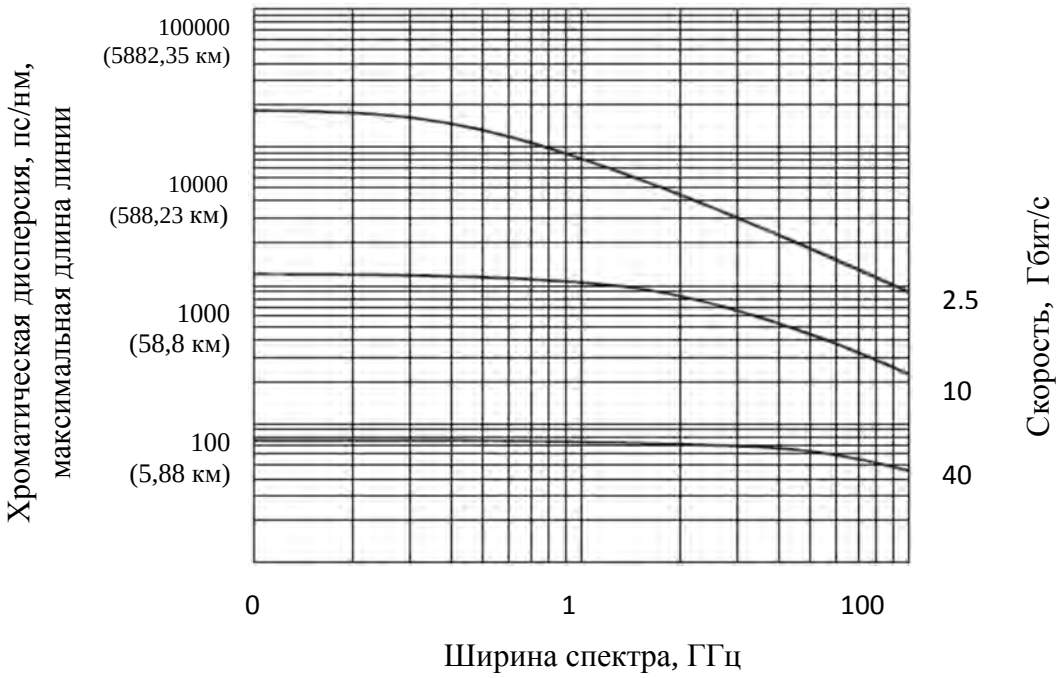


Рисунок. Максимальная допустимая хроматическая дисперсия для волокна G.652 в зависимости от ширины спектра источника на 1550 нм для некоторых битовых скоростей NRZ без частотной модуляции при ухудшении по мощности 1 дБ. В скобках указана максимальная длина в километрах

Список используемых источников

1. РД 45.047-99. Линии передачи волоконно-оптические на магистральной и внутризоновых первичных сетях ВСС России. Техническая эксплуатация.

2. Воронцов А. С. и др. Оптические кабели связи российского производства. Справочник. М. : ЭКО-ТРЕНДЗ, 2003.

3. Фриман Р. Волоконно-оптические системы связи. М. : Техносфера, 2004. 495 с.

4. ОСТ 45.104-97. Стыки оптические систем передачи синхронной цифровой иерархии. Классификация и основные параметры.

5. ОСТ 45.178-2001. Системы передачи с оптическими усилителями и спектральным уплотнением. Стыки оптические. Классификация и основные параметры.

6. ОСТ 45.90-96. Стыки цифровых каналов и групповых трактов первичной сети взаимоувязанной сети связи Российской Федерации. Методы испытания основных параметров.

УДК 621.391
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПОДХОДОВ УПРАВЛЕНИЯ МНОГОУРОВНЕВОЙ ОБЛАЧНОЙ СТРУКТУРОЙ

А. Н. Волков, В. Н. Коваленко, А. С. А. Мутханна

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

Количество устройств интернет вещей с каждым годом непрерывно увеличивается. Увеличивается также и объем генерируемого трафика. Поэтому в новом поколении сетей 5G применяется технология для снижения нагрузки и обратных задержек – MEC. Архитектура MEC основана на многоуровневой облачной структуре, однако в официальных международных документах не определен принцип того, на каком уровне архитектуры выбирается вычислительное облако для контроля обработки пользовательских данных. Поэтому в данной статье предлагается сравнить три архитектуры по управлению выбора вычислительного облака. Многоуровневую облачную структуру предлагается реализовать на платформе OpenStack.

IoT, 5G, MEC, OpenStack, облачные вычисления.

Введение

На данный момент времени концепция «Интернет вещей» продолжает бурно развиваться. С тех пор как в 1999 году Кевином Эштеном впервые был употреблен термин «интернет вещей», число устройств, подключенных к сети интернет, с каждым годом становилось только больше и больше. По мнению некоторых экспертов, количество устройств в сети интернет будет превышать 20 миллиардов. Кроме того, ожидается, что трафик от устройств в 2020 году увеличится в 200 раз, а в 2030 году – в 20000, если сравнивать с объемами трафика 2010 года. Поэтому, сетям придется оперировать огромными потоками данных, поступающими большого количества устройств с доступом в интернет, что будет приводить к большой загруженности сети и ее перегрузке [1].

Для решения данной проблемы разрабатываются сети, которые должны прийти на смену 4G и которые будут обладать сверхвысокой плотностью и ультрамалыми задержками – сети 5G/IMT-2020.

Исследованием 5G занимается государственно-частное партнерство – 3P (5G *Infrastructure Public Private Partnership*) [2]. Одна из основных задач создания сотовых систем 5G – обеспечение скорости передачи данных порядка 10 Гбит/с [2]. По мнению ITU и 3GPP, ключевыми технологиями при организации сетей 5G будут технологии виртуализации сетевых функций (NFV), программно-конфигурируемых сетей (SDN), а также технологии для разгрузки базовой сети и обеспечения низких задержек – граничные вычисления множественного доступа (MEC) и взаимодействия устройство-устройство (D2D) [1].

Граничные вычисления. Мобильные и Множественного доступа

Технология Multi-access Edge Computing (граничных вычислений множественного доступа MEC), раньше имело название мобильных граничных вычислений (*Mobile Edge Computing*) и ее основная концепция заключалась в применении в сотовой сети вычислительного облака, располагающегося на границе сети радиодоступа. Данный подход позволяет предоставить возможность обработки данных на входе в сеть, тем самым исключая ряд составляющих общей задержки [1].

Европейский институт стандартизации электросвязи (ETSI), являющийся ведущей организацией по исследованию технологии MEC, выяснил что данную технологию можно применять не только в мобильных, но и в других сетях с беспроводной связь, что и послужило причиной переименования этой технологии.

К основным характеристикам MEC [1]:

1. Локальность – изолированная работа вычислительных облаков MEC от других частей сети. При этом сохраняя доступ к локальным ресурсам.

2. Близкое расположение относительно источников информации.

3. Обеспечение низких показателей задержки.

4. Получение информации о состоянии сети и местоположении любых устройств в ней.

Вычислительное облако может быть размещено:

1. На базовой станции LTE (eNB).

2. На контроллере базовых станций (RNC).

3. При соединении с несколькими сайтами (несколько eNB).

4. На границе с базовой сетью.

В архитектуре MEC определяются следующие типы облаков:

1. Микро-облако (*Micro cloud*) с небольшими вычислительными и запоминающими ресурсами.

2. Мини-облако (*Mini cloud*), обладающее, по сравнению с микро-облаком, более высокими вычислительными и запоминающими ресурсами. Располагается на следующем, после микро-облака, уровне сетевой архитектуры.

3. Главное облако (*Main cloud*), обладающее наибольшими вычислительными и запоминающими возможностями среди всех облаков сети. Является самым главным вычислительным блоком и обрабатывает пользовательские данные, которые не могут быть обработаны ни в микро, ни в мини-облаке.

Международные стандарты ETSI содержат эталонную функциональную схему технологии MEC, но в них не определено какой тип облака (микро, мини или главное облако) ответственен за определение уровня сетевой архитектуры, на котором будут обрабатываться пользовательские данные [3].

Поэтому в данной работе предлагается сравнить три различные архитектуры для выбора уровня обработки пользовательских данных (пакеты информации могут обрабатываться либо микро, либо мини, либо главным облаком). Параметром сравнения трех сетей предлагается взять общую задержку, включающую время доставки пакета данных до обрабатывающего его облака и время обработки самого пакета.

Реализация сетей с MEC технологиями будет осуществляться на облачной платформе OpenStack.

Вычислительное облако и облачная платформа OpenStack

Облачные вычисления – это особый вид вычислительных услуг, с помощью которого пользователю предоставляются вычислительные возможности и ресурсы самых разнообразных баз данных, хранилищ в сети и серверов [1].

Одно из наиболее важных преимуществ при использовании облачных технологий – хранение данных с помощью хранилищ больших объемов [1].

Все предоставляемые услуги облачных серверов разделяют на [3]:

1. Инфраструктура как услуга (IaaS).
2. Платформа как услуга (PaaS).
3. Программное обеспечение как услуга (SaaS).

OpenStack – платформа для облачных вычислений с открытым исходным кодом и свободным доступом к разработке, распространению и развитию программного обеспечения на ее основе. OpenStack находит применение при развертывании облаков типа IaaS, так как основной целью разработки данной облачной платформы было обеспечение работы облачных приложений. При написании приложений на облачной платформе

OpenStack применяется принцип горизонтальной масштабируемости виртуальных машин, при котором отдельные виртуальные машины не критичны для функционирования всего приложения и не требуют высокой доступности [4].

Предлагаемые архитектуры управления

В данной работе предлагается три подхода к управлению обработкой пользовательского трафика (рис. 1):

1. Данные управления передаются на микро-облако, и, если оно не может обработать пользовательский трафик, данные управления передается далее на обработку мини облаку.

2. Данные управления поступают на обработку мини-облаку

3. Данные управления передаются только главному облаку (серверу).

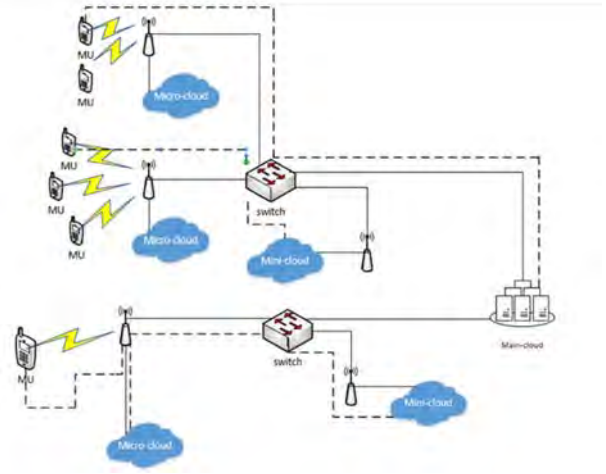


Рис. 1. Три вида архитектуры управления обработкой пользовательского трафика

В данном эксперименте был рассмотрен лишь случай, когда на одном из трёх уровней облачной архитектуры выбиралось: какое облако может обрабатывать пользовательский трафик.

Управлением всей облачной архитектурой осуществлял сервер (главное облако).

Параметры эксперимента

Имитация работы и сравнение общих задержек трех различных архитектур управления обработкой пользовательского трафика производилось в программном комплексе AnyLogic (рис. 2, 3, табл., см. ниже).

В данном эксперименте имитационная модель обладала следующими характеристиками:

1. Размеры пакетов данных – 1500 байт для пользовательской информации и 300 байт для данных управления.

2. Генерируемый трафик мог обрабатываться в 25 % случаях на микро-облаке, в 50 % на мини облаке, в 25 % на главном облаке (сервере).

3. Доставка пакетов данных до микро, мини и главного облаков занимала 3, 12 и 90 мс соответственно.

4. Так как при передаче информации управления до мини облака, пакеты проходили тот же маршрут, что и при отправке на микро-облако,

то в первом способе организации архитектуры управления для большей достоверности из времени доставки на мини облако вычиталось время доставки на микро-облако (12 – 3 = 9 мс).

5. Скорость обработки одного пакета для микро, мини и главного облака – 1, 2 и 8 мбит/с соответственно.

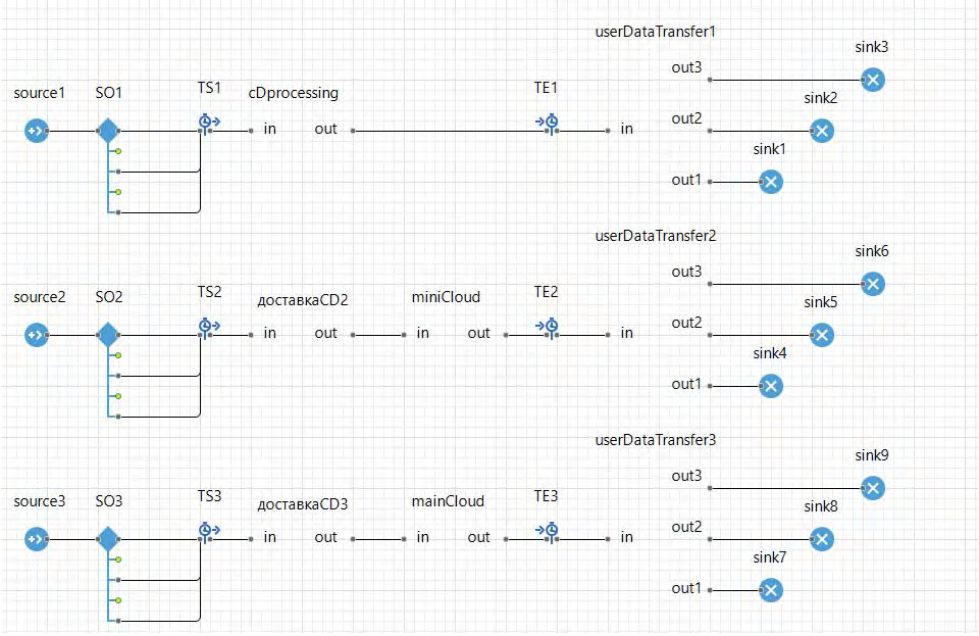


Рис. 2. Схема имитационной модели в программном комплексе AnyLogic

ТАБЛИЦА. Значение общей средней задержки в сети

Способы управления / среднее время обработки	Данных управления, мс	Пользовательских Данных, мс
микро и мини облако	13	49
только мини облако	1	49
Только главное облако	95	130

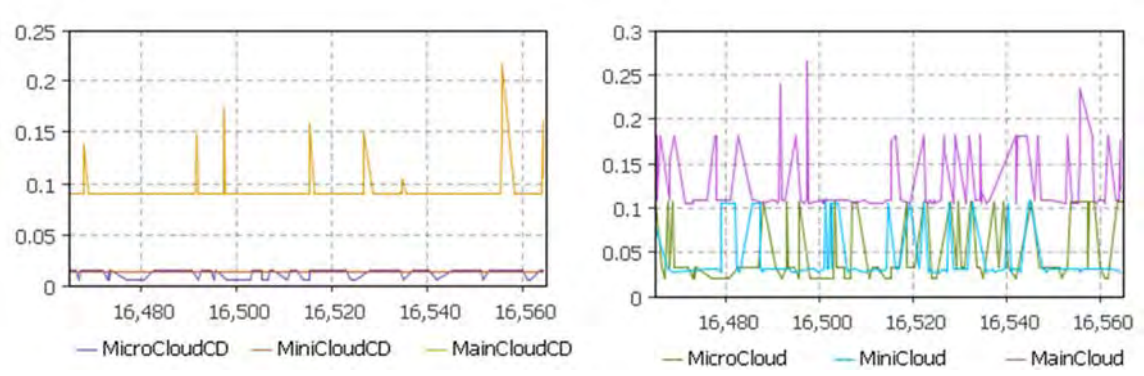


Рис. 3. Графики зависимости общей задержки пакетов данных (слева только данных управления, справа – учитывается и время обработки пользовательских данных)

Результаты Эксперимента

1. Каждый из способов управления будет наиболее эффективен при определенном виде трафика: 1 – трафик, поступающий на микро-облако, второй на мини-облако, третий на сервер.

2. Теоретически, если в первом случае принять решение о том, какой уровень должен обрабатывать пользовательские данные, может только мини-облако, то первый способ займет больше времени, чем второй.

3. В данном эксперименте большее влияние на общую задержку оказывала задержка доставки до микро, мини или главного облака.

Список используемых источников

1. Филимонова М. И., Атея А. А., Мутханна А. С. Исследование облачных вычислений в сотовых сетях // Информационные технологии и телекоммуникации. 2017. Т. 5. № 3. С. 45–59.

2. Abdelhamied A. Ateya, Ammar Muthanna, Andrey Koucheryavy. 5G framework based on multi-level edge computing with D2D enabled communication // Conference: Advanced Communication Technology (ICACT), 2018 20th International Conference on, At Chuncheon-si Gangwon-do, Korea (South), Korea (South).

3. Облачные технологии. Кратко об основном [Электронный ресурс]. URL: http://www.uipdp.com/articles/2012-02/11.html

4. Маркелов А. OpenStack. Практическое знакомство с облачной операционной системой, 4-е изд. М. :ДМК Пресс, 2018. 306 с. ISBN 978-5-97060-652-0.

УДК 007.51
ГРНТИ 50.47.02

АКТУАЛЬНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

В. Н. Волкогонов, А. М. Гельфанд, В. С. Деревянко

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

Автоматизированные системы управления играют большую роль в современном мире. Они позволяют повысить производительность труда, а также оптимизировать процесс управления. АСУ осуществляют контроль за всеми основными видами деятельности, а также выполняют функции планирования и прогнозирования. Их появление во многом улучшает и упрощает процессы управления.

автоматизированные системы управления, контроль объектов, управление процессами, технологии.

В настоящее время наблюдается бурное развитие и применение современных средств вычислительной техники, происходит внедрение методов оптимизации производства. Особое место в оптимизации производства и процессов, а также обеспечении управления занимают автоматизированные системы управления (АСУ). Трудно представить современный мир без данных технологий. Ярким примером АСУ является система «Умный дом».

Автоматизированные системы управления – совокупность аппаратных и программных средств, которые предназначены для управления различными процессами и осуществления контроля объектов. Данные системы управление высоко востребованы в современном мире. АСУ решают задачи по сбору информации, ее обработки, хранения и анализа. Введение автоматизированных систем управления позволяет минимизировать численность персонала, повысить эффективность и качество управления и функционирования объекта [1]. Не углубляясь в сложные структурные схемы, АСУ можно представить в следующем виде (рис. 1):

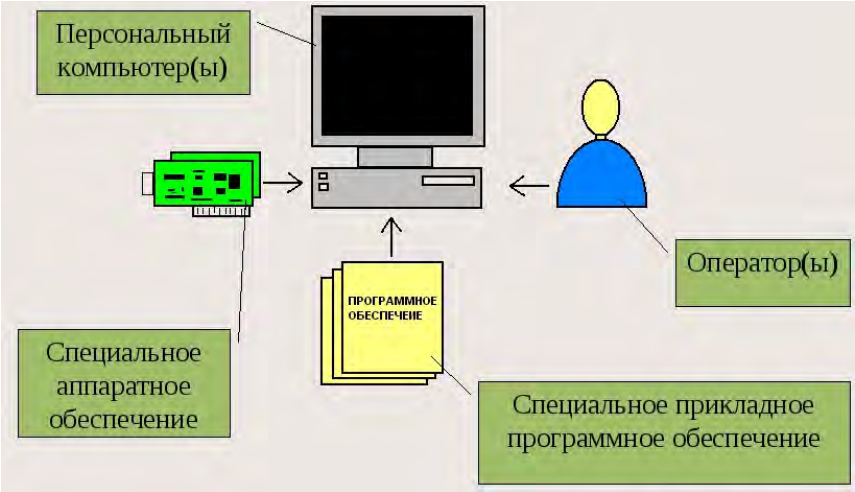


Рис. 1. Общее представление АСУ

АСУ имеют ряд преимуществ, среди которых [2]:

– планирование и экономичное использование ресурсов;
– сокращение потерь рабочего времени;
– сокращение производственных затрат;
– обработка большого количества данных в кратчайшие сроки;
– дистанционное управление технологическим процессом.

Данные системы управления играют большую роль на современных предприятиях. В связи высоким ростом технологий, устаревшая техника заменяется на более мощное оборудование. Технологии автоматизации позволяют осуществлять контроль за различными операциями и процессами, а также вносить изменения. Машины позволяют выполнять технически

сложные и трудоемкие виды деятельности, в которых у персонала возникнут трудности. Автоматизированная система имеет защиту от ошибочных действий персонала: сигнализация, сообщения тревоги, блокировка систем. Это позволяет избежать непредвиденных неприятностей.

Несмотря на достоинства автоматизированных систем связи, существуют также и некоторые проблемы с их внедрением. Например, они могут быть связаны с непредусмотренными трудовыми и финансовыми затратами. Зачастую трудности могут быть связаны с устаревшим оборудованием, а также старыми версиями операционных систем. Все проблемы необходимо анализировать и решать на этапе проектирования систем автоматизации. Для того, чтобы АСУ работали стабильно и без осложнений должен быть обеспечен постоянный контроль за системой. Нужно основательно заниматься обеспечением безопасности систем управления, так как они могут быть подвержены различным угрозам. Необходимо уделить больше внимания информационной безопасности, потому что это крайне важный вопрос и одна из основных проблем АСУ.

При внедрении автоматизированных систем управления предприятия могут столкнуться с такими трудностями, как увеличение нагрузки персонала, частичная или полная реорганизация структуры, изменения в управлении различными процессами [3]. Но это временные трудности, которые появляются на начальных этапах внедрения.

Оборудование АСУ имеет в составе следующие элементы [4]:

– модули ввода-вывода;
– контроллеры;
– измерители;
– датчики;
– панели оператора;
– источники питания.

Это лишь несколько примеров элементов, которые содержат АСУ. Их может быть намного больше.

Появление АСУ во многом положительно повлияло на повседневную жизнь. Разрабатываются системы и устройства, которые способны обеспечить необходимый контроль за различными объектами и видами деятельности. Это способствует улучшению работы человека. Как пример, можно привести автоматизированную систему управления наружным освещением (рис. 2), которая обеспечивает централизованный контроль за работой, а также реагирует на различные непредвиденные ситуации [5].

Другим примером данной технологии является автоматизированная система управления дорожным движением (рис. 3). Задача системы состоит в эффективном регулировании потоков транспорта, а также создании условии, при которых будет обеспечена безопасность и снижение транспортных задержек [6].

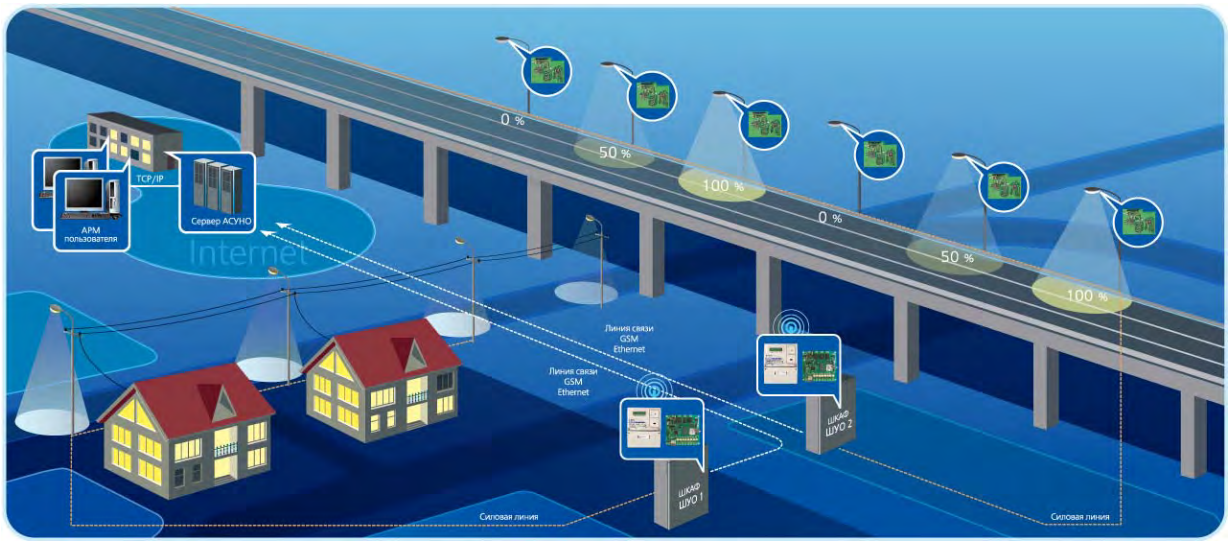


Рис. 2. Автоматизированная система управления наружным освещением

Существует множество других подобных систем управления, с которыми общество сталкивается каждый день. Они доказывают своё положительное влияние на повседневную жизнь.

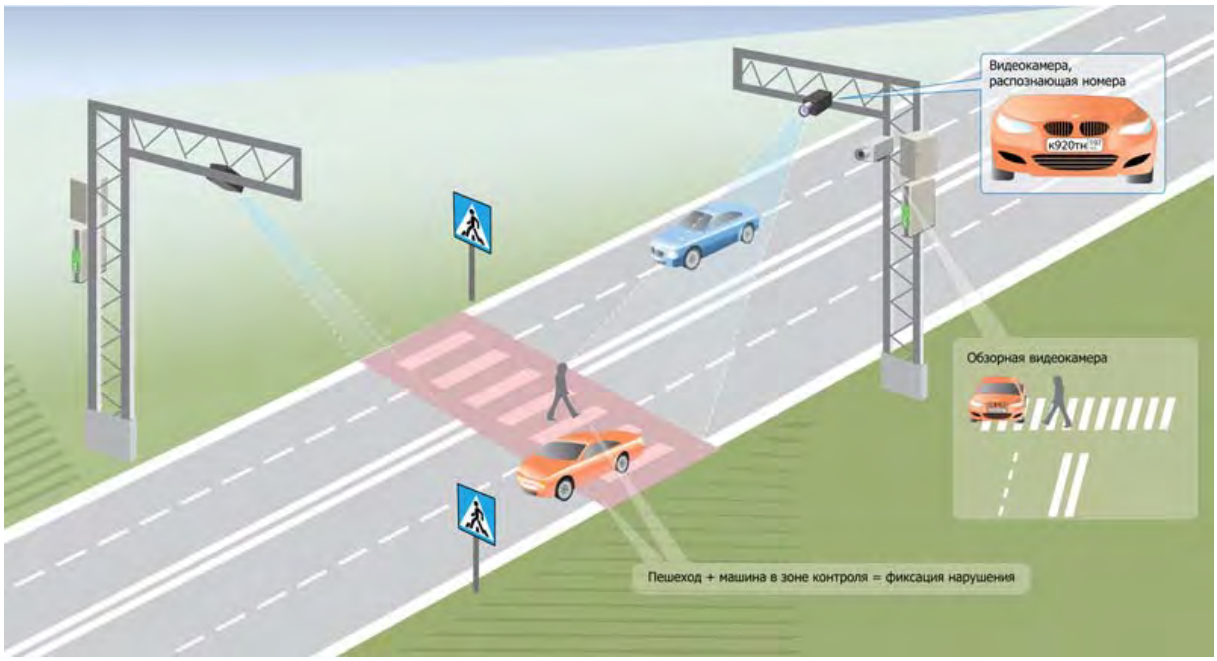


Рис. 3. Автоматизированная система управления дорожным движением

На основании вышеперечисленного можно установить, что автоматизированные системы управления играют важную роль и вносят большой вклад в современный мир. Их использование оптимально влияет на различные виды деятельности, работу предприятий, производительность. Но нельзя оставлять без внимания то, что для стабильной работы данных

систем управления необходимо вести тщательный контроль за ними и обеспечить функциональную и информационную безопасность. Тема, связанная с АСУ наиболее актуальна в современном информационном мире. Системы контроля и управления будут все более востребованы с развитием технологий.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности. учебное пособие; Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». СПб, 2012.

2. Душин С. Е., Красов А. В., Кузьмин Н. Н. Моделирование систем управления : учебное пособие для студентов высших учебных заведений, обучающихся по направлению 220400 «Управление в технических системах» / Под ред. С. Е. Душина. М., 2012.

3. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

4. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141–146.

5. АСУНО [Электронный ресурс]. URL: https://cdelct.ru/vidy (дата обращения 29.01.2019).

6. АСУДД [Электронный ресурс]. URL: https://studwood.ru/2155750/tehnika (дата обращения 29.01.2019).

УДК 004.01
ГРНТИ 10.19.61

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В. Н. Волкогонов, А. М. Гельфанд, М. Р. Карамова

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

В целях реализации конституционного права граждан на неприкосновенность частной жизни, личную и семейную тайну Правительством Российской Федерации установлены требования к обеспечению безопасности персональных данных при их об-

работке с использованием средств автоматизации. Важно отметить, что теперь работы по обеспечению безопасности персональных данных при их обработке являются неотъемлемой частью работ по созданию соответствующих информационных систем.

обеспечение, безопасность, персональные данные.

Актуальность выбранной темы заключается в том, что сосредоточение больших объемов персональных данных (ПДн) граждан в информационных системах персональных данных (ИСПДн), широкое использование сетевых технологий привело к опасности их утечки и уничтожения или изменения с возможностью возникновения значительных социальных последствий. Это вынуждает принимать адекватные меры по защите ИСПДНн от угроз несанкционированных разрушительных воздействий.

Обеспечение безопасности ПДн при их обработке в ИСПДн, на сегодняшний день регулируется Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», которые направлены на решение следующих задач:

– предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

– недопущение воздействия на технические средства автоматизированной обработки ПДн, в ходе которого может быть нарушено их функционирование;

– своевременное обнаружение фактов НСД к ПДн;

– обеспечение возможности оперативного восстановления ПДн, изменённых или уничтоженных вследствие НСД к ним;

– постоянный контроль за обеспечением уровня защищенности ПДн [1, 3].

В соответствии с законом «О персональных данных» – это любая информация, относящаяся к определенному или определяемому, на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, иная информация. На данный момент работы по обеспечению безопасности ПДн в соответствии с законом и действующими нормативными и методическими документами должны проводиться применительно к ИСПДн:

– государственных органов, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;

– муниципальных органов, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;

– юридических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных;

– физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных (за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд).

Под организацией работ по обеспечению безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях эксплуатации ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) угроз безопасности ПДн в ИСПДн, восстановление функционирования ИСПДн после нейтрализации угрозы с целью минимизации ущерба от возможной реализации таких угроз.

Для разработки и осуществления мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн оператором или уполномоченным им лицом назначается структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности ПДн. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на оператора.

Порядок организации обеспечения безопасности ПДн состоит из:

– оценки обстановки;

– обоснования требований по обеспечению безопасности ПДн и формулирования задач защиты ПДн;

– разработки замысла обеспечения безопасности ПДн;

– выбора целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

– решения вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

– обеспечения реализации принятого замысла защиты;

– планирования мероприятий по защите ПДн;

– организации и проведения работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (улучшения) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДНн или ее элементов в ИСПДн, а также

решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн [2];

– разработки документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;

– развертывания и ввода в опытную эксплуатацию СЗПДн в ИСПДн;

– доработки СЗПДн по результатам опытной эксплуатации.

Правительство Российской Федерации с учетом возможного вреда субъекту ПДн, объема и содержания обрабатываемых ПДн, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности ПДн устанавливает:

1) уровни защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных;

2) требования к защите ПДн при их обработке в ИСПДн, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн [4].

В рамках обеспечения безопасности ПДн при их обработке в ИСПДн разрабатывается разрешительная система доступа к обрабатываемой в ИСПДн информации, которая предусматривает установление единого порядка обращения со сведениями, содержащими ПДн и их носителями, определяет степень ограничения на доступ к данной информации и степень ответственности за сохранность предоставленной информации.

Контроль обеспечения требуемого уровня защищенности ПДн заключается в проверке выполнения требований нормативных документов по защите персональных данных, а также в оценке выполнения и эффективности принятых мер. Мероприятия по контролю защищенности ПДн могут проводиться как уполномоченными работниками подразделения по технической защите информации, так и на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации [5].

В соответствии с положениями Федерального закона от 8 августа 2001 г. № 128 «О лицензировании отдельных видов деятельности» и требованиями постановления Правительства Российской Федерации от 16 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации» операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке.

Список используемых источников

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» принят Государственной Думой 08.07.2006, одобрен Советом Федерации 14.07.2006.
2. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
3. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. Трудовой кодекс Российской Федерации. Принят Государственной Думой 21 декабря 2001 года. Одобрен Советом Федерации 26 декабря 2001 года.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ БЕЗОПАСНОСТИ WI-FI СЕТЕЙ

В. Н. Волкогонов, А. А. Казанцев, А. И. Катасонов, Г. А. Орлов

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

Wi-fi сети получили широкое распространение в современном мире, фактически, они стали важным инструментом коммуникации, благодаря, их гибкости, эффективности и низкой стоимости, с другой стороны они передают данные с использованием радиоволн, которые обычно чувствительны к подслушиванию. Для обеспечения защиты используются множество протоколов. Из них заострим внимание на WEP и WPA, которые все еще широко используются. Используя эти протоколы, существует вероятность перехвата необходимого количества пакетов для восстановления секретного ключа. В данной статье производится поиск лучшего способа защиты беспроводных сетей, чтобы уменьшить среднее количество пакетов перехвата, необходимых для восстановления секретного ключа.

Wi-fi. Сети, безопасность, WPA.

Введение

Беспроводные сети становятся важным инструментом коммуникации из-за их гибкости, эффективности и низкой стоимости. С другой стороны, беспроводные сети имеют множество ограничений в отношении традиционных сетей, таких как уменьшенные данные хранения и потребление малой мощности. В беспроводных сетях управление связью обрабатывается про-

токолами вида: WEP, WPA и WPA2, предназначенными для защиты сообщений. Целью данного исследования является определение проблем безопасности в беспроводных сетях. Мы фокусируемся на протоколах WEP и WPA, которые все еще широко используются, но также не могут обеспечить защиту от различных угроз и уязвимостей, таких как FMS-атака, основанная на слабости Инициализационного вектора (IV). Наш вклад состоит в том, чтобы найти лучший способ защиты беспроводных сетей, чтобы уменьшить среднее количество пакетов перехвата, необходимых для восстановления секретного ключа.

Протоколы Wi-Fi

Стандартные беспроводные устройства, а именно стандарта 802.11 IEEE позволяют подключать любое устройство с широкополосным подключением на расстоянии нескольких сотен метров в открытой среде. WiredEquivalentPrivacy (WEP), входящая в стандарт IEEE 802.11 широко применяется на устройствах WLAN. Данная система предназначена для обеспечения конфиденциальности, аутентификации и целостности, подобных проводным сетям. WEP основан на схеме шифрования RC4 и CRC-32 для целостности данных и использует секретный ключ “*k shard*” от 5 до 13 байтов. Для получения зашифрованного текста C и его контрольной суммы ICV из открытого текста M ключ *k* объединяется с вектором инициализации IV 3 байта в соответствии со следующей формулой:

$$C = M \,||\, ICV(M) \oplus RC4(K) \,||\, IV,$$

где || обозначает оператор конкатенации, а $\oplus$ – побитовый исключительный оператор OR (рис. 1).

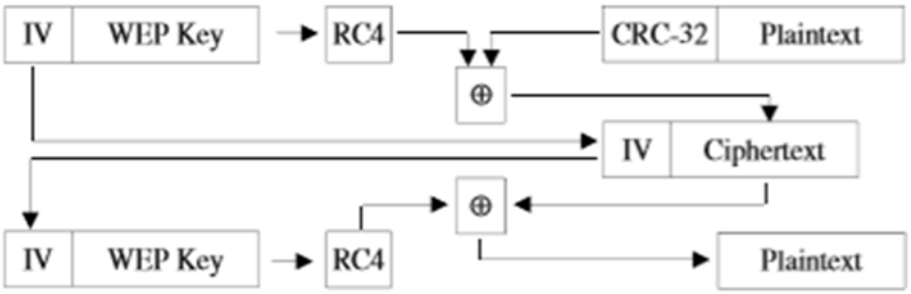


Рис. 1. Процесс инкапсуляции WEP

IV является краеугольным ключом безопасности WEP. Он увеличивается для каждого испущенного пакета, чтобы два последующих пакета не могли быть зашифрованы одним и тем же ключом. Защищенный доступ Wi-Fi (WPA) представляет собой усовершенствованную версию стандарта 802.11i, разработанную Wi-Fi-Aliance в 2001 году. Он основан на протоколе

целостности временного ключа (TKIP), надежном алгоритме шифрования, построенном вокруг WEP. Он позволяет генерировать случайное ключевое слово, которое отключает атаки на основе статистического анализа. WPA включает некоторые улучшенные свойства, такие как код целостности сообщения (MIC) и ключ хэш-функции, чтобы избежать атак типа IV. На рис. 2 показан процесс WPA-TKIP, где TK, DA, SA обозначают соответственно временный ключ, адреса отправителя и получателя, а || – оператор конкатенации.

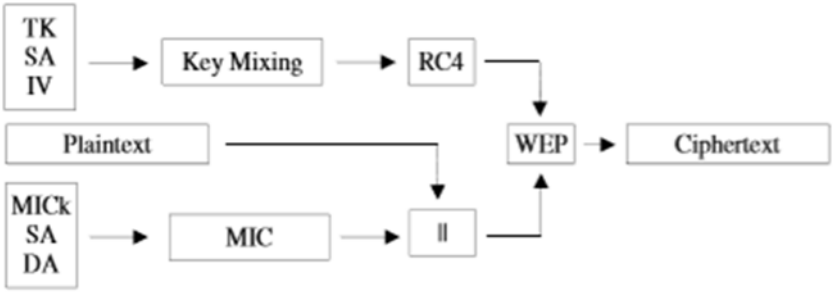


Рис. 2. Процесс инкапсуляции WPA

WPA2 является сертифицированным преемником WPA, построен на протоколе Counter-Mode (CCMP) на основе алгоритма Advanced Encryption Standard (AES). Он использует 128-битную длину ключа с 48-битным IV, который обеспечивает больше защиты данных и контроля доступа.

Обзор безопасности протоколов Wi-Fi

Конфиденциальность и целостность данных – это самая важная проблема безопасности беспроводных. Безопасность WEP основана на структуре RivestCipher 4 (RC4), алгоритме потокового шифрования, где открытый текст X-ored с последовательностью случайных байтов, сгенерированных алгоритмом планирования ключей (KSA) и алгоритмом псевдослучайного генерации (PRGA), части RC4. Эти байты построены на 64-битной длине ключа, но действительно 40 бит фиксированы. Остальные 24 бита (IV) предлагают только 16 миллионов возможностей и, по статистике, дают 50 % вероятность повторного использования (IV) после менее 5000 пакетов, однако он может быть уязвим для парадоксальной атаки на день рождения. Кроме того, WEP использует один ключ, общий для всех узлов и точек доступа, и не часто изменяется. Слабость (IV) была обнаружена Фльюхрером С., с помощью атаки FMS. Идея заключалась в выявлении слабых клавиш, которые могут быть использованы для определения набора выходных битов. Подобно FMS-атаке, атака Korek пытается выявить начальные биты из блоков данных, генерируемых алгоритмом PRGA. Таким

образом, злоумышленник может прослушивать все незашифрованные пакеты, не будучи обнаруженными точкой доступа. Аналогичным образом, другие атаки также выполнялись на TKIP. Атака BT заключалась в том, чтобы выполнять незначительные изменения в коротком пакете ARP и DNS для восстановления открытого текста и потока пакетов и, в свою очередь, перейти к DoS и ARP-атакам отравления. Атака БТ была улучшена атакой Огигаси-Мори в сочетании с которой «человек в центре» атаки для сокращения время выполнения.

Обзор атак FMS

Секретный ключ *k* и вектор инициализации (IV) составляют основную слабость протокола WEP. Только 3 байта IV изменяются для каждого переданного пакета, в то время как 13 байтов *k* все еще статичны. ФМС, известная атака открытого текста основана на двух условиях:

а) На итерации *i* KSA, если бы мы достигли стадии, где $x = Si$, $y = Si\,[x]$, $x + y = Si\,[x] + Si\,[Si\,[y]]$, то вероятность 5 %, что ни один из элементов *x*, *y* и $x + z$ не будет использоваться в последующих итерациях, а $S\,[x] + S\,[S\,[1]]$ может быть первым байтом, сгенерированным PRGA. Эта ситуация называется разрешенным состоянием.

б) В разрешенном состоянии говорится о том, что значение следующего ключевого байта *b* ключа *k* имеет 5 %-ную вероятность если $S\,[1] < I$ и $S\,[x] + S\,[S\,[1]] = I + b$, где *Out* – первый выход PRGA; I, длина IV и *S*, $S - 1$ являются векторами состояний KSA для первых *b* итераций. В применении WEP предполагается, что мы знаем первые байты секретного ключа $k\,[3]$, …, $k\,[a + 2]$. Первоначально мы имеем $a = 0$, поэтому известны только 3 байта IV. FMS пытается смоделировать первые *x* итераций KSA, что позволяет определить перестановку $Sx - 1$ и соответствующие индексы $ix - 1$ и $jx - 1$. Следующее значение *i* также известно ($ix = x$), но следующее значение *j* зависит от следующего выбранного байта ключа. Как видно, успех такой идеи зависит от слабого IV. Слабый IV позволяет выявлять информацию о ключевых байтах, имеет конкретный вид ($a + 3$, 255, *x*), где *a* обозначает *k*-байт, который нужно найти, и *x* не имеет значения [1].

Экспериментальное исследование

Цель эксперимента – проверить эффективность FMS-атаки на реальной среде Wi-Fi, ее стоимости и, если возможно, внести свой вклад в ее улучшение. Эксперименты проводились на частоте 3,2 ГГц; среда включает в себя пакет aircrack-ng служб в системе Linux. Также необходимо установить беспроводную карту в режиме монитора. Для сбора данных был использован инструмент airdump-ng, который переключается на целевые пакеты AP из одного канала. Используется совместимый сетевой интерфейс, который

позволяет генерировать и вставлять пакеты для увеличения трафика. [3] Захваченные IV были разделены на три файла в зависимости от их специфики: специфическая форма IV, ключевой зависимый слабый IV и независимый от ключа слабый IV. Кроме того, все записи IV были сохранены в другом файле, который использовался для исчерпывающего теста поиска. Переходим к атаке, которая кажется образцом: для каждого ключевого байта мы выбираем файл IV, каждый IV объединяется с секретным ключом и переходит к первым трем итерациям алгоритма KSA. [2] Затем мы можем искать каждый ключевой байт, который проверял разрешенное условие, используя aircrack-ng. На рис. 3 и 4 изображены изменение времени и трафика процессора с каждой категорией IV.

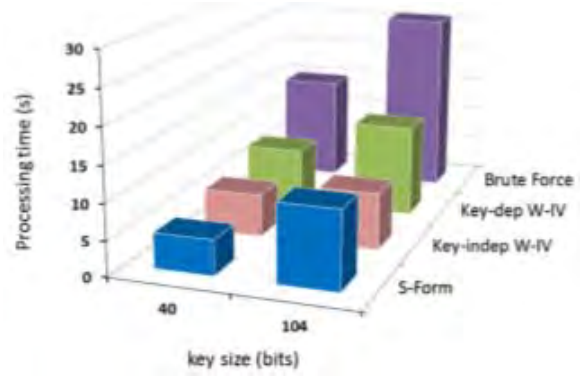


Рис. 3. Изменение времени процессора с каждой категорией

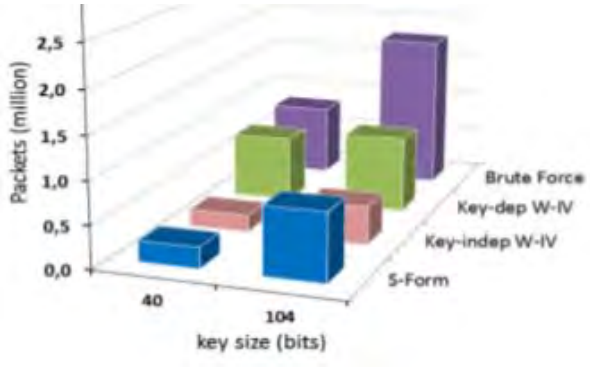


Рис. 4. Изменение трафика процессора с каждой категорией

Заключение

Протоколы Wi-Fi подтверждают, что решение безопасности проводных сетей до сих пор представляет интерес и по сей день. Однако такие протоколы не полностью защищены и могут быть нацелены на ключевые атаки восстановления в реальном мире.

Наши эксперименты показывают, что FMS не является полной атакой на восстановление ключей, но может быть улучшена путем сбора пакетов; поэтому ключевая независимая стратегия «слабый-IV» представляется лучшим способом выбора слабых клавиш и позволяет выявлять секретные ключи менее чем за 10 секунд со средним количеством полумиллиона пакетов.

Основываясь на предыдущих результатах, мы можем заключить, что ключевая безопасность протоколов, основанных на алгоритме RC4, просто предотвращает произвольные уязвимости, а не вредоносные злоумышленники. Инициализационные векторы IV, по-видимому, являются самым слабым звеном в процессе безопасности. Алгоритм AES, основанный на протоколах, более устойчив к атакам, но выглядит очень дорогостоящим для развертывания в активных сетях из-за их схемы шифрования (CCMP).

Список используемых источников

1. Красов А. В., Ягудин И. Р. Анализ активных сетевых атак: arp-spoofing и dns-spoofing // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII международная научно-техническая и научно-методическая конференция : сб. науч. ст. В 4-х томах. 2018. С. 520–526.
2. Алейников А. А., Билятдинов К. З., Красов А. В., Левин М. В. Контроль, измерение и интеллектуальное управление трафиком : монография. СПб. : ЦНИТ «Аристон», 2016. 92 с.
3. Алейников А. А., Билятдинов К. З., Красов А. В., Кривчун Е. А., Крысанов А. В. Технические аспекты управления с использованием сети интернет : монография. СПб. : ЦНИТ «Аристон», 2016. 305 с.

УДК 004.056.53
ГРНТИ 81.93.29

ОТКРЫТЫЕ ДАННЫЕ ГОСУДАРСТВЕННОГО ОРГАНА И ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В. Н. Волкогонов, А. Ю. Ломакин

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

Открытые данные зачастую служат средством обмена информацией о действиях и финансовых операциях правительства. Они являются гарантом прозрачности работы и развития организации. В данной статье рассмотрены проблемы обеспечения информационной безопасности в сфере BIG Data. В статье рассмотрены понятие и характеристики больших данных и открытых данных.

большие данные, открытые данные, информационная безопасность, ФСТЭК.

Открытые данные – информация (в том числе документированная), созданная в пределах своих полномочий государственными органами, их территориальными органами, органами местного самоуправления или организациями, подведомственными государственным органам, органам местного самоуправления, либо поступившая в указанные органы и организации, которая подлежит размещению в сети Интернет в формате, обеспечивающем ее автоматическую обработку в целях повторного использования без предварительного изменения человеком (машиночитаемый формат), и может свободно использоваться в любых соответствующих закону целях любыми

лицами независимо от формы ее размещения (простая совокупность сведений, база данных и т. д.).

Можно выделить наиболее важные характеристики:

– актуальность и достоверность открытых данных;

– открытость опубликованных данных;

– обеспечение возможности использования открытых данных, в том числе для повторного использования;

– расширение сотрудничества с пользователями открытых данных и с поставщиками негосударственных открытых данных.

Только при выполнении вышеперечисленных условий может быть достигнут максимальный эффект от их использования.

Открытые данные подразумевают, по своей сути, в первую очередь совместимые данные. Совместимость определяет способность разнообразных систем и организаций работать вместе – взаимодействовать и совмещать различные наборы данных. При построении больших и сложных информационных систем совместимость крайне важна, поскольку она позволяет различным компонентам системы работать вместе. Подобная ситуация наблюдается и по отношению к данным – в основе данных лежит одна открытая информация, которая может быть объединена с другой открытой информацией.

Совместимость – главный ключ к получению практической выгоды открытости информации, позволяющая совмещать различные наборы данных для предоставления лучших сервисов.

Решение данной проблемы лежит в плоскости BIG DATA («больших данных»).

Понятие BIG DATA («большие данные») - преодолело в последнее время стремительное развитие от концепции до набора технологий, относящихся к данной сфере.

Чтобы понять, что же вкладывается в понятие BIG DATA, необходимо рассмотреть их основные характеристики – объем, скорость и многообразие.

Большие данные – это данные больших объемов, высоких скоростей и огромного разнообразия информационных активов, которые требуют рентабельных, инновационных форм обработки информации для более широкого ее понимания и принятия релевантных решений. Определения «больших данных» относительны и зависят от таких факторов, как – время и тип данных. То, что может считаться большими данными сегодня может не соответствовать их пределу в будущем [1].

Помимо этих, общепринятых характеристик, разными участниками рынка выдвигаются дополнительные требования к BIG DATA. Так, напри-

мер, IBM дополняет их характеристикой – «достоверность», которая присуща тем или иным источникам, SAS представляет – «изменчивость и сложность», как две дополнительные характеристики больших объемов данных, а Oracle – представила «ценность данных», как атрибут больших данных (данные полученные в первоначальном виде имеют более низкое значение, чем те, которые получены путем их анализа) [2].

Обычно большие данные поступают из трех источников:

– интернет (соцсети, форумы, блоги, СМИ и другие сайты);

– корпоративные архивы документов;

– показания датчиков, приборов и других устройств.

Большие данные бесполезны в вакууме. Их потенциальная ценность разблокирована только тогда, когда использована для принятия решений [3].

Процесс обработки «больших данных» включает в себя следующие основные этапы:

– процесс извлечения данных из различных разнородных источников информации;

– их очистка, преобразование (на данной стадии процесса могут применяться как заданные правила, так и методы аналитики);

– представление данных.

Дальнейшая обработка полученных данных осуществляется с помощью:

– методов моделирования и анализа (в том числе машинное обучение, искусственные нейронные сети, распознавание образов, прогнозную аналитику, имитационное моделирование, пространственный и статистический анализ и т. п.);

– их интерпретации.

Проходя все вышеперечисленные этапы «большие данные» существенно повышают, по выражению Oracle, «ценности данных».

Исходя из выше сказанного, применения концепции BIG DATA к построению открытых данных можно решить проблемы их использования, упомянутых ранее.

Если смотреть с точки зрения информационных технологий, то под термином BIG DATA подразумевается большое количество продуктов. На них распространяется требования Методического документа «Меры защиты информации в государственных информационных системах» утвержденного ФСТЭК России от 11 февраля 2014 года.

Если речь заходит про безопасность, то важно не только понимать, какой результат приносит BIG DATA, но и какими терминами оперирует, а также как получаются те или иные выводы на основе полученной информации. Здесь необходим инструментарий, который будет давать полное

представление обо всех потоках данных. Зная, что хранится, можно выработать необходимый комплекс мер защиты информации [5].

Для обеспечения защиты больших данных необходимо реализовать следующий комплекс мер защиты:

– необходимо использовать механизмы аутентификации и идентификации пользователей системы;

– разграничить права доступа для пользователей при обращении к системе;

– управление запуском, установкой и управления файлами системы;

– вести учет, контроль и использование переносных носителей информации;

– обеспечить мониторинг событий информационной безопасности при обработке больших данных с целью дальнейшего расследования возможных инцидентов;

– реализовать антивирусную защиту;

– обеспечить защиту серверных компонентов систем от вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации;

– выявление, анализ уязвимостей информационной системы и оперативное устранение выявленных уязвимостей. Отделить персональные данные от других данных;

– обеспечение целостности и доступности информации;

– обеспечить безопасность конечных устройств, в том числе мобильных;

– использования межсетевого экранирования, а также обеспечить защиту хранилища данных с помощью механизмов шифрования и хеширования.

При реализации концепции открытых данных государственного органа необходимо уделять повышенное внимание при реализации мероприятий защиты информации на всех уровнях – на уровне используемых программно-аппаратных комплексах, сетевом оборудовании, системном программном обеспечении, а также прикладном программном обеспечении [6].

Big Data открывает большие возможности по обработке данных, которые до этого считались невозможным, применив данную концепцию в плоскости открытых данных позволить решить многие проблемы, например такие как актуальность, достоверность, а также структурировать все открытые данные в одном месте для дальнейшего их использования.

Список используемых источников

1. Котенко И. В., Ушаков И. А. Методики поиска инсайдеров в компьютерных сетях на основе технологий больших данных // 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. 501–506.
2. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика : материалы XV международной науч. конф., Санкт-Петербург, 26–28 окт. 2016 г. С. 168–169. URL: http://spoisu.ru/files/ri/ri2016/ri2016_materials.pdf (дата обращения 25.01.2019).
3. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств elastic stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.
4. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events // IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017.
5. Красов А. В., Ушаков И. А. Подготовка специалистов в области информационной безопасности в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича // Инновации. 2013. № 7 (177). С. 92–97.
6. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности : учебное пособие, Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». Санкт-Петербург, 2012. 396 с.

УДК 004.7
ГРНТИ 49.33.29

УЯЗВИМОСТИ ПРОГРАММНО-ОПРЕДЕЛЯЕМЫХ СЕТЕЙ

В. Н. Волкогонов, А. И. Преображенский, И. А. Ушаков

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

SDN – архитектура, которая разделяет функцию управления, определяющую направление сетевого трафика, и функцию данных, которая передает трафик в необходимое место. В SDN-сетях основные функции маршрутизаторов и коммутаторов перенесены на центральный сетевой контроллер, что значительно упрощает мониторинг состояния сети и применение сетевых политик. Благодаря централизованной системе управления, SDN обладает огромным потенциалом и рядом серьёзных преимуществ перед традиционной сетевой архитектуре, которые предоставляют более эффективные

способы противодействия сетевым угрозам. В работе описана архитектура SDN и протокол OpenFlow, а также приводятся потенциальные угрозы SDN-сетей с точки зрения информационной безопасности.

SDN, программно-определяемая сеть, уязвимости, Openflow, контроллер.

Современные сетевые системы часто обновляются из-за постоянных изменений в стандартах связи, повышений требований к стандартам безопасности и к качеству обслуживания. В традиционных сетях этапы перехода требуют больших затрат не только денежных средств, но и времени. При внедрении новых глобальных сетевых политик приходится заменять оборудование, которое еще может быть пригодно для работы, но не поддерживает новые стандарты. Кроме того, приходится отдельно переконфигурировать каждое устройство, что может привести к рискам ошибочной конфигурации [1].

В SDN-сетях (*Software Defined Networking*) основные функции маршрутизатора и коммутатора перенесены на центральный контроллер, с помощью которого значительно упрощается мониторинг сети и применение новых политик.

Архитектура SDN, предполагает совершенной иной способ к реализации сетевой инфраструктуры, которая, с точки зрения информационной безопасности, не лишена потенциальных угроз.

Архитектура программно-конфигурируемой сети состоит из четырёх основных принципов [2]:

– плоскость управления и передачи трафика разделены. Сетевое оборудование становится простым устройством для пересылки информации;
– передача данных основываются на потоках, а не на адресе назначения;
– для передающих устройств, контроллер SDN является внешним объектом;
– центральных сетевой контроллер взаимодействует с сетевым оборудованием, позволяет с помощью программирования контролировать сетевой инфраструктурой. Это фундаментальное свойство SDN, что и является его основным преимуществом перед традиционной сетевой архитектурой [3].

Программно-конфигурируемые сети представляют ряд возможностей для управления сетевой инфраструктурой и обеспечения информационной безопасности. Сочетание централизованной точки управления и программируемой сети позволяет модифицировать современные сетевые устройства и систему сетевой безопасности, увеличив их возможности и повысив общую производительность (рис. 1, см. ниже).

OpenFlow считается одним из первых стандартов программно-определяемых сетей. Первоначально он определил протокол связи в среде SDN,

который позволяет контроллеру SDN напрямую взаимодействовать с сетевыми устройствами, такими как коммутаторы и маршрутизаторы, как физические, так и виртуальные, поэтому он может лучше адаптироваться к изменяющимся требованиям [4]. Для работы в среде OpenFlow любое устройство, которое хочет установить связь с контроллером SDN, должно поддерживать данный протокол. Через этот интерфейс контроллер SDN вносит изменения в таблицу потоков коммутатора/маршрутизатора, позволяя сетевым администраторам разделять трафик, управлять потоками для обеспечения оптимальной производительности и начинать тестирование новых конфигураций и приложений.

Рис. 1. Сравнение традиционной сети и SDN-сети

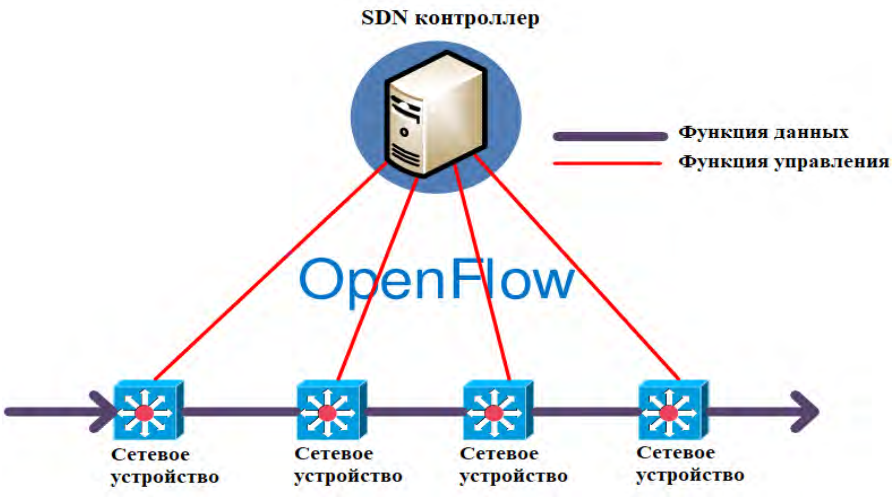


Рис. 2. OpenFlow – протокол управления процессом обработки данных

Для сетевых устройств, функционирующих по архитектуре программно-конфигурируемой сети, ключевыми угрозами являются разновидность таких атак, как «отказ в обслуживании», подмена контроллера и т. д. Основной для множества атак становится центральный сетевой контроллер, из-за переноса на него «аналитической» составляющей сети. Вместо сетевых устройств целью большинства атак становятся контроллер сети и сетевые приложения, через которые обращаются к контроллеру. Атаки типа «отказ в обслуживании» являются одними из самых примитивных и одновременно эффективных способов нарушения работы сети SDN. Угроза безопасности следует из алгоритма работы SDN-коммутатора. При получении пакета, который не походит под текущие правила flow таблицы, он может направить полностью пакет на контроллер для анализа или сохранить пакет в памяти коммутатора, а на контроллер отправить только заголовки [5].

Для атакующих, данные методы предоставляют обширные возможности для реализации отказа в обслуживании с помощью формирования потока пакетов в SDN-сети. Опираясь на эти алгоритмы можно предугадать действия SDN-сети в подобных ситуациях.

– Коммутатор будет передавать большое количество неизвестного трафика на контроллер для анализа. Из-за чего будут расходоваться процессорные ресурсы коммутатора. Если коммутатор будет передавать только заголовки на контроллер, тогда расход процессорных ресурсов снизится, однако значительно возрастет расходование памяти коммутатора, если он будет буферизировать весь неизвестный трафик [6].

– Поток трафика от коммутатора до контроллера будет нагружать канал связи. Снижение скорости доставки сообщения может сказаться на всех коммутаторах. На канал связи будет оказано повышенное воздействие, если коммутатор начнет пересылать пакет целиком.

– Контроллер начинает принимать и анализировать поток неизвестного трафика, расходуя процессорное время и память, формируя очередь, снижая при этом общую скорость сетевых решений.

– Контроллер будет генерировать ответные сообщения на запросы от атакованного коммутатора, нагружая канал связи [7].

Начав выполнять команды, полученное от контроллера, коммутатор будет нагружать собственный процессор и память. Если в командах будет содержать новые правила, то проверка нового потока на коммутаторе будет занимать значительно больше времени, т.к. таблица потоков значительно увеличится. А также возможно переполнение таблицы.

В результате, подобная, атака может привести к следующим последствиям:

– Перегрузка процессора и памяти коммутатора. Медленная обработка легитимных пакетов, в худшем случае они будут полностью отбрасываться.

– Перегруженность канала связи приведёт к медленной доставке потоков, данных через задействованные узлы связи.

– Перезагрузка центрального контроллера сети из-за обработка управляющих легитимных сообщений будет невозможна.

Определение сетевых служб и сканирование портов – актуальные угрозы безопасности большинства информационных систем. Данные уязвимости для SDN-сети являются критическими из-за уязвимости OpenFlow и наличия немалого количества трафика управления.

Не стоит забывать и про уязвимость систем с централизованными управления к DoS/DDoS-атакам.

Высокий уровень лабильности протокола OpenFlow, также является его уязвимостью к атакам подмены [8]. Протокол позволяет взаимодействовать между коммутатором и контроллером на базе протокола TCP без использования шифрования, а поддержка протокола TLS не является обязательной для реализации.

Архитектура SDN кардинально изменяет представление о структуре сети, следовательно, появляются новые уязвимости, вызванные фундаментальными особенностями сети. Кроме того, большинство угроз актуальных для традиционных сетей имеют место быть в той или иной степени для SDN-сетей. Не стоит забывать и о том, какие преимущества предоставляет SDN архитектура для развития инструментов безопасности. Централизованное управление и программируемые сети в совокупности позволяют повысить эффективность всех сетевых структур, начиная от применения новых конфигураций, заканчивая повышением эффективности средств обеспечения безопасности сети.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности : учебное пособие, Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». Санкт-Петербург, 2012. 396 с.

2. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция : сб. науч. ст. 2016. С. 348.

3. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

4. Уильям Столлингс. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Part II, 2015.

5. K. Calvert, S. Bhattacharjee, E. Zegura, and J. Sterbenz. Directions in Active Networks // IEEE Communications magazine, p. 72–78, October 1998.

6. OpenFlow Switch Specification Ver 1.5.1, 2016 [24.01.2019]. URL: https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf
7. В поисках идеальной сети: OpenFlow и все-все-все [24.01.2019]. URL: https://habr.com/ru/company/performix/blog/224211/
8. Сетевые технологии SDN – Software Defined Networking [24.01.2019]. URL: https://habr.com/ru/company/muk/blog/251959/

УДК 519.87
ГРНТИ 10.19.61

МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНИЗАЦИИ

В. А. Волостных[1], Ю. В. Гвоздев[2], В. В. Карганов[1]

[1]Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

При создании и модернизации информационных систем требуется оценка их эффективности. Одним из важнейших показателей эффективности информационных систем организации является защищенность обрабатываемой информации и защищенность системы от потенциальных воздействий, что и определяет необходимость моделирования информационных систем функционирующих в условиях угроз безопасности. К числу важнейших этапов, определяющих успех моделирования, относятся выбор показателей оценки эффективности информационных систем. В статье рассматриваются подходы к выбору показателей и критериев оценки эффективности информационных систем организаций, а также подходы к построению математической модели информационной системы организации, функционирующей в кризисной ситуации.

информационная безопасность, информационная система, моделирование, показатели оценки эффективности.

В современных условиях очень остро стоит вопрос обеспечения информационной безопасности (ИБ) как на уровне государства, так и на уровне отдельных организаций и предприятий [1, 2]. Под ИБ организации понимается состояние защищенности интересов организации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств ИБ – конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации [2]. Приоритетность свойств ИБ определяется значимостью информационных активов для интересов организации.

Для оценки уровня ИБ и выявления уязвимостей системы защиты информационной системы (ИС) специалисты организаций нередко прибегают к моделированию ИС, функционирующих в условиях воздействия угроз ИБ организаций. Под ИС принято понимать совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств, а под угрозой ИБ организации понимается совокупность факторов и условий, создающих опасность нарушения ИБ организации, вызывающих или способных вызвать негативные последствия (ущерб/вред) для организации [2].

Моделирование – один из наиболее распространенных способов изучения различных процессов и явлений. К несомненным достоинствам оценки уровня ИБ организации путем создания модели ИС относится возможность проведения исследований без прекращения функционирования действующей ИС организации, и чем сложнее и масштабнее система, тем значительнее выигрыш. Однако процесс моделирования ИС, по мнению авторов, иногда может вызвать затруднения. В соответствии с [3, 4] основными этапами этого процесса могут быть:

определение цели исследования (моделирования);

сбор (получение) исходных данных об ИС организации и системе обеспечения ИБ;

определение показателей функционирования ИС;

определение критериев оценки функционирования ИС;

выбор вида модели ИС;

разработка модели ИС;

использование модели ИС;

интерпретация и анализ результатов моделирования ИС;

практическое использование результатов моделирования ИС.

Поскольку цель исследования сформулирована в начальной части статьи, то перейдем к рассмотрению второго этапа. Предлагается сбор исходных данных производить группе исследователей, в состав которых несомненно должны входить ведущие специалисты подразделений, создававших и эксплуатирующих ИС, а также специалисты подразделений обеспечения защиты информации и аналитики. Метод сбора данных – в форме обследования ИС. По результатам обследования может составляться акт, с текстовыми и графическими приложениями, отражающими структуру и топологию ИС, технические и эксплуатационные характеристики средств обработки информации и средств защиты информации, но основное внимание необходимо обратить на информационные ресурсы организации и требования по обеспечению их безопасности.

Важным этапом исследования является выбор показателя уровня обеспечения ИБ организации, показателя, определяющего эффективность функционирования ИС в условиях реализации потенциальных угроз [4].

Известно, что под показателем эффективности сложных систем понимается такая числовая характеристика системы, которая характеризует степень приспособленности системы к выполнению поставленных перед ней задач. При выборе показателя исходят из того, что он должен объективно характеризовать систему, иметь прямую связь с ее целевым назначением, быть чувствительным к изменению основных параметров и, наконец, должен быть достаточно простым, иметь понятный физический смысл, быть удобным для вычисления, анализа и отображения в виде таблиц и графиков [3, 5]. При исследовании сложных систем, к которым без сомнения относятся ИС организаций, необходимо составить графическую модель, отображающую информационные процессы в организации с указанием требований, предъявляемых руководством организации к информационным ресурсам и информационным процессам. Далее целесообразно определить характер деятельности организации и на основе этого выделить целевую функцию. Для коммерческих организаций это может быть прибыль, для образовательных организаций уровень знаний выпускников и т.д., после чего формулируется основной (обобщенный) показатель, исходя из вышеизложенных требований.

При определении критерия ИБ надо описать численное значение показателя, при котором обеспечивается требуемый уровень эффективности функционирования организации (например, уровень снижения производительности труда или уровень снижения прибыли при реализации потенциальных угроз ИБ организации). Поскольку выбор показателя и критерия оценки ИБ является одним из важнейших этапов исследований, то на этом этапе в группу исследователей необходимо включать профильных ведущих специалистов организации.

Очевидно, что основным видом модели ИС функционирующей в условиях воздействий является математическая модель. Поскольку ИС крупной организации является сложной системой, то создать аналитическую модель достаточно проблематично. Более реальным вариантом является статистическая модель, тем более что, исследуемые процессы носят вероятностный характер. Наиболее предпочтительным вариантом создания модели ИС для исследования характеристик ИБ организации авторы считают статистическую модель с элементами аналитических выражений.

На этапе создания модели целесообразно выявить все подсистемы ИС организации и описать в количественных значениях их характеристики для стационарного режима. Далее наступает самый ответственный этап формирование модели угроз ИБ. Модель угроз безопасности информации это физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [2]. Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ Модель угроз ФСТЭК

России. При этом необходимо описать модель нарушителя ИБ организации. Нарушитель ИБ организации: физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение ИБ организации. Условием реализации угрозы безопасности информации, обрабатываемой в ИС, может быть недостаток или слабое место в системе защиты ИС – уязвимость ИС. Вероятность реализации угрозы и возможный ущерб интересам организации целесообразно определять методом экспертных оценок. Целесообразно применять метод Дельфи [3].

При расчете основного показателя, характеризующего потери организации, предлагается следующий подход. Поскольку угрозы воздействуя на ИС организации, приводят к нарушению управленческого цикла путем задержки документированной и недокументированной информации между субъектами и объектами управления на время ($t_{зад}$), то временные показатели можно положить в основу при расчете экономических эффектов, тогда критерием оценок может служить подход в оценке своевременности управленческих решений и связанных с этим производственных (образовательных или других) процессов. В этом случае уровень обеспечения ИБ коммерческой организации можно отобразить выражением:

$$Y_{иб} = \frac{S_0 - S_y}{S_0},$$

где $Y_{иб}$ – уровень обеспечения ИБ; S_0 – прибыль организации при функционировании ИС в стационарном состоянии без воздействия угроз; S_y – прибыль организации при реализации угроз.

В целях определения абсолютного значения экономических потерь $S_п$ можно использовать обобщенное выражение:

$$S_п = S_0 - S_y,$$

где $S_п$ – абсолютное значение экономических потерь.

Поскольку спектр угроз безопасности ИС достаточно широк, и последствия реализации угроз могут быть как восстанавливаемые путем замены оборудования или отдельных средств ИС (прямые экономические потери), так и путем восстановления программного обеспечения (опосредованные потери), которые можно вычислить через заработную плату работников служб безопасности, работников управленческого аппарата [4, 6]. Кроме того, необходимо учитывать убытки, связанные с невыполнением или срывом договорных обязательств. Тогда $S_п$ можно определить выражением:

$$S_п = \sum_{i=1}^{m} S_{i\text{тех}} + \sum_{j=1}^{n}\left(S_{\text{зпл}j} * t_{\text{раб}}\right) + \sum_{l=1}^{k} S_{l\text{дог}},$$

где $S_{i\text{тех}}$ – стоимость i-го образца техники для замены вышедших из строя элементов ИС; $S_{\text{зпл}j}$ – заработная плата работников, участвующих в восстановлении ИС в единицу времени; $t_{\text{раб}}$ – время восстановления ИС; $S_{l\text{дог}}$ – стоимость штрафных санкций за срыв договорных условий.

Поскольку ИС организации состоит из широкого спектра подсистем, то скорее всего, некоторые подсистемы прямого влияния на основной показатель не оказывают, но нарушение порядка их функционирования может нарушить одно из важнейших требований к информации, а именно конфиденциальность, поэтому в модель необходимо вводить некоторые ограничения или вводить дополнительные показатели состояния ИБ ИС организации. В ряде случаев убытки предприятия при нарушении конфиденциальности некоторой информации можно учесть через штрафные санкции (например, за нарушение законодательства о персональных данных).

По результатам моделирования воздействий на ИС различных угроз необходимо определить вклад каждой подсистемы ИС в эффективность функционирования организации по основному показателю. Однако, основной показатель может не обладать чувствительностью, поэтому далее необходимо провести декомпозицию ИС и проводить исследования каждой подсистемы, выявляя уязвимости в них и апробируя те или иные организационные и технические меры защиты ИС и/или самой информации. В этих целях вырабатываются дополнительные (частные) показатели, которые позволят более детально провести анализ ИС [4]. При определении дополнительного показателя необходимо исходить из основного назначения данной информационной подсистемы и обрабатываемых ею информационных ресурсов.

В процессе исследований систем можно вводить ограничения на учет каких-либо факторов, если они не влияют на результат исследований.

Рассмотренный подход к моделированию ИС, безусловно, носит лишь концептуальный характер, поэтому авторы будут развивать и детализировать изложенные в статье предложения, доводя их до конкретных алгоритмов.

Список используемых источников

1. Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. М. : Изд-во стандартов, 2009.

3. Вентцель Е. С. Исследование операций. М. : Советское радио, 1972. 552 с.

4. Карганов В. В., Пилявец О. Г., Парфиров В. А., Шевченко А. А. Моделирование процесса распространения сложных сигналов на объектах автоматизации в интересах обеспечения информационной безопасности // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019. № 1–2 (127–128). С. 63–68.

5. Бусленко Н. П. Исследование сложных систем. Главная редакция физико-математической литературы издательства. М. : Наука, 1978.

6. Батов В. Ю., Драчев В. О., Карганов В. В. Обеспечение информационной безопасности при проведении научных исследований в организациях // Национальная безопасность России: актуальные аспекты. Всероссийская научно-практическая конференция : сб. ст. 2018. С. 6–18.

УДК 65.012.8
ГРНТИ 10.19.61

АНАЛИЗ НОРМАТИВНЫХ ПРАВОВЫХ ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

В. А. Волостных, Ю. В. Гвоздев, П. А. Кононов

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

Важнейшим фактором обеспечения безопасности организации является обеспечение информационной безопасности. Обеспечение информационной безопасности определяется рядом нормативных правовых документов. Основным документом является Доктрина информационной безопасности Российской Федерации, утвержденная Президентом РФ в 2016 году. Одним из факторов обеспечения информационной безопасности организации является защита информации и информационных систем от возможных угроз. В статье рассмотрены нормативные правовые и руководящие документы, регламентирующие порядок обеспечения информационной безопасности в организациях.

информационная безопасность, защита информации, законодательство Российской Федерации.

Обеспечение информационной безопасности – весьма важный аспект деятельности любой организации. В данной статье рассматривается классификация нормативной правовой базы в области информационной безопасности и динамика изменений законодательства о защите информации.

Правовую основу обеспечения безопасности составляет Конституция Российской Федерации, как основной закон государства, нормативно-правовой акт, имеющий высшую юридическую силу, принятый 12 декабря 1993 года.

Базовым законом в области защиты жизненно важных интересов государства является закон РФ «О безопасности», принятый 5 марта 1992 г. На сегодняшний день данный закон утратил силу и ему на смену пришел

новый Федеральный закон «О безопасности», утвержденный 28 декабря 2010 года № 390-ФЗ.

Базовым документом, определяющим политику информационной безопасности в России, и юридически закрепляющим понятие информационной безопасности является Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Данный документ пришел на смену Доктрине информационной безопасности, действовавшей в России с 2000 года. В Доктрине под информационной безопасностью Российской Федерации понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [1].

Согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» под информационной безопасностью организации понимается состояние защищенности интересов организации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности - конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации [2].

Основополагающим среди российских законов, посвященных вопросам обработки и защиты информации, следует считать закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года №149-ФЗ. В нем даются основные определения и намечаются направления развития законодательства в данной области.

Со дня вступления в силу данного Федерального закона признаны утратившими силу Федеральный закон от 20 февраля 1995 г. «Об информации, информатизации и защите информации» и ряд других законодательных актов.

Законодательство Российской Федерации в области информационной безопасности состоит из ряда групп нормативных правовых документов. К ним относятся законодательство о государственной тайне, законодательство об информации конфиденциального характера, включающее в себя законодательство о персональных данных, об информации ограниченного распространения, законодательство о коммерческой тайне и т. д. Указанные

группы документов могут включать в себя федеральный закон, постановление(я) Правительства РФ, Указ(ы) Президента РФ, решение(я) МВК по защите государственной тайны, приказы Роскомнадзора, ФСБ и ФСТЭК России, государственные (национальные) стандарты и ведомственные документы, а также документы организации.

Законодательство Российской Федерации о государственной тайне регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности. Базовым документом является закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне». Положения закона отражают практическую деятельность по защите сведений, составляющих государственную тайну. Нормативными правовыми документами по защите государственной тайны являются:

– Постановление Правительства РФ № 3-1 от 5.01.2004 года;

– Постановление Правительства РФ от 06.02.2010 N 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне»;

– Перечень сведений, отнесенных к государственной тайне (утвержден Указом Президента РФ от 30 ноября 1995 г. № 1203);

– Постановление Правительства РФ от 15.04.1995 N 333 «О лицензировании деятельности предприятий…»;

– Постановление Правительства РФ № 870 от 04.09.1995 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;

– Постановление Правительства РФ от 26.06.1995 N 608 «О сертификации средств защиты информации»;

– Руководящие документы ФСБ и ФСТЭК России.

Законодательство о персональных данных также состоит из множества нормативных актов, однако оно очень молодо, а, следовательно, далеко не полно. 19 декабря 2005 г. был принят федеральный закон № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных». Одновременно с этим был принят федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». ФЗ № 152 определяет основные понятия, принципы и условия обработки ПДн, устанавливает права и обязанности Субъекта и Оператора, а также меры по обеспечению безопасности персональных данных при их обработке. На сегодняшний день существует ряд нормативных актов, развивающих положения ФЗ №152. К ним относятся:

– Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России 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»;

– иные нормативные правовые акты.

Законодательство о коммерческой тайне также не стоит на месте. В федеральный закон № 98-ФЗ «О коммерческой тайне» периодически вносятся изменения и бизнес-процессы регулярно подвергаются изменениям, а значит и перечень сведений, представляющих коммерческую ценность, также изменяется.

Данные о динамике изменения законодательства РФ в области информационной безопасности приведены в таблице.

ТАБЛИЦА. Динамика изменения законодательства РФ в области информационной безопасности

Нормативные акты / Периоды времени	1995–2000	2001–2005	2006–2010	2011–2015	2016–н/в
Указ Президента РФ 1995 № 1203	1	4	10	10	12
Постановление Правительства РФ 1994 № 1233	–	–	–	1	2
Закон1993 № 5485-1	1	4	4	5	2
ФЗ 2006 № 149	–	–	1	16	16
ФЗ 2006 № 152	–	–	7	8	5
ФЗ 2004 № 98	–	–	3	2	1

Таким образом, очевидно следующее, что динамично изменяющееся законодательство РФ в области информационной безопасности, необходимость его постоянного отслеживания требует квалифицированных кадров по обеспечению защиты информации, а также внесения соответствующих корректив в систему защиты организации.

Не стоит забывать и о нормативно-правовых актах, устанавливающих различные виды ответственности за нарушение требований законодательства в области информационной безопасности. К таким актам относятся Уголовный кодекс РФ, Трудовой кодекс РФ, Гражданско-правовой кодекс, Кодекс об административных правонарушениях.

Законодательством РФ не установлен комплект нормативных локальных документов по защите государственной тайны, персональных данных, конфиденциальной информации, которые должна разрабатывать организация. Единственным условиям является то, что они должны быть необходимыми и достаточными для выполнения обязанностей, предусмотренных законодательством.

Примерное количество локальных актов в организации по защите государственной тайне может составлять 30–35 ед., по защите персональных данных – 30–40 ед., по защите конфиденциальной информации – 10–15 ед.

При изменении законодательства РФ принимать новые локальные акты не требуется, а следует вносить коррективы в уже существующие.

Таким образом, анализ нормативных правовых документов в сфере обеспечения информационной безопасности позволяет сделать следующие выводы:

1. Нормативно-правовая база в области информационной безопасности представляет собой обширные группы документов различного уровня.

2. Нормативно-правовая база в области информационной безопасности регулярно обновляется и совершенствуется.

3. Изменения в нормативной правовой базе государства влечет за собой необходимость внесения соответствующих изменений в локальные акты организаций.

4. В связи с изложенным, считается необходимым систематическая переподготовка персонала, обеспечивающего информационную безопасность организации.

5. Целесообразно в положение о подразделении по защите информации (информационной безопасности) и в должностных инструкциях персонала этих подразделений внести пункт: мониторинг и анализ нормативных правовых документов в сфере обеспечения информационной безопасности.

Список используемых источников

1. Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

2. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: ввод в действие с 01.10.2009. М. : Изд-во стандартов, 2009.

3. Малюк А. А, Горбатов В. С., Королев В. И. и др. Введение в информационную безопасность: учебное пособие для вузов // Под ред. В. С. Горбатова. М. : Горячая линия – Телеком, 2011. 288 с.

4. Новиков В. К., Галушкин И. Б., Аксенов С. В. Информационная безопасность и защита информации. Организационно-правовые основы // Под ред. В. К. Новикова. М. : Горячая линия – Телеком, 2017. 312 с.

УДК 65.012.8
ГРНТИ 10.19.61

АНАЛИЗ СТРУКТУРЫ РУКОВОДСТВА ЗАЩИТОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

В. А. Волостных, Ю. В. Гвоздев, П. А. Кононов

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

Проблема обеспечения безопасности персональных данных в высших учебных заведениях является актуальной на сегодняшний день. В связи с большим объемом обрабатываемых персональных данных, высокими темпами роста информатизации образования и увеличения потенциальных угроз безопасности персональных данных, обеспечение безопасности персональных данных должно строиться на основе комплексного подхода. Обеспечение защиты персональных данных определяется рядом нормативных правовых документов. Основным документом является Федеральный закон № 152-ФЗ от 27.07.2006 г. «О персональных данных». В данной статье проведен анализ структуры руководства защитой персональных данных в высших учебных заведениях.

защита информации, персональные данные, обработка персональных данных.

На сегодняшний день в высших учебных заведениях (вузах) обрабатывается огромное количество информации, отнесенной к персональным данным (ПДн). Персональные данные обучающихся, работников, абитуриентов, посетителей и других категорий субъектов ПДн обрабатываются как автоматизированным способом, так и неавтоматизированным. Основным законом, регламентирующим порядок обработки и защиты персональных данных, является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [1].

Проанализировав закон, становиться понятно, что вузы являются операторами ПДн и соответственно, на них распространяется действие закона № 152-ФЗ.

Соблюдение требований законодательства при обработке ПДн для вузов является сложным, трудоемким и затратным процессом. Ненадлежащее исполнение требований законодательства может обернуться значительными негативными последствиями, как для самих вузов, так и для физических лиц, чьи данные обрабатываются.

При этом необходимо учитывать, что вузы обладают рядом особенностей, таких как публичность, постоянно меняющаяся аудитория, территори-

альная рассредоточенность ресурсов, использование современных информационных технологий. Основная проблема по обеспечению защиты ПДн в вузах – это значительное отличие процессов, ресурсов и характера информационных потоков, характерных для типовой организации [2].

Для того чтобы выполнить требования закона, оператору необходимо определить перечень ПДн, которые обрабатываются в вузе и в каких структурных подразделениях ведется обработка. Для построения эффективной системы защиты персональных данных в организации должна быть налажена структура управления процессами обработки персональных данных.

На рис. выделены структурные единицы, где ведется обработка ПДн обучающихся, работников, посетителей, абитуриентов в вузе и показана структура руководства защитой персональных данных.

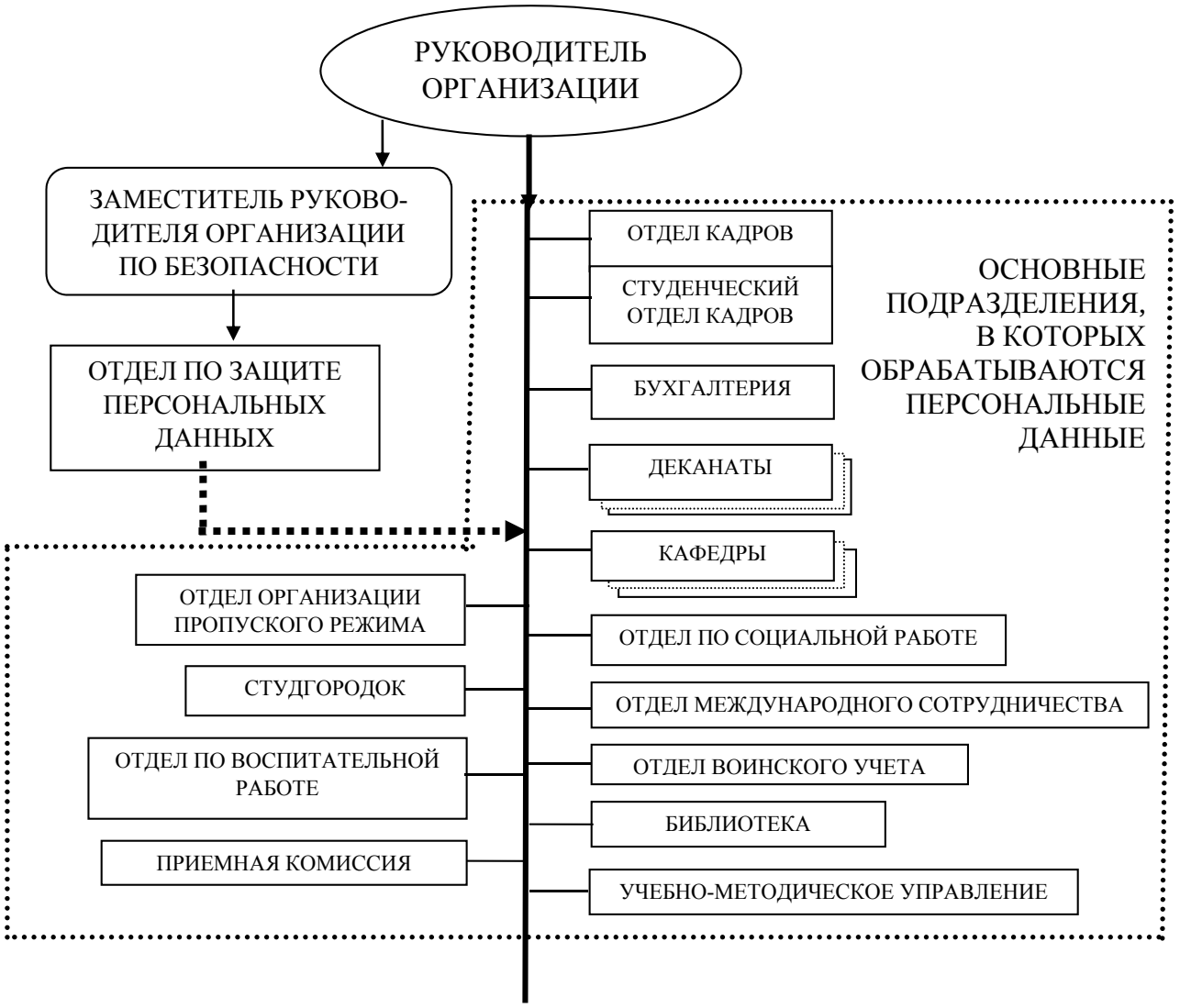


Рисунок. Структура руководства защитой персональных данных

Руководство деятельностью вуза осуществляется ректором. В обязанности ректора входит утверждение локальных нормативных документов, издание приказов, касающихся вопросов обеспечения безопасности персональных данных.

У ректора вуза может быть заместитель по безопасности, который может назначаться ответственным за организацию обработки персональных данных.

Общее руководство деятельностью структурных подразделений, в которых ведется обработка персональных данных, осуществляет ректор вуза.

Ориентировочное число структурных подразделений вуза, в которых обрабатываются персональные данные субъектов, составляет примерно 15 структурных подразделений.

Перечень лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ, утверждается приказом ректора и составляет примерно 400 человек. Также приказом или распоряжением в структурных подразделениях вуза, в которых обрабатываются персональные данные, должны быть назначены лица, ответственные за сохранность материальных носителей персональных данных, и ответственные за помещения, в которых ведется обработка персональных данных.

Под автоматизированной обработкой персональных данных понимается их обработка при помощи средств вычислительной техники (СВТ). Количество СВТ, применяемых для обработки персональных данных в вузе, составляет ориентировочно 100 шт.

ВУЗ осуществляет обработку персональных данных следующих категорий субъектов:

– обучающихся – 1500 субъектов;
– абитуриентов – 700 субъектов;
– работников – 700 субъектов;
– посетителей – 1000 субъектов ежегодно.

Вопрос обеспечения защиты ПДн в вузе не столь однозначен, как это кажется на первый взгляд. Нетиповая структура, открытость для посетителей, большой круг пользователей внутри вуза не позволяют однозначно формализовать процессы, протекающие в нем. И для выполнения требований закона первоочередной задачей оператора является определение перечня ПДн обрабатывающихся в системе и с какими образовательными и трудовыми процессами вуза связана обработка ПДн [3].

К основным проблемам, с которыми сталкиваются должностные лица вуза при организации обработки персональных данных, можно отнести:

– большой объем обрабатываемых персональных данных различных категорий;

– необходимость существенного финансирования работ, связанных с технической защитой информационных систем персональных данных (ИСПДн);

– территориальная рассредоточенность ресурсов ИСПДн;

– выход многих ИСПДн в сеть общего пользования (Интернет).

В современном вузе хранятся и обрабатываются большие объемы бумажных документов с персональными данными, съемные носители с персональные данными, встроенные в ПЭВМ носители с персональными данными и в связи с этим, проблема соответствия требованиям по обработке персональных данных и обеспечению их безопасности в вузе становится стандартной проблемой.

В связи с вышеизложенным, в вузе может быть создан отдел по защите персональных данных, который может подчиняться заместителю руководителя по безопасности. Данный отдел может осуществлять свою деятельность во взаимодействии с другими структурными подразделениями вуза, а также в пределах своей компетенции со сторонними организациями. На него могут быть возложены функции обеспечения безопасности персональных данных в вузе с использованием правовых, организационных и технических мер, необходимых и достаточных для обеспечения обязанностей, предусмотренных ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» [4].

Таким образом, анализ структуры руководства защитой персональных данных в вузе позволяет сделать следующие выводы:

1. Нормативно-правовая база, регламентирующая обработку и защиту персональных данных в высшем учебном заведении, представляет собой многообразие документов различного уровня.

2. Ответственным за организацию обработки персональных данных может быть назначен один из заместителей руководителя организации – проректор. Если в вузе есть должность проректора по безопасности, то целесообразно эти обязанности возложить на него.

3. Большой объем обрабатываемых персональных данных, динамично меняющаяся аудитория вуза, высокий темп роста информатизации образования приводит к тому, что в вузах предлагается создавать отдел (группу) по защите персональных данных.

4. На основе практического опыта ряда технических вузов предлагается возлагать на отдел по защите персональных данных следующие задачи:

– анализ нормативных правовых документов по обеспечению защиты персональных данных;

– анализ информационных систем персональных данных (ИСПДн), в которых обрабатываются персональные данные;

– разработка правовых, организационных и технических мероприятий по обеспечению безопасности персональных данных;

– оформление и доведение руководящих и методических документов по обеспечению безопасности персональных данных в вузе и его подразделениях;

– обучение должностных лиц, непосредственно обрабатывающих персональные данные, приемам и способам обработки персональных данных соответствующим законодательным актам РФ и локальным актам вуза;

– осуществление внутреннего контроля и аудита соответствия обработки персональных данных законодательству РФ.

5. Для качественного выполнения законодательства РФ необходимо обеспечить систематическое повышение квалификации персонала, обеспечивающего безопасность персональных данных в вузе.

Список используемых источников

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Волостных В. А., Штеренберг С. И., Гвоздев Ю. В. Проблемы обеспечения безопасности персональных данных в высших учебных заведениях // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 134–141.

3. Малюк А. А, Горбатов В. С., Королев В. И. и др. Введение в информационную безопасность: учебное пособие для вузов // Под ред. В. С. Горбатова. М. : Горячая линия – Телеком, 2011. 288 с

4. Новиков В. К., Галушкин И. Б., Аксенов С. В. Информационная безопасность и защита информации. Организационно-правовые основы // Под ред. В. К. Новикова. М. : Горячая линия – Телеком, 2017. 312 с.

УДК 65.011.56
ГРНТИ 50.01.85

ПРЕДОСТАВЛЕНИЕ УСЛУГ НА БАЗЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В СЕТЯХ NGN/IP

М. Ю. Волщуков, Д. С. Ковярова

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

В настоящий период времени информационные технологии стали консолидировать большое количество различных информационных систем. Они становятся взаимопроникающими, в связи с этим появляются новые возможности. Предоставление услуг потребителям является одной из актуальнейших задач в мире информационных технологий.

С появлением большого количества разнообразных систем, сервисов и технологий возникает проблема их взаимодействия, интеграции и использования. Оптимизировать информационные ресурсы и более гибко ими управлять позволяют разнообразные технологии, в частности на сегодняшний день для решения подобных задач широко используется технология облачных вычислений.

облачные вычисления, сетевая инфраструктура, технология, NGN/IP, гетерогенная среда, информационная система, ИТ.

На сегодняшний день информационные технологии объединяют все больше и больше разнообразных ИТ-систем [1]. Они становятся взаимопроникающими, предоставляя за счет этого новые возможности. Передача данных в сетях с распределенной архитектурой и предоставление услуг потребителям является одной из актуальнейших задач в мире ИТ-технологий.

Развитие информационных технологий привело к ситуации, когда конкретная информационная система становится похожей на многомерные пазлы. Чтобы они совпали, должны быть соблюдены разнообразные требования: интерфейсы на уровне «железа», «состава данных», «программного обеспечения», правила обмена, физическая совместимость и т. д. и т. п.

Одним из необходимых требований к информационным системам становится поддержка ее функционирования в гетерогенной сетевой инфраструктуре.

Данное требование необходимо учитывать на всех уровнях формирования потребностей пользователей в различных сервисах и оценки совместного функционирования в целом всех частей инфотелекомуникационных систем, проектирования ИТ-инфраструктуры, функционирования процессов обработки, хранения, передачи данных, оптимизации ИТ-ресурсов [1]. С появлением большого количества разнообразных сервисов потребителю становится трудно в них ориентироваться.

Оптимизировать ИТ-ресурсы и более гибко ими управлять позволит технология облачных вычислений [2].

Первые идеи об использовании вычислений как публичной услуги были предложены еще в 1960-х известным ученым в области информационных технологий, изобретателем языка Lisp, профессором MIT и Стэнфордского университета Джоном Маккарти. Появление первой технологии, близкой к современному пониманию термина «cloud computing», приписывается компании Salesforce.com, основанной в 1999 году. Именно тогда и появилось первое предложение нового вида b2b продукта «Программное обеспечение как сервис» (“*Software as a Service*”, “SaaS”).

Далее, история облачных вычислений продолжала развиваться, концепция постепенно выкристаллизовывалась, до тех пор, пока в 2006 года

компания Amazon не запустила платформу Amazon Web Service (AWS), модернизировав свои центры обработки данных, которые, как и большинство компьютерных инфраструктур, использовали лишь 10 % от их емкости.

Облачные вычисления (рис.1) стали результатом слияния большого количества технологий и направлений [2].

Рис. 1. Технологии, повлиявшие на облачные вычисления

Можно считать, что компания Amazon сыграла ключевую роль в открытии рынка облачных вычислений во всем мире, оптимизировав как собственные ресурсы, так и начав получать с ранее простаивавших ресурсов прибыль. Спустя всего несколько лет, в 2008 году, были анонсированы облачные платформы от Microsoft и Google, Windows Azure и Google App Engine соответственно. В 2010 году увидел свет первый выпуск платформы Windows Azure.

Согласно исследованиям iKS-Consulting по итогам 2019 года, рынок облачных услуг в России по сравнению с 2018 годом вырос на 25 % и достиг 68,4 млрд руб. 70 % рынка облачных услуг приходится на SaaS. Согласно оценке экспертов, в ближайшие годы рынок будет расти в среднем на 23 % в год и к 2022 году может достичь объема в 155 млрд руб. (рис. 2, см. ниже).

Настоящий вопрос актуализируется ввиду не устоявшихся требований и часто противоречивого понимания облачных технологий, используемых в различных областях человеческой деятельности.

В настоящее время у телекоммуникационных операторов возникает необходимость перехода на более высокий уровень предоставления услуг, внедрение новых сервисов в рамках острой конкуренции на рынке. Развитие различных сервисов требует улучшения сетей связи, а в частности, их транспортной инфраструктуры, подсистем коммутации, доступа и управления.

Именно эти причины послужили началу создания сетей следующего поколения или NGN (*Next Generation Networks*) [4]. Сети нового поколения дают оператором широкий круг возможностей предоставления клиентам мультимедийных услуг и конвергенции, фиксированной и мобильной, а также беспроводной и проводной связи.

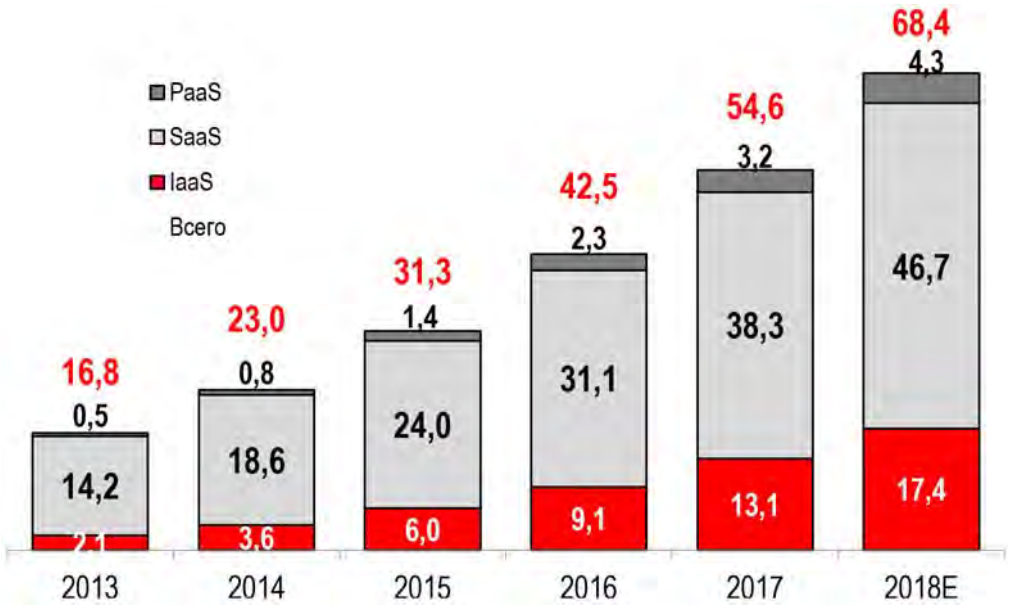


Рис. 2. Объем рынка облачных услуг в России по итогам 2013–2018 гг.

Использование технологии NGN/IP открывает множество вариантов реализации сервисов поверх стандартной транспортной среды – от интерактивного телевидения, VoIP до Web-служб. Сеть следующего поколения делает сервис доступным для потребителя вне зависимости от его местонахождения и используемых интерфейсов.

Сетевые операторы на данном этапе стремятся преобразовать существующую инфраструктуру в платформу, которая будет полностью основана на IP, то есть в NGN. Переход к единой мультисервисной транспортной среде для передачи трафика разного рода существенно облегчит предоставление услуг пользователям, снизит затраты и позволит функционировать новым сервисам.

Рассмотрим смоделированную архитектуру сети, с помощью которой будет осуществляться предоставление услуг (рис. 3, см. ниже).

Подводя итоги, можно сказать, что в данной статье описываются актуальные вопросы, связанные с оказанием услуг на базе гетерогенных сетей, со значимостью аспекта взаимосвязанного функционирования (интеграции) всех частей инфотелекомуникационных системы, а также внедрение новых технологий таких, как облачные вычисления и всех их компонентов [1].

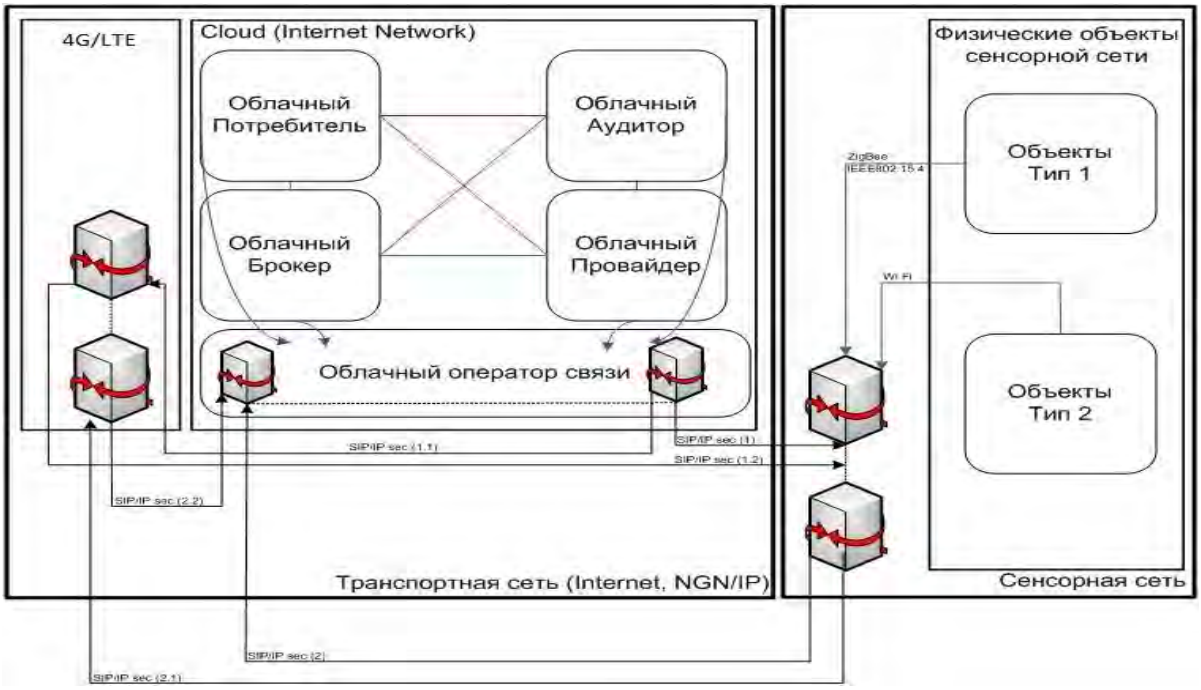


Рис. 3. Архитектура сети предоставления услуг на базе облачных вычислений с использованием NGN/IP

В данной статье представлены тенденции развития облачных вычислений, а также требования к стадиям реализации ИТ-решений в гетерогенной среде, обеспечивающие гарантированный результат сбора, хранения, обработки, передачи и представления данных в информационной системе, «живущей» в гетерогенной среде.

Список используемых источников

1. Волщуков М. Ю. Аспекты функционирования информационных систем в гетерогенной сетевой инфраструктуре // Информационные технологии и телекоммуникации. 2017. Т. 5. № 3. С. 23–29.

2. Гребнев Е. Облачные сервисы. Взгляд из России. М. : CNews, 2011. 282 с.

3. Объемы и прогнозы развития мирового рынка облачных вычислений. Журнал Мир Телекома. 2013. № 1. 60 с.

4. Макаренко С. И., Чаленко Н. Н., Крылов А. Г. Сети следующего поколения NGN // Систем управления, связи и безопасности. 2016. № 1. С. 81–101.

Статья представлена научным руководителем, кандидатом технических наук, доцентом А. Г. Владыко.

УДК 004.056.5
ГРНТИ 81.93.29

АНАЛИЗ УЯЗВИМОСТЕЙ УСТРОЙСТВ ВВОДА И СЧИТЫВАНИЯ ИДЕНТИФИКАЦИОННЫХ ПРИЗНАКОВ

Д. М. Воронцов, В. Д. Жмуров, И. Б. Паращук

Военная академия связи им. Маршала Советского Союза С. М. Буденного

Рассматриваются проблемы выбора устройств ввода и считывания идентификационных признаков и уязвимостей этих устройств в соответствии с предложенной классификацией.

устройство ввода идентификационных признаков, устройство считывания идентификационных признаков, уязвимость, классификация, контроль объекта, несанкционированный доступ, ограниченный доступ.

Прогресс в области применения информационных технологий сопровождается повышением требований к стабильности функционирования информационных систем и устойчивости при попытках нарушения их безопасности. Благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества информационных систем, а также контроля и управления различными объектами. К таким объектам (критическим) можно отнести информационно-телекоммуникационные системы специального назначения, банковские системы, атомные станции, системы управления воздушным и наземным транспортом, а также системы обработки и хранения сведений, составляющих государственную тайну. Для нормального и безопасного функционирования подобных систем необходимо поддерживать их безопасность и целостность [1].

В наше время ограничить доступ к критическим объектам и обезопасить их от саботажа с диверсией позволяют устройства ввода и считывания идентификационных признаков. Большое разнообразие типов и видов таких устройств могут поставить в трудную ситуацию потребителя при выборе необходимого средства защиты. Тем самым анализ уязвимостей устройств ввода и считывания идентификационных признаков, который облегчит выбор потребителя, является актуальным на сегодняшний день.

Прежде чем рассматривать уязвимостей устройств ввода и считывания идентификационных признаков стоит выделить типы и виды этих устройств. На настоящий момент существует два основных типа УВСИП

это механические и биометрические, которые включают в себя виды. Механические включают в себя такие виды как: инфракрасный-код, штрихкод, магнитная полоса, индуктивный, радиоканальные карты, Smart-карты. Из которых ИК-код, штрих-код, индуктивный код и магнитная полоса практически не используются в современных системах, так как они зарекомендовали себя как не слишком удобные в использовании или плохо защищенные от несанкционированного использования. При работе современных систем контроля и управления доступом сегодня наиболее широко применяются радиоканальные карты, а также Smart-карты и биометрические считыватели. Биометрические УВСИП в свою очередь представляют такие виды как: отпечаток пальца, радужка глаза, голосовой ввод, распознавание лица, сетчатка глаза, геометрия руки._Важным отличием биометрических УВСИП, особенно ценным в технологиях, обеспечивающих безопасность, является считывание одного из параметров человека, а не карты или идентификатора. Таким образом, идентификационные данные не могут быть переданы другому человеку или украдены, а это незаменимо для обеспечения безопасности на режимном предприятии. К тому же считывание биометрических показателей является очень надежным методом идентификации. Таким образом, можно не учитывать человеческий фактор и вовсе отказаться от охраны пропускного пункта. Однако за все достоинства подобных устройств ввода идентификационных признаков приходится платить уменьшением пропускной способности за счет медленного темпа работы, ограниченные условия эксплуатации и дороговизны. Именно из-за этого биометрические системы контроля и управления доступом не слишком распространены. Однако в случае, когда речь идет об особо секретных объектах или важных зонах предприятия, эти недостатки сглаживаются тем, что количество лиц, имеющих допуск, ограничено. И в большинстве случаев высокая цена не останавливает владельцев предприятий. Все это окупается надежным способом идентификации человека, которую обеспечивает естественная неповторимость биометрических параметров каждого человека [2].

Рассматривать уязвимости таких механических УВСИП как ИК-код, штрих-код, индуктивный код и магнитная полоса не имеет смысла, так как они уже зарекомендовали себя как неудобные и плохо защищенные от несанкционированного доступа системы. Поэтому радиоканальные и Smart-карты являются самыми популярными используемыми механическими УВСИП. Эти устройства схожи, но из уязвимостей у них только то, что как радиоканальную карту, так и Smart-карту может использовать постороннее лицо при умышленной краже.

При этом радиоканальная карта считывается устройством чтения с образованием радиоканала, к которому злоумышленники могут получить сво-

бодный доступ и считать или скопировать данные необходимые для прохода через защиту такого устройства. При копировании данных появляется возможность производства радиоканальной карты, которая будет открывать доступ через устройство чтения. Так же использование радиоканальных карт не ограничивает доступ на различные уровни защиты. Карта установленного типа откроет любой типовой замок без каких-либо ограничений [3].

Smart-карты в свою очередь являются усовершенствованными радиоканальными картами. Доступ к радиоканалу между считывающим устройством и картой так же остается простым и открытым, но теперь карта имеет еще свой уникальный идентифицирующий чип, который отвечает за привилегии доступа и защиту от копирования карты. Чтобы злоумышленнику использовать скопированные данные с радиоканала для прохода через такое устройство нужно будет необходимо создать Smart-карту с полученными данными и уникальным чипом. После чего взломать базу данных считывателя предприятия и добавить туда номер чипа в необходимый уровень доступа. Smart-карт необязательно является картой она так же может быть в виде токена или электронного ключа, могут быть различные вариации.

У биометрических УВСИП есть две общие уязвимости. В отличии от механических УВСИП первым требуется питание от сети, когда в свою очередь механические могут обойтись источником постоянного тока. Тем самым у биометрических УВСИП появляется электроуязвимость. Так же если взломать базу данных объекта где хранятся образцы биометрии, то злоумышленнику достаточно добавить необходимый ему образец, чтобы получить доступ к объекту. Поэтому при использовании любых биометрических УВСИП стоит делать акцент на защиту серверов и баз данных. При всем при этом каждый вид биометрических УВСИП имеет свои уязвимости [4].

Считывание отпечатка пальца в наше время является распространенным средством защиты, но должной гарантии безопасности дать не может в связи с тем, что образец пальца для разблокировки системы или открытия доступа несложно репродуцировать. Два самых известных способа – это по отпечатку пальца на поверхности какого-либо личного предмета лица чей отпечаток нужно воспроизвести, а также по фото. Чтобы репродуцировать по фото, нужна хорошего качества фотография, на которой запечатлен необходимый палец и с помощью инверсной печати на обычной бумаге воспроизводится картинка, которая является моделью отпечатка пальца. Таким способом в 2014 году хакером Яном Крисслером был скопирован отпечаток пальца министра обороны Германии Урсулы фон дер Лайен.

Идентификация радужки глаза удобный и имеющий быструю скорость считывания способ защиты, но обладающий низким уровнем безопасности, так как считыватели сканируя отсылаются к определенным позициям и точкам радужки глаза, которые забиты в базе и никак не идентифицируют

подлинность сканируемого образца. Таким образом для того чтобы обойти защиту через считыватель достаточно использовать фотографию личности имеющей права доступа к объекту. Так же у самого считывателя присутствует уязвимость к солнечному свету, поэтому использование таких УВСИП вне помещения не рекомендуется.

Сканирование сетчатки глаза получило практическое применение в середине 50-х годов прошлого века. На данный момент такой способ аутентификации является одним из самых безопасных так как рисунок кровеносных сосудов глазного дна абсолютно уникален, даже у близнецов такие рисунки не совпадают. Репродуцировать данный биологический идентификатор практически невозможно, поэтому у злоумышленников единственный способ обойти систему защиты это загрузить шаблон сетчатки глаза, с помощью которого они собираются получить доступ к объекту. Но эта система одна из немногих, которые имеют особый психологический недостаток. Так как не всякому человеку приятно смотреть в темное отверстие, где что-то светит в глаз.

Распознавание лица опирается на постоянный тепловой портрет человека. Отсюда появляется уязвимость термозависимости, которая может приводить к большой вероятности ошибки первого рода (отказ в доступе для зарегистрированного пользователя). Применение таких систем на улице не имеет смысла, а в помещении только при условиях постоянной температуры.

Аутентификация по геометрии руки применяет метод использования формы кисти руки. Из-за того, что отдельные параметры формы рук не являются уникальными, то используется несколько характеристик. Считываются изгибы пальцев, их длина, толщина, ширина и толщина тыльной стороны руки, расстояние между суставами и структура кости. Могут также сканироваться мелкие детали, например, морщины на коже. Такие системы имеют хороший уровень безопасности и обеспечивают достаточную безопасность, но имеют ряд недостатков. При распухании тканей руки, а также ушибах могут возникать проблемы с аутентификацией, так как может происходить искажение исходной структуры. В том числе такое заболевание как артрит может помешать применению сканеров.

Данная классификация не является полной и открыта для дополнений, но уже на этом этапе разработки облегчает принятие решения по выбору необходимой системы устройств ввода и считывания идентификационных признаков. Потребитель, опираясь на описанный материал, может скомбинировать свою систему защиты от несанкционированного доступа подходящую для его объекта, что является актуальным в наше время.

Список используемых источников

1. Биометрические системы аутентификации [Электронный ресурс] // Wikipedia. URL: http://www.glavsetstroy.ru/articles.php/articles.php?id=355 (дата обращения 26.02.2017).

2. Биометрическая аутентификация: защита систем и конфиденциальность пользователей [Электронный ресурс] // Открытые системы. URL: https://www.osp.ru/os/2012/10/13033122 (дата обращения 07.03.2017).

3. Мартынова Л. Е., Умницын М. Ю., Назарова К. Е., Пересыпкин И. П. Исследование и сравнительный анализ методов аутентификации // Молодой ученый. 2016. № 19. С. 90-93.

4. БИОМЕТРИКА: Статистические и динамические методы аутентификации [Электронный ресурс] // Научный портал по биоинформатике. URL: http://www.bioinformatix.ru/biometrika/biometrika-statisticheskie-i-dinamicheskie-metodyi-biometricheskoy-autentifikatsii.html (дата обращения 07.03.2017.)

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ТЕНДЕНЦИЙ ИНФОРМАЦИОННЫХ УГРОЗ И УЯЗВИМОСТЕЙ

В. А. Гаврилюк А. А. Чечулин

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

В статьее будут рассмотрены основные изменения информационных угроз и уязвимостей, присущих программным и аппаратным средствам от различных производителей. Для этого будет проведен количественный и качественный анализ уязвимостей из открытых баз данных предоставляемых National Institute of Standards and Technology, например, Common Platform Enumeration и Common Vulnerabilities and Exposures. В качестве рассматриваемых критериев взяты: общий уровень угрозы, какие именно функции системы попадают под угрозу, вектор атаки, сложность реализации и то какое ПО, аппаратура или их совокупность находятся в зоне риска. На основании полученных данных будут сделаны выводы о тенденциях и векторе проблем информационной безопасности, что позволит сделать прогнозы о дальнейшем развитии угроз.

уязвимость, анализ защищенности, информационная безопасность, угроза, программно-аппаратное обеспечение.

Сегодня тяжело представить современный мир без информационных технологий, которыми пользуются все от обычных людей до огромных компаний и целых государств. Но столь сложная технология не может не содержать в себе недочетов, которые, без должной защиты, могут использовать

злоумышленники для хищения ценной информации или нанесения ущерба информационной системе, что ведет к финансовым и репутационным потерям, поэтому информационная безопасность – это вещь, которой нельзя пренебрегать, и чтобы эффективно и пользоваться, необходимо проанализировать текущее состояние информационных угроз

CVE (англ. *Common Vulnerabilities and Exposures*) – база данных общеизвестных уязвимостей информационной безопасности. Поддержкой CVE занимается организация MITRE. Полностью с CVE можно ознакомится в Национальной Базе Уязвимостей США (NVD [1]). В данный момент насчитывает более 118 тысяч уязвимостей.

Так же имеются следующие аналоги, также представляющие собой описания уязвимостей [2, 3, 4, 5]:

BID – эта классификация используется исключительно на портале SecurityFocus, классификация более сжатая чем в CVE, но может дать достаточно наглядную информации.

Secunia – не имеет особых преимуществ, но именно они предлагают платную подписку на свою базу уязвимостей.

ISS X-Force – помимо стандартных метрик содержит временные метрики.

В данной работе будет использоваться описание уязвимостей в формате CVE, так как база уязвимостей в этом формате общедоступна, часто обновляется и предоставляет необходимый объем данных

Формат CVE содержит набор характеристик для описания уязвимости. Каждая уязвимость имеет свой уникальный Cve-ID (Cve-Год-номер), текстовое описание уязвимостей, ссылки на источники, а также наборы метрик, которые содержат в себе параметры, детально характеризующие угрозу, список уязвимого программного обеспечения и аппаратуры, а также уровень угрозы (score), измеряющийся от 1 (незначительная проблема) до 10 (критическая угроза).

Связь уязвимости с программно-аппаратными платформами описывается в формате CPE (*Common Platform Enumeration*). Он представляет собой способ описания всех продуктов, операционных систем и устройств.

На сайте NVD представлены описания уязвимостей CVE в виде XML-файлов. Каждый отчет представляет собой сборник уязвимостей за отдельно взятый год, но для удобства обработки в этой работе они были объединены, так же из-за большого количества данных ручной анализ не представляется возможным, поэтому была составлена SQL база данных.

Из полученных данных на рис. 1 видно, что количество уязвимостей с каждым годом растет. Это вызвано увеличением количества продуктов, выходящих за год. Возможная причина всплеска найденных уязвимостей в 2017–2018 годах – это возросшее количество IoT (*Internet of Things*) –

устройств и соответственно уязвимостей в таких устройствах, что сходится с отчетом Cisco за 2018 год [6].

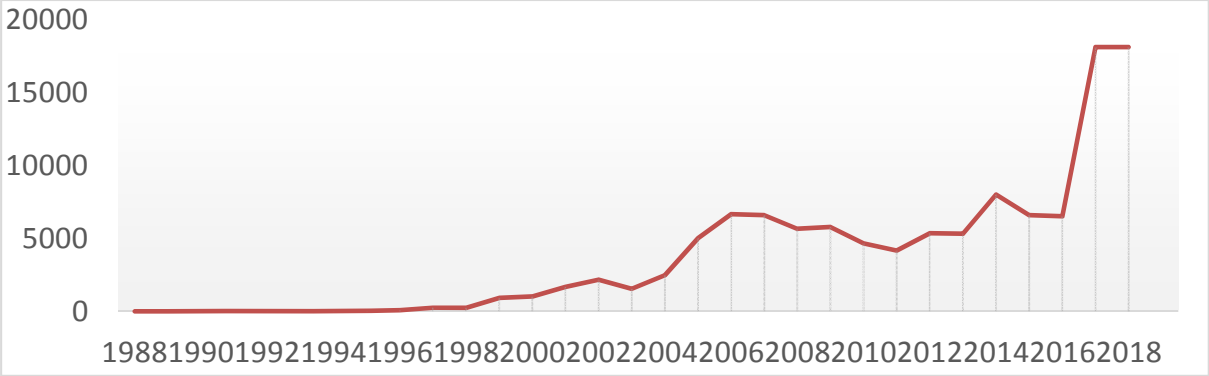


Рис. 1. Число найденных уязвимостей за год

Как можно заметить из графика на рис. 2, средний уровень угрозы постепенно снижается. При этом, на рис. 3, видно, что это вызвано не падением числа угроз с высоким уровнем, число которых довольно стабильно, а увеличением числа уязвимостей со средней угрозой.

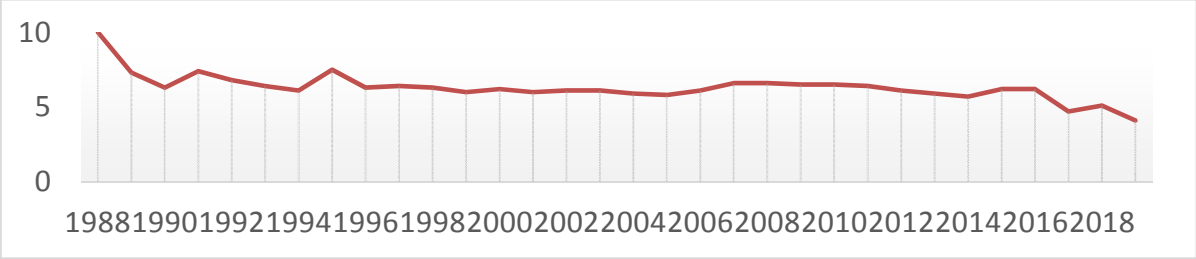


Рис. 2. Средний уровень угрозы

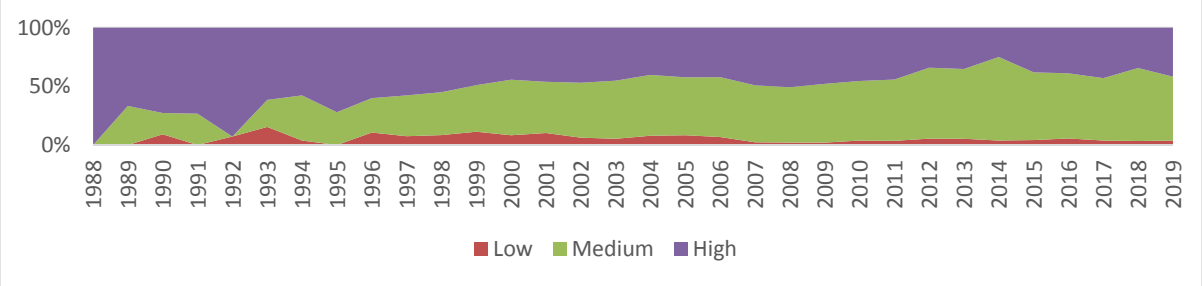


Рис. 3. Распределение уровней угроз по годам

Примечание: под низкими угрозами принимаются уязвимости с уровнем угрозы меньше 3, средние между 3 и 7, высокие 7 и выше.

Резкий всплеск количества уязвимых версий в 2018 году у Mac OS (рис. 4, 5) вызван большим количеством одних и тех же уязвимостей (например, CVE-2017-13873), присутствующих практически в каждой версии

ОС (операционной системы). По общему количеству находимых уязвимостей лидирует Debian, но у Mac OS гораздо чаще затрагивается большее количество версий. ОС Windows, в свою очередь, имеет самый высокий средний уровень угрозы.

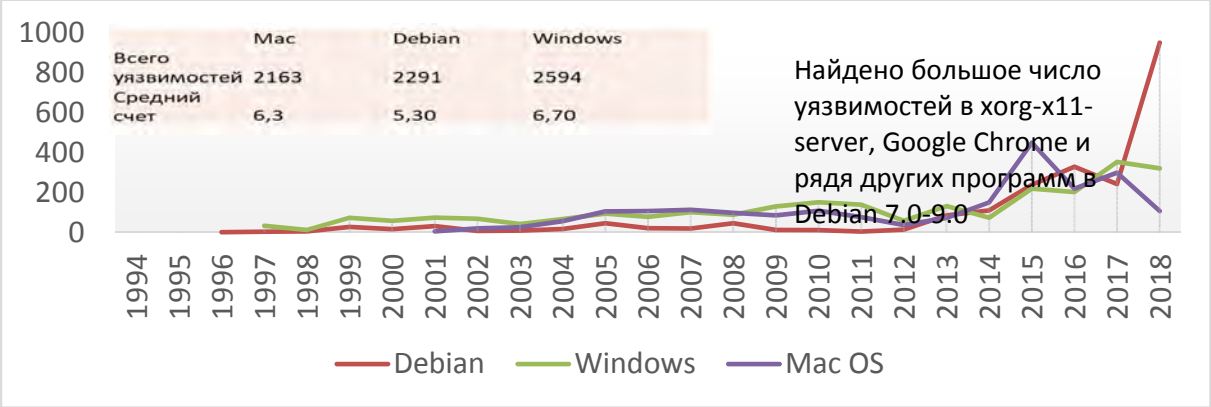


Рис. 4. Количество уязвимостей в системах за год

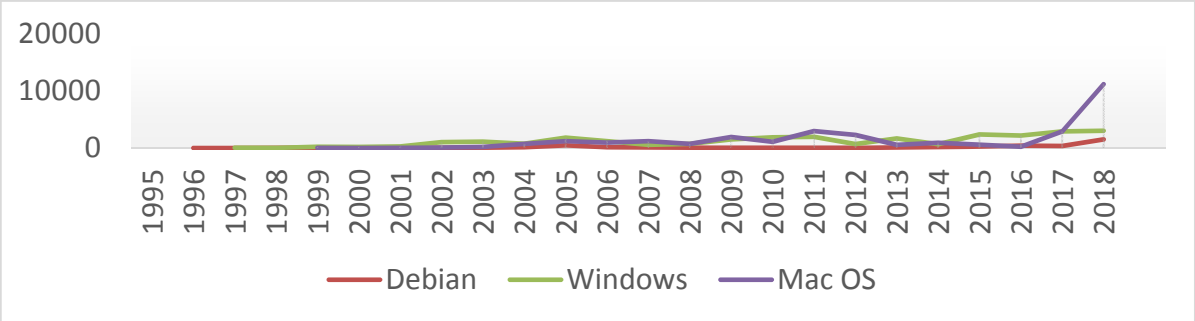


Рис. 5. Покрытие уязвимостями

Далее рассмотрим зависимость количества уязвимостей относительно жизненного цикла ОС на примере Windows Vista:

Всплески уязвимостей в первом квартале 2010 г. и частично третьем 2011 вызваны тем, что в этот момент Vista находилась на пике своей популярности, согласно статистике по ОС W3School (рис. 6, 7) [7]. Несмотря на уже крайне низкий к этому моменту уровень популярности Vista, имеется всплеск в марте 2017 г., связанный с нахождением уязвимостей свойственным большому количеству продуктов Microsoft.

Из данных графиков можно сделать вывод, что в основном количество находимых уязвимостей прямо зависит от популярности программы в данный момент, но это не исключает того, что проблемы могут быть найдены спустя большой промежуток времени из-за содержания родственных модулей в более поздних версиях программы.

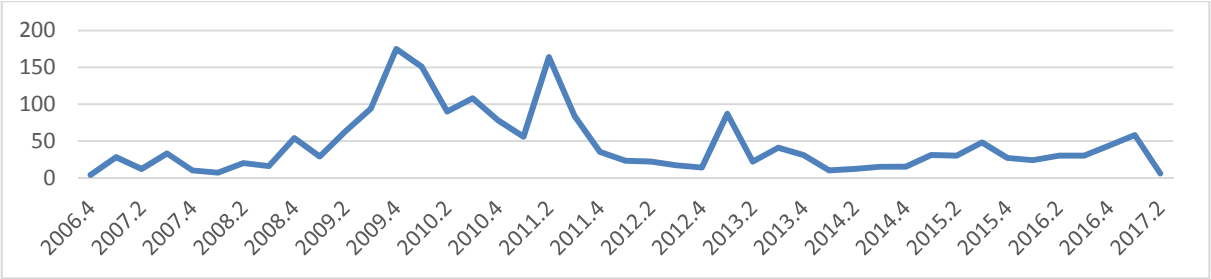


Рис. 6ю Распределение количества уязвимостей по кварталам

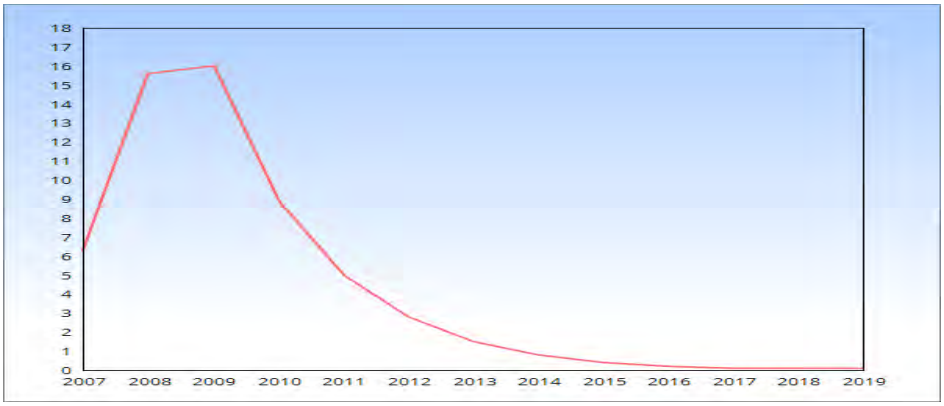


Рис. 7. Популярность (процент рынка ОС) по годам

В заключение хотелось бы сказать, что IT развивается как никогда быстро, и такой рост неминуемо скажется и на количестве новых уязвимостей. Стоит обратить особенное внимание на программные элементы, которые содержатся в большом количестве программного обеспечения, т. к. уязвимости в них могут поставить под угрозу сразу большое число устройств, а также нельзя игнорировать IoT, который сейчас активно развивается и несет в себе потенциальные уязвимости.

Список используемых источников

1. National Vulnerability Database. URL: https://www.nvd.nist.gov (дата обращения 03.04.2019).

2. Федорченко А. В., Чечулин А .А., Котенко И. В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. 2014. № 5. С. 74–76.

3. BID. URL: https://www.securityfocus.com/bid (дата обращения 03.04.2019).

4. Secunia. URL: https://secuniaresearch.flexerasoftware.com/community/advisories/ (дата обращения 03.04.2019).

5. X-Froce. URL: https://www.ibm.com/ru-ru/security/xforce (дата обращения 03.04.2019).

6. Cisco 2018. Годовой отчет по информационной безопасности С.31. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf (дата обращения 03.04.2019).

7. W3school OS Platform Statistics. URL:https://www.w3schools.com/browsers/browsers_os.asp (дата обращения 03.04.2019).

УДК 004.056
ГРНТИ 49.33.35

РАЗРАБОТКА КОМПЛЕКСНОГО АЛГОРИТМА КЛАССИФИКАЦИИ ВЕБ-САЙТОВ ДЛЯ ВЫЯВЛЕНИЯ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Д. А. Гайфулина[1,2], Э. Р. Хаванская[2], А. А. Чечулин[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В работе предложен подход к задаче классификации веб-сайтов для выявления нежелательной информации в сети Интернет, основанный на одновременном использовании разнородных аспектов веб-страниц. Определены этапы обработки данных веб-сайтов для задачи классификации. Представлены результаты экспериментов по анализу алгоритмов классификации веб-сайтов на основе разных методов машинного обучения. Выявлена и обоснована необходимость совместного использования алгоритмов классификации и предложен комплексный алгоритм классификации веб-сайтов для выявления нежелательной информации в сети Интернет. Для предложенного алгоритма приведена экспериментальная оценка результатов его применения.

нежелательная информация, запрещенная информация, Интернет, Data Mining, машинное обучение, защита от информации, классификация веб-сайтов.

Нежелательная информация в сети Интернет представляет собой информационный объект и/или совокупность объектов, содержащих противоправную, сомнительную, вредоносную информацию. Защиту пользователей от подобной информации можно разделить на два основных направления: ограждение несовершеннолетних от нежелательных материалов (системы родительского контроля) и блокировку контента, нарушающего законодательство [1]. Данные мероприятия осложняются большими объемами информации в сети Интернет, высокой изменчивостью содержимого и усложнением структуры веб-страниц. Анализ веб-страниц с целью обнаружения нежелательной информации требует использования не только «черных» и «белых» списков веб-ресурсов, но и автоматических систем классификации веб-страниц по их содержимому.

Целью проводимого исследования является защита пользователей сети Интернет от нежелательной информации. Основное направление работы заключается в повышении качества классификации веб-страниц для выявления нежелательной информации в сети Интернет. Задачами исследования являются:

1) определение общего подхода к классификации веб-страниц;

2) оценка алгоритмов классификации с использованием методов машинного обучения;

3) разработка комплексного алгоритма классификации веб-страниц;

4) оценка разработанного алгоритма.

Подход к обучению и использованию систем классификации веб-страниц основан на обработке исходных («сырых») данных веб-страниц, принадлежащих к заранее определенным категориям (темам) и применении методов машинного обучения. Схема общего подхода к автоматизированной классификации веб-страниц представлена на рис. 1.

Рис. 1. Поход к классификации веб-страниц

Веб-страницы отличаются от текстовых документов более высокой сложностью. Прежде всего, тем, что они полуструктурированы с помощью HTML-тэгов разметки, связаны между собой ссылками, содержат фрагменты кода, исполняемого как на стороне сервера и клиента. Как правило, для решения задач классификации используются следующие аспекты веб-страниц:

1) текстовое содержимое [2];

2) адрес размещения в сети Интернет (URL) [3],

3) структурные признаки (статистика HTML-тегов) [4],

4) объекты, не связанные с текстом (например, медиаконтент),

5) информация о веб-странице (информация от WHOIS-серверов, возраст, страна регистрации);

6) ссылки на данную страницу;

7) ссылки на сторонние ресурсы на анализируемой веб-странице.

Классификация веб-страниц по текстовому содержимому является наиболее широко применяемым методом, состоящим из двух этапов. Первый этап состоит в предобработке (индексации) текстового содержимого для представления его в виде множества термов (слов) с некоторыми весами, отражающими значимость каждого слова для конкретной категории. Вторым этапом являются классификация веб-страницы или обучение на множестве веб-страниц. Входными параметрами являются признаки веб-страниц, полученные на первом этапе, а также заранее определенное количество категорий, выходным параметром – категория анализируемой веб-страницы.

В рамках проводимого исследования проведена экспериментальная оценка алгоритмов машинного обучения для решения задач классификации веб-страниц. Проанализирована выборка из 17248 веб-страниц, адреса которых значатся в категорированных списках веб-сайтов [5, 6]. Исходные данные принадлежат следующим категориям: наркотики/алкоголь, религия, порнография, агрессия, азартные игры, оружие и категория, указывающая на неизвестный результат. Количество веб-страниц для каждой категории было взято одинаковым и равным 2464. Содержимое веб-страниц включает как полной текст странницы, так и текст в HTML-тегах. Приняты к оценке следующие методы машинного обучения: деревья решений, метод опорных векторов, наивный Байесовский классификатор и логистическая регрессия. Выбор классификаторов был сделан на основании изученных работ по классификации, в которых данные методы себя хорошо зарекомендовали [7, 8]. Для оценки качества данных классификаторов использовались численные метрики:

1) аккуратность (*accuracy*);

2) полнота (*recall*);

3) точность (*precision*);

4) F-мера [4].

На рис. 2 приведена оценка аккуратности для классификации веб-страниц для каждого набора данных по тегам, на рис. 3 – по категориям (см. ниже). Данная оценка характеризует отношение количества веб-страниц, по которым классификатор принял правильное решение, к общему количеству веб-страниц всех категорий.

По полученным результатам можно отметить, что метод опорных векторов дает более высокие результаты качества классификации для полного текста страницы (91 %). В то же время для текстов, включенных в теги, более высокие результаты показывают иные классификаторы (наивный Байесовский классификатор для тега <Description> 82 %, логистическая ре-

грессия для <H1> 75 %). Схожее различие наблюдается, если оценить классификацию для исследуемых категорий. Таким образом, использование конкретного классификатора не является достаточным для более точного определения категории нежелательной информации.

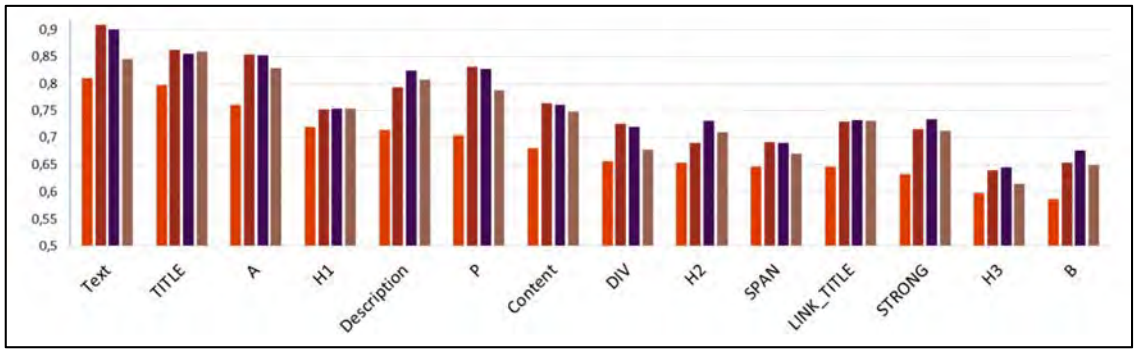


Рис 2. Оценка аккуратности классификации веб-страниц по тегам

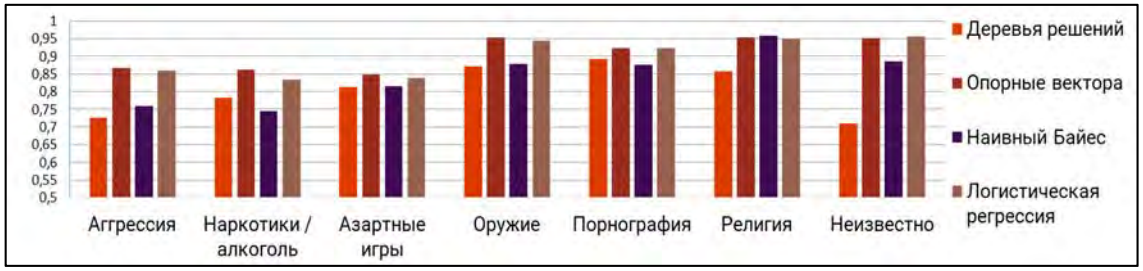


Рис.3. Оценка аккуратности классификации по категориям

Предлагается разработать комплексный алгоритм классификации веб-страниц, который позволит использовать технологию параллельного обучения базовых классификаторов на разных аспектах веб-страниц. На этапе финальной классификации голосованием выбирается решение классификатора с наибольшим весом для данной характеристики. Также в разрабатываемом алгоритме вводится дополнительная обработка текстового содержимого в качестве машинного перевода с иностранного языка. Это обусловлено тем, что система классификации, предназначенная для анализа веб-страниц на одном языке, может некорректно работать с данными на другом.

Для разработанного комплексного алгоритма был проведен эксперимент по оценке качества классификации на том же наборе исходных данных. Описанные ранее классификаторы использовались в качестве базовых. Для машинного перевода содержимого веб-страниц использовались сервисы Яндекс.Переводчика. На рис. 4 и 5 приведена оценка аккуратности для классификации по текстовому содержанию веб-страниц.

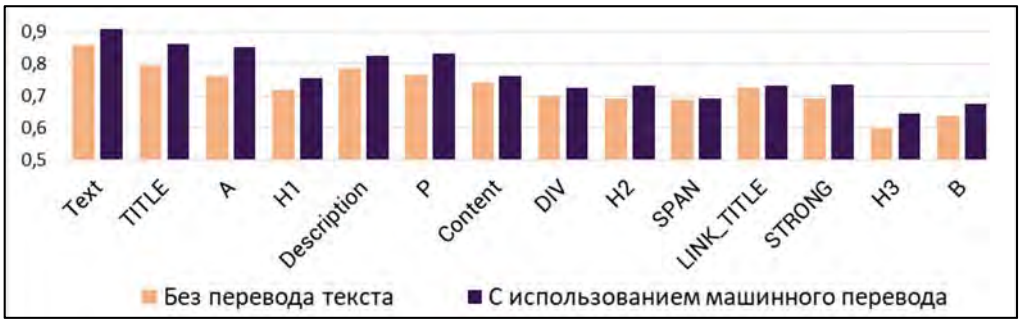


Рис 4. Оценка аккуратности классификации по тегам

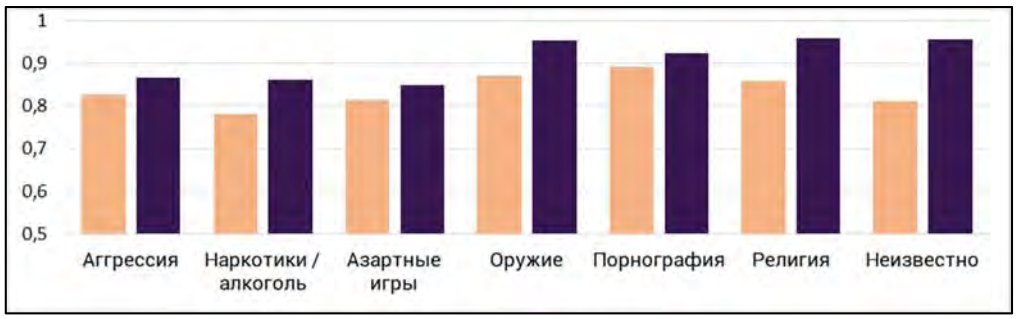


Рис 5. Оценка аккуратности классификации по тегам

В результате проведенного исследования предложен подход к задаче классификации веб-страниц для выявления нежелательной информации в сети Интернет, основанный на одновременном использовании разнородных аспектов веб-страниц. Определены этапы обработки данных веб-страниц для задачи классификации. Представлены результаты экспериментов по анализу алгоритмов классификации веб-страниц на основе различных методов машинного обучения. Предложен комплексный алгоритм классификации веб-страниц для выявления нежелательной информации в сети Интернет, включающий себя этап машинного перевода текстового содержимого веб-страниц на иностранных языках. Для предложенного алгоритма приведена экспериментальная оценка результатов его применения. В направлении дальнейших работ планируется усовершенствование алгоритма для достижения более высоких показателей качества классификации. Также предполагается использование дополнительных аспектов веб-страниц для повышения качества классификации.

Работа выполнена при финансовой поддержке гранта РНФ 18-11-00302 в СПИИРАН.

Список используемых источников

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 25.11.2017).

2. Kotenko I., Chechulin A., Komashinsky D. Evaluation of Text Classification Techniques for Inappropriate Web Content Blocking // Proc. of the IEEE8th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2015), Warsaw, Poland, Sept. 24–26, 2015. 2015. PP. 412–417.

3. Khonji M., Iraqi Y., Jones A. Enhancing Phishing E-Mail Classifiers: A Lexical URL Analysis Approach // Intern. Journal for Information Security Research. 2012. Iss. 6. PP. 236–245.

4. Комашинский Д. В., Котенко И. В., Чечулин А. А. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности. 2011. № 2. С. 102–106.

5. URLBlacklist [Электронный ресус]. URL: http://urlblacklist.com/ (дата обращения 08.12.2017).

6. DMOZ [Электронный ресус]. URL: https://www.dmoz.org/ (дата обращения 08.12.2017).

7. Patil A. S., Pawar B. V. Automated Classifcation of Web Sites using Naive Bayesian Algorithm // Proc. of the Intern. Multiconf. of Engineers and Computer Scientist, 2012. P. 466.

8. Qi X., Davison B.D. Web Page Classification: Features and algorithms // ACM Computing Surveys (CSUR). 2009. PP. 1–31.

УДК 004.056
ГРНТИ 81.93.29

МЕТОДЫ И МЕТОДИКИ АНАЛИЗА НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Т. О. Гамидов[1], В. А. Десницкий[1,2], О. С. Дудкина[1], Д. В. Сахаров[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
2Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Социальный анализ используется давно, еще до появления компьютерных сетей и Интернета. К примеру, телефонные или физические опросы также являются социальным анализом. С развитием Интернета и социальных сетей, таких как VK.com, Одноклассники, личная информация пользователей начала перемещаться в социальные сети. И возможностей для анализа публичной информации стало больше. В данной работе исследуются методы и методики анализа социальных сетей, которые могут быть использованы в системах мониторинга и противодействия нежелательной информации. В связи с высоким уровнем цифровизации общества, погруженности личности в информационное пространство социальных сетей тема исследования представляется актуальной.

SNA, узел, сеть, DNA, меры измерения, отношения, неориентированный граф, ориентированный граф, поиск людей, структура отношений.

С каждым годом, из-за быстрого роста социальных сетей, таких как Вконтакте, Одноклассники, Facebook, Twitter и т. д., исследование социальных сетей становится все более популярным и актуальным. В социальных сетях пользователи обмениваются сообщениями, выкладывают публикации, комментируют и реагируют на различные события, загружают фотографии и другие медиа данные, т.е. проявляют социальную активность. Используя методы социального анализа, а также контент-анализа, можно выявлять и бороться с распространением нежелательной информацией [1]. Под «анализом социальных сетей» понимается процесс исследования, направленный на изучение, социальных отношений в терминах теории сетей. Выделяют 2 основных понятия: 1) понятие «узла» (отдельный участник в сети) и 2) «связи» (отношения между этими участниками, такие как дружба, родство, положение в организации, и т. д.). Также выделяют 2 основных подхода к анализу социальных сетей: структурный и динамический.

Структурный подход – это подход, который заостряет внимание непосредственно на форме сети и интенсивности взаимодействий узлов в сетях друг с другом [2].

Динамический подход – это подход, непосредственно заостряющий внимание на изменениях в структуре сети с течением времени.

Social Network Analysis (SNA) – это метод, который используется для отображения и измерения отношений между людьми, группами, организациями и другими связанными информационными объектами. Узлами в сети являются люди и группы, в то время как связи между ними показывают отношения между узлами. SNA обеспечивает как визуальный, так и математический анализ человеческих отношений. Главными плюсами данного метода является то, что при помощи него мы можем определять людей, команды и подразделения, которые играют центральную роль, а также различать узкие места в сети. Определяющей чертой метода SNA является ее ориентация на структуру отношений, а в основе этого метода лежит математическая теория графов. Граф в свою очередь состоит из вершин, которыми являются люди, группы, организации и другие информационные объекты, а также из ребер, которыми являются отношения между ними. Отношения между узлами могут быть как симметричными, так и несимметричными.

Симметричные отношения – это, например, дружба в социальных сетях, соавторство[3].

Несимметричные отношения – цитирование статей, комментирование публикаций т. д.

Для визуализации узлов с симметричными отношениями используется неориентированный граф (рис. 1), а для узлов с несимметричными отношениями, ориентированный (рис. 2).

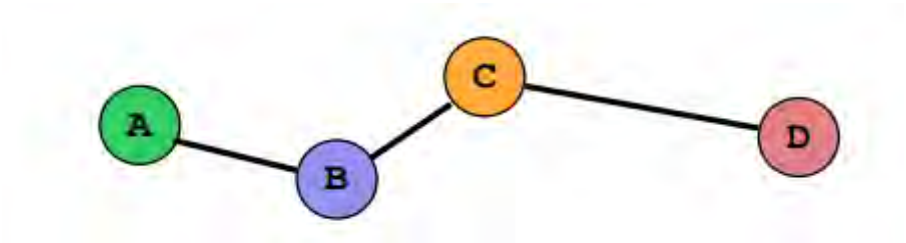


Рис. 1. Неориентированный граф, отношения между узлами симметричны

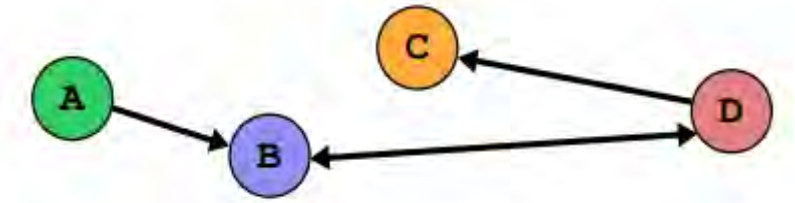


Рис. 2. Ориентированный граф, отношения между узлами несимметричны

Исследователи, для анализа и измерения социальных сетей используют различные меры измерения, такие как:

1. Центральность по степени – мера измерения, в которой происходит присвоение оценки важности, основанная исключительно на количестве связей (ребер), удерживаемых каждым узлом. Использовать эту концепцию нужно для поиска людей с большим количеством связей, популярных людей, людей, которые могут хранить большую часть информации, или людей, которые могут быстро связаться с более широкой сетью.

2. Центральность по посредничеству – мера измерения, в которой измеряется сколько раз узел находился на кратчайшем пути между другими узлами. Для вычисления центральности по посредничеству узла берутся все возможные пары других узлов и для каждой пары вычисляется доля кратчайших путей между этими узлами, которые бы проходили через данный узел. Сумма этих долей и составляет центральность по посредничеству для узла. Если у какого-либо узла высокий показатель центральности по посредничеству, можно предположить, что он – единственная связь между различными частями сети или «узкое горлышко». При разрушении «узкого горлышка» граф распадается.

3. Центральность по близости – эта мера измерения оценивает каждый узел на основе их «близости» ко всем остальным узлам в сети. Эта мера измерения вычисляет кратчайшие пути между всеми узлами, а затем присваивает каждому узлу оценку на основе его суммы кратчайших путей. Используется для поиска людей, которые лучше всех могут наиболее быстро влиять на всю сеть. Такая мера подходит для выявления эффективных путей и каналов распространения информации или противодействия этому.

Контент-анализ – это метод исследования, который позволяет систематически анализировать данные, собранные в ходе исследования, для того

чтобы можно было сделать обобщения в отношении категорий, представляющих интерес для исследователя. Существует количественный (также называемый содержательным) и качественный (также называемый структурным) контент-анализ. Суть количественного контент-анализа заключается в выявлении частоты появления исследуемых отдельных показателей (например, тем, слов, таблиц, фотографий, видео и т. д.). Качественный контент анализ позволяет анализировать смысловое содержание текста и подтекст как включенный автором намеренно, так и неосознаваемый им [4].

Более специализированной областью, связанной с SNA, является метод изучение динамического поведения сетей, формально известный как Dynamic Network Analysis (DNA). Социальные сети (и даже сети в целом) чаще всего демонстрируют структурные изменения с течением времени, то есть добавление или удаление узлов, или ребер. Определяющей чертой метода DNA является его ориентация на изменение структуры отношений со временем [5], в отличие от метода SNA, который ориентируется только на структуре отношений.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № 18-71-10094) в СПИИРАН.

Список используемых источников

1. Виткова Л. А., Потехин И. Ю., Сахаров Д. В. Проблема выявления информационно-психологического воздействия в информационной инфраструктуре Российской Федерации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международной научно-технической и научно-методической конференции : сб. науч. ст. в 4-х томах. 2017. С. 166–170.

2. Саенко И. Б., Чечулин А. А., Виткова Л. А. Концепция интеллектуальных систем аналитической обработки цифрового сетевого контента с целью обнаружения нежелательной информации // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 6–7.

3. 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. № 4. С. 362–377.

4. Котенко И. В., Чечулин А. А., Комашинский Д. В. Автоматизированное категорирование веб-сайтов для блокировки веб-страниц с неприемлемым содержимым // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 62–68.

5. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Monitoring and counteraction to malicious influences in the information space of social networks // 10th International Conference on Social Informatics (SocInfo). 2018. PP. 159–167.

УДК 65.011.56,
ГРНТИ 06.81.12

АНАЛИЗ ТЕХНОЛОГИИ BLOCKCHAIN И СФЕРЫ ЕЕ ПРИМЕНЕНИЯ

А. С. Ганюшин, В. С. Елагин

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

Стимулом для появления блокчейна стал кризис 2008 года, когда люди разуверились в традиционных финансовых институтах и инструментах. Возникла необходимость в платежных инструментах, независящих от политически вовлеченных эмиссионных центров и неотягощенных трансграничными ограничениями, а также не требующих безусловного доверия со стороны участников. В следствие чего появился биткоин, а с ним и блокчейн. Позже стало понятно, что блокчейн можно использовать не только для криптовалют.

Блокчейн – это система распределенного децентрализованного хранения реестров с повышенным доверием к обеспечению целостности информации.

Блокчейн, публичный блокчейн, частный блокчейн, смарт-контракт.

О причинах и предпосылках

На текущий момент появилось огромное количество идей, как и где можно использовать технологию блокчейн. На это указывает основная задача данной технологии: обеспечение целостности хранимых и обрабатываемых данных в недоверенной среде. Под недоверенной средой подразумевается:

– к участию допускаются узлы с различной степенью доверия;
– все узлы имеют одинаковые права;
– отсутствует централизованное управление;
– отсутствует единая политика безопасности;
– необходим механизм согласования действий узлов при обработке и хранении информации [1].

На основании всех этих факторов вытекает основная цель использования блокчейна – создание доверительных условий при обмене информацией и активами между несколькими равноправными и независимыми сторонами.

Основные характеристики

Поскольку на данной технологии могут строиться разные типы сервисов и приложений, то и выделяют публичный, частный и промежуточный блокчейн.

Публичный (открытый) блокчейн – каждый участник обладает всем объемом возможностей и прав. Доступ в систему никем не контролируется.

Публичный блокчейн характеризуется полной децентрализацией и возможностью поддерживать работоспособность сети в равной степени всеми участниками, т.е. любой пользователь сможет проверять данные и транзакции, добавляя их в децентрализованный реестр.

Частный (закрытый) блокчейн – все функции делегированы узлам на основании допуска, который регламентируется организатором или сообществом.

Участники, имеющие статус сообщества, могут лишь пользоваться услугами цепи, осуществляя транзакции, либо отправляя какие-либо данные. Организаторы цепи имеют более высокую степень допуска – они проверяют операции, которые осуществляются пользователями.

Промежуточные формы – определяет различную степень закрытости блокчейна. Например:

– Открытость для чтения – данные читать смогут все желающие, но проводить транзакции – только допущенные участники.

– Открытость для транзакций – можно допускать к проводке транзакций всех желающих, но право поддерживать целостность блокчейна (формирование блоков и проверку транзакций) оставить за ограниченным кругом узлов.

– Другие варианты.

У блокчейна есть ряд преимуществ, которые делают его весьма привлекательным для внедрения в сферы жизни. К основным преимуществам блокчейн можно отнести следующее [1]:

– Прозрачность. Система позволяет осуществить в ней операции только по схеме, утвержденной всеми участниками.

– Безопасность. Каждый участник системы имеет доступ только к оговоренному сегменту информации. Все остальные данные шифруются. Нет «хозяина сервера», который владеет всеми данными.

– Надежность. Система использует распределенную сеть участников для хранения информации, а не один сервер, поэтому нарушить ее работу практически невозможно.

– Неизменность данных. В системе технически невозможно изменить данные в одностороннем порядке, поэтому отсутствует необходимость сверок.

– Оперативность. Обмен данными в системе происходит в режиме реального времени.

Примеры использования

XXI век – век цифровизации, а значит есть много сфер применения блокчейна. Как отмечалось выше, технологию блокчейн можно применить в различных областях. Ниже перечислена лишь малая часть сфер применения данной технологии:

– государственные услуги;
– единая база контрагентов, их рейтинг, скоринговая оценка;
– операции с товарами и сырьем;
– история производства товара, происхождение комплектующих;
– фиксация сделок;
– логистика;
– и др [1].

Далее рассмотрим реальные варианты использования технологии блокчейн на двух примерах.

Верификация поставок в факторинге

Сеть: платформа объединяет учетные системы контрагентов в одну информационную сеть и автоматизирует взаимодействие участников (рис. 1).

Модули: модульный дизайн платформы позволяет участникам выбрать необходимые для конкретных задач компоненты. Api sdk для разработчиков позволит создать нужные бизнесу модули самостоятельно или привлекая сторонних разработчиков [2].

Технологический потенциал: сеть без точки отказа, неизменность истории событий и быстрый обмен информацией. Потенциал блокчейна.

Внедрение блокчейна дает ощутимые преимущества и удобства при проверке обмена товаров поставщика на деньги заказчика (рис. 2, см. ниже).

Рис. 1. Модульное представление верификации поставок в факторинге

Расчеты с контрагентами

Использование блокчейна можно внедрить при формировании расчетов с контрагентами (рис. 3). Его внедрение пойдет на пользу всем сторонам процесса за счет некоторых преимуществ [2]:

– скорость проведения операций сокращается с 2–3 часов до 20 секунд;

– все данные об операциях хранятся в зашифрованном виде;

– взаимодействие участников полностью автоматизировано;

– сокращаются затраты на ИТ инфраструктуру;

– переход к расчетам с агентами в режиме онлайн;

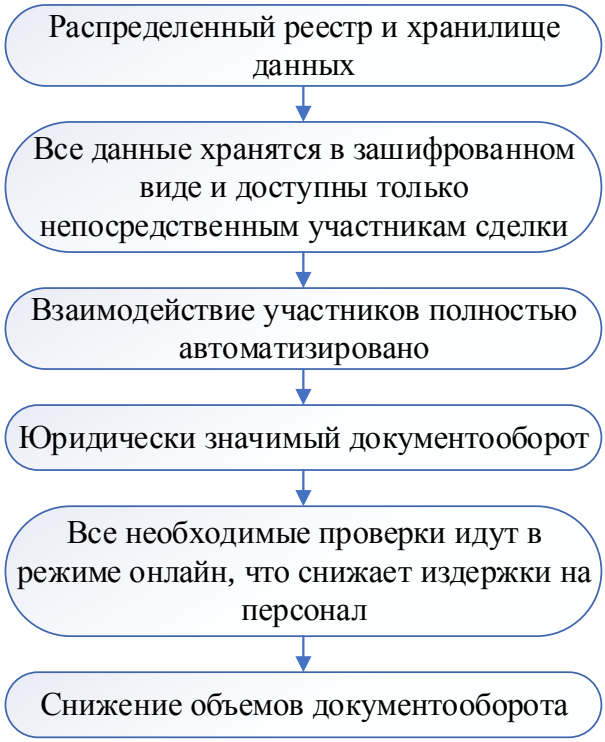


Рис. 2. Преимущества внедрения блокчейн в верификацию поставок в факторинге

– все необходимые проверки идут в режиме онлайн, что снижает издержки на персонал и отсутствие риска человеческого фактора;

– исчезает необходимость размещения гарантийного депозита или оформления банковской гарантии на будущие расчеты;

– сокращается время взаимных расчетов и получения вознаграждения.

Рис. 3. Схема расчета с контрагентами

Для большего понимания рассмотрим поэтапное взаимодействие с контрагентом (рис. 4).

Как видно из схемы использование блокчейн увеличит скорость обработки операций, а, соответственно, принесет финансовые выгоды.

Рис. 4. Поэтапное взаимодействие с контрагентом

Общие выводы

В данной статье была рассмотрена технология блокчейн. Основываясь на характеристиках данной технологии и вариантах ее применения, мы выяснили, что сферы использования могут быть самые различные.

Кроме того, были рассмотрены два практических варианта применения технологии блокчейн: Верификация поставок в факторинге и Расчеты с контрагентами, где наглядно показали, какие преимущества дает внедрение блокчейна.

На основании вышеизложенного можно сделать вывод о целесообразности использования блокчейн во многих сферах нашей жизни для обеспечения удобства, сокращения издержек, повышения надежности и безопасности.

Список используемых источников

1. Воронов А. В. Основы технологий Blockchain и их применения. Введение в тему // ДЕМО Газпромнефть, 2019. 31 с.

2. Баландин А. В. Практические примеры применения технологии блокчейн // Digital Horizon, 2019. 11 с.

УДК 654.254
ГРНТИ 49.13.13

ИНЖЕНЕРНЫЕ МЕТОДИКИ РАСЧЕТА ОПТИЧЕСКИХ ХАРАКТЕРИСТИК ТРАНСПОРТНОЙ СЕТИ СВЯЗИ НА БАЗЕ WDM

Р. С. Гашков[1], А. К. Канаев[1], В. Ф. Тукмачев[2]

[1]Петербургский государственный университет путей сообщения имени Александра I
[2]Институт по проектированию сигнализации, централизации, связи и радио на железнодорожном транспорте «Гипротранссигналсвязь»

При проектировании транспортной сети связи на базе WDM следует, исходя из назначения системы, сформулировать предъявляемые к ней требования, что в дальнейшем определит процесс проектирования, техническую эффективность и экономическую целесообразность принятых решений. В статье рассматриваются стандартные методики расчета характеристик оптических каналов, существующие проблемы при расчетах, а также приведено обоснование необходимости создания инженерной методики расчета оптических каналов.

транспортная сеть связи (ТрСС), WDM – wavelength-division multiplexing, оптические каналы, элементы оптического тракта.

Стандартные методики расчета оптических каналов

Рекомендацией МСЭ-Т G.680 определён порядок расчёта характеристик передачи оптического канала при каскадном включении оптических сетевых элементов. При этом оптическими сетевыми элементами принято считать [1]:

– линейный сегмент WDM, в который входят оптические усилители, оптический кабель, компенсаторы дисперсии; мультиплексор OADM или ROADM;

– фотонный коммутатор (OXC или PXC);

– полностью оптические конверторы волн AOWC (*All-optical Wavelength Converters*);

– оптический 2R или 3R регенератор.

Оцениваемыми характеристиками передачи являются:

– оптическое отношение сигнал/шум OSNR;

– остаточная дисперсия RD (Residual Dispersion);

– поляризационная модовая дисперсия PMD (*Polarization Mode Dispersion*) и поляризационно-зависимые потери PDL (*Polarization-Dependent Loss*);

– накопление неравномерности частотной характеристики передачи в оптическом канале (*Ripple* – размах (неравномерность) уменьшения коэффициента передачи в пределах диапазона частот или длин волн канала);

– случайное изменение уровня мощности канала на выходе сетевого элемента и др.

В каждом оптическом сетевом элементе ONE (*Optical Network Element*) происходит уменьшение величины OSNR, вызванное добавлением собственных помех. По этой причине при каскадировании различных сетевых элементов (оптических усилителей, оптических коммутаторов, оптических мультиплексоров вывода/ввода и т. д.) происходит снижение помехоустойчивости в каждом из оптических каналов, что может привести к увеличению числа ошибок цифровой передачи при регенерации сигналов. При проектировании протяженных оптических каналов с коммутацией и усилением необходимо точно определить OSNR и сравнить с допустимыми значениями, которые приводятся в технической документации [2].

При определении OSNR также должны учитываться параметры потери, обусловленные дисперсией передатчика, оптические шумы нелинейного происхождения в волоконных световодах, оптических усилителях, оптических коммутаторах, межканальные помехи, интерференционные помехи, поляризационные зависимые потери. Однако, пока неизвестны детальные методики расчета этих потерь, предлагается использовать в расчётах интегральную величину потерь в оптическом канале, указанную в характеристиках интерфейсов.

Для учёта сужения частотной характеристики передачи должны вводиться дополнительные потери на уменьшение OSNR. Однако в известных стандартных методиках расчёта линий с OADM и ROADM этому не уделено внимание. Также не уделяется внимание и потерям за нелинейные искажения и помехи, за случайные переключения оптических каналов при защитных действиях, при добавлении каналов или их исключении [3].

Стандартом G.680 предусмотрено только общее указание по определению минимально допустимого значения OSNR с учетом допустимого OSNR приёмника транспондера и максимального штрафа для OSNR в оптическом тракте [3].

Таким образом, задача определения максимального штрафа оптического тракта с учетом ряда негативных факторов остаётся актуальной.

Передовые компании производители WDM систем разрабатывают и внедряют способы решения проблем в данной области. Все необходимые расчеты включаются в стоимость оборудования линейного тракта, что не позволяет самостоятельно контролировать или модернизировать проектирование транспортной сети.

Обоснование необходимость создания инженерной методики расчета оптических каналов

Особое внимание необходимо уделить автоматизации всех расчетов и визуализации. А также интегрировать методики расчетов по рекомендациям МСЭ-Т и передовых компаний, занимающихся системами WDM. На данный момент ведется разработка данной (универсальной) методики, в которой используются принципы модульности построения структурной схемы, вывода основных параметров/характеристик на участке оптоволоконной линии, перед усилителем и после усилителя с необходимыми компенсаторами [4].

Необходимость создания универсальной методики заключается в решении существующих проблем при расчетах оптических каналов и получения широких возможностей, а именно:

– полная независимость потребностей заказчика от производителя оборудования систем WDM, который включает в его стоимость и расчеты по транспортной сети;

– независимость от производителя ведет к повышению информационной безопасности, так как вся информация остается у заказчика;

– возможность модернизации транспортной сети без участия производителя;

– минимальное время расчета за счет автоматизации универсальной методики;

– уменьшение трудозатрат;

– снижение стоимости расчета по универсальной методике;

– для работы с данной методикой нет необходимости в специалистах высокого уровня;

– возможность быстрой корректировки исходных данных для получения оптимальных данных рассчитанных характеристик оптических каналов.

Список используемых источников

1. Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи (ATM, PDH, SDH, SONET и WDM). М. : Радио и связь, 2000. 468 с.

2. Листвин В. Н., Трещиков В. Н. WDM системы: научное издание. М. : Издательский Дом «Наука», 2013. 300 с.

3. Фокин В. Г. Оптические мультиплексоры OADM/ROADM и коммутаторы PXC в мультисервисной транспортной сети: учебное пособие, ГОУ ВПО «СибГУТИ». Новосибирск, 2011. 204 с.

4. Канаев А. К. Концептуальная модель сетей и систем связи железнодорожного транспорта / Транспорт Российской Федерации. 2015. № 2 (57). С. 45–48.

УДК 004.056
ГРНТИ 81.93.29

ЗАЩИТА ДЛЯ РАСПРЕДЕЛЕННЫХ ОТКАЗОВ В ОБСЛУЖИВАНИИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

А. М. Гельфанд, Н. А. Косов, А. В. Красов, Г. А. Орлов

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

С развитием информационных технологий, развиваются облачные вычисления и увеличивается количество уязвимостей, используя которые можно получить доступ к защищаемой информации. Одна из возможных атак – это DDoS атака, используя которую можно перегрузить сервис облачных технологий. В статье рассматриваются принципы работы облачных вычислений и варианты защиты от DDOS-атак.

DDoS, информационные технологии, атака, облако.

Облачные вычисления обеспечивают повсеместный доступ по запросу к вычислительным ресурсам, которые могут быть обеспечены с минимальным взаимодействием с поставщиками сервисов услуг. Многие предприятия реализовали такие облачные вычисления с учетом таких характеристик, как самообслуживание по требованию, широкий доступ к сети, объединение ресурсов, быструю эластичность и измерительные услуги. Данные характеристики позволяют пользователям сосредоточиться на своих бизнес процессах, пока вычислительные ресурсы управляются поставщиком облачных услуг (ПОУ) [1]. Модель облака снижает затраты на бизнес, упрощая процесс установки обновлений аппаратного и программного обеспечения и обеспечивая доступность и адаптивность вычислительных ресурсов. Действия клиентов в облаке контролируется ПОУ. Неординарные несоответствия использования ресурсов влияют на доверие к клиенту и, следовательно, влияют на услуги, которые они получают. Одной из проблем, которая препятствует принятию облачных вычислений, является забота безопасности всех заинтересованных сторон от ПОУ, клиентов и пользователей. Мощность (вычислительная способность) облака является привлекательным ресурсом для эксплуатации со стороны нападавших для запуска дальнейших атак. После успешной компрометации облако становится потенциальной угрозой как для облака, так и для внешнего объекта. К примеру, самая большая DDoS-атака в истории Норвегии прервала онлайн-платежные системы крупных фирм в числе которых находились: пять банков, три авиакомпаний, две телекоммуникационные компании и одна страховая компания. Высокий рост развития атак демонстрирует важность постоянно

развивающихся систем обороны против них. Проблемы еще более усложняются различными настройками моделей облака и подотчетностью всех сторон осуществления безопасности в каждой из этих установок.

Облачные модели наследуют в себе слабые стороны разрешающих технологиях, например, виртуализации, при этом они проходят через стандартные интернет-протоколы. Виртуализация является основной технологией использования облачной вычислительной модели. Важной особенностью безопасности ВМ является изоляция [2]. Защитные методы против атак на изоляцию можно разделить на те, которые изолируют (исключают) работу виртуальных машин и тех, которые сосредоточены на изоляции общих ресурсов (утеря контроля над ресурсами). Первый из этих подходов может ограничить способность системы планировать работу легальных виртуальных машин. Для реализации второго метода необходим процесс посредничества и мониторинга для анализа запросов ресурсов и назначения этих запросов виртуальным машинам. Кроме того, для реализации политики, необходимой для применения изоляции, требуется много перехватчиков операционных систем, и это сложно задать распределенной системе [2]. Облачные характеристики, обеспечивающие гибкость и масштабируемость, также создают новые угрозы, которые могут быть усилены анонимностью Интернета. Поскольку пользовательские взаимодействия с облаком регулируются традиционными интернет-протоколами, атаки становятся более трудными для обнаружения, а саму атаку становится проще реализовать. В данной статье рассматриваются DDoS-атаки, большинство из которых, используют ресурсы службы переполнения буфера для блокировки или задержки ответа на законные запросы пользователей. В отличие от традиционных DDoS-атак, DDoS против облака приводит к потенциальному сбою работы системы, которые пересекают традиционные организационные границы. Это связано с тем, что данные управляются ПОУ, а данные для разных организаций могут храниться на одном физическом оборудовании. Таким образом, масштабируемость облака представляет собой основные проблемы безопасности по сравнению с традиционными сетями [3].

Атаки DDoS имеют два значения: либо они становятся неспособными доставлять своим пользователям сервис, как определено в их соглашении, или у них есть свои ресурсы, скомпрометированные для запуска атаки на другое место. В этом разделе анализируются предлагаемые системы, направленные на защиту облака от атак DDoS. Дерево фильтрации, которое выступает в качестве сервис-брокера в рамках модели сервис-ориентированной архитектуры (СОА) [3]. Предлагается добавить ссылочный элемент подписи к каждому запросу СОА, чтобы убедиться, что он исходит из правильного источника. Двойные сигнатуры генерируются с использованием хэшированных характеристик каждого СОА-огибающей, таких как количе-

ство дочерних элементов или элементов заголовка. IP-адрес клиента хранится в заголовке сообщения вместе с головоломкой, которая хранится как часть файла WSDL. Предлагаемая система должна сканировать каждый пакет индивидуально, что может привести к конкретному месту в ситуациях DDoS-атак.

Также автором предлагается система отслеживания и фильтрации. Отслеживание СОА используется путем добавления тега к СОА-пакетам для записи принятого маршрута [4]. Эта система не может идентифицировать источник атаки, поскольку тег добавляется только к пакету, когда он относительно близок к серверу. Тесты, используемые в документе, не учитывают поддельные IP-адреса или тот факт, что злоумышленник, скорее всего, использует зомби-машины.

Также существует другая модель отслеживания, в которой используется DataProtectionManager (менеджер защиты данных) и данные обучения для информирования фильтров в нейронной сети. Эта система имеет вероятность успешного определения примерно 75 % трафика атак, а также значительные временные изменения в скорости обнаружения атаки от 20 мс до 1 с, которые могут привести к сбою проверенных пользователей при доступе к системам [5]. Система предназначена для защиты от чрезмерного XML, чрезмерного шифрования, потокового HTTP-трафика, подмены вебсервисов и принудительного анализа. Обратный прокси адрес используется как фильтр для перехвата всех запросов на обеспечение. Этот фильтр не добавляет никаких накладных расходов в облаке, и пользователи не замечают никакого эффекта на их обслуживание. Веб-служба принимает только запросы, поступающие из системы защиты, в которой была произведена проверка. Однако сам сервер защиты может быть восприимчив к атакам извне, особенно от инсайдеров. Чтобы добавить дополнительную безопасность к этому подходу, для пользователей, пытающихся подключиться к вебслужбам, необходимо принудительно требовать проверки подлинности [6].

Атаки LOS (медленных приложений) нередко обнаруживаются с использованием методов сопоставления образцов или методов измерения порога из-за их низкой тактики потребления ресурсов. Эта система на основе ссылок снижает атаки с использованием инфраструктуры, определенным программным обеспечением. Существуют методы, используемые для обнаружения LOS DDoS [6].

Эти методы вводят подход «исцеления», который переносит легитимных пользователей с компромиссов на вновь созданные виртуальные машины. Использование «SharkTanks» представлено как области изоляции для потенциально вредоносного трафика. Это позволяет отслеживать подозрительных пользователей, продолжая получать подходящий уровень доступа к приложениям в случае неправильного перенаправления законного пользователя. Чтобы ограничить информацию, которую злоумышленники

могут обнаружить с помощью атак сканирования, используют автономные свойства генерации облачной базы для предоставления услуг на случайно сгенерированных и назначенных прокси-узлах. Машины злоумышленников с использованием поддельных IP-адресов становятся неэффективными, так как они не будут получать сообщения переназначения сервера. За этим следует внедрение сильных методов аутентификации, чтобы предотвратить доступ внешних злоумышленников к прокси-узлам [4]. Эта система полностью зависит от того, скрыты ли IP-адреса ключевых компонентов, но нет описания того, как это может быть достигнуто.

В настоящее время все наборы данных, используемые для создания моделей, используемых системой, хранятся централизованно сервером приложений, что делает его целью для злоумышленников. Автор предлагает «жадный» алгоритм, который обеспечивает «почти оптимальное» средство для назначения пользователей прокси-узлам, позволяя им «перетасовывать», когда атака обнаруживается против прокси-узла. Повторная перетасовка пользователей между вновь созданными узлами позволяет системе идентифицировать инсайдеров, запускающих атаку. Этот подход расширен в системах маленького цикла, где вводится новый выбор алгоритмов для оптимизации планов переназначения времени выполнения.

Оба подхода используют количество постоянных ботов, которое содержит интеллект для миграции серверов в качестве ключевого показателя для расчета оптимизированного шаблона «перетасовки» [5]. Однако в реальном мире это значение можно только оценить. В ВМ отдельные пользователи облака защищены путем создания клонов виртуальных IPS системах, необходимых для фильтрации трафика. Процедура очередей определяется для расчета количества клонов IPS, необходимых для поражения атаки DDoS. Автор предполагает, что для поражения DDoS-атак система защиты должна иметь доступ к большему количеству ресурсов, чем у нападавших. Это означает, что атаки DDoS вряд ли повлияют на всю облачную службу. Тем не менее облачные ресурсы, доступные отдельным клиентам, ограничены, что делает их уязвимыми для DDoS-атак. Опубликованные результаты теоретической оценки показывают, что решение клонирования IPS эффективно и что облако содержит достаточное количество незанятых ресурсов для преодоления атаки.

Следующая предложенная система касается некоторых ограничений сетей наложения, скрывающих местоположение целевых серверов с использованием маршрутизаторов шлюза. Она защищает облака от инсайдерских атак и скомпрометированных пользовательских хост-машин. Каждый прокси-узел содержит фильтр, который представляет собой структуру данных, которая может эффективно проверять наличие определенных значений [7]. Когда выдается предупреждение об атаке, развертываются несколько прокси-серверов пользователя, причем количество пользователей,

назначенных каждому из них, уменьшается вдвое до тех пор, пока не будут обнаружены злоумышленники. Следующая система представляет собой обзор систем защиты от DDoS-атак в беспроводных территориальных сетях (WBAN). Устройства WBAN ограничены ресурсами, что делает их идеально связанными с облаком, где могут выполняться сложные вычислительные требования. Для WBANS было предложено несколько низко-затратных систем. Например, система, которая размещает ПОУ в разных местах облака, которые сотрудничают для обмена предупреждениями о атаке. Эта система предполагает, что узел будет иметь доступную пропускную способность для отправки оповещения, когда он находится под атакой. Большинство предлагаемых моделей обороны в основном сосредоточены на одном типе или точке атаки.

Для разработки эффективной системы обороны и защиты необходимо интегрировать аспекты этих исследовательских систем для защиты от более широкого спектра атак. Это требует усилий, направленных на обеспечение надежной интеграции основных технологий облачных вычислений, чтобы избежать появления новых уязвимостей для модели.

Список используемых источников

1. 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.

2. Красов А. В., Лосин Е. П., Ушаков И. А. Проблема безопасности передачи групповых рассылок в IP-сетях // VI Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х томах. 2017. С. 295–301.

3. Красов А. В., Швидкий А. А. Использование возможностей масштабирования облачной инфраструктуры для оптимизации процесса создания лабораторных стендов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2 томах. 2015. С. 1580–1584.

4. Гельфанд А. М., Пестов И. Е., Катасонов А. И., Рязанцев К. С. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8 С. 91–97

5. Штеренберг С. И. Методика построения поисковой системы для примитивной программы адаптивного действия // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 52–57.

6. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, strong and processing security information and events // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017.

7. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. А. О действующей инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 535–537.

УДК 621.391
ГРНТИ 49.29.15/49.29.17

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПОТЕРЬ В СВАРНЫХ СОЕДИНЕНИЯХ ОПТИЧЕСКИХ ВОЛОКОН

С. Ф. Глаголев, П. М. Лещев

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

На первых этапах развития волоконно-оптической связи коэффициент затухания оптических волокон имел величину порядка нескольких дБ/км и потери на соединение в десятые доли и даже единицы децибел не казались чрезмерными. В настоящее время минимальный коэффициент затухания в волокнах с чисто кварцевой сердцевиной составляет 0,16 дБ/км, а типовое значение 0,2 дБ/км. Потери на соединение 0,2 дБ уменьшают допустимую длину оптической линии на 1 км. Наименьшие потери порядка сотых долей дБ/км обеспечиваются сваркой оптических волокон современными сварочными аппаратами. Однако малые потери достигаются тщательным соблюдением технологии сварки и подготовки свариваемых оптических волокон. Данная работа посвящена вопросам экспериментального измерения потерь в сварных соединениях при различных нарушениях технологии подготовки волокон.

сварка оптических волокон, сварочный аппарат, потери в соединении волокон, оптический рефлектометр, подготовка к сварке.

На нынешнем этапе развития телекоммуникационной отрасли, когда километровые потери в оптических волокнах (ОВ) составляют 0,16–0,22 дБ/км, потери в 0,3–1 дБ на соединение, которые предлагают производители механических соединителей, становятся недопустимо большими. Единственной альтернативой им выступает сварка ОВ (при данном способе соединения потери составляют всего 0,01 – 0,03 дБ) [1].

Рассмотрим основные факторы, влияющие на качество сварки.

Нагрев свариваемых волокон

Для сварки оптических волокон (ОВ) их концы необходимо нагреть до температуры около 2000° [2]. Чаще всего используется электрическая дуга между двумя электродами. При этом профиль теплового поля дуги зависит от чистоты электродов, которые при длительном использовании загрязняются частицами диоксида кремния и/или пыли. Искажения профиля нагрева ухудшают качество соединения и увеличивают потери.

В процессе нагрева, тепло от нагретых концов, свариваемых ОВ, распространяется по каждому из них, образуя три области в зависимости от расстояния до места соединения ОВ:

– на расстоянии до 500 мкм поверхность ОВ расплавляется и сглаживается поверхностным натяжением;

– на расстоянии 0,5–2 мм ОВ нагревается до температуры, меньшей температуры плавления, но значительно превышающей температуру окружающей среды. Это приводит к появлению дефектов, ухудшающих прочность сварного соединения;

– на расстоянии свыше 2 мм температура ОВ мало отличается от температуры окружающей среды и структура волокна сохраняется.

Силы сжатия, растяжения и изгиба

Для сварки ОВ жестко закрепляются на расстоянии от 5 до 20 мм от торцов. При этом достаточно минимального воздействия на ОВ (падение пылинки на конец ОВ, вибрация сварочного аппарата), чтобы произошло смещение отъюстированных концов. Это приводит к увеличению потерь в сварке.

Во время сварки размягченные концы ОВ спрессовываются вместе. При этом ОВ в области сварки стремится принять изогнутую форму. Это может приводить к перекосам сердцевин ОВ в месте сварки.

Поверхностное натяжение

Когда два расплавленных конца ОВ соприкасаются друг с другом, их оболочки выравниваются за счет поверхностного натяжения, даже если первоначально они имели смещение. Однако при этом может произойти смещение сердцевин в месте соединения. Для диоксида кремния поверхностное натяжение имеет значение около 0,3 Н/м в диапазоне необходимых для сплавления ОВ температур [2].

При нагреве ОВ в течение длительного промежутка времени или при слишком большой температуре нагрева поверхностное натяжение может вызвать уменьшение диаметра ОВ в непосредственной близости от места соединения. Этот эффект может быть полезен при сращивании ОВ с разными диаметрами.

Диффузия примесей

Параметры ОВ зависят от легирующих примесей. При сварке ОВ нагреваются до высоких температур и происходит диффузия легирующих примесей из сердцевины в оболочку, а также из одной сердцевины в другую. При этом в месте соединения изменяются оптические и механические свойства ОВ. Влияние диффузии увеличивается с уменьшением диаметра сердцевины ОВ, а ее скорость прямо пропорциональна температуре. Это явление может иметь положительный эффект при сращивании разнородных ОВ, делая плавным переход сердцевины первого волокна в сердцевину второго. Однако в случае слишком продолжительного или сильного нагрева может произойти частичное «слияние» сердцевины и оболочки, что негативно отразится на потерях в месте сращивания.

В данной работе были проведены экспериментальные исследования с целью определения фактических потерь, вносимых сварными соединениями в линию, и влияния подготовки ОВ на качество сварки.

Все элементы экспериментальной установки показаны на рис. 1. В качестве источника излучения и измерителя потерь в сварке использовался оптический рефлектометр (OTDR). Сваривались между собой два стандартных ОВ длиной порядка 100 м. Данное положение нормализующей (компенсационной) катушки было выбрано с целью удлинения значимого участка рефлектограммы. В случае выполнения плохого, исследуемого соединения, на участке, соответствующем катушки, на расстояниях кратных длине участка «рефлектометр-место сварки», были бы хорошо заметны пики, вызванные многократными отражениями зондирующего импульса.

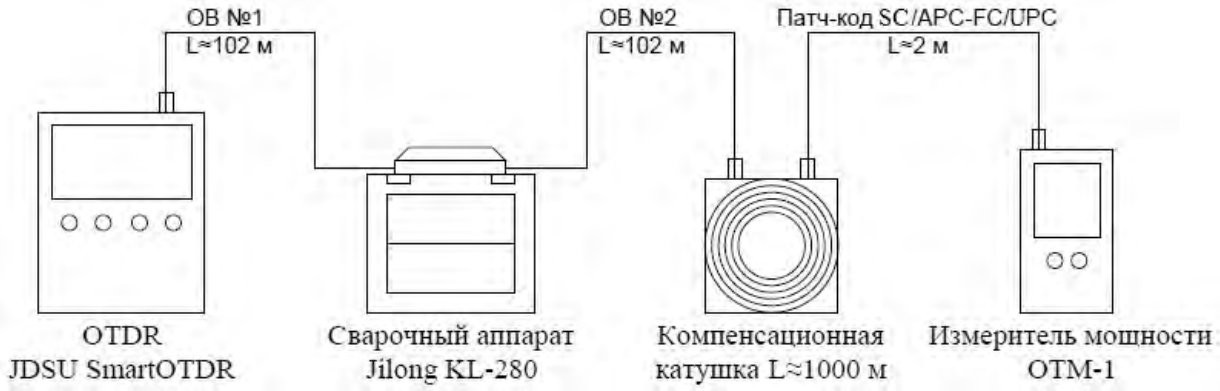


Рис. 1. Схема экспериментальной установки

С целью исследования зависимости потерь, вносимых сваркой, от качества подготовки ОВ был проведен ряд испытаний от a) до e). Условия испытаний изменялись четыре раза от «лучшего» a), с соблюдением всех требований по подготовке ОВ [3], к «худшему» d) варианту. Затем был по-

вторен первый (лучший) вариант e). Во всех случаях, кроме d), для подготовки торцов ОВ использовался высококачественный скалыватель Fujikura CT-30. Для очистки сколотых торцов в вариантах a) и e) использовались фирменные безворсные спиртовые салфетки, в остальных – салфетки для рук, известного производителя. Результаты испытаний и измерений представлены в таблице 1.

ТАБЛИЦА. Результаты экспериментальных исследований

№ изм.	Этап измер.	Длина волны, нм	Потери по сварочному аппарату, дБ	Потери на участке, содержащем сварку по рефлект., дБ	Комментарий
1	До сварки	1310	–	1,834	Крепкое соединение
		1550		0,745	
	После сварки	1310	0,01	0,051	
		1550		0,03	
2	До сварки	1310	–	1,042	Волокно сломалось в районе сращивания после открытия зажимов
		1550		0,564	
	После сварки	1310	0,01	0,053	
		1550		0,038	
3	До сварки	1310	–	1,839	Волокно сломалось в районе сращивания во время теста на прочность
		1550		0,273	
	После сварки	1310	0,01	0,044	
		1550		0,019	
4	До сварки	1310	–	>10	Сварочный аппарат не допустил сварку
		1550		>10	
	После сварки	1310	–	–	
		1550		–	
5	До сварки	1310	–	1,39	Крепкое соединение
		1550		0,34	
	После сварки	1310	0,01	0,026	
		1550		0,025	

Ниже приведена последовательность испытаний:

a) Подготовка торцов ОВ с соблюдением установленной технологии.

b) Нарушение технологии при протирке торцов ОВ.

c) Нарушение технологии при протирке торцов ОВ и искусственное загрязнение торцов путем прикосновения к ним пальцем.

d) Нарушение технологии при протирке торцов ОВ. Скол производился канцелярским ножом.

e) Повтор испытания а) с соблюдением установленной технологии.

Отметим, что до сварки ОВ потери в соединении большие и легко измеряются с помощью OTDR. После сварки потери становятся очень маленькими и практически не видны на рефлектограмме. Для их оценки использовалось измерение затухания Δa между двумя курсорами $\Delta l = 133 - 94 = 39$ м.

Так, например, из рефлектограммы (рис. 2), полученной в пятом испытании на длине волны 1310 нм, следует, что потери на участке Δl ОВ, в центре которого находится сварка, составили $\Delta a = 0{,}026$ дБ. Потери в соединении для установленной длине волны определялись по выражению:

$$a = \Delta a - \alpha \cdot \Delta l = 0{,}026 - 0{,}4 \cdot 0{,}04 = 0{,}01 \text{ дБ}.$$

Рис. 2. Рефлектограмма, полученная в пятом испытании после сварки

Результат совпал с оценкой потерь самим сварочным аппаратом по анализу изображения места стыка свариваемых ОВ (рис. 3, см. ниже).

Заключение

1. Предложена схема и методика измерения потерь в сварках и других неоднородностях.

2. Показано, что определение потерь в сварках самим рефлектометрам обладает требуемой точностью.

Список используемых источников

1. Листвин А. В., Листвин В. Н., Швырков Д. В. Оптические волокна для линий связи. М. : ЛЕСАрт, 2003. 296 с.

2. Yablon A. D. Optical Fiber Fusion Splicing. Somerset, USA : Springer, 2005. 308 p.

3. Rüdiger P. Field guide to optical fiber technology. Bellingham, Washington USA : SPIEpress 2010. 128 p.

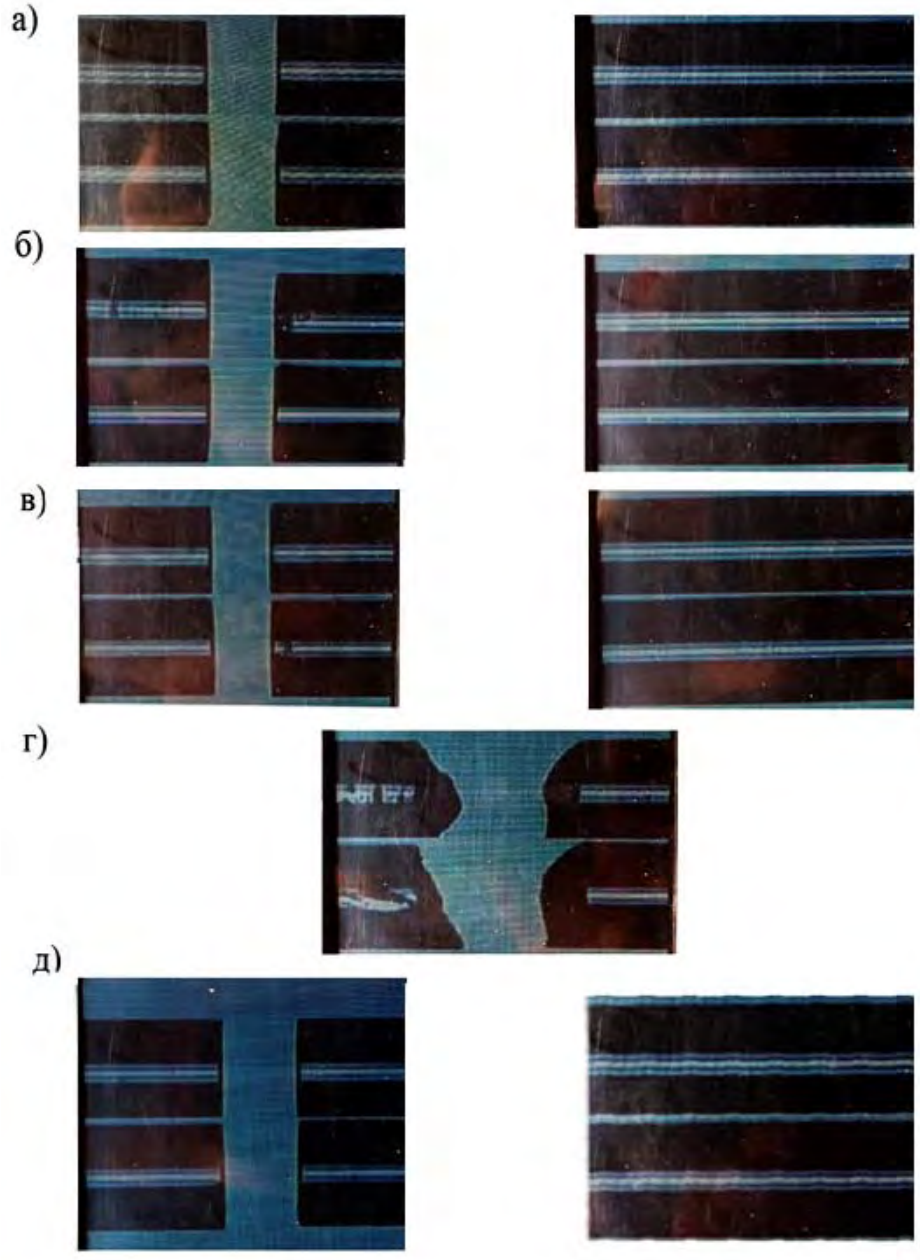


Рис. 3. Изображения свариваемых ОВ в сварочном аппарате до и после сварки

УДК 65.011.56
ГРНТИ 83.77.01

ОЦЕНКА КЛИЕНТСКОГО ОПЫТА С ПОМОЩЬЮ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

А. Б. Гольдштейн, А. А. Кормановская

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

Текущая конкурентная ситуация на рынке телекоммуникаций заставляет компании операторов пересматривать подходы к бизнесу и направлять свой вектор развития не в сторону услуг, а в сторону клиентов и их удовлетворенности. В связи с этим компании активно внедряют в свои бизнес-процессы концепцию Customer Experience Management. Данная концепция включает в себя совокупность методов, процессов и технологий, которые позволяют управлять клиентским опытом. Сам клиентский опыт формируется из огромного количества различных факторов, которые складываются при взаимодействии клиента с компанией. И одним из важнейших аспектов при грамотном построении процесса взаимодействия с клиентом – является совокупный анализ клиентского опыта. В данной работе рассматривается оценка клиентского опыта с помощью нечетких когнитивных карт.

Customer Experience, Customer Experience Management, когнитивные карты, нечеткая логика.

За последние несколько десятилетий рынок телекоммуникаций претерпел большие изменения. С каждым днем конкуренция между компаниями становится все более напряженной. И на сегодняшний день рынок диктует операторам необходимость пересматривать свой подход к бизнесу и ставить на первый план задачи по организации управления взаимоотношениями с клиентами, в том числе задачи по увеличению лояльности, удержанию клиентом. Ведь стоимость привлечения нового клиента в 5–7 раз дороже, чем удержание старого [1]. Поэтому многие компании все активнее внедряют в свои бизнес-процессы концепцию Customer Experience Management – управление клиентским опытом, которая включает в себя совокупность процессов, методов и технологий, ориентированных на управление впечатлениями, которые клиент получает в процессе взаимодействия с компанией.

При этом понятие Customer Experience (CE) складывается из множества факторов, и представляет собой совокупность впечатлений, желаний и ощущений, которая возникает в процессе взаимодействия компании оператора с клиентом на протяжении всего жизненного цикла клиента (*Customer Lifecycle*), начиная от поиска информации об услуге/сервисе, а заканчивая

окончанием ее использования. Customer Lifecycle состоит из девяти этапов, которые представлены ниже:

1. *Be Aware* – описывает деятельность клиента и оператора, которые относятся к маркетинговым аспектам работы с клиентом.

2. *Interact* – определяет маркетинговые аспекты работы с клиентом, но уже начинается двустороннее взаимодействие клиента и оператора. На данном этапе определяется, каким образом клиент запрашивает детали услуги и предложения для бронирования или предварительного заказа.

3. *Choose* – описывает выбор предложения для покупки. На данном этапе клиент окончательно определяется с конфигурацией и выбором услуги. Так же на данном этапе описываются и такие важные аспекты, как инсталляция и первичная настройка выбранной клиентом услуги.

4. *Consume* – характеризует аспекты, связанные с использованием сервиса, а именно с удовлетворенностью клиента, качества предоставляемого сервиса и др.

5. *Manage* – определяет возможности управления сервисом, получение помощи при использовании сервиса, а также запросы, связанные с устранением неисправностей работоспособности сервиса.

6. *Pay* – характеризует жизненный цикл клиента с точки зрения возможностей и удобства оплаты уже подключенного сервиса, его тарификации, управления тарификацией, получения и управления счетами.

7. *Renew* – описывает аспекты, связанные с обновлением соглашения на использование сервиса (возобновлением договорных отношений клиента и оператора).

8. *Recommend* – характеризует аспекты, связанные с упоминаний сервиса и компании в различных источниках. На данном этапе также рассматриваются вопросы, связанные с наращиванием оператором лояльности клиента.

9. *Leave* – определяет аспекты, связанные с прекращением взаимоотношений между клиентом и оператором, включает в себя процедуру отключения сервиса/услуги.

Если проанализировать весь жизненный цикл клиента, можно сделать вывод, что факторами, формирующие клиентский опыт, являются различные аспекты деятельности компании оператора, например, технические характеристики сети оператора связи, разнообразие предоставляемых услуг, качество и возможности предоставляемого сервиса [2], уровень развития каналов взаимодействия с клиентом и т. д. Становится очевидно, что именно агрегация и совокупный анализ данных позволит операторам построить грамотную политику взаимодействия с клиентом, но без специализированных математических методов это сделать просто невозможно [2].

На данный момент существует огромное количество различных методов по анализу данных, например, нейронные сети, байесовские сети, нечеткие когнитивные карты. Но последние являются одним из перспективных направлений современной теории поддержки и принятия решений.

Нечеткие когнитивные карты появились в последней четверти XX века и сразу приобрели популярность. На сегодняшний день нечеткие когнитивные карты – это база для описания проблемно-ориентированных систем динамического моделирования в различных областях (финансы, образование, бизнес, медицина) [3]. Когнитивная карта отображается в виде знакового ориентированного графа:

$$\mathrm{G} = \langle V, E \rangle,$$

где V – множество факторов; $V_i \in V, i = 1, 2, \ldots, k$; E – набор связей между элементами данного множества.

Дуга $eij \in E$, $i, j = 1, 2, \ldots, n$ соединяет вершины графа, которые соответствуют ключевым факторам проблемного поля, наиболее значимым для управления проблемой [4]. Влияние факторов друг на друга может быть:

– положительным (+) – характеризует влияние фактора *A* на фактор *B*, при этом, если фактор *A* изменяется в большую сторону, то непосредственно и фактор *B* также изменяется в большую сторону и наоборот;

– отрицательным (-) – характеризует влияние фактора *A* на фактор *B*, при этом, если фактор *A* изменяется в большую сторону, то фактор *B* изменяется в меньшую сторону, если фактор *A* изменяется в меньшую сторону, то фактор *B* измениться в большую сторону [5];

– нулевым (0) – характеризует отсутствие влияния фактора *A* на фактор *B*.

Такой математический аппарат дает возможность работать с данными как качественного, так и количественного типа, причем степень использования количественных данных может увеличиваться в зависимости от возможностей количественной оценки взаимодействующих факторов в итерационном цикле моделирования [2].

Давайте рассмотрим применение нечетких когнитивных карт для анализа клиентского опыта. В качестве исследования были выбраны метрики, стандартизованные организацией *TM Forum*, которые позволяют оценивать клиентский опыт на различных этапах жизненного цикла клиента (*Customer Lifecycle*), а именно на этапах “Choose”, “Consume” и “Manage”. Для построения нечеткой когнитивной карты необходимо:

– выделить ключевые факторы;

– определить между ними взаимосвязь;

– определить между ними степень влияния.

Процесс выделения ключевых факторов состоит из последовательности определенных шагов – проведение SWOT и PEST анализа предметной

области, выделение наиболее важных факторов, оказывающие различные влияния на исследуемую область [4]. В результате анализа формируется проблемное поле в виде совокупности ключевых факторов и описывается с помощью формулы, которая была представлена выше. Итак, для исследования ключевыми показателями были выбраны следующие метрики:

– этап “Choose”: CH-C-1 (*Customers Acquired*), CH-C-3 (*Orders Successful*), CH-C-11 (*Hours to Deliver, from Request to Delivery*), CH-F-2 (% *Orders of Enquiries*), CH-F-25 (*Seconds per Account Activation, from Request to Activation*);

– этап “Consume”: CO-C-4 (*Seconds per Call Origination, from CM Service Request to Alerting*), CO-C-7 (% *Calls Dropped Perceived*), CO-C-8 (% *Call Good Voice Quality*), CO-E-7 (*Product Subjective Score* (*Enterprise*)), CO-E-10 (% *Streaming Sessions Disconnected*), CO-F-1 (*Network* NPS), CO-F-7 (*Service Interruptions*), CO-C-104 (% *Bandwidth Utilisation*), CO-C-107 (# *Minutes Between Service Interruptions – Minimum*), CO-E-100 (# *ms* SDH *Peer-to-Peer Transfer Delay – Mean*), CO-E-102 (% *Packets Lost*);

– этап “Manage”: M-C-5 (# *First Contact Resolutions*), M-C-6a (*Incidents Resolved*), M-C-6c (*Incidents Due Closure*), M-C-9a (# *Minutes to Resolve Incident, from Incident Opened to Incident Resolved*), M-C-12 (# *Repeat Contacts*), M-F-3 (*Support Hotline Subjective Score – Manage Service/Profile*), M-F-8 (*Online Channel Subjective Score – Receive Help*), M-F-23 (% *Service Configurations Failed*), M-F-24 (# *Minutes per Service Configuration, from Request to Configuration*) [6].

После этапа выделения ключевых факторов, необходимо оценить, как они взаимосвязаны между собой и как влияют на целевой фактор (положительно, отрицательно или вообще не влияют). Для наглядности связь факторов представлена в виде матрицы взаимовлияния в таблице, которая отображает ключевые факторы этапа «*Manage*» жизненного цикла клиента.

ТАБЛИЦА. Матрица взаимовлияния факторов когнитивной модели

Ключевой фактор / Влияющий фактор	M-C-6a	M-C-5	M-C-6c	M-C-9a	M-C-12	M-F-3	M-F-8	M-F-23	M-F-24	Целевой
M-C-6a	x	+	0	0	–	+	+	0	0	+
M-C-5	0	x	0	0	–	+	0	0	0	+
M-C-6c	+	0	x	–	–	+	+	0	0	+
M-C-9a	0	0	–	x	0	–	0	0	0	–
M-C-12	0	+	0	0	x	–	–	0	0	–
M-F-3	0	+	0	0	0	x	0	0	0	+
M-F-8	0	0	0	0	0	+	x	0	0	+

Ключевой фактор / Влияющий фактор	M-C-6a	M-C-5	M-C-6c	M-C-9a	M-C-12	M-F-3	M-F-8	M-F-23	M-F-24	Целевой
M-F-23	0	–	0	0	0	–	–	x	0	–
M-F-24	0	–	0	0	0	–	–	+	x	–

Далее ключевые и целевые факторы, их взаимосвязь, а также влияние друг на друга можно визуализировать в виде нечеткой когнитивной карты (рис.).

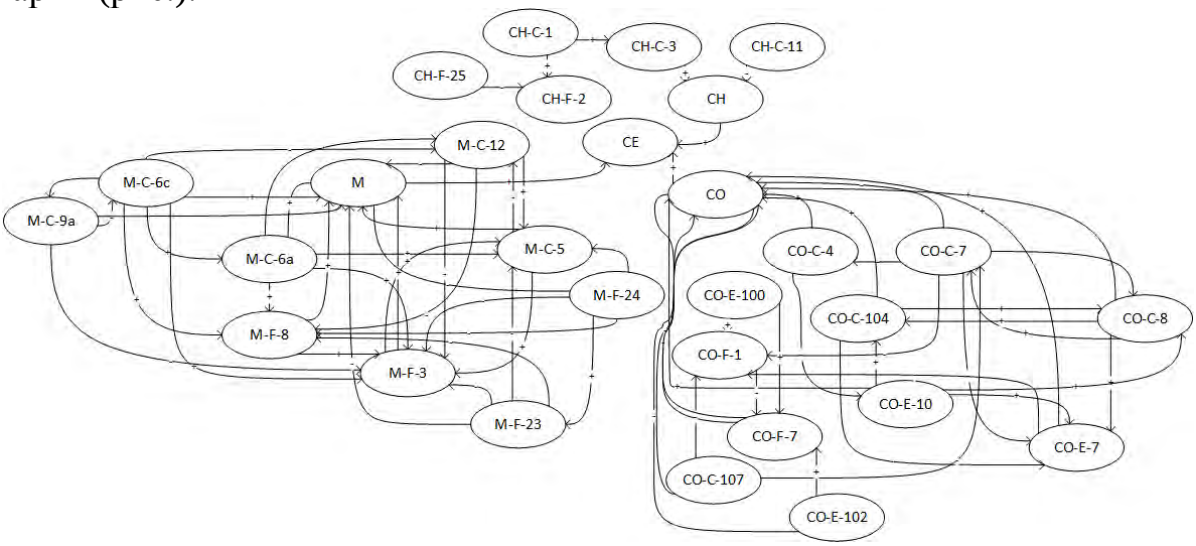


Рисунок. Когнитивная карта моделируемой области

В рамках данной статьи были рассмотрены возможности использования когнитивных карт и нечеткой логики применительно к оценки клиентского опыта на различных этапах жизненного цикла клиента. Именно применение нечетких когнитивных карт позволяет реализовывать эффективное управление Customer Experience. Зная матрицу взаимовлияний факторов, можно вполне с высокой точностью моделировать и визуализировать возможные результаты воздействия на один или несколько факторов.

Список используемых источников

1. Пожарский Н., Лихачев Д., Кисляков С. Использование когнитивных карт и нечёткой логики в разработке OSS/BSS решений для операторов связи // T-Comm – телекоммуникации и транспорт. 2017. Т. 11, № 11. С. 21–25.

2. Кулинич А. Систематизация когнитивных карт и их методы анализа // Когнитивный анализ и управление развитием ситуаций // Труды VII Международной конференции / Под ред. З. К. Авдеевой, С. В. Ковриги. М. : Институт проблем управления РАН, 2007. С. 50–56.

3. Маренко М., Мальцева М., Применение когнитивного моделирования для анализа проблем малого бизнеса // Известия Иркутской государственной экономической академии. 2015. Т. 25, № 6. С. 59–65.

4. Акишин В. А. Пользовательский опыт в когнитивной модели управления сетью оператора связи // T-Comm – телекоммуникации и транспорт. 2017. Т. 11, № 10, С. 13–18.

5. Палюх Б. В. Нечеткая когнитивная карта как инструмент моделирования инновационной деятельности на региональном уровне // Международный научно-практический журнал – Программные продукты системы. 2012. № 4. С. 30–34.

6. TM FORUM. GB962A_Lifecycle_Metrics_R15.0.1. TM Forum; December, 2015.

УДК 654.1
ГРНТИ 83.77.01

ПРИМЕНЕНИЕ МЕТОДОВ ТЕОРИИ ХАОСА ДЛЯ ПРОГНОЗИРОВАНИЯ НАГРУЗКИ КОНТАКТ-ЦЕНТРА

А. Б. Гольдштейн, Д. А. Терентьев

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

На современном рынке контакт-центры остаются эффективными инструментами взаимодействия с клиентами. Важнейшей проблемой в этом случае является поддержание оптимального качества обслуживания. Неотъемлемой частью данного процесса является прогнозирование нагрузки на контакт-центр с последующим составлением расписания для сотрудников, что позволяет добиться требуемого качества обслуживания и оптимизировать расходы на персонал. В данной статье исследуется возможность применения методов прогнозирования теории хаоса для данной задачи, приводится сравнительный анализ их эффективности.

теория хаоса, прогнозирование, контакт-центр, WFM.

Контакт-центры стали логичным развитием Call-центров в условиях развития и конвергенции сети передачи данных и сети ТФОП. Качественный прием вызовов, возможность обновлять статистические данные о клиентах и предоставление им исчерпывающей информации позволяют комплексно организовать продажу товаров и услуг, предоставляемых компанией, не теряя и систематизируя поступающую от клиентов информацию разного рода. Все это может стать отличным инструментом для успешного ведения бизнеса. Для создания благоприятного впечатления от пользования услугами контакт-центра необходимо обеспечить хороший уровень качества обслуживания. Для этого, в том числе, требуется оптимально выбирать производительность контакт-центра для снижения времени ожидания.

Этого можно достичь, прогнозируя нагрузку на систему. Появление различных типов обращений (IP-телефония, различные чаты, электронная почта и т. д.), увеличение количества услуг контакт-центров привели к тому, что существующие методы прогнозирования уже могут не в полной мере гарантировать точный прогноз, т. к. поступающая нагрузка начала демонстрировать хаотичный характер, о чем будет сказано позднее.

Важным аспектом управления работой контакт-центра является управление персоналом (*Work force management*). WFM это общее название цикла процессов планирования результатом которого является расписания для персонала обычно на недельный период. Анализ производится на основе данных о входящем трафике за предыдущие периоды и производительности операторов. Итогом работы становится расписание для каждого оператора кол центра.

WFM применительно к контакт-центрам можно разбить на несколько этапов:

– прогнозирование нагрузки на определенных временных интервалах (обычно 30 мин.);

– определение количества операторов, и при необходимости операторов с определенной квалификацией, которые должны находиться в определенный временной интервал на рабочих местах;

– формирование расписания работы сотрудников контакт-центра.

Для качественной работы процедур WFM необходимо производить максимально точное прогнозирование. Ведь эти данные являются входными для всех остальных этапов, точность результатов которых будет полностью зависеть от них по принципу GIGO (*Garbage in garbage out*) [1].

Именно поэтому объектом нашего исследования стала теория хаоса или теория нелинейных детерминированных динамических систем, являющаяся одним из математических аппаратов, которые могут помочь в решении данной задачи.

Теория хаоса является математическим аппаратом, позволяющим анализировать динамические системы, находящиеся в состоянии хаоса. Динамической называется система, для которой задана функциональная зависимость между временем и положением ее элементов в фазовом пространстве. Фазовое пространство иначе можно назвать пространством состояний, каждой точке которого соответствует состояние системы [2].

Явление динамического хаоса характеризуется кажущейся случайностью процесса, хотя он определяется детерминированными законами. Причиной таково поведения является высокая чувствительность таких систем к изменению начальных условий.

Для прогнозирования процессов можно использовать следующие методы:

– простое нелинейное прогнозирование (*Simple nonlinear prediction*);

– локальное линейное прогнозирование (*Locally linear prediction*);

– глобальная полиномиальная аппроксимация (*Global function fits*).

Пусть нашей целью будет спрогнозировать значение хаотичного временного ряда $x(t + T)$.

Первоначально необходимо сформировать фазовое пространство из оригинального временного ряда $x(t)$. Создадим вектор состояний $\mathbf{x}(t)$ с координатами равными задержанной на кратные промежутки времени соответствующей точкой оригинального временного ряда $x(t)$: $\mathbf{x}_1(t) = x(t)$, $\mathbf{x}_2(t) = x(t - \tau)$, $\mathbf{x}_3(t) = x(t - 2\tau)$, $\mathbf{x}_d(t) = x(t - (d - 1)\tau)$ где τ – время задержки, d – размерность (должна превышать размерность аттрактора).

Следующим шагом будет определение функциональной зависимости между текущем состоянием $\mathbf{x}(t)$ и будущим $\mathbf{x}(t+T)$:

$$\mathbf{x}(t + T) = f_T(\mathbf{x}(t)).$$

Нашей задачей будет нахождение предиктора F_T аппроксимирующего f_T.

Для борьбы с накапливанием ошибки используется метод локальной аппроксимации, что предполагает использование только ближайших состояний для создания прогноза. Найдем k ближайших соседей $\mathbf{x}(t)$, то есть такие состояния $\mathbf{x}(t')$, что при $t' < t$ норма вектора $\| \mathbf{x}(t)\text{-}\mathbf{x}(t') \|$ будет минимальна.

Следующим шагом будет создание предиктора, связывающего каждый вектор $\mathbf{x}(t')$ из области определения с соответствующим $x(t'+T)$ из области значений. В простейшем случае нелинейного предсказания в качестве такого предиктора выбирается локальная аппроксимация константой, то есть используем аппроксимацию ближайших соседей. Тогда предсказание выглядит таким образом:

$$x(t + T) = \frac{1}{|U_m|} \sum_{x(t') \in U_m} \mathbf{x}(t' + T),$$

где U_m – окрестность $\mathbf{x}(t)$, за исключением самой $\mathbf{x}(t)$.

Данный метод и получил название простое нелинейное прогнозирование.

Для получения более достоверных результатов в случае, когда f_T довольно гладкая, можно использовать линейную локальную аппроксимацию в рамках метода локального линейного прогнозирования. В этом случае предсказание примет вид:

$$x(t + T) = a_n \mathbf{x}(t) + b_n,$$

где a_n, b_n находятся из (1)

$$\sum_{x(t') \in U_m} (\mathbf{x}(t' + T) - a_n \mathbf{x}(t') - b_n)^2 \to min. \qquad (1)$$

И последним рассмотренным методом будет глобальная полиномиальная аппроксимация. Данный метод может быть использован в случае, когда метод локальной линейной аппроксимации невозможно применить в силу, например, отсутствия решения для условия (1). В таком случае для поиска F_T воспользуемся условием [3].

$$\sum_t (\mathbf{x}(t' + T) - f_T(\mathbf{x}(t')))^2 \to min.$$

Перейдем к формированию временного ряда, поведение которого будет прогнозироваться.

Для работы сформируем из исходного временного ряда $p = \{p(t_1), p(t_2), \ldots, p(t_n)\}$, представляющего собой вызовы, обладающие рядом параметров, эквивалентный ряд с равным шагом (необходимо для верного прогнозирования) Δt, $Y = \{Y(\Delta t), Y(2\Delta t), \ldots, Y(N\Delta t)\}$, каждый элемент которого представляет собой общее время обработки вызовов операторами за время Δt. $Y_N = \frac{1}{\Delta t}\sum_{t_i>(N-1)\Delta t}^{t_i<N\Delta t} T(t_i)$, где T время одного разговора принятого в момент t_i.

Таким образом, временной ряд представляет собой нагрузку на участке Δt.

В качестве исходного временного ряда воспользуемся данными вызовов контакт-центра анонимного банка. Каждый вызов описывается записью в текстовом файле, содержащей 17 параметров (их описание приведено в документе). Имеются данные за год, разбитые по месяцам. Один текстовый файл на месяц. В каждом файле записи об около 30 000 вызовов.

Стоит отметить, что сформированный временной ряд является хаотичным, т.к. имеет неотрицательный показатель Ляпунова. Развернутое доказательство данного суждения будет приведено в одноименной дипломной работе. Таким образом теория хаоса вполне подходит для описания и прогнозирования данного процесса [4].

Используем Δt = 30 мин., данное значение подходит с точки зрения практического использования в WFM, выбор так же обусловлен свойствами временного ряда нагрузки, рассмотрение которых осталось за рамками данной статьи [5].

Таким образом получаем временной ряд, представляющий собой нагрузку контакт-центра на протяжении месяца (для эксперимента был выбран май).

В качестве интервала прогнозирования выберем одну неделю – оптимальный вариант для использования в WFM.

Таким образом у нас получились 3 варианта прогноза.

Для оценки эффективности выбранных нами математических методов спрогнозирована уже существующая часть временного ряда. Сравним прогноз с реальным значением (рис. 1–3 синий график с маркером точка – реальные значения, зеленый график с маркером круг – прогноз) и рассчитаем абсолютную погрешность прогноза, представляющую собой абсолютное значение разности спрогнозированных значений и реальных значений на протяжении всего недельного интервала прогнозирования для трех использованных методов (рис. 4).

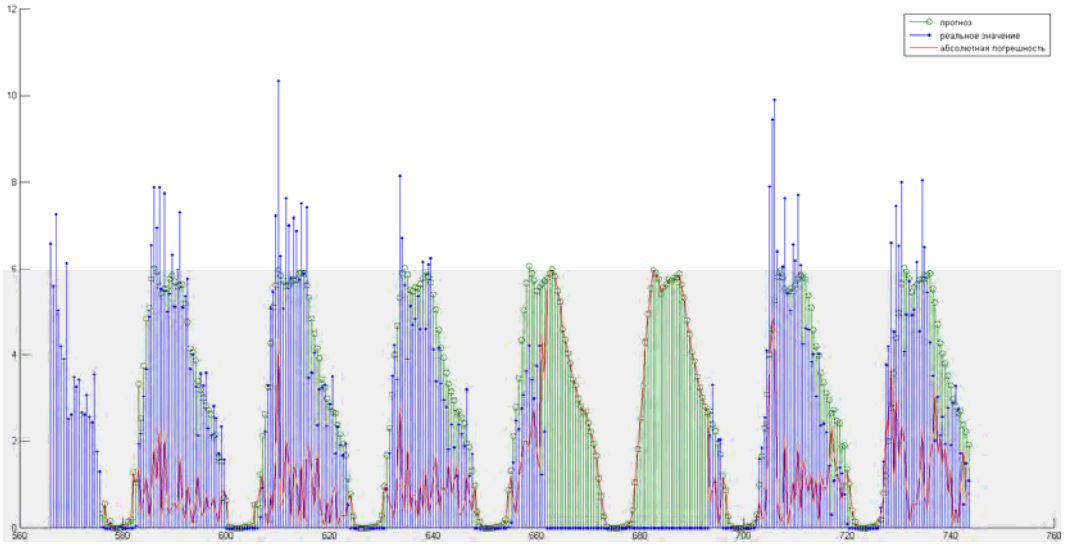


Рис. 1. Прогноз с использованием метода простого нелинейного прогнозирования

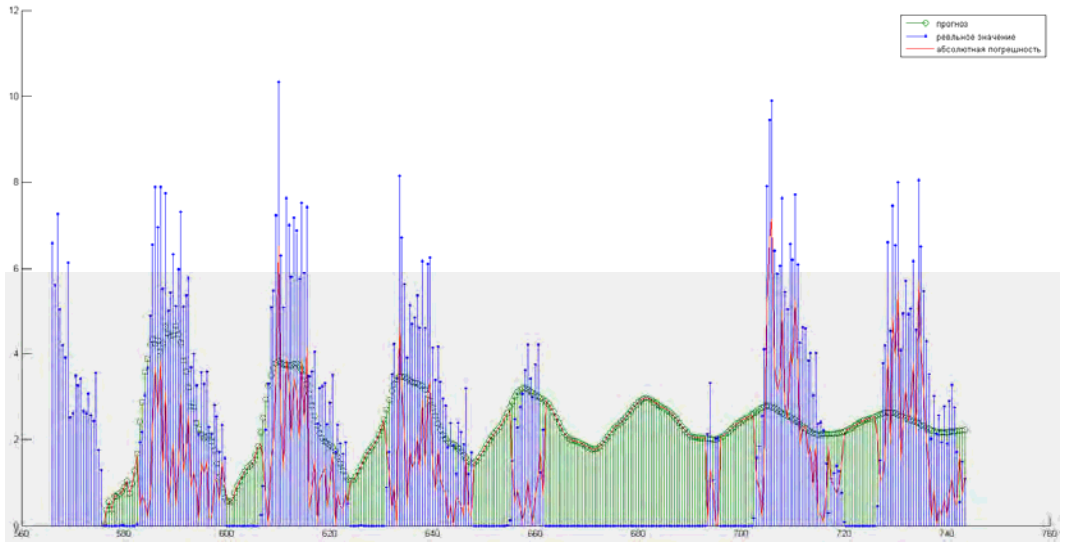


Рис. 2. Прогноз с использованием метода локального линейного прогнозирования

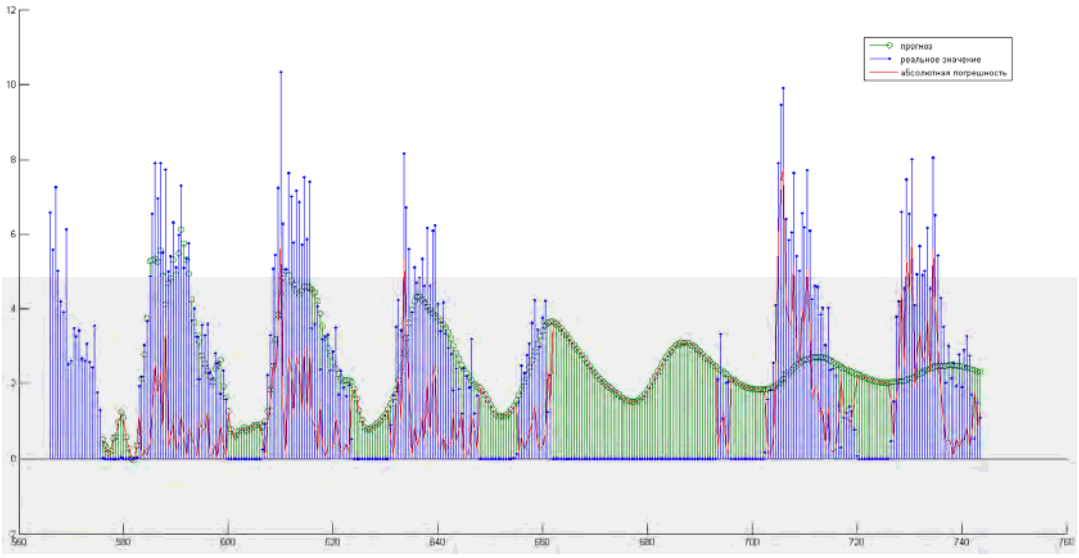


Рис. 3. Прогноз с использованием метода глобальной полиномиальной аппроксимации

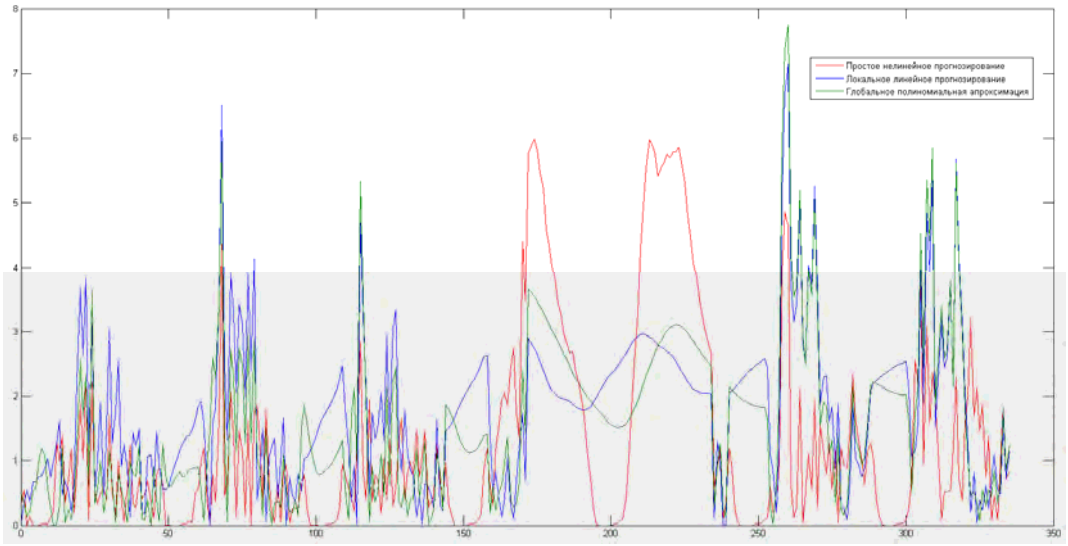


Рис. 4. Сравнение графиков абсолютных погрешностей прогноза

Анализ полученных графиков показал, что лучше всего со своей задачей справился метод простого нелинейного прогнозирования, показав неплохие результаты как на краткосрочный прогноз (около суток), так и среднесрочный (неделя). Остальные методы давали приемлемый результат примерно на суточном интервале. можно сделать вывод, что для прогнозирования нагрузки контакт-центров оптимально выбрать именно его. Следующим нашим шагом может быть построение на его основе рабочего алгоритма работы системы прогнозирования WFM для контакт-центров.

Список используемых источников

1. Koole G. Call Centers Optimization, Amsterdam: MG books, 2013, pp. 1–4.

2. George Contopoulos. Highlights of chaos research [Электронный ресурс] // The Nonlinear Sciences archive, 2018. URL: https://arxiv.org/pdf/1807.09492.pdf (дата обращения 07.04.2019).

3. J. Doyne Farmer John J. Sidorowich Predicting chaotic time series // Physical review letters. 1987. N 8. pp. 845–848.

4. Мун Ф. Хаотические колебания: Вводный курс для научных работников и инженеров: пер. с англ. М. : Мир, 1990. С. 71–73.

5. The Latest Techniques for Call Centre Forecasting [Электронный ресурс] // Call center helper: электронный журнал. 2019. URL:https://www.callcentrehelper.com/the-latest-techniques-for-call-centre-forecasting-117394.htm (дата обращения 07.04.2019).

УДК 65.011.56
ГРНТИ 49.01.85

ПРОГНОЗИРОВАНИЕ С ПРИМЕНЕНИЕМ НЕЙРОННОЙ СЕТИ В СИСТЕМАХ КЛАССА OSS

А. Б. Гольдштейн, А. А. Шестакова

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

Системы класса OSS являются особо востребованными для компаний, которые подчеркивают клиентоориентированность своего бизнеса, работающих в условиях высокой конкуренции и динамичности. Они дают инструментарий для детального анализа коренных причин текущей ситуации в компании. В сочетании с нейронными сетями системы класса OSS становятся мощнейшим инструментом для бизнеса. Свойство нейронной сети обучаться делает её наиболее привлекательной. В системах класса OSS нейронные сети чаще всего используются для прогнозирования. В сфере телекоммуникаций прогнозу могут подлежать такие параметры, как отток клиентов, лояльность клиентов, а также расчёт оптимального количества операторов call-центров.

системы класса OSS, нейронная сеть, лояльность, отток клиентов, операторы call-центров.

В настоящее время всё больше компаний начинают искать пути для сокращения издержек. Такими путями могут стать отбрасывание балласта, жесткое контролирование расходов, повышение требований к производительности труда сотрудников.

Одним из главных инструментов для проведения подобных мероприятий являются системы класса OSS [1, 2].

Такие системы наиболее интересны для компаний, работающих в условиях высокой конкуренции и быстро изменяющейся среды, ориентирован-

ных на удовлетворение клиентов. В первую очередь к ним относятся телекоммуникации, розничная и оптовая торговля, страхование, банки. В статье более подробно рассмотрено применение WFM-систем для сферы телекоммуникаций.

В сочетании с нейронными сетями, WFM становится мощнейшим инструментом для бизнеса. Нейронная сеть обладает таким важным свойством, как возможность к обучению, что безусловно делает её ещё более привлекательной.

Среди всех методов обучения можно выделить два класса:

1. Детерминированный метод итеративно корректирует параметры сети, основываясь на ее текущих параметрах, величинах входов, фактических и желаемых выходах. Пример: метод обратного распространения ошибки.

2. Стохастические методы изменяют параметры сети случайным образом. При этом сохраняются только те изменения, которые привели к улучшениям. Такие методы могут попасть в «ловушку» локального минимума.

В системах WFM нейронные сети чаще всего применяются для прогнозирования. Основной идеей прогнозирования является то, что предыдущие изменения действительно в какой-то степени предопределяют будущие.

Эффективное прогнозирование помогает гарантировать, что компания будет приносить прибыль, и что капитал вкладывается рационально.

В сфере телекоммуникаций прогнозу могут подлежать такие параметры, как отток клиентов, лояльность клиентов, а также расчёт оптимального количества операторов call-центра. Ухудшение качества предоставляемых услуг может подталкивать клиентов к отказу от их использования или полному уходу от оператора связи. Уровень лояльности клиента имеет существенное значение при определении комплексного уровня лояльности клиентов к услуге связи и оказывает влияние на величину комплексной оценки качества обслуживания клиентов на региональном уровне.

Схожесть некоторых функций WFM-системы для сотрудников технических служб оператора связи позволила создать систему управления контакт-центрами как оператора связи, так и служб такси, грузовых терминалов, магазинов и т. д., реализующую, например, функции составления и оптимизации расписаний или распределения нагрузки между работниками.

Цели системы:

– минимизировать затраты на операторов;
– повысить лояльность клиентов;
– увеличить эффективность работы управляющего звена;
– повысить лояльность операторов.

На основе таких данных, как графики смен, предпочтения операторов, прогнозируемая нагрузка, информация об особых событиях операторов,

бизнес-правила и регламенты обедов/перерывов можно грамотно спланировать расписание приёма звонков/перерывов/обедов; оценить качество составленного расписания (рис. 1).

Рис. 1. Планирование в WFM-CC

Используя такие параметры как допустимое время ожидания в очереди, среднее время постобработки, среднее время разговора, уровень сервиса, историю принятых звонков за предыдущие периоды можно спрогнозировать:

– оптимальное число операторов, которое сможет обработать поток звонков клиентов с заданным качеством обслуживания;

– количество звонков, которое может поступить в разное время с учетом праздников, погодных условий, настроений клиентов и других факторов (рис. 2).

Рис. 2. Прогнозирование в WFM CC

На графиках наглядно продемонстрирована проблема избытка/недостатка операторов в часы наивысшей нагрузки системы звонками (рис. 3).

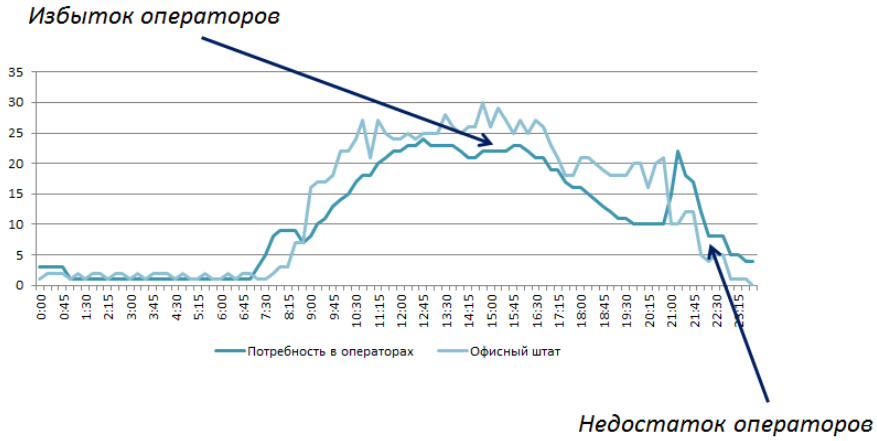


Рис. 3. График связи числа операторов и количества звонков в часы наивысшей нагрузки системы звонками

Эта проблема легко решается с помощью прогнозирования, следствием чего является составление для операторов гибких графиков работы (рис. 4).

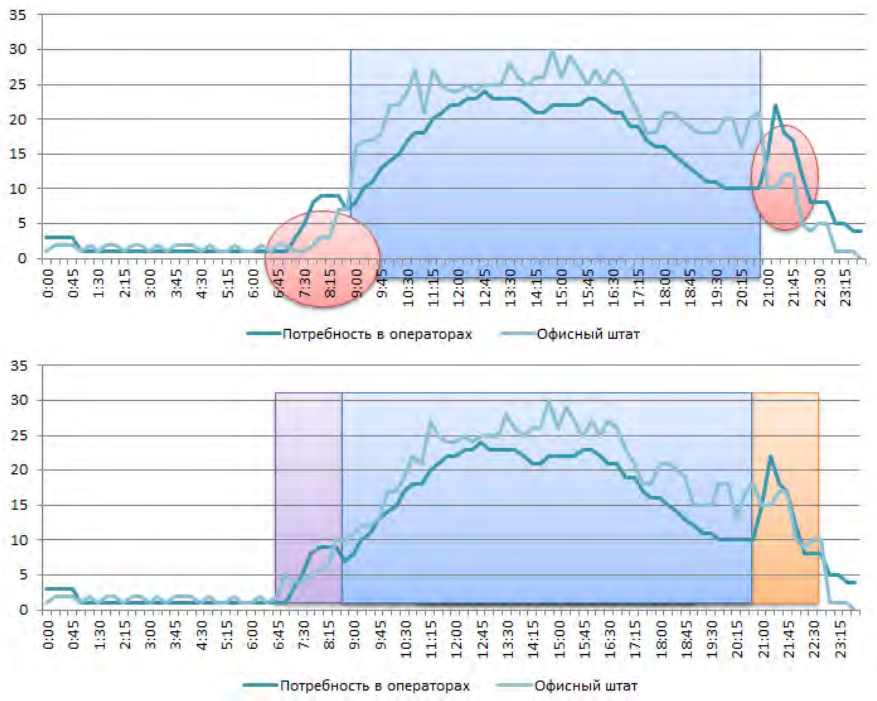


Рис. 4. Пример варьирования начала смены с сохранением её длительности.

Наиболее часто используемой структурой нейронной сети является однослойная нейронная сеть с прямым распространением – однослойный парцептрон, состоящий из искусственных нейронов. Искусственный нейрон

имитирует в первом приближении свойства биологического нейрона, главная функция которого – формировать выходной сигнал в зависимости от сигналов, поступающих на его входы [3].

На вход искусственного нейрона поступает некоторое множество сигналов, каждый из которых является выходом другого нейрона. Каждый вход умножается на соответствующий вес, аналогичный синаптической силе, и все произведения суммируются, определяя уровень активации нейрона.

На рис. 5 представлена модель, реализующая эту идею. Множество входных сигналов, обозначенных x_1, x_2,…, x_n, поступает на искусственный нейрон.

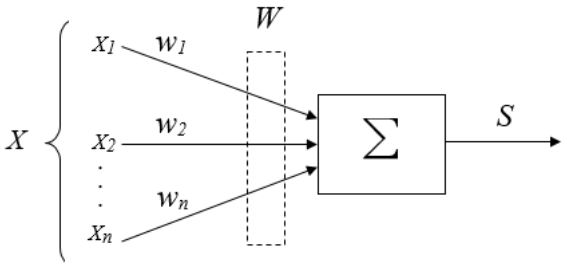


Рис. 5. Модель искусственного нейрона

Каждый вес соответствует «силе» одной биологической синаптической связи. Текущее состояние нейрона определяется как взвешенная сумма его входов:

$$S = \sum_{i=1}^{n} x_i w_i,$$

где n – число входов нейрона; x_i – значение i-го входа нейрона; w_i – вес i-го синапса.

Процесс обучения нейронной сети заключается в подстройке ее внутренних параметров под конкретную задачу. Алгоритм работы нейронной сети является итеративным, его шаги называют эпохами или циклами.

Эпоха – одна итерация в процессе обучения, включающая предъявление всех примеров из обучающего множества и, возможно, проверку качества обучения на контрольном множестве.

Процесс обучения осуществляется на обучающей выборке. Обучающая выборка включает входные значения и соответствующие им выходные значения набора данных. В ходе обучения нейронная сеть находит некие зависимости выходных полей от входных.

В качестве входных данных используются исторические данные.

Набор параметров изменяется в соответствии с поставленной задачей прогнозирования.

В заключении отметим: WFM-системы в совокупности с нейронными сетями – это сбор, управление, распределение и анализ информации с целью выработки такого видения проблемы, которое позволяет принять наилучшее решение. Такая система поддерживается данными из хранилищ, методами разработки данных, технологиями поддержки принятия решений, способствует увеличению доходов операторов связи, повышению лояльности клиентов и продаже пакетов услуг с заданной вероятностью.

Список используемых источников

1. Colin Ashford, Pierre Geuthier: OSS Design Patterns. Berlin : Springer, 2009. 151 p.
2. TM Forum [Электронный ресурс]. URL: https://www.tmforum.org, (дата обращения 10.01.2019).
3. Галушкин А. И. Нейронные сети. Основы теории. М. : Горячая линия – Телеком, 2012. 496 с.

УДК 621.391
ГРНТИ 49.33.29

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ОБУЧЕНИЯ ПОСТРОЕНИЮ ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЕЙ SDN

И. М. Гордеев, М. В. Модель, А. С. А. Мутханна

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

В данной статье рассматривается вопрос обучения построению современных сетей SDN. Для построения и поддержания программно-конфигурируемых сетей в существующих условиях, требуются подготовленные специалисты, обладающие необходимым набором теоретических знаний и практических навыков. В целях решения данной задачи, авторы статьи предлагают программный комплекс, который предоставляет возможность изучения теории, прохождения тестирования, а также моделирования сетей SDN. С помощью разработанного программного комплекса был создан сайт, позволяющий изучить основные принципы построения и работы SDN сетей, применить полученные знания для построения виртуальных программно-конфигурируемых сетей, а также проверить себя с помощью тестирования.

программно-конфигурируемые сети, SDN, обучение.

Программно-конфигурируемые сети – это новая парадигма коммуникации, разработанная для экономически эффективных динамических сетей. Основная идея SDN заключается в физическом разделении плоскости управления и плоскости передачи данных через программируемые контроллеры, что обеспечивает динамическое конфигурирование и управление всей сетью. Этот процесс полностью отличается от традиционных сетей, в которых плоскость передачи данных отвечает за весь процесс коммуникации, и обе плоскости интегрированы в одном устройстве. Плоскость передачи данных включает в себя все устройства, отвечающие за пересылку трафика

через сеть. Плоскость управления содержит в себе все устройства, используемые для принятия решения по обработке трафика. Концепция SDN охватывает взаимодействие между плоскостями управления и передачи данных, поскольку плоскость управления контролирует и управляет всеми устройствами в плоскости передачи данных. Плоскость управления отвечает за установку параметров конфигурации и определения ролей пересылки всех устройств передачи данных, которые выполняют пересылку трафика на основании полученных инструкций [1].

Предприятия, перевозчики и поставщики услуг окружены рядом конкурирующих сил. Монументальный рост мультимедийного контента, взрыв облачных вычислений, влияние растущего использования мобильных устройств и продолжающееся давление со стороны бизнеса с целью сокращения расходов при сохранении неизменных доходов – все это приводит к хаосу в традиционных бизнес-моделях.

Чтобы не отставать, многие из этих игроков обращаются к технологии SDN, чтобы революционизировать дизайн и работу сети.

SDN позволяет программировать поведение сети централизованно с помощью программных приложений, использующих открытые API. Открывая традиционно закрытые сетевые платформы и внедряя общий уровень управления SDN, операторы могут управлять всей сетью и ее устройствами последовательно, независимо от сложности базовой сетевой технологии.

Есть четыре критических области, в которых технология SDN может иметь значение для организаций.

1) Программируемость сети: SDN позволяет контролировать поведение сети с помощью программного обеспечения, которое находится за пределами сетевых устройств, которые обеспечивают физическое соединение. В результате операторы сетей могут адаптировать поведение своих сетей для поддержки новых услуг и даже отдельных клиентов. Отделяя аппаратное обеспечение от программного обеспечения, операторы могут быстро внедрять инновационные, дифференцированные, новые услуги – без ограничений, закрытых и проприетарных платформ.

2) Логическая централизация интеллекта и контроля: SDN построен на логически централизованных сетевых топологиях, которые обеспечивают интеллектуальное управление сетью и сетевыми ресурсами. В традиционных методах управления сетью, устройства функционируют автономно с ограниченной осведомленностью о состоянии сети. Благодаря централизованному управлению, который обеспечивает сеть на основе SDN, управление полосой пропускания, восстановление, безопасность и политики могут быть высокоинтеллектуальными и оптимизированными, и организация получает целостное представление о сети.

3) Абстракция сети. Сервисы и приложения, работающие по технологии SDN, абстрагируются от базовых технологий и оборудования, которые обеспечивают физическое соединение. Приложения будут взаимодействовать с сетью через API, а не через интерфейсы управления, тесно связанные с оборудованием.

4) Открытость. Архитектура SDN создает новую эру открытости, которая обеспечивает совместимость с несколькими поставщиками, а также способствует развитию независимой от поставщиков экосистемы. Открытость проистекает из самого подхода SDN. Открытые API поддерживают широкий спектр приложений, включая облачную оркестровку, OSS / BSS, SaaS и сетевые приложения, важные для бизнеса. Кроме того, интеллектуальное программное обеспечение может управлять оборудованием различных производителей с помощью открытых программных интерфейсов, таких как OpenFlow. Наконец, из SDN интеллектуальные сетевые сервисы и приложения могут работать в общей программной среде [2].

Ключевым преимуществом технологии SDN является возможность для операторов сети писать программы, использующие API-интерфейсы и позволяющие приложениям контролировать поведение сети. SDN позволяет пользователям разрабатывать сетевые приложения, осуществлять интеллектуальный мониторинг состояния сети и автоматически адаптировать конфигурацию сети по мере необходимости [2].

В России изучением технологии SDN занимаются такие компании, как Ростелеком, Netcracker, Huawei, Nokia. Сервис-провайдеры изучают возможности технологии программно-конфигурируемых сетей, чтобы обеспечить автоматизацию и программируемость своих транспортных оптических сетей для быстрого развертывания новых, приносящих доход сетевых сервисов, таких как пропускная способность по требованию (*Bandwidth-on-Demand*), и снижения затрат, связанных с предоставлением сервисов, их обслуживанием и восстановлением.

Согласно исследованию аналитической группы OSP Data, посвященному актуальным вопросам текущего состояния и перспектив развертывания программируемых сетей SDN (рис. 1), в ходе которого были опрошены представители 143 компаний, интерес компаний к программно-конфигурируемым сетям растет [3].

Исходя из этого можно сделать вывод, что для внедрения и последующего поддержания программно-конфигурируемых сетей в существующей сетевой инфраструктуре, компаниям необходимы специалисты со знаниями и навыками построения и управления программно-конфигурируемой сетью. Авторы статьи, для решения данной задачи предлагаю разработанный программный комплекс по изучению программно-конфигурируемых сетей SDN.

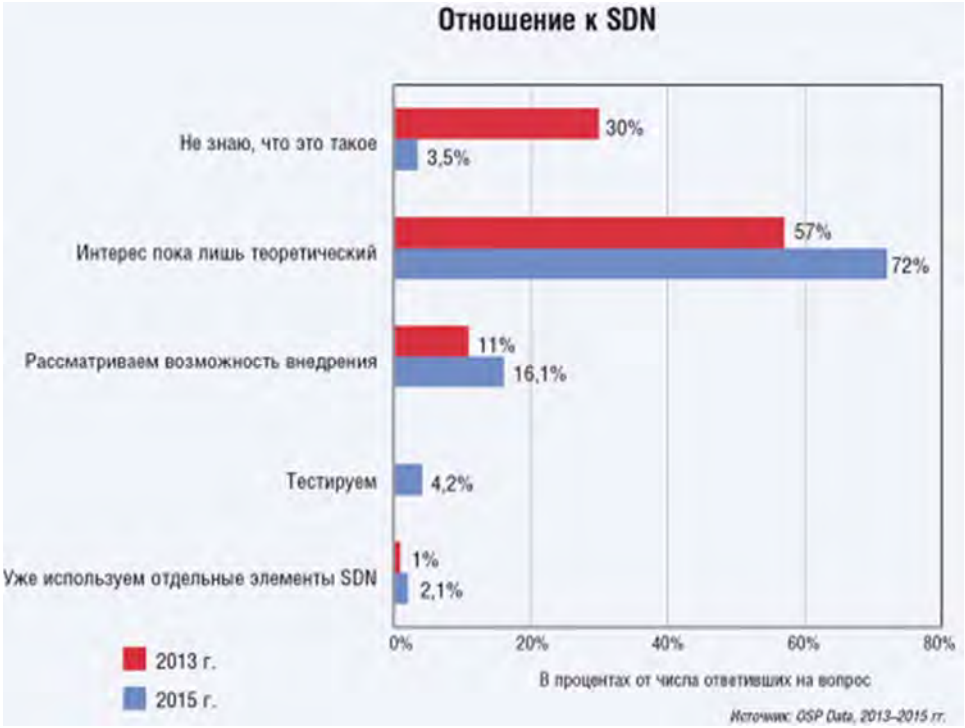


Рис. 5. Изменение отношения заказчиков к SDN с 2013 года

Программный комплекс представляет собой веб-сайт, созданный на сервере, включающим в себя веб-сервере Apache, базу данных MySQL и AAA-сервер. Структура программного комплекса представлена на рис. 2.

Рис. 6. Структура программного комплекса

Сервер планируется разместить на базе университета, в уже существующей лаборатории программно-конфигурируемых сетей. Таким образом, обучающиеся с помощью персональных компьютеров, через глобальную сеть смогут подключаться к серверу для изучения программно-конфигурируемых сетей из любой точки мира, где есть выход в интернет. Пример подключения к серверу показан на рис. 3.

Пример того, как выглядит интерфейс веб-сайта можно увидеть на рис. 4 (см. ниже).

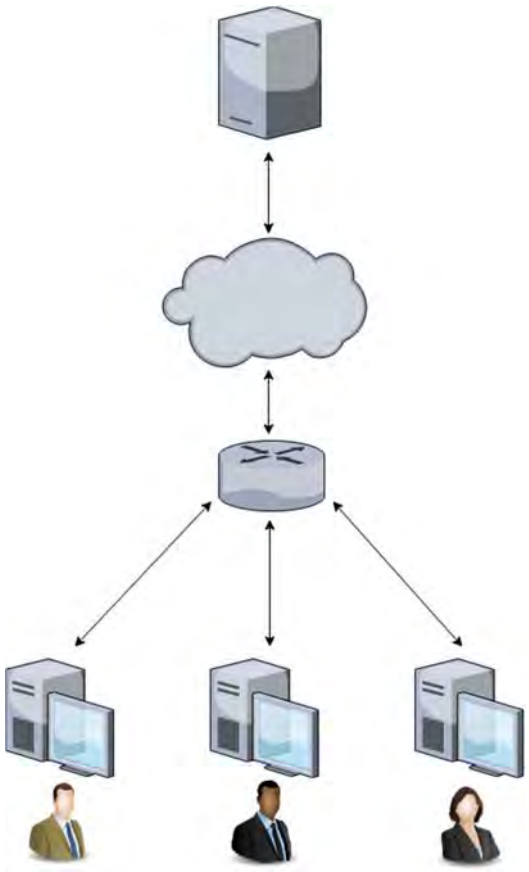


Рис. 7. Подключение к серверу

Таким образом, была проанализирована технология SDN и её особенности. Предложенный программный комплекс позволяет обеспечить обучение технологии SDN, что в свою очередь позволит ускорить внедрения технологии за счет большего числа специалистов.

Список используемых источников

1. Ateya, Abdelhamied A., Ammar Muthanna, Anastasia Vybornova, Abeer D. Algarni, Abdelrahman Abuarqoub, Y. Koucheryavy, and Andrey Koucheryavy. Chaotic salp swarm algorithm for SDN multi-controller networks // Engineering Science and Technology, an International Journal (2019).

2. Rob Tomkins // Ciena Corporation. 2017. [Электронный ресурс]. URL: https://www.ciena.com/insights/what-is/What-Is-SDN.html

3. Барсков А. SDN: чего хотят заказчики [Электронный ресурс] // Open Systems Publications. 2017. URL: https://www.osp.ru/iz/rusnet/articles/13047394

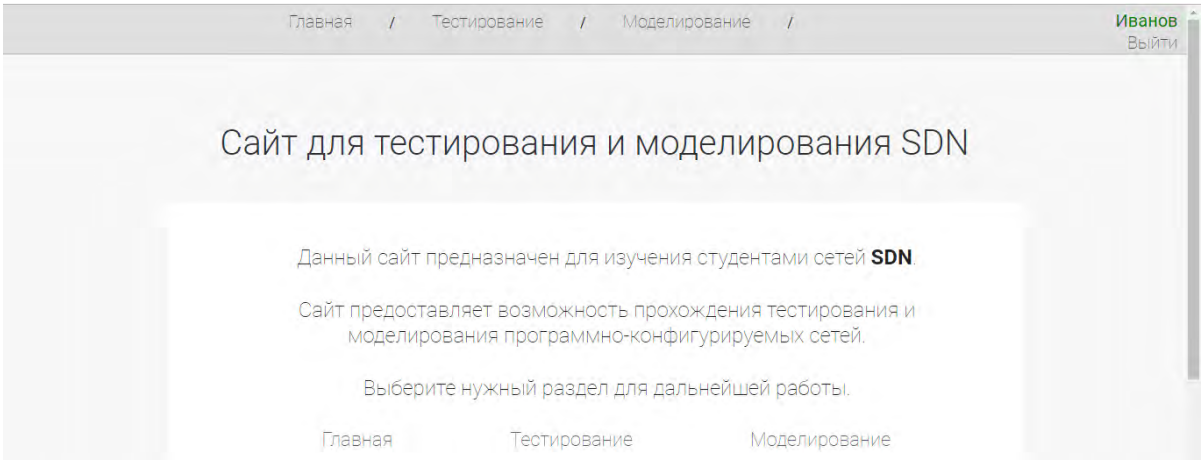


Рис. 8. Интерфейс веб-сайта

УДК 519.876.5:519.6:004.357
ГРНТИ 49.03.03

СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ ЧЕРЕЗ ВОЗДУШНЫЙ АУДИОКАНАЛ МАРКИРОВАННЫМИ АУДИОСИГНАЛАМИ

М. В. Гофман, А. А. Корниенко

Петербургский государственный университет путей сообщения Императора Александра I

Развивается методика цифрового маркирования аудиосигналов, ориентированная на скрытую передачу данных через воздушный аудиоканал. Внедряемый цифровой маркер занимает весь слышимый частотный диапазон. Каждый цифровой маркер переносит один бит информации. Решение о значении переданного бита выносится на основании знака центрального значения взаимно-корреляционной функции. Невысокая вычислительная сложность предлагаемого метода маркирования позволяет использовать его для беспроводного обмена информацией между обычными смартфонами. Методика позволяет выполнять цифровое маркирования как речевых, так и музыкальных аудиосигналов, без появления каких-либо заметно слышимых артефактов. Информация внедряется в виде маркера в частотную область аудиосигнала, путём амплитудной модуляции его частотных составляющих.

стеганография, маркирование аудосигналов, скрытая передача данных.

Актуальность задачи маркирования аудиосигналов

Маркирование аудиосигналов – это процесс внедрения дополнительной информации в аудиосигнал. Наибольшее распространение получили следующие области применения цифрового маркирования.

– Защита авторских прав, при распространении аудио, видео и изображений в цифровых форматах. В этих случаях внедряемый сигнал содержит, например, авторские данные или лицензионные ограничения, или же предотвращает или затрудняет неавторизованное копирование.

– Добавление управляющей информации. Внедряемый сигнал может, например, разрешать или запрещать копирование некоторому копирующему устройству, которое руководствуется цифровым маркером перед выполнением процедуры дупликации. Или же, согласованный с неким стандартом проигрыватель аудиодисков может проверить наличие маркера перед тем как воспроизвести аудио с диска.

– Организация канала утечки информации (*air-gap attack*) – скрытая передача данных осуществляется во время воспроизведения слышимого сигнала динамиком компьютера.

– Удалённое управление устройствами. В этом случае цифровой маркер, скрытый в обычном аудиосигнале, вводит устройство в режим восприимчивости к определённым командам. Например, интерактивное развлекательное телевидение или общеобразовательное направление.

– Определение местоположения объекта. В помещениях, особенно многоэтажных домах, применение глобальных систем позиционирования, таких как ГЛОНАСС или GPS весьма неэффективно, с точки зрения точности. Поэтому применяют локальные системы позиционирования, к которым можно отнести системы, например, обменивающиеся ультразвуковыми сигналами.

– Скрытая беспроводная передача при радиомолчании. В определённых ситуация радиопередача может быть запрещена, в таком случае беспроводную связь можно организовать при помощи передачи маркированных аудиосигналов.

– Дополнительный способ обмена информацией. Передача и приём маркированных аудиосигналов является альтернативным способом взаимодействия между смарт-устройствами, помимо широко используемых инструментов, таких как Wi-Fi и Bluetooth.

Постановка задачи и путь её решения

Предположим, что: частотные характеристики передающего (динамика) и принимающего (микрофона) устройств заранее неизвестны; возможно применение типовых методов пред-/пост-обработки цифровых аудиосигналов: сжатие с потерями, фильтрация и т. п. Исходя из этих предположений можно сделать следующие выводы: заранее оказывается неизвестным, на каких частотах сигналы могут слишком сильно ослабляться динамиком и микрофоном; методы пред-/пост-обработки могут разрушить элементы маркера. Один из путей решения задачи с такими ограничениями является использование всего слышимого диапазона частот для внедрения маркера.

Методика цифрового маркирования

В методы скрытой передачи маркированными аудиосигналами во всём слышимом диапазоне частот значительный вклад внесли ученые Японии (научная школа Ю. Накашимы) и Китая (научная школа З. Сжэнга). Разработанные этими школами методы маркирования [1, 2] позволяют осуществлять скрытую передачу при значительных величинах сил встраивания.

Процедура цифрового маркирования аудиосигналов лежит во основе системы скрытой передачи данных с помощью таких сигналов. Она включает в себя три этапа: этап построения маркера, этап внедрения маркера

в аудиосигнал и этап выделения маркера из маркированного аудиосигнала. Цифровое маркирование аудиосигнала предполагает создание из информации такого маркера и его внедрение в аудиосигнал таким образом, что становится возможным его выделить даже при условии, что маркированный аудиосигнал или стегоаудиосигнал подвергнется преднамеренной или ненамеренной атакам.

В статьях [3, 4] предлагается метод маркирования цифровых аудиосигналов. Для скрытой передачи используется следующее свойство обычных аудиосигналов. Спектры смежных последовательностей отсчётов аудиосигнала обычно имеют близкие амплитудные спектры. Используется комбинация методов расширения спектра и метода «лоскута».

Этап 1: построение маркера. Бит информации $x \in \{0,1\}$ заменяется на вектор:

$$y = (2x - 1)(\alpha \otimes \beta \otimes \gamma),$$

где $\otimes$ – произведение Кронекера, α, β – это двоичные векторы, обладающие хорошими автокорреляционными свойствами, γ – двоичный вектор, учитывающий частотные свойства аудиосигнала. Разработаны две методики построения таких последовательностей γ, которые учитывают свойство схожести амплитудных спектров смежных последовательностей отсчётов обычных цифровых аудиосигналов. Первая методика для передачи использует целочисленную последовательность, а для приёма дробно-рациональную последовательность, тогда как вторая методика и для передачи, и для приёма создаёт одну и ту же целочисленную последовательность.

Этап 2: внедрение маркера в аудиосигнал. Маркер внедряется в частотную область аудиосигналов путём амплитудной модуляции частотных составляющих последовательностей отсчётов аудиосигнала. Выбор модулируемых частотных составляющих не ограничен, как в большинстве существующих методов, только частотами, близкими к ультразвуку. Внедрение допустимо в весь слышимый диапазон частот.

Этап 3: выделение маркера из стегоаудиосигнала, принятого после передачи через воздушный аудиоканал. Выделение маркера осуществляется с помощью окна считывания, двигающегося с шагом в один отсчёт. Решение о наличии маркера и о значении внедрённого информационного бита опирается на методику порогового декодирования.

Результаты имитационного моделирования

Частотную составляющую принятого стегоаудиосигнала можно определить равенством:

$$R(i, j, i_{\text{шаг}}) = h(i, j, i_{\text{шаг}})Z(i, j) + n_{\text{фон}}(i, j, i_{\text{шаг}}),$$

где i, j – это номер частотной составляющей и номер блока отсчётов аудиосигнала, соответственно, $i_{\text{шаг}}$ – шаг смещения считывающего окна, $Z(i, j)$ – частотная составляющая исходного стегоаудиосигнала, h и $n_{\text{фон}}$ – мультипликативный и аддитивный шумы.

При имитационном моделировании в качестве последовательностей α и β использовались коды Касами и Голда длинами 255 и 127, соответственно. При дисперсии аддитивного шума в 15 дБ вероятность успешной передачи близка к 0,9, когда используются последовательность:

$$\gamma = (1 \quad 1 \quad -1).$$

Результаты натурных экспериментов

При выполнении натурных экспериментов в качестве последовательностей α и β использовались коды Касами и Голда длинами 255 и 127, соответственно. В качестве аппаратных средств использовалась доступная и недорогая аппаратура: динамики Sennheiser MX170 (максимальная мощность 30 мВт), микрофон Philips SBC ME570 (диапазон частот от 20 до 16 кГц). Мощность динамика в ОС Windows была установлена на 50 % при проведении всех натурных экспериментов. Музыкальная композиция: успешная скрытая передача на расстояние 70 см. Речевой сигнал: успешная скрытая передача на расстояние 5 см.

Заключение

Результаты имитационного моделирования и натурных экспериментов показали, что разработанная в статьях [3, 4] методика позволяет осуществлять скрытую передачу информации в слышимом диапазоне частот. Методика обладает небольшой вычислительной сложностью, что позволяет применять её для скрытой связи даже между обычными смартфонами. Отсутствие особых требований к количественным характеристикам частотных составляющих, в которые выполняется внедрение маркера, делает разработанный метод применимым для широкого спектра аудиосигналов. Номера частотных составляющих исходного аудиосигнала, в которые будет внедряться информация, а также последовательности α, β, γ могут быть использованы в качестве ключа для скрытой передачи.

Список используемых источников

1. Nakashima Y., Tachibana R., Babaguchi N. Watermarked movie soundtrack finds the position of the camcorder in a theater // IEEE Transactions on Multimedia. 2009. V. 11. No 3. pp. 443–454.

2. Zhang Z., Wu X. An audio covert communication system for anolog channels // International Conference on Electrical and Control Engineering. Wuhan, China. 2010. pp. 3279–3282.

3. Гофман М. В., Корниенко А. А., Мирончиков Е. Т., Никитин А. Б. Цифровое маркирование аудиосигналов для робастной скрытой акустической связи через воздушный аудиоканал // Труды СПИИРАН. 2017. № 6. С. 185–215.

4. Гофман М. В., Корниенко А. А., Мирончиков Е. Т. Методика цифрового маркирования аудиосигналов для скрытой акустической связи через воздушный аудиоканал // Известия Петербургского университета путей сообщения. 2018. № 2. С. 280–294.

УДК 004.71
ГРНТИ 49.37.29

ОБЗОР СОВРЕМЕННОЙ АРХИТЕКТУРЫ 5G НА ОСНОВЕ КОНЦЕПЦИИ СЛАЙСИНГА

А. А. Гребенщикова, В. С. Елагин

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

В работе рассматривается перспективная технология для сетей 5G, предоставляющая услуги, адаптированные к конкретным требованиям пользователей по качеству услуг – слайсинг и её основные составляющие. Также, в данной статье рассматривается технология SDN, получившее широкое признание в качестве многообещающего метода для реализации разбиения сети на основе виртуализации сетевых функций. Облачная виртуализация сетей доступа и ядра сети обладает преимуществами объединения физических ресурсов, распределения программного обеспечения и централизации управления.

Из-за разнообразия сценариев применения 5G технологий, современные методы мобильного управления особенно должны гарантировать бесшовную передачу данных в сетях с применением сетевого сегментирования. Используя данную работу, можно оценить зрелость текущих предложений и методов, чтобы определить ряд открытых вопросов для будущих исследований.

сетевое сегментирование, архитектура, пятого поколения мобильной связи 5G, программно-конфигурируемая сеть SDN, виртуализация сетевых функций NFV.

Введение

Главной целью 5G остаётся удовлетворение требований пользователей по качеству услуг в различных системных сценариях (например, в области передачи данных или задержки) [1]. В тех случаях, когда необходимо бесшовное широкодоступное покрытие, системы пятого поколения должны предоставлять пользователям бесперебойные высокоскоростные услуги передачи данных, доступных в любом месте и в любое время, даже на крайних

сотах или с высокой мобильностью (более 500 км/ч). В условиях метрополитена, где плотность и объём спроса на беспроводной трафик высоки, сети 5G обязаны обеспечить плотное покрытие горячей точки. А в сценариях, где необходимы надежные соединения большого количества широкополосных узлов с низким энергопотреблением (например, беспроводных датчиков), пятое поколение должно иметь возможность подключать миллионы устройств в условиях низкого энергопотребления и низкой стоимости на устройство [2].

Для того, чтобы предоставлять индивидуальные надежные услуги, используя ограниченные сетевые ресурсы, именно сетевое сегментирование стремительно набирает популярность и распространение. Благодаря индустрии беспроводных технологий, слайсинг считается основным инструментом конвергенции сетевых услуг, а также сервисом по предоставлению индивидуальных услуг по требованию [3, 4, 5].

Концепция сетевого сегментирования

Концепция сетевого сегментирования, изображённая на рис. 1, имеет три составляющие:

1) Уровень служебного интерфейса.
2) Уровень интерфейса сетевого сегментирования
3) Уровень ресурсов [6].

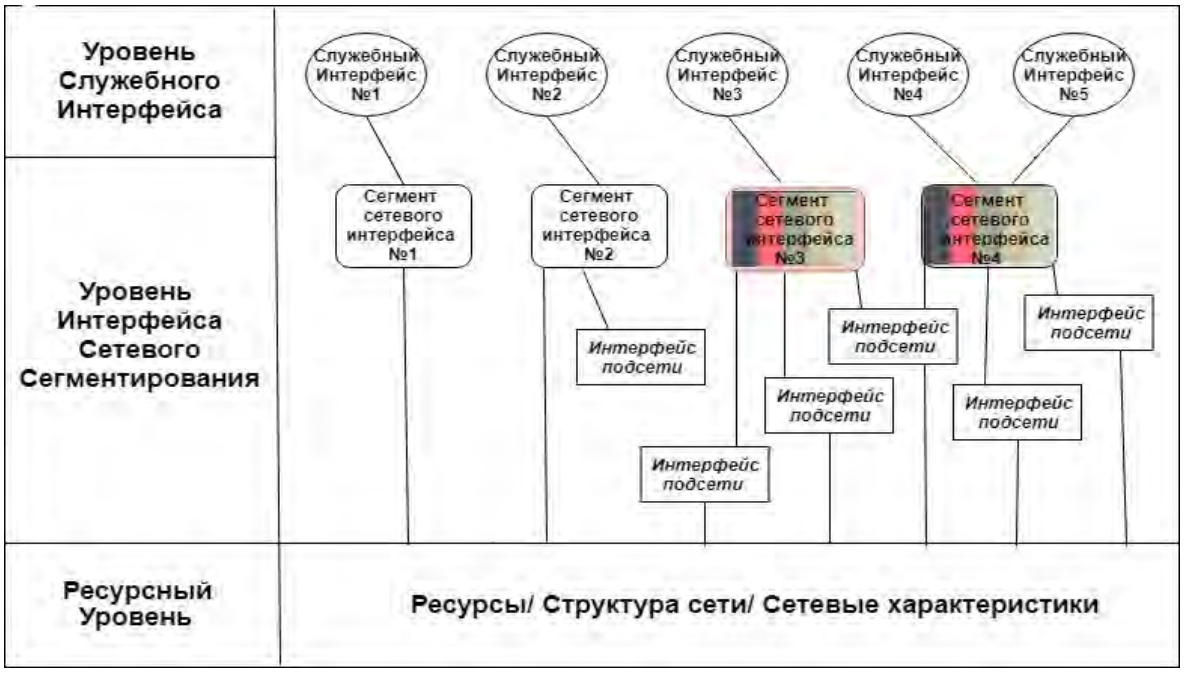


Рис. 1. Концептуальная схема сетевого сегмента

В контексте слайсинга определение понятия «интерфейс» имеет смысл быть как динамическая конструкция. Истолковывать данное слово следует

базируясь на времени разработки и проектирования, а также следует уточнить производные слова «шаблон» или «план».

Уровень служебного интерфейса предоставляет либо бизнес-услуги, либо услуги для оконечного пользователя, в зависимости от требований для реализации служб. В связи с тем, что обычно услуги могут предоставляться сетевым оператором или третьими лицами, уровень служебного интерфейса имеет возможность успешно выступать как в роли первого, так в роли и второго.

Сетевой оператор использует План Сетевого Сегмента для создания Сегмента Сетевого Интерфейса, что в свою очередь обеспечивает необходимый набор сетевых характеристик для работы Служебного интерфейса. Следует отметить тот факт, что Сегмент Сетевого Интерфейса может использоваться несколькими Служебными Интерфейсами.

Сегмент сетевого интерфейса может состоять из одного и более Интерфейсов подсети либо напрямую иметь подключение к Уровню ресурсов. Точно так же План Подсети используется для создания Интерфейса Подсети для формирования набора сетевых функций, которые работают на физических или логических ресурсах.

Суть концепции наследования, связывающая такие составляющие как «План сетевого сегмента» и «Интерфейс сетевого сегмента», изображена на рис. 2 [6].

Рис. 2. Концепция наследования

Имеются некоторые примеры Сегмента Сетевого Интерфейса: Enhanced MBB, M2M, Enterprise и Industry. Также напомним Сетевые Интерфейсы Подсети: IMS (IP мультимедийная подсистема) и другие. Данная концепция может быть расширена для любого сценария, предусмотренного для применения инфраструктуры сетевого сегментирования.

Сетевая архитектура 5G на основе сегментирования

Программно-определяемая сеть SDN получило широкое признание в качестве многообещающего метода для реализации среза сети, на основе

виртуализации сетевых функций (NFV) [7]. Каждый коммерчески готовый сервер можно рассматривать как пул виртуальных машин (VMs), работающих на коммерческом стандартном аппаратном и программном обеспечении. Централизованные процессоры в значительной степени виртуализированы, а пул ресурсов введен для выполнения сегментирования услуг в соответствии с различными требованиями по качеству обслуживания (QoS) [8]. Логическая архитектура системы 5G на базе слайсинга приведена на рис. 3 [2].

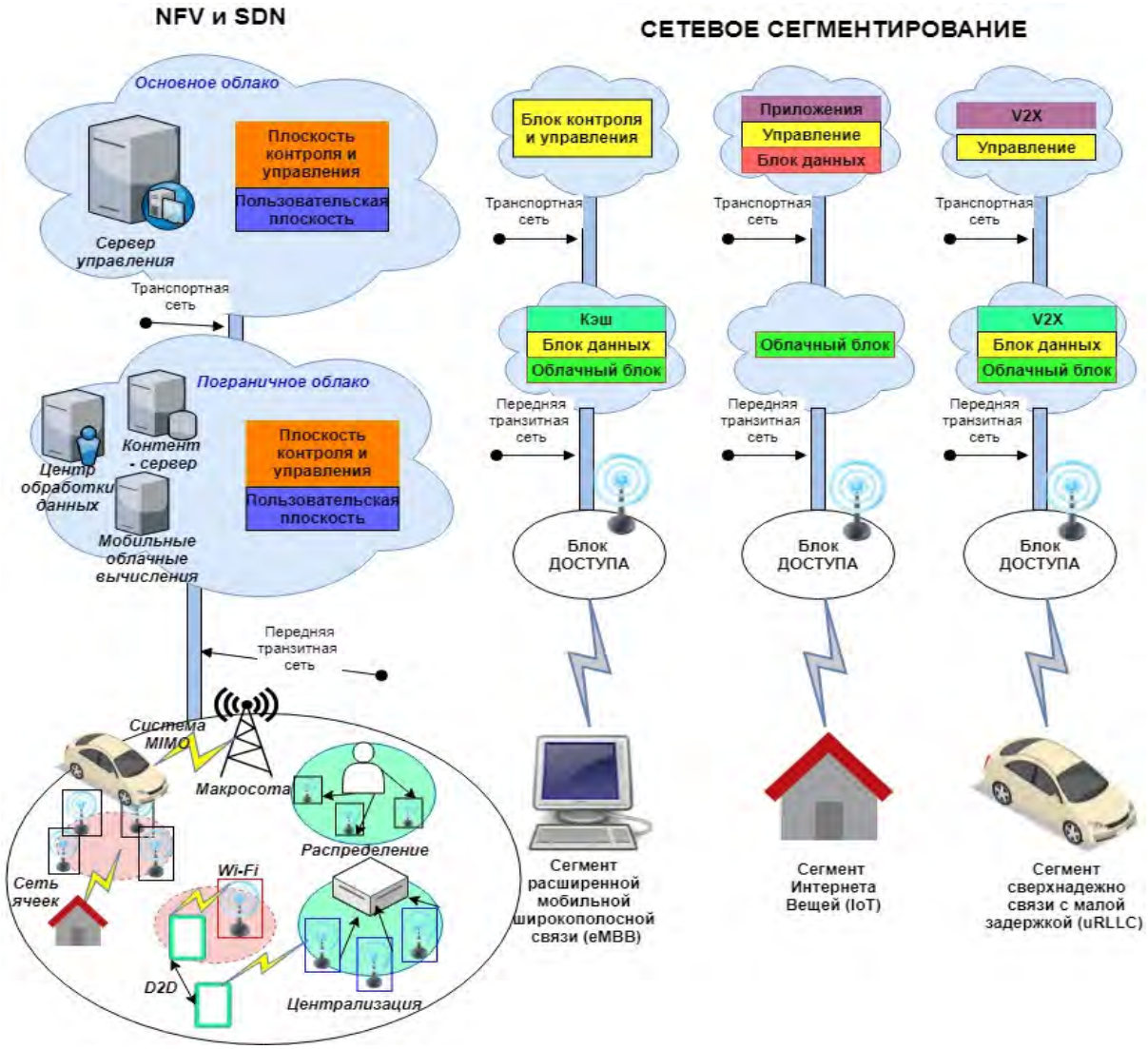


Рис. 3. Сетевая архитектура 5G на основе сегментирования

Сегментирование сети можно реализовать после виртуализации и переопределения программного обеспечения архитектуры системы, как описано выше. Определенный набор сетевых функций и модулей распределения ресурсов, изолированных от других сегментов сети – представляет

собой сквозной сегмент [3]. Например, слайс расширенной мобильной широкополосной связи (*the enhanced mobile broadband*, eMBB) требует большой полосы пропускания для поддержки услуг с высокой скоростью передачи данных, таких как потоковое видео высокой четкости и дополненная реальность.

Решающее значение для сегмента сверхнадежной связи с малой задержкой (*the ultra-reliable and low-latency communication*, uRLLC) для предоставления услуг, которые чрезвычайно чувствительны к задержке, таких как автономное вождение и Интернет транспортных средств (*vehicle-to-everything*, V2X), будут иметь надежность, низкая задержка и безопасность. Для слайса uRLLC все выделенные функции должны быть созданы в пограничном облаке. Вертикальные приложения будут размещены на верхнем уровне для поддержки внешних услуг, требуемых различными коммерческими арендаторами, для сегмента Интернета Вещей (*Internet of Things*, IoT), который обслуживает большое количество статических или динамических устройств машинного типа (например, датчиков и мониторов) [2].

Заключение

Используя SDN, сети 5G могут соединять виртуальные машины, распределенные в основном облаке и пограничном облаке, создавая соответствие между ними. Кроме того, контроллеры SDN могут централизованно управлять разбиением сети.

Сетевая архитектура 5G на основе сегментирования сети радикально изменит традиционные схемы планирования и развертывания. Так как слайсинг адаптируется к сетевым приложениям и требованиям пользователей, а значит сети 5G могут предоставлять сквозные специализированные услуги в соответствии с индивидуальными требованиями приложений.

Список используемых источников

1. A. Osseiran et al. Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project // IEEE Commun. Mag., vol. 52, no. 5, May 2014, pp. 26–35.

2. Haijun Zhang, Na Liu, Xiaoli Chu, Keping Long, Abdol-Hamid Aghvami, and Victor C. M. Leung Network Slicing Based 5G and Future Mobile Networks: Mobility, Resource Management, and Challenges // IEEE Communications Magazine, August 2017, p. 140.

3. M. Jiang, M. Condoluci, and T. Mahmoodi. Network Slicing Management & Prioritization in 5G Mobile Systems // Euro. Wireless 2016, Oulu, Finland, 2016, pp. 1–6.

4. P. Rost et al. Mobile Network Architecture Evolution toward 5G // IEEE Commun. Mag., vol. 54, no. 5, May 2016, pp. 84–91.

5. Ericsson. Ericsson White Paper: 5G System, Jan. 2015.

6. Sebastian Thalanany (US Cellular) Peter Hedman (Ericsson) Description of Network Slicing Concept // NGMN 5G Project Requirements & Architecture – Work Stream E2E Architecture Version 1.0.8, 14th September 2016, pp. 4–6.

7. V. Yazici, U. C. Kozat, and M. O. Sunay. A New Control Plane for 5G Network Architecture with a Case Study on Unified Handoff, Mobility, and Routing Management // IEEE Commun. Mag., vol. 52, no. 11, Nov. 2014, pp. 76–85.

8. M. Peng et al. Fronthaul-Constrained Cloud Radio Access Networks: Insights and Challenges // IEEE Wireless Commun., vol. 22, no. 2, Apr. 2015, pp. 152–60.

УДК 654.01
ГРНТИ 49.38.49

АНАЛИЗ ПЕРСПЕКТИВ РАЗВИТИЯ СЕТЕЙ СВЯЗИ ПЯТОГО ПОКОЛЕНИЯ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

И. В. Гришин, С. Н. Михеева, К. А. Подгорная

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

В статье предпринята попытка анализа перспектив внедрения сетей связи пятого поколения на территории Российской Федерации. Рассмотрены такие вопросы как зависимость области телекоммуникаций от зарубежного оборудования и программного обеспечения, а также связанные с этим риски, появляющиеся при внедрении сетей связи пятого поколения. Рассмотрены вопросы предоставления мобильным операторам необходимых полос частот и стоимости внедрения сетей операторами.

сети связи пятого поколения, 5G, eMBB, mMTC, URRLC.

В настоящее время мир готовится к внедрению пятого поколения сетей мобильной связи, которое, как прогнозируется, кардинальным образом должно изменить жизнь человечества в целом, сформировав новое, так называемое «информационное общество».

Применяемые в сетях пятого поколения технологии сделают возможным существование «умных» городов, онлайн-медицины, онлайн-образования, положительно скажутся на ростах внутреннего валового продукта государств.

Бесспорными лидерами в развитии сетей связи 5G являются Китай и США, находясь в условиях острой конкурентной борьбы. Российские производители на рынке оборудования сетей связи пятого поколения пока никак не представлены.

В то же время является очевидным преимущество тех стран, которые при принятии стандартов в области телекоммуникаций опираются на технологии отечественных производителей, и основное соперничество между

США и Китаем ведется именно за право установления собственных технических стандартов в качестве мировых и получение прибыли за использование своих патентов. Так, США, призывают страны, связанные с ними союзническими отношениями, отказаться от закупок оборудования китайских производителей, обосновывая это возможными угрозами национальной безопасности со стороны Китая. Согласившись с доводами США, Австралия ввела запрет на использование оборудования компаний ZTE и Huawei [1]. Аналогичный запрет введен в Новой Зеландии, хотя, как отметил представитель новозеландкой службы безопасности, данное решение было принято самостоятельно. Обе страны помимо США входят в состав разведывательного альянса пяти англоязычных государств AUSCANNZUKUS.

В программе 2017 года «Цифровая экономика Российской Федерации» [2] было объявлено, что к 2020 году сети связи 5G будут внедрены во всех городах с численностью населения более 1 млн человек. В последующем планируемые масштабы внедрения сети изменялись, и на сегодняшний день планируется в 2020 году запуск пилотного проекта только в одном городе Российской Федерации. Однако со всей очевидностью встает вопрос о том, оборудование каких производителей будет задействовано в рамках данного пилотного проекта и последующего подключения к данному проекту десяти городов в 2021 году?

Для анализа возможных результатов использования оборудования зарубежных производителей на территории Российской Федерации можно обратиться к тексту новой редакции стратегии кибербезопасности США, опубликованной в сентябре 2018 года. В тексте данного документа говорится о России как о стране, которая наряду с такими странами как Иран, Китай и Северная Корея «использует киберпространство как средство для борьбы с Соединенными Штатами, их союзниками и партнерами, часто с безрассудством, на которое она никогда не осмелилась бы в других областях» [3]. Там же заявляется, что США намерены задействовать все возможные инструменты для противодействия киберугрозам со стороны противников: дипломатические, информационные, военные («как кинетические, так и кибернетические»), финансовые, разведывательные и пр. Обращает на себя внимание то, что инструменты противодействия в цифровом пространстве рассматриваются Соединенными Штатами Америки как военные.

Тем не менее, в разделе, посвященном информационной безопасности дорожной карты программы цифровой экономики срок перехода на компьютерное, серверное и телекоммуникационное оборудование преимущественно отечественных производителей на всех объектах информационной инфраструктуры Российской Федерации датируется IV кварталом 2024 года. Таким образом, можно считать, что при соблюдении сроков по внедрению сетей связи пятого поколения в городах с численностью населения более 1 млн человек мобильными операторами на протяжении четырёх

лет будет применяться зарубежное оборудование и программное обеспечение, импортозависимость от которых не только подрывает технологический суверенитет государства, но и делает возможным за счет дополнительных программно-аппаратных функций, не указанных в документации, сбор разведывательной информации и удаленное управление оборудованием.

Какие же именно услуги должна предоставлять сеть связи пятого поколения? Международный союз электросвязи (МСЭ-R) выделяет три основные группы услуг:

1) Усовершенствованная подвижная широкополосная связь (eMBB) – предоставляет услуги высокоскоростной передачи данных, такие как передача потокового видео высокого разрешения, передача файлов больших объемов, дополненная реальность и др.

Заявленные скорости передачи: 2 Гбит/с и более в нисходящем потоке для диапазонов ниже 6 ГГц, и до 20 Гбит/с в нисходящем потоке для диапазонов частот выше 6 ГГц с задержкой по времени на уровне радиоинтерфейса не более 4 мс.

2) Интенсивный межмашинный обмен (mMTC) обеспечивает взаимодействие огромного количества устройств, расположенных с высокой плотностью. Предоставляет услуги отслеживания материальных активов, организации «умного» сельское хозяйство, «умных» городов, мониторинга энергопотребления и др.

Максимальная плотность подключенных устройств в условиях города –$1 \cdot 10^6$ устройств/км^2. Срок автономной работы – до 10 лет.

3) Сверхнадежная передача данных с малой задержкой (URLLC) – услуга, обеспечивающая связь с сверхмалыми задержками между терминалами. Возможная область применения: управление автономными транспортными средствами, дистанционное наблюдения за больными, автоматизация производства. Предполагаемая задержка по времени на уровне радиоинтерфейса – не более 1 мс.

В приведенном выше описании услуг представлены только некоторые области применения. Однако, и из данного перечня видно количество объектов привлекательных для информационных атак значительно увеличилось, также следует отметить значительное увеличение количества подключаемых оконечных устройств. Использование зарубежных технологий и оборудования в таких областях как управление технологическими процессами, транспортными средствами, медицине в случае атак может привести к значительным негативным техническим эффектам. Можно утверждать, что обеспечение информационной безопасности может быть достигнуто только на уровне микросхем, но, как отметил премьер-министр Дмитрий Медведев, состояние дел в российской радиоэлектронной промышленности является весьма уязвимым: некоторые технологии и изделия в стране пока

не производятся [4]. Однако следует отметить, что отечественные разработки оборудования для сетей пятого поколения уже ведутся, и даже существуют отдельные готовые решения как, например, у компаний Элтекс, Т8, Микран и ряда других.

Предоставление вышеперечисленных услуг становится возможным только при выполнении ряда технических требований, к которым относятся также возможность использования частотных диапазонов, способных обеспечивать наилучшие характеристики распространения радиосигналов.

Многие производители телекоммуникационного оборудования, а также ряд мобильных операторов считают оптимальным для начальных этапов развития сети диапазон частот 3300–3800 МГц. Однако в Российской Федерации данная полоса радиочастот отводится для пользования радиоэлектронных средств радиолокационных служб, фиксированной спутниковой службы и фиксированной беспроводной связи. В марте 2019 года Министерство обороны в своем отзыве на проект концепции развития сетей пятого поколения отказало в передаче данного диапазона частот под нужды мобильных операторов [5], что может существенно замедлить внедрение сетей 5G.

Расчистка частотного диапазона для сетей 5G обойдется государству в несколько десятков миллиардов рублей. Рассчитанные общие капитальные затраты операторов на развертывание сетей пятого поколения в городах с численностью населения более 1 млн человек к 2024 году в зависимости от условий использования инфраструктуры могут составить от 114 до 163 миллиардов рублей. Планируемые затраты на развитие отрасли в целом четырьмя операторами составят от 550 до 610 миллиардов рублей [6]. Следует также отметить, что расчеты стоимости производились как в долларах, так и в рублях. Расчеты в рублях производились для проектно-изыскательских и строительно-монтажных работ, что подразумевает под собой строительство опор, вышек и подготовку помещений. Расчеты в долларах производились для расчета стоимости закупок необходимого оборудования: узлов ядра, агрегации и доступа транспортной сети, макросотовых и микросотовых базовых станций.

Планируемый экономический эффект от внедрения сетей связи пятого поколения к 2025 году должен составить 3,9 триллионов рублей. Из них 2,3 триллиона рублей придётся на долю операторов, остальное приходится на смежные области [6].

Цифры расходов операторов только на развертывание сети выглядят весьма внушительно, и можно сделать вывод, что значительные объемы этих денежных средств могут уйти к зарубежным, а не отечественным производителям телекоммуникационного оборудования, которые из-за этого могут остаться в роли вечно отстающих. С другой стороны, отталкиваясь от тех же цифр, можно спрогнозировать, что полномасштабного внедрения

сетей пятого поколения на территории Российской Федерации в ближайшие пять лет ожидать не стоит, что дает возможность отечественным производителям разработать необходимые сетевые элементы и программное обеспечение и тем самым уменьшить риски, связанные с переходом на сети пятого поколения.

Список используемых источников

1. Австралия запретила Huawei ввезти оборудование для развертывания 5G-сетей (23.08.2018) // Электронное периодическое издание «Ведомости». URL: https://www.vedomosti.ru/technology/news/2018/08/23/778846-avstraliya (дата обращения 28.03.2019).

2. ПРОГРАММА «Цифровая экономика Российской Федерации» // Распоряжение Правительства РФ от 28.07.2017 N 1632-р

3. National Cyber Strategy of the United States of America (09.2018) // whitehouse.gov. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения 01.02.2019).

4. Импортозамещение вычислительной техники и микроэлектроники (12.12.2018). URL: http://www.tadviser.ru: http://www.tadviser.ru/index.php/Статья:Импортозамещение_вычислительной_техники_и_микроэлектроники (дата обращения 02.01.2019)

5. Минобороны отказалось передавать операторам частоты для 5G (28.03.2019) // Электронное периодическое издание «Ведомости». URL: https://www.vedomosti.ru/ technology/articles/2019/03/28/797714-minoboroni-otkazalos-peredavat-5g (дата обращения 28.03.2019).

6. Бутенко В., Девяткин Е., Суходольская Т. Сети связи 5G/IMT-2020 и IoT – во все сферы национальной экономики // Электросвязь. 2018. № 8. С. 6–11.

УДК 654.739
ГРНТИ 49.33.29

АНАЛИЗ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ СЕТЕЙ СВЯЗИ НА ВЫСОКОСКОРОСТНЫХ МАГИСТРАЛЯХ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

В. Г. Дементьев, В. С. Елагин

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

В данной статье приведены основные особенности построения сетей связи на высокоскоростных магистралях, для примера будет приведена специфика магистралей железнодорожного транспорта, отличительной особенностью которого является высокая скорость движения подвижный составов, а также крупный объем пользовательского и служебного трафика.

сети связи, коммутация, маршрутизация, транспондер.

В современном мире построение полноценной сети связи невозможно без специализированного коммутационного и мультиплексного оборудования. Основными «фрегатами» данного оборудования на сегодняшний день являются компании Cisco Systems, Inc., США, и Huawei Technologies Co., Ltd, Китай. Несмотря на конкуренцию за лидерство в мировом рынке данных корпораций, существуют также и отечественные компании, поставляющие в отрасль промышленности и транспорта оборудование, по своим характеристикам не уступающее зарубежным аналогам. Одним из примеров таких производителей является российская компания «Т8», выпускающая DWDM и CWDM системы, востребованные не только на отечественном рынке, но и за рубежом.

К сетям связи на высокоскоростных магистралях предъявляются повышенные относительно обычных участков пути требования. Оборудование (чаще всего устанавливается в 19” шкафы, особой надежностью которых выделяется немецкий производитель «*Rittal*») вне зависимости от функционального назначения должно иметь следующие характеристики и возможности:

– резервирование по питанию (мультиплексное и коммутационное оборудование), подразумевает подключение как от сети переменного тока, так и от источника бесперебойного питания с аккумуляторным резервом (чаще всего, на 8 часов);

– возможность работы в режиме «1+1» – резерв по связи для коммутационного оборудования и по питанию для инверторного силового оборудования;

– общий резерв по передаче трафика;

– модульный конструктив для коммутационного и мультиплексного оборудования, подразумевает возможность установки в «базу» модулей (плат) различного назначения под каждый конкретный случай (предъявляемые к функциональным возможностям плат требования существенно различаются в зависимости от целевого назначения модуля связи, в котором и устанавливается телекоммуникационное оборудование).

Далее речь пойдет о конкретных примерах оборудования сетей связи в порядке иерархии проектирования. Начать следует с DWDM-систем.

Агрегирующий транспондер MS-400E – выпускается российской компанией «Т8». Данное оборудование позволяет организовывать передачу до 4×100 Гбит/с клиентских сигналов в 2×200 Гбит/с или 1×400 Гбит/с.

Блок поддерживает передачу по двум длинам волн по 200 Гбит/с или по одной 400 Гбит/с. MS-400E передает данные в OTN формате с использованием коррекции ошибок Soft-FEC. Лазер с перестройкой длины

волны с шагом 12,5 ГГц позволяет организовать до 96 DWDM каналов 400 Гбит/с в С-диапазоне и сетке 100 ГГц.

Данный транспондер стал выпускаться компанией «Т8» относительно недавно и уже показал себя на РЖД РФ.

Ниже по уровню иерархии проектирования сетей связи находится мультиплексное оборудование. Мультиплексор представляет собой комбинированное цифровое устройство, обеспечивающее поочередную передачу на один выход нескольких входных сигналов. Он позволяет передавать (коммутировать) сигнал с желаемого входа на выход, в этом случае выбор требующегося входа реализуется определенной комбинацией управляющих сигналов. Число мультиплексных входов принято называть количеством каналов, их может быть от 2 до 16, а число выходов называют разрядами мультиплексора, обычно это 1–4.

Надежным поставщиком мультиплексного оборудования на сегодняшний день является конструкторское бюро «Пульсар-Телеком». Главная выпускаемая единица – мультиплексор СМК-30, наиболее часто используемый в построении сетей связи и сетей передачи данных общетехнологического и оперативно-технологического назначения.

Мультиплексоры используется для агрегации каналов различного вида и перевода трафика в цифровые каналы Е1 для дальнейшей передачи информации (в основном, с помощью подключения к DWDM – системам).

Коммутаторы и маршрутизаторы являются неотъемлемой частью сетей связи, ниже представлены основные серии данного оборудования, наиболее подходящие для установки именно на высокоскоростных магистралях:

1) Маршрутизаторы Cisco серии ASR, коммутаторы Cisco серии 2960RX.

2) Маршрутизаторы Huawei серии AR2000, коммутаторы Huawei серии S5720.

Данная аппаратура позволяет организовать как локальные сети связи (в пределах нескольких узлов), так и глобальные.

При подключении всех элементов сетей связи согласно иерархии сети, последними по уровню подключаются оконечные устройства. Они могут представлять из себя как датчики пожарной и охранной сигнализаций, устанавливающиеся на объекте связи, так и различные устройства оповещения пассажиров и рабочего персонала, устанавливаемые на станциях, пассажирских платформах и вдоль путей. Последние включают в себя:

– динамики, устанавливаемые в помещении;

– колонки экстренного вызова в различной комплектации (зависит от размеров станции);

– громкоговорители, устанавливаемые на опорах вдоль платформ и путей;

– информационные табло;

– автоматизированные рабочие места (АРМ) диспетчеров и радистов (в случае наличия на объекте связи радиобюро). Именно через АРМ осуществляется управление и мониторинг средств связи.

Ниже представлены фрагменты схемы транспортной сети высокоскоростного участка (рис. 1, 2).

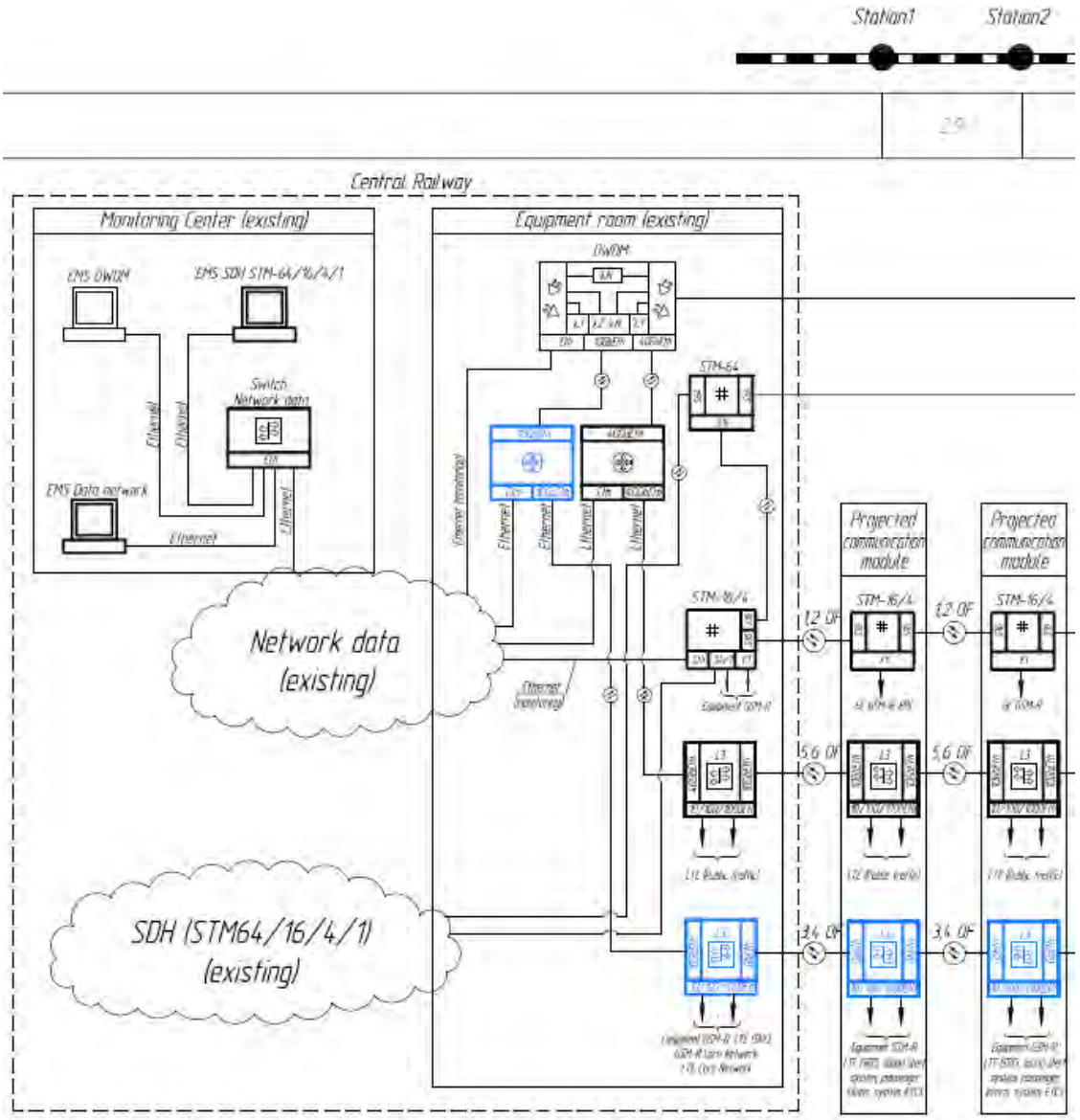


Рис. 1. Фрагмент схемы, включающий в себя станцию мониторинга и управления сетями связи

Крупные станции с устанавливаемым DWDM – оборудованием служат для резервирования сети связи [1], частота установки данного оборудования (кол-во DWDM – систем на участке путей) зависит от нескольких факторов [2]:

1) предполагаемый уровень передаваемого трафика;

2) максимально возможное расстояние между взаимоподключаемыми системами DWDM.

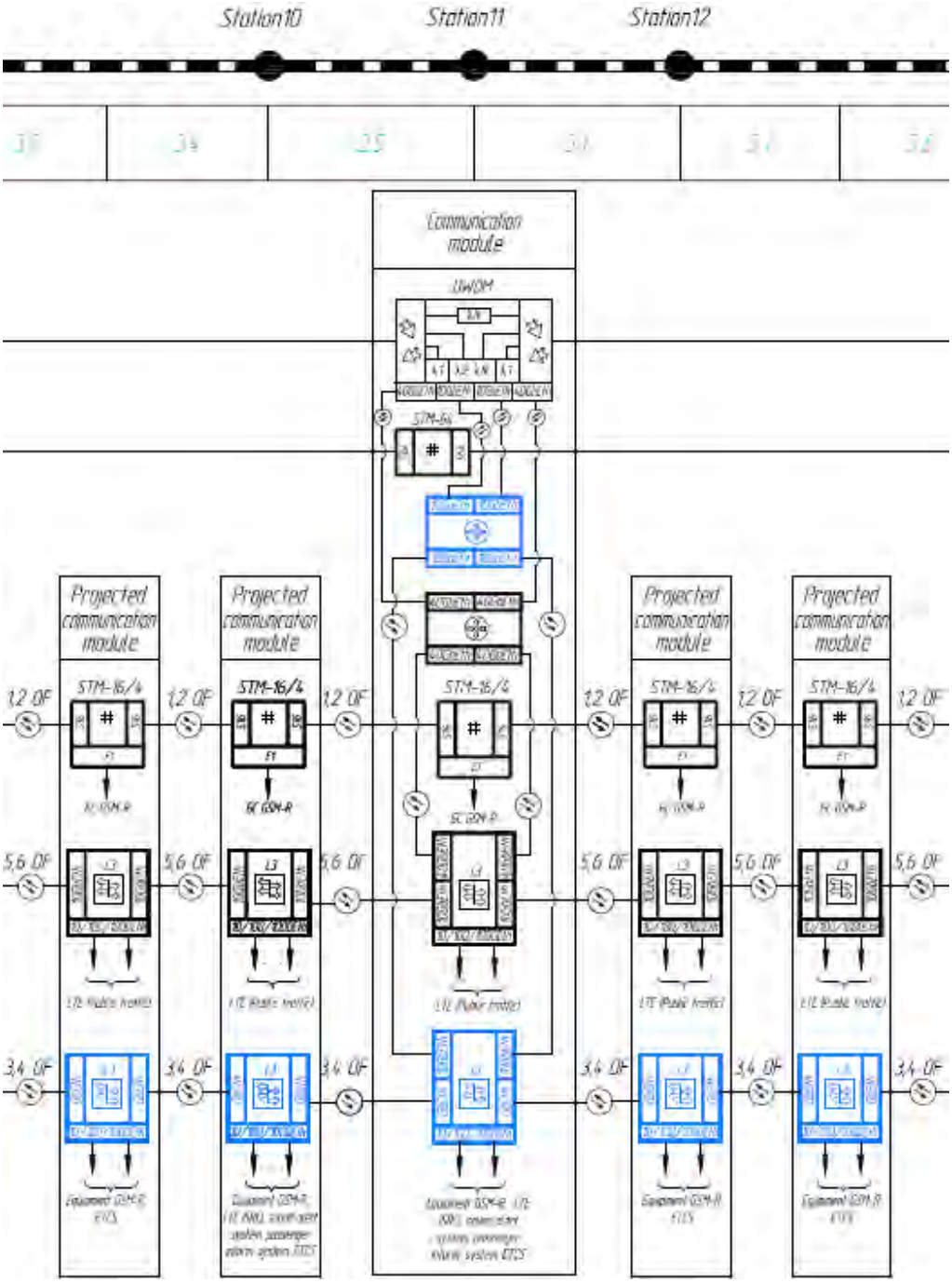


Рис. 2. Фрагмент схемы, включающий в себя крупную станцию (*Station*11) с установленной DWDM-системой передачи, организовывающей резерв передачи пользовательского и служебного трафика

На основе характеристик оборудования и материалов, используемых при построении сетей связи на высокоскоростных магистралях, можно выделить 3 проблемы, часто возникающих при проектировании данных сетей.

1) Удаленность двух узлов связи друг от друга (на расстояние, превышающее возможности передачи данных для систем связи. В таких случаях устанавливаются промежуточные коммуникационные модули. Сам модуль связи является важной частью крупных сетей связи, представляет собой небольшое здание с аппаратной, комнатой охраны и несколькими второстепенными помещениями для персонала.

2) Для проводных сетей связи (подразумевающих прокладку ВОЛС) важен рельеф местности и характеристики почвы. Горная местность или, например, северные широты с промерзлым грунтом и неустойчивой породой (из-за смены времен года и, как следствие, возможных локальных сдвигов слоев почвы) существенно повышают затраты ресурсов на прокладку кабелей, т. к. пренебрежение данными особенностями среды неизбежно приводит к обрыву ВОК [3].

3) Совместимость оборудования разных производителей. Нередко возникают ситуации, когда производитель (например, мультиплексного оборудования) не может со стопроцентной вероятностью гарантировать точную передачу данных, ввиду наличия у оконечного оборудования специфических интерфейсов (например, радио интерфейс С1-ФЛ-БИ). В таких случаях проверка осуществляется опытным путем. Таким образом, устройство связи, чья совместимость с другим оборудованием связи не гарантирована, не может быть включено в состав сетей связи. В отсутствии подтверждения совместимости устройств от их производителей, ответственность за их совместимость и корректное функционирование полностью несет проектная организация, формирующая состав проекта и спецификации, содержащие в себе все проектируемое оборудование сетей связи.

Список используемых источников

1. Гольдштейн Б. С., Соколов Н. А., Яновский Г. Г. Сети связи : учебник. СПб.: БХВ-Петербург, 2014. 401 с. ISBN 978-5-9775-2798-9.

2. Иванов В. С., Никитин Б. К., Пирмагомедов Р. Я. Строительство ВОЛС. Современные технологии и организация : учебное пособие; Федеральное агентство связи, Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича». СПб. : СПбГУТ, 2015. Ч. 1. 70 с. : ил., табл.

3. Гурлев И. В. Экологические проблемы при прокладке волоконно-оптической линии связи в грунте на Крайнем Севере // Науковедение. 2016. Т. 8, № 6.

УДК 621.396.67
ГРТНИ 47.45.29

АНАЛИТИЧЕСКИЙ ОБЗОР ПОЛОСКОВЫХ АНТЕННЫХ УСТРОЙСТВ БЕСПРОВОДНЫХ СЕТЕЙ

Н. Д. Денисов, В. А. Мешалкин

Военная академия связи им. Маршала Советского Союза С. М. Буденного

В статье дан обзор наиболее распространённых видов малогабаритных печатных микрополосковых антенн. Рассмотрена их конструкция, дан анализ характеристик, проведено сравнение разных видов печатных микрополосковых антенн. Для более сложных разновидностей печатных микрополосковых антенн приведены расчётные соотношения для их резонансных частот.

антенна, микрополосковая антенна, беспроводные сети, беспроводная связь.

В современное время ни один человек не обходится без интернета. Оперативный поиск информации из приятной возможности превратился в необходимость. В связи с этим практически каждое мобильное устройство сейчас оснащается модулем Wi-Fi для подключения к точкам доступа в интернет. Это делает технологию Wi-Fi крайне востребованной. Постепенно стандарты этой технологии совершенствуются, чтобы обеспечить более высокую скорость и стабильность подключения. В свою очередь совершенствуются и клиентские устройства, становясь всё более миниатюрными и более производительными.

На данный момент превалируют устройства, поддерживающие версию стандарта IEEE 802.11n и диапазон 2,4 ГГц. Однако из-за их большого количества возникла проблема – малое количество непересекающихся каналов, что в перспективе может сильно сказаться на качестве подключения из-за взаимных помех работающих рядом устройств. Эту проблему можно решить, если использовать диапазон 5 ГГц, т.к. на нём количество непересекающихся каналов больше. В связи со всем вышеперечисленным проблема разработки миниатюрных антенных систем, работающих на диапазонах 2,4 и 5 ГГц, весьма актуальна.

Рассмотрим основные разновидности таких антенных систем.

Основной разновидностью низкопрофильных всенаправленных излучателей является семейство планарных инверсных L- и F-образных антенн [1]. Они являются развитием простейшего L-образного вибратора, расположенного в перевернутом виде (отсюда термин «инверсный»)

над плоским экраном (рис. 1). Такая согнутая конструкция позволяет разместить антенный излучатель, например, внутри мобильного телефона, размещая его вдоль длинной стороны корпуса. L-вибратор запитывается с одного конца, а второй конец нагружен на эквивалентную емкость, а второе его окончание через воздух либо диэлектрик оказывается нагруженным на эквивалентную емкость.

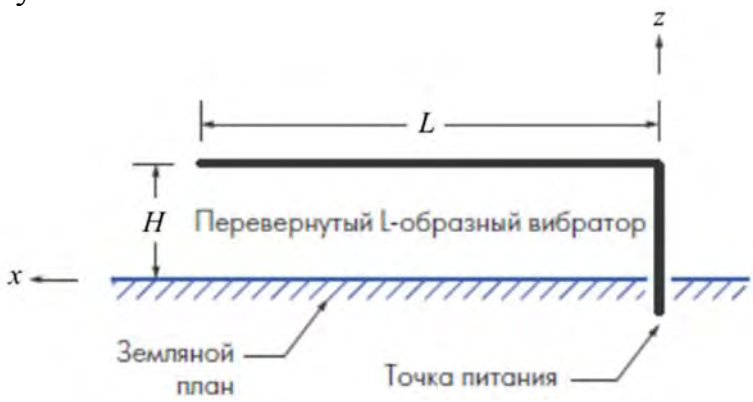


Рис. 1. Перевернутый L-образный вибратор

Перевернутая L-антенна (*Inverted-L antenna*, ILA) достаточно проста в изготовлении. Основные электрические характеристики такой антенны подобны характеристикам короткой штыревой антенны. Диаграмма направленности (ДН) рассматриваемой L-антенны практически идентична ДН короткого штыря, который является всенаправленным в плоскости, перпендикулярной к его оси, и не излучает в соосном направлении. Однако дополнительное излучение, обусловленное геометрией перевернутого L-вибратора, отклоняет его ДН от всенаправленной формы. Резонансная длина волны L-вибратора λ определяется его геометрическими размерами согласно выражению: $\lambda = 4(H + L)$, где H – высота вибратора над заземленным экраном, L – длина горизонтального сегмента вибратора.

Развитием L-вибратора является перевернутая F-образная антенна (рис. 2), представляющая собой соосный тандем из двух L-образных вибраторов разной длины.

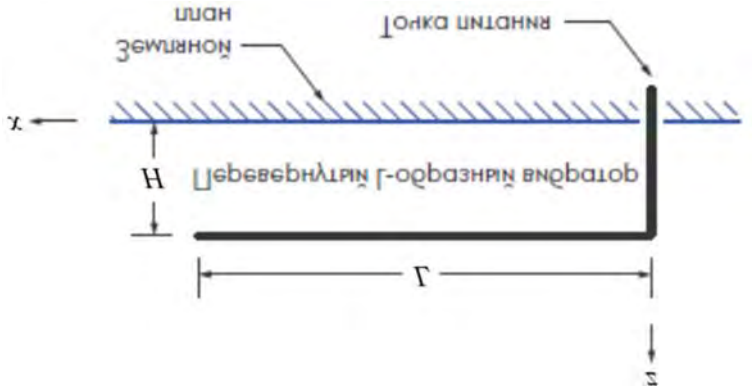


Рис. 2. Перевёрнутый вибратор F-типа

Внешняя вертикальная стойка F-антенны нагружена на корпус, а подача сигнала осуществляется через «внутреннюю» вертикальную секцию. Дополнительный L-сегмент позволяет изменять величину входного сопротивления антенны и значительно упрощает ее согласование. Подбирая расстояние между вертикальными секциями, можно обеспечить приемлемое по величине реактивное сопротивление антенны. Величина *S* не влияет на резонансную частоту такого излучателя. За счет существенного улучшения согласования антенны на резонансной частоте может быть достигнута величина КСВ < 2, при этом ширина рабочей полосы частот составляет всего 1,5 %, что считается слишком малой величиной для приложений Wi-Fi (типичные проводные F-антенны имеют полосу не более 2 %).

Развитием планарных L- и F- антенн является PIFA антенна (*Planar Inverted-F Antenna*), показанная на рис. 3 (см. ниже) [2].

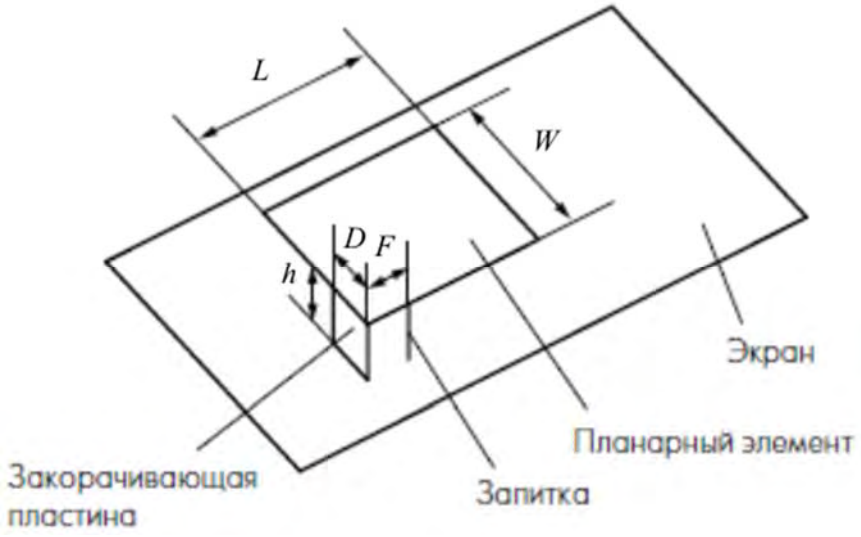


Рис. 3. Планарная антенна PIFA

Электрические характеристики такой антенны зависят от геометрии верхней пластины и размеров вертикальной заземляющей стенки. Ширина закорачивающей пластины D влияет на ширину полосы пропускания антенны. Наибольшая полоса определяется совпадением ширины пластины *D* и длины горизонтального излучателя *W*. Для соотношения длин сторон *W/L* = 2 достигается полоса рабочих частот 10 %. При уменьшении соотношения, диапазон рабочих частот сужается до 1 %.

Наилучшее согласование имеет PIFA-антенна с соотношением *D/W* = 1. Для антенн этого типа отсутствуют строгие математические соотношения, позволяющие точно рассчитать влияние места расположения фидерной линии на характеристики антенны, вследствие чего, для достижения требуемых параметров инвертированной антенны F-типа, используются численные, либо программные методы оптимизации.

Наиболее точно величину резонансной частоты рассчитал Minh-Chau T Huynh [3]. После рассмотрения всех частных случаев зависимости резонансных частот от геометрии PIFA, им были получены следующие выражения, представленные в таблице.

ТАБЛИЦА. Резонансные частоты для разных габаритов PIFA

Условие	Расчётная формула
$D = 0$	$L + W + h = \lambda/4$
$D = W$	$L + h = \lambda/4$
$0 \le D/W < 1,\ W / L \le 1$	$\frac{D}{W}\frac{1}{L+h} + \left[1 - \frac{D}{W}\right]\frac{1}{L+h+W-D} = \frac{4}{\lambda}$
$0 \le D/W < 1,\ W / L > 1$	$(\frac{D}{W})^{\frac{W}{L}}\frac{1}{L+h}\left[1 - (\frac{D}{W})^{\frac{W}{L}}\right]\frac{1}{L+h+W-D} = \frac{4}{\lambda}$

Большие габариты являются основным недостатком рассмотренных PIFA антенн. Поэтому более широкое распространение получил метод расширения полосы пропускания рассматриваемого типа антенн за счет фрезеровки в горизонтально расположенной пластине прорезей различной геометрии.

Многодиапазонные PIFA антенны для мобильных средств связи развиваются. Их конструкция усложняется. Имеются разновидности PIFA антенн с интегрированными микрополосковыми и диэлектрическими резонансными антеннами.

Для сокращения длины антенны используют так называемую «зигзагообразную» конструкцию. Пример антенны типа «Зиг-заг» показан на рис. 4.

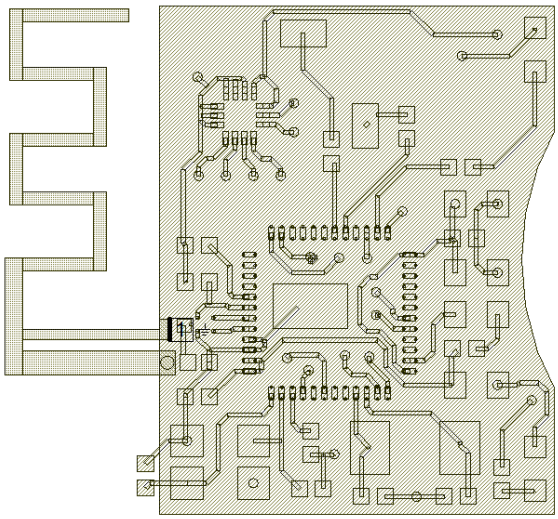


Рис. 4. Пример антенны «Зиг-заг»

Список используемых источников

1. Драбкин А. Л., Зузенко В. Л., Кислов А. Л. Антенно-фидерные устройства; изд-е 2-е, испр., доп. и перераб. М. : Сов. радио, 1974. 536 с.
2. Слюсар. В. Многодиапазонные антенны мобильных средств связи [электрически малые антенны (ЭМА)] // Электроника: наука, технология, бизнес. 2006. № 8. С. 90–96.
3. Minh'Chau T. Huynh. A. Numerical and Experimental Investigation of Planar Inverted'F Antennas for Wireless Communication Applications // In: Master Thesis of Science in Electrical Engineering. Virginia Polytechnic Institute and State University. Blacksburg, Virginia. Oct. 19, 2000. 123 p. URL: http://scholar.lib.vt.edu/theses/available/etd'10242000'22130026/unrestricted.

УДК 004.77
ГРНТИ 28.23.29

АНАЛИЗ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

В. А. Десницкий[1,2], П. И. Думенко[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации
Российской академии наук

В работе анализируются нарушения в области информационной безопасности современных мобильных приложений, актуальные методы защиты программного кода и данных, основные виды атак и уязвимости, а также наиболее важные аспекты разработки безопасных мобильных приложений под управлением операционной системы Android. Эти аспекты включают локальное требование хранения данных; требования к аутентификации и управлению сессиями; требования к сетевой связи; и устойчивость к обратному инжинирингу. Анализ ключевых компонентов мобильной экосистемы и обеспечение защиты критически важных данных пользователя. Действенность предлагаемых решений подтверждается на примере задачи защиты программного кода на языке Java и среды разработки Android Studio.

информационная безопасность, критически важные данные (КВД), мобильные приложения, ОС Android.

Введение

В наше время многие крупные корпорации, а также физические лица все больше полагаются на мобильные программные приложения для поддержки своих критически важных инициатив. При разработке любого при-

ложения под мобильную платформу следует учитывать, что данные, с которыми впоследствии будет взаимодействовать мобильное приложение, могут представлять определенный интерес для посторонних лиц.

С ростом числа разработок мобильных приложений, повышается их капиталоёмкость, а вместе с этим и желание злоумышленников произвести атаку на строго конфиденциальные данные. Механизмов взлома и извлечения критических данных из мобильных устройств довольно много, каждый год появляются новые алгоритмы, но вместе с тем растёт и сложность механизмов противодействия, способных своевременно нейтрализовать угрозы. В наименьшей степени этим тенденциям подвержены закрытые платформы, в частности одной из которых является iOS, поскольку архитектура её построена таким образом, что в ней практически невозможно появление вирусов. Проще и уязвимее разработка приложений под операционную систему Android [1].

В работе анализируются методы защиты программного кода и данных, основные виды атак и уязвимости, а также наиболее важные аспекты разработки безопасных мобильных приложений под управлением операционной системы Android. Эти аспекты включают локальное требование хранения данных; требования к аутентификации и управлению сессиями; требования к сетевой связи; и устойчивость к обратному инжинирингу (реверсингу). Действенность предлагаемых решений подтверждается на примере задачи защиты программного кода на языке Java и среды разработки AndroidStudio.

Виды атак и уязвимости мобильных приложений

Среди огромного разнообразия мобильных приложений, находящихся в свободном доступе, сегодня выделяют следующие виды атак на них и уязвимости общего характера без привязки к конкретной платформе [2].

– декомпиляция файла приложения (.ipa-файлы для *Apple iOS* и .apk-файлы для *Google Android*) и разбор локально сохраненных данных. Защита данного параметра, представляющего важное значение, лежит на плечах мобильного разработчика;

– перехват/подмена данных, передаваемых по сети (MITM-атаки). Большая часть существующих приложений для современных девайсов имеют клиент-серверную архитектуру, следовательно, регулярно занимаются обменом больших объемов информации. Несмотря на активное стремление мобильной и веб-разработки к полному переходу на HTTPS-протокол общения, не стоит полагаться на единственный рубеж защиты в виде защищенного канала связи;

– рутование устройства и атака на приложение и применяемые в нем алгоритмы через внешние отладочные инструменты;

– атаки на протокол NFC;

– несанкционированный прием зловредных обновлений;

– установка вредоносных приложений, замаскированных под легитимный софт;

– подключение к не доверенным устройствам (док-станции, зарядные устройства и др.).

Среди существующих уязвимостей мобильных приложений наиболее существенными представителями являются следующие:

– использование незащищенных локальных хранилищ. Хранить важную информацию в слабо защищенных локальных хранилищах, специфических для конкретной платформы, очень опасно;

– хранение КВД в коде (в статических константных строках, в ресурсах приложения и т. п.). Подобная уязвимость легко вскрывается третьей стороной при наличии базовых навыков декомпиляции;

– применение алгоритмов с хранением приватного ключа. Приватный ключ, находящийся внутри программного кода или ресурсах мобильного приложения, также возможно получить стандартным методом декомпиляции;

– использование асимметричного алгоритма с приватным ключом, хранящимся на стороне сервера;

– игнорирование факта наличия рутованных или зараженных устройств;

– хранение КВД в защищенных хранилищах, но в открытом виде.

*Под определение КВД попадают все данные, которые не должны быть доступны третьей стороне, это касается как персональных данных пользователя, так и его приватных данных.

Мобильная экосистема

Все мобильные устройства функционируют в определенной среде, именуемой мобильной экосистемой, которая состоит не только из мобильных устройств, а также области, которая соединяет девайс с другими устройствами и информационной системой в целом. Ключевыми компонентами мобильной экосистемы включают в себя следующие компоненты [3].

Технологический стек мобильных устройств: оборудование, операционная система (ОС) и встроенные компоненты мобильного устройства (например, базовая радиостанция, датчики, загрузчик, изолированные среды исполнения, карта модуля идентификации абонента [SIM]); мобильные приложения; сети (например, сотовая связь, Wi-Fi, Bluetooth, NFC) и услуги, предоставляемые локальным оператором; мобильная инфраструктура производителя, включая магазины мобильных приложений, обновле-

ния и резервное копирование, услуги, предоставляемые производителем мобильных устройств или операционной системой; корпоративные мобильные сервисы и инфраструктура, управление мобильными устройствами (*Mobile Devices Management*), корпоративные магазины мобильных приложений и управление мобильными приложениями (*Mobile Application Management*).

Все эти отдельные компоненты экосистемы должны учитываться при оценке безопасности мобильных устройств (рис. 1).

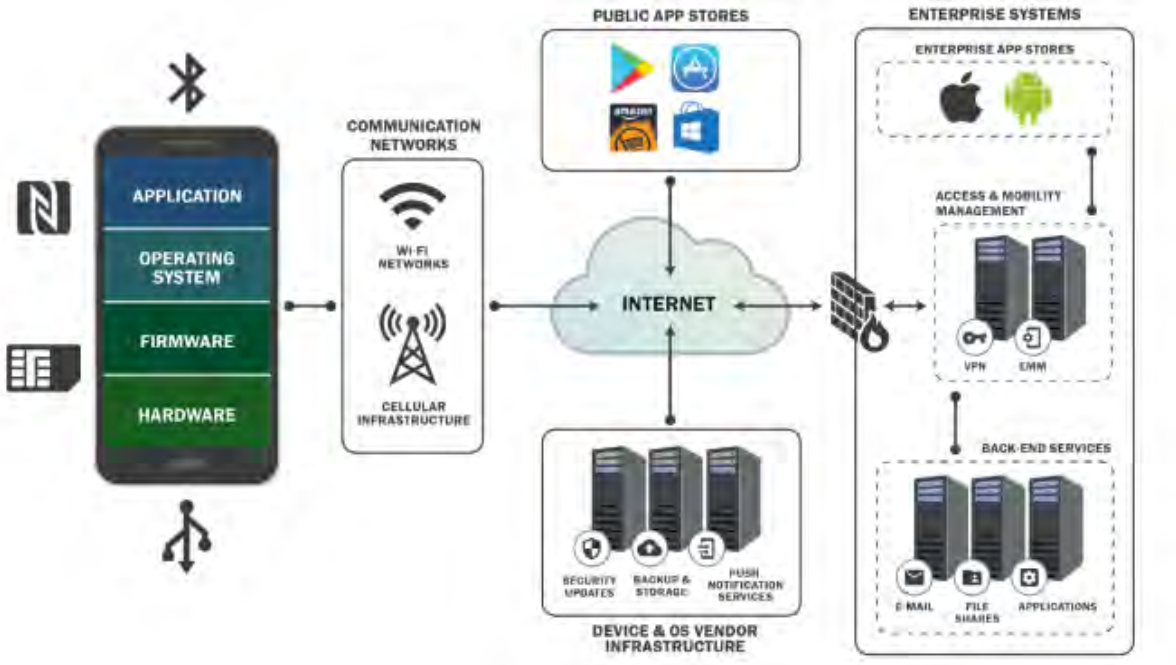


Рис. 1. Обзор мобильной экосистемы [3]

Набор функций ОС может быть расширен за счет установки дополнительных специальных мобильных приложений. Они могут хранить наши настройки, историю, пароли и другие конфиденциальные данные. Они отслеживают нашу деятельность, чтобы определить наши предпочтения. Кроме того, они передают пользовательские данные в удаленную конечную точку службы для синхронизации. Каждое действие, выполняемое такими приложениями, должно быть надлежащим образом защищено от возможных утечек данных.

Безопасность Android-приложений

Как уже было сказано, разработка приложений под мобильную оболочку Android требует более детальной проработки, поскольку она более уязвима к атакам со стороны злоумышленников. Большая часть Android-приложений получают статус «уязвимых» ввиду следующих источников проблем. Первые – сетевые, связанные с коммуникацией с сервером. В этом случае данные пользователя передаются незащищенным способом. Вторые

связаны с проблемой хранения данных: когда информация хранится где-то в открытом виде (например, на SD-карте), либо она не зашифровывается, другими словами, когда к ним есть доступ извне. Третий вид проблем – воздействие сторонних приложений на пользовательское. Таким образом, стороннее приложение может получить несанкционированный доступ к устройству, выполнить какие-то действия от имени пользователя, кражу информации или ее модификацию.

Анализ базовых проблем Android-приложений

При рассмотрении любого приложения, функционирующего под управлением мобильной ОС Android, следует произвести анализ manifest-файла, потому что в нем обязательно должны быть описаны все компоненты Android-приложения, такие как Activity, Service, BroadcastReceiver, ContentProvider. Поэтому при поиске каких-то проблем, необходимо обращать внимание на эти компоненты [4].

```
<service
        android:enabled="true"
        android:exported="true"
        android:name="com.acompli.accore.ACCoreService"/>
```

Рис. 2. Объявление данных в manifest-файле приложения [4]

В данном случае был объявлен сервис в manifest-файле одного приложения, он явно экспортируется – это потенциальный вектор атаки (рис. 2). Если изучить файлы-исходники данной программы, то можно понять, что сервис позволяет, например, удалить авторизованного пользователя в этой программе. Очередной важный момент: использование той или иной компонентой Интент-фильтры, которые по-автоматически наделяют компоненту свойством «экспортируемости». Другими словами, если Интернет-фильтр присутствует, то компонента уже публичная.

Пример уязвимости Яндекс-почты для Android

Появление уведомления о каком-либо событии, отображающемся в соответствующей панели и над которым можно произвести ряд действий. Важно определить, что означает подобное событие. Оно обрабатывается при помощи публичного BroadcastReciever. Другими словами, злоумышленник может послать любой broadcast – подобрать ID письма и, допустим, удалить его (рис. 3).

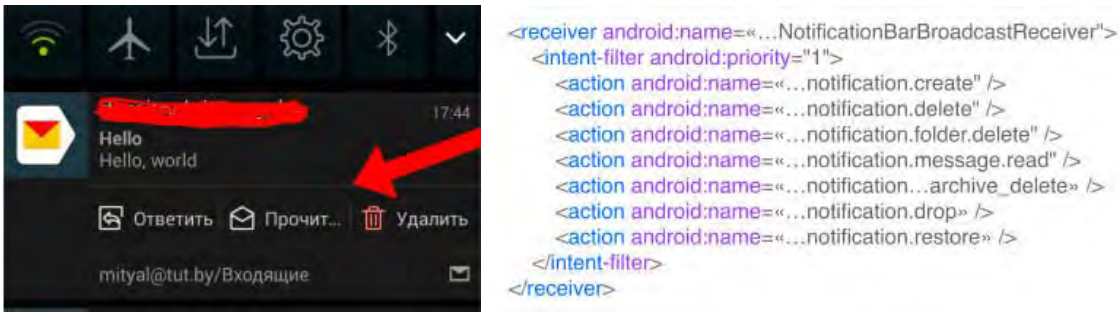


Рис. 3. Уязвимость Яндекс-почты для оболочки Android [4]

Решением в подобной ситуации послужит присвоение компоненту статус недоступной извне, а также установить дополнительно параметр permission. Вторую операцию производить необязательно, главное – если она не экспортируется, значит, уже никто не сможет к ней подключиться и что-то выполнить (рис. 4).

```
<receiver android:name="...NotificationBarBroadcastReceiver"
        android:permission="com.yandex.mail.permission.write"
        android:exported="false">
```

Рис. 4. Объявление компоненты статуса «закрытой» и установка permission [4]

Безопасность мобильных приложений жизненно важна для приложений, обрабатывающих пользовательские данные. Наиболее важными аспектами безопасности мобильных приложений являются безопасность хранения локальных данных [5]; аутентификация и управление сессиями; сетевое взаимодействие и устойчивость к обратному инжинирингу [6]. Чтобы обеспечить необходимый уровень безопасности, должны использоваться только проверенные алгоритмы и библиотеки.

Работа выполнена при финансовой поддержке Гранта РФФИ № 19-07-00953.

Список используемых источников

1. Six J. Application Security for the Android Platform.O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.: 2012. 112 с.

2. Безопасность данных в разработке мобильных приложений [Электронный ресурс] // Хабрахабр. URL: https://habr.com/ru/post/327760/ (дата обращения 22.03.2019).

3. DHS Study on Mobile Device Security – April 2017 – FINAL, 125 p.

4. Безопасность Android-приложений. Лекция в Яндексе [Электронный ресурс] // Хабрахабр. URL: https://habr.com/ru/company/yandex/blog/310926/ (дата обращения 22.03.2019).

5. Desnitsky V. A., Kotenko I. V. Modeling and analysis of security incidents for mobile communication mesh ZigBee-based network // Proceedings of 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM). 2017. PP. 500–502.

6. Десницкий В. А., Котенко И. В. Модель защиты программного обеспечения на основе механизма «удаленного доверия» // Известия высших учебных заведений. Приборостроение. 2008. Т. 51. № 11. С. 26–31.

УДК 004.056
ГРНТИ 19.31

СБОР И АНАЛИЗ ДАННЫХ О КАНАЛАХ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНОЙ СЕТИ TWITTER

В. А. Десницкий[1,2], И. П. Зуев[1], П. В. Карельский[1], М. М. Ковцур[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Социальные сети получают все большее распространение как предмет анализа. Исследуются события и данные из сетей для получения ранее неизвестной информации. Для формирования набора данных можно пользоваться различными инструментами, даже использовать стандартный набор пакета MS Office. Статья посвящена сбору и анализу данных о каналах распространения в социальной сети Twitter.

большие данные, twitter, каналы распространения информации, социальные сети, NodeXL.

Выявление канало распространения в информационном пространстве общества и государства сегодня является одной из актуальных задач в области информационной безопасности. Множество исследователей и проектов все больше направлено на выработку мер и способов нахождения и противодействия вредоносному влиянию в социальных сетях [1, 2, 3].

В данной работе авторы исследуют каналы распространения в микроблоге «Твиттер» с целью выявления источника распространения нежелательной информации [4].

Анализ

«Твиттер» на сегодняшний день является одним из самых популярных сервисов микро-блогов. Он относится к такому типу социальных сетей как «Социальные сети для авторских записей». В нем пользователи создают и публикуют текстово-медийный контент.

Как и любая другая социальная сеть, «Твиттер» имеет особые каналы распространения, характерные именно для этой социальной сети. Каналы

распространения информации должны обеспечивать равноправный, своевременный и не связанный с чрезмерными расходами доступ пользователей к интересующей их информации.

Можно выделить следующие виды каналов:

1) событие (по хэштегу),
2) аккаунт,
3) твит,
4) упоминание.

Далее стоит определить модель данных сети «Твиттер». Она также в целом является уникальной для отдельно взятой социальной сети.

Модель данных сети «Твиттер» (рис. 1) состоит из следующих объектов: аккаунт, аудитория, событие, твит.

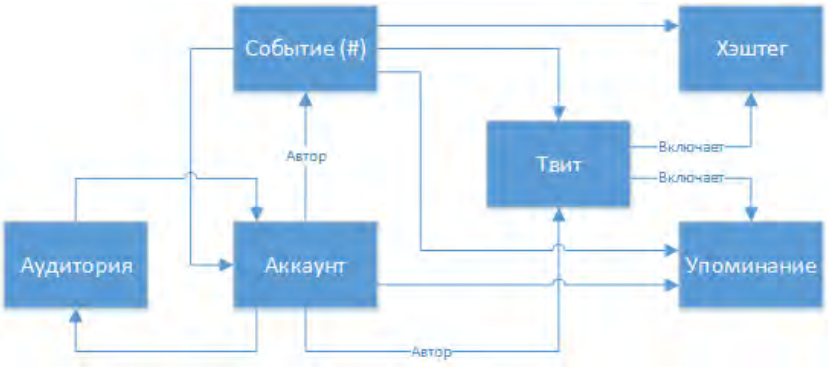


Рис. 1. Модель данных Твиттер

У каждого аккаунта в социальной сети есть свое имя и уникальный id, который является переменной типа string. Этот id совершенно точно определяет аккаунт среди всех пользователей социальной сети.

У каждого аккаунта есть так называемые читатели, т.е. его аудитория, которая, в свою очередь, так же состоит из определенных аккаунтов, имеющих те самые уникальные id, что позволяет точно определить, какие люди, т. е. аккаунты, подписаны на тот или иной профиль.

Также аккаунт публикует уникальные записи, называемые твитами, которые имеют уникальный числовой идентификатор.

Определенный аккаунт также может стать автором распространения какого-либо события, передаваемого через «хэштеги», или упомянуть аккаунт другого пользователя через «упоминания». Отсюда следует, что событие характеризуется твитами, в которых упоминается уникальный идентификатор события – «хэштег», а также id аккаунтов, в твитах которых данный уникальный идентификатор использовался, и, в некоторых случаях, упоминаниями, которые ссылаются на определенный аккаунт, от которого пользователь получил информацию.

Соответственно, вспомогательными объектами в данном случае являются «хэштеги», которые характеризуют определенное событие, и «упоминания», которые делают ссылку на определенный аккаунт в сети «Твиттер».

Именно эти вспомогательные объекты и являются частью методов распространения информации в данной социальной сети. С их помощью пользователи получают не только уникальный параметр, который можно использовать для поиска информации по событию в целом, но и также определить те аккаунты, которые в распространении информации участвовали.

Эксперимент

Для сбора информации для анализа каналов распространения использовалось ПО «NodeXL» [5]. В работе было выбрано событие, а именно чемпионат Европы по футболу 2020 года. «Хэштег» «#EURO2020». В результате выгрузки появилось 2 тысячи записей с «хэштегом» «#EURO2020».

Следующим этапом является выполнение анализа полученных данных. Для этого строится граф для последующего анализа.

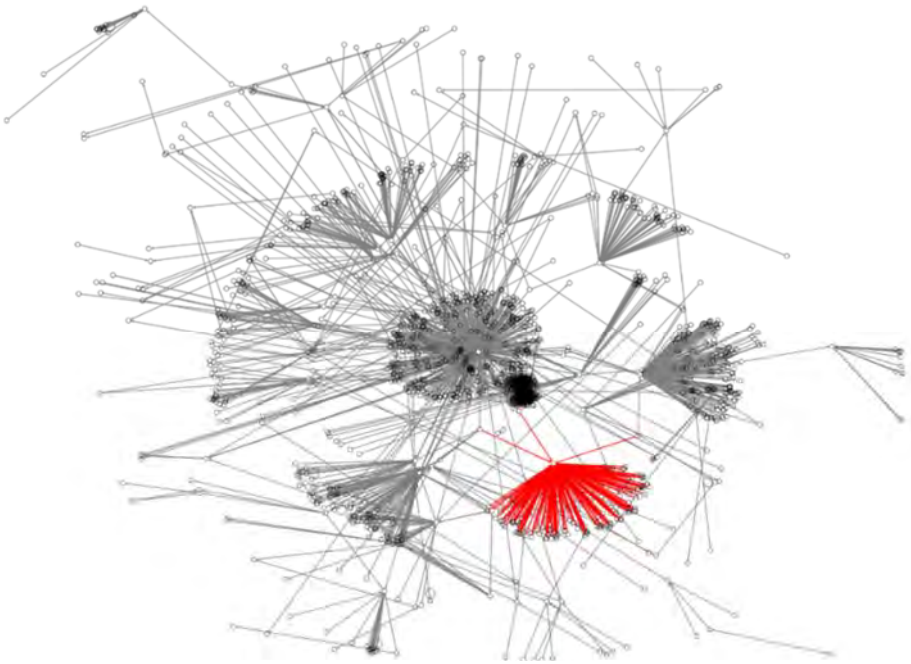


Рис. 2. Визуализация канала распространения в Твиттере по «#EURO2020»

На рис. 2 показан получившийся граф. При выборе определенной вершины графа, можно наблюдать распространение определенного «твита». На рис. 3 в таблице – имена Twitter-аккаунтов, которые участвуют в связях.

Выделяется несколько скоплений связей, что свидетельствует о нескольких масштабных аккаунтах (т.е. аккаунтов с большой аудиторией читателей), в которых имеется упоминание выбранного нами «хэштега».

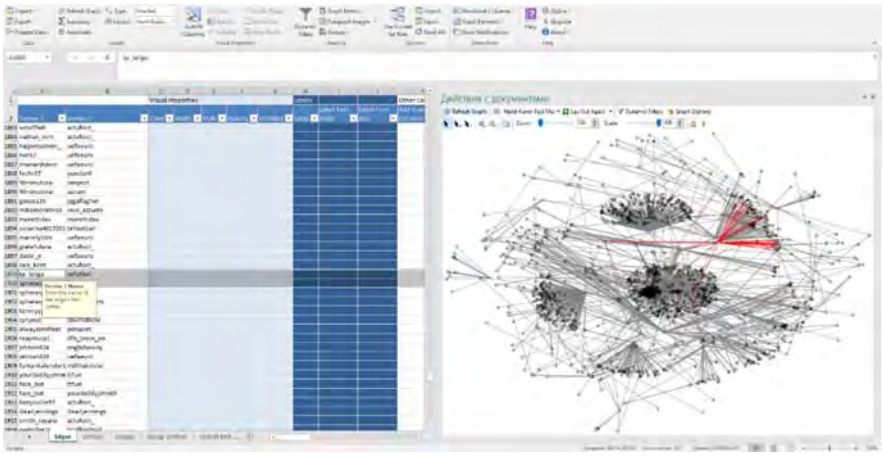


Рис. 3. Анализ канала распространения в Твиттере по «#EURO2020»

Одно из самых больших скоплений вершин – это скопление вокруг официального аккаунта «UefaEuro», у которого свыше 1,3 миллиона читателей (рис. 4).

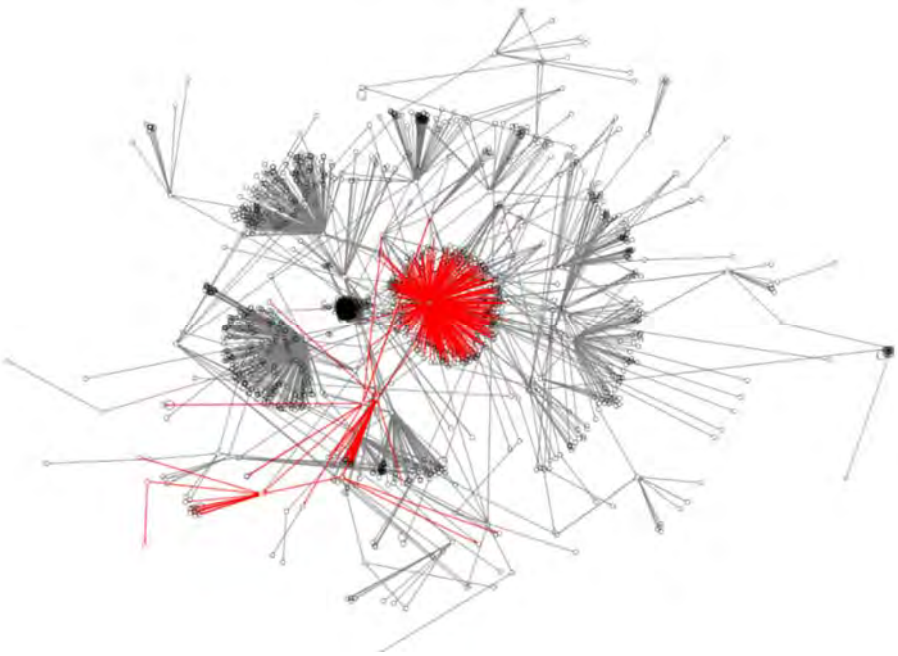


Рис. 4. Канал распространения информации аккаунта «UefaEuro»

Именно из-за такого большого количества читателей канал распространения у такого аккаунта будет наиболее обширным.

Например, на рис. 5 (см. ниже) видно, что информация, которая была опубликована в одном из твитов официального аккаунта «UefaEuro» прошла через как минимум 8 других аккаунтов, при этом ознакомилось с данной информацией свыше 100 человек.

Еще одним аккаунтом с большим числом скоплений связей является аккаунт «EURO2020» (рис. 5), который насчитывает порядка 370 тысяч читателей. Проанализируем и его в качестве канала распространения информации.

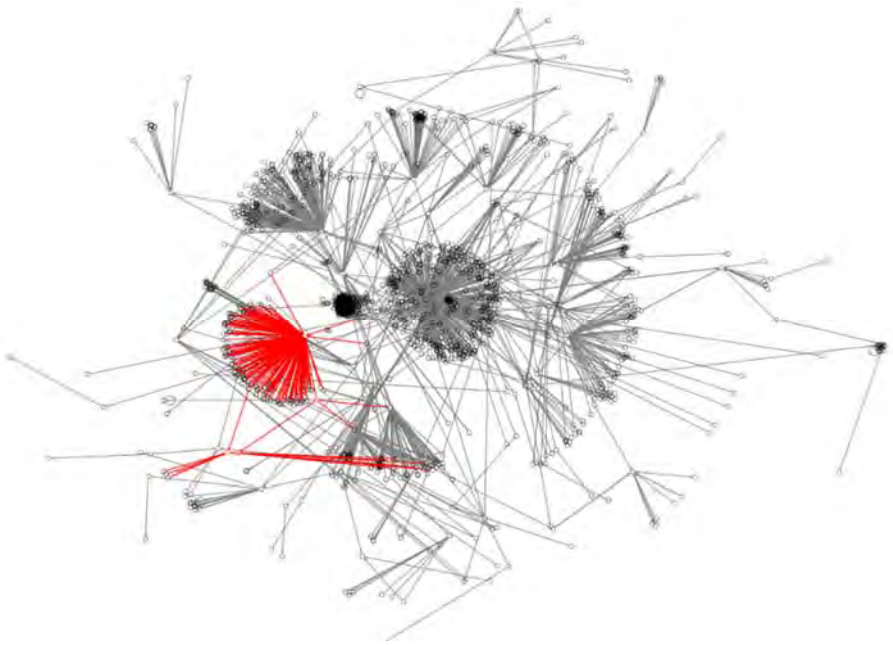


Рис. 5. Канал распространения «EURO2020»

Из-за того, что число читателей у данного аккаунта много меньше предыдущего, выбранный канал распространения получился намного меньше предыдущего – около 4 аккаунтов участвует в распространении информации, около 50–70 человек могло получить информацию из такого канала.

Исходя из полученных результатов можно сказать, что информация, распространяющаяся посредством «хэштега», проходит через большее количество человек. Злоумышленнику или противнику стало проще «запустить» какой-либо «хэштег» и распространить нежелательную информацию. При этом, наиболее популярные в мире «хэштеги» попадают в специальный список «Актуальные темы», что повышает шансы распространения информации об определенном событии.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-71-10094) в СПИИРАН.

Список используемых источников

1. Левкин И. М., Науменко К. А., Виткова Л. А. Особенности информационно-психологического воздействия в интернете // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 365–367.

2. Комашинский Д. В., Котенко И. В., Чечулин А. А. Категорирование веб-сайтов для блокирования веб-страниц с неприемлемым содержимым // Системы высокой доступности. 2011. № 2. С. 102–106.

3. Kotenko I., Saenko I., Chechulin A., Desnitsky V., Vitkova L., Pronoza A. Monitoring and counteraction to malicious influences in the information space of social networks // 10th International Conference on Social Informatics (SocInfo). 2018. PP. 159–167.

4. Виткова Л. А., Дойникова Е. В. Поддержка принятия решений по противодействию нежелательной информации // Информационные технологии в управлении (ИТУ-2018) : материалы конференции. 2018. С. 398–403.

5. NodeXL [Электронный ресурс]. URL: https://www.smrfoundation.org/nodexl/ (дата обращения 20.01.2019).

УДК 004.7
ГРНТИ 49.33.29

РАЗРАБОТКА МОДЕЛЕЙ ВЗАИМОДЕЙСТВИЯ БПЛА ДЛЯ БЫСТРОРАЗВОРАЧИВАЕМЫХ ЛЕТАЮЩИХ СЕТЕЙ ЭКСТРЕННЫХ СЛУЖБ

Ч. З. Динь, Р. В. Киричек

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

Успех любой поисково-спасательной операции зависит от времени, необходимого для поиска пропавшего человека и от оснащения. Использование беспилотных летательных аппаратов может повысить эффективность поисково-спасательных операций за счет авиационной поддержки процесса поиска. Существуют решения на базе БПЛА, которые способны обнаружить пропавшего человека с помощью систем компьютерного зрения, инфракрасных датчиков и обнаружения сигналов мобильного телефона. Таким образом, чтобы повысить эффективность использования ресурсов и уменьшить стоимость операции поиска пропавших людей в данном статье представлены модели взаимодействия БПЛА для летающих сетей экстренных служб.

беспилотный летательный аппарат, поисково-спасательная операция, летающая сеть, экстренная служба.

Каждый год большое количество людей по всему миру погибает в результате несвоевременно оказанной помощи. Примерами могут быть землетрясения, цунами и другие стихийные бедствия естественного и искусственного происхождения. Кроме этого, немалая часть людей пропадает в лесах из-за отсутствия возможности связаться с экстренными службами. Эффективность поисково-спасательной операций может быть повышена за счет

использования новых подходов по обнаружению пострадавших, которые базируются на использовании группы беспилотных летательных аппаратов (БПЛА) с навесным оборудованием – летающей сети [1, 2]. Такая сеть, позволяет сократить время, необходимое для обнаружения пострадавших, а также сократить количество людей, задействованных в поисково-спасательной операций [3].

Одним из основных видов связи современного общества является мобильная связь. Абонентские терминалы сетей сотовой подвижной связи представляют миниатюрные компьютеры, которые способны выполнять множество операций и функций. Однако, фактически вся связь завязана на инфраструктуру, при разрушении которой невозможно связаться экстренными службами, а также родными и близкими, чтобы сообщить подробности случившегося. Таким образом, возникает задача организация связи в случае разрушения или частичного разрушения сетей сотовой подвижной связи.

Для решения такой задачи можно рассмотреть организацию летающей сети на базе БПЛА общего пользования. На сегодняшний день большинство мобильных телефонов поддерживают технологии Wi-Fi IEEE 802.11 n/ac. В этой связи, можно рассмотреть возможность передачи голоса поверх Wi-Fi на базе приложений Voice over Wi-Fi (VoWi-Fi) [4]. Предполагается, что для организации связи вся зона бедствия должна быть полностью покрыта радиосигналом Wi-Fi. БПЛА с навесным оборудованием являются мобильными точками доступа и передают данные на базовую станцию, которая функционирует в обычном режиме. В такой сети каждый БПЛА может рассматриваться как мобильный гетерогенный шлюз [5], который поддерживает несколько технологии передачи данных:

– IEEE 802.11n/ac между БПЛА и абонентом;
– IEEE 802.11p между БПЛА.

Следует отметить, что в VoWi-Fi все звонки осуществляются через оператора с традиционной нумерацией и идентификацией абонентов мобильной сети.

На рис. 1 и 2 (см. ниже) представлены две модели взаимодействия летательных аппаратов для летающих сетей экстренных служб: одноранговая модель и иерархическая модель.

В иерархической модели (рис. 2), летающий сегмент состоит из двух уровней. На первом уровне взаимодействуют головные беспилотные летальные аппараты (ГБПЛА). Его особенность заключается в том, что ГБПА связываются друг с другом по технологии IEEE 802.11p в супер-режим, который позволяет осуществлять передачу данных до 750 м. В рамках предлагаемых моделей и для стабильности функционирования мы выбираем скорость передачи 6 Мбит/с (в обычном режиме расстояние передачи до 100 м и скорость до 12 Мбит/с) [6, 7].

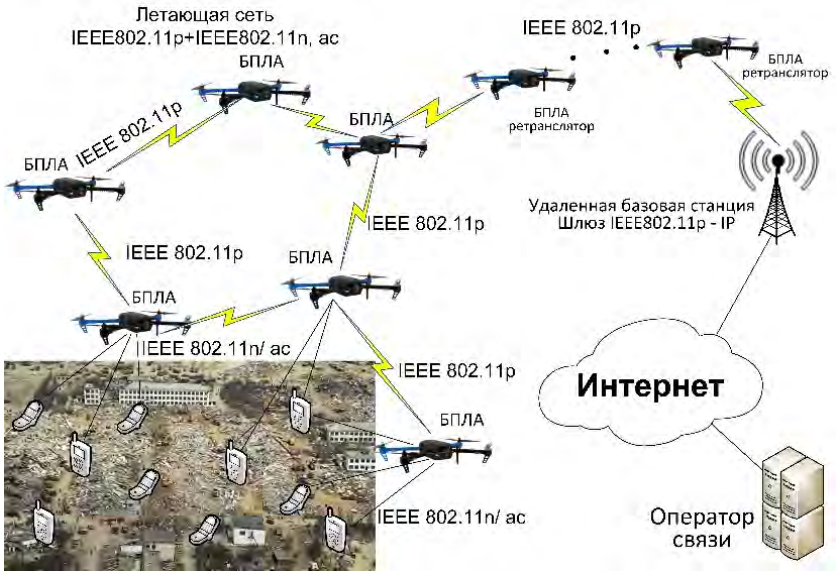


Рис. 1. Одноранговая модель взаимодействия БПЛА
для летающих сетей экстренных служб

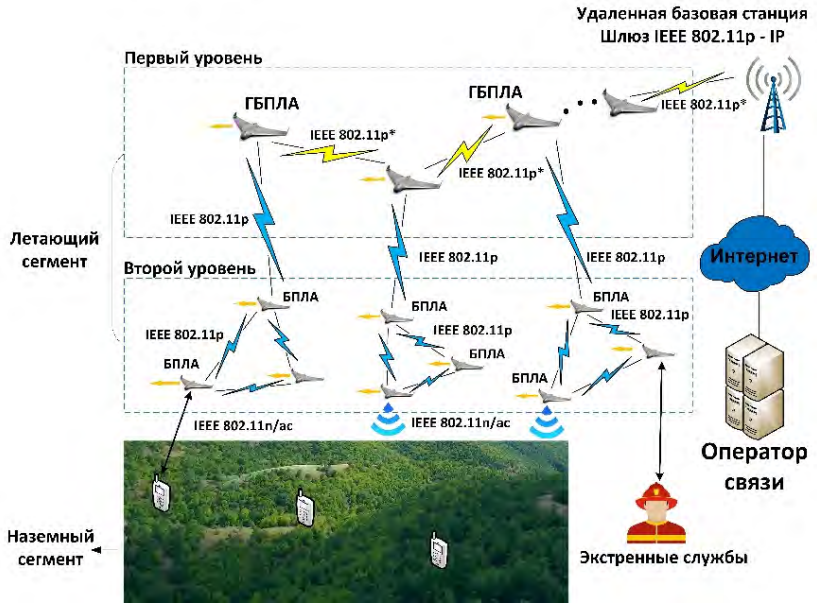


Рис. 2. Иерархическая модель взаимодействия БПЛА
для летающих сетей экстренных служб

Ниже рассмотрим процесс передачи голоса с от абонента 1 к абоненту 2 в зоне бедствия через летающую сеть после установления соединения через оператора сетей сотовой подвижной связи. Для обеспечения приемлемого качества передачи голоса сетевая задержка должна быть не более 100 мс [8].

Процесс передачи голоса описывается с помощью модели многофазной системой массового обслуживания (СМО) [9]. В соединении между двумя

абонентами каждый БПЛА представлен однофазной СМО. Мы предполагаем, что входящие потоки на каждый летательный аппарат имеют одинаковые свойства, в связи с этим рассмотрим модель СМО M/M/1 для двух модельных сетей [10]. Рис. 3 показывается, что задержка доставки голосового трафика от абонента 1 к абоненту 2 представляется суммой среднего времени доставки на всех фазах, которая показывает в формуле (1).

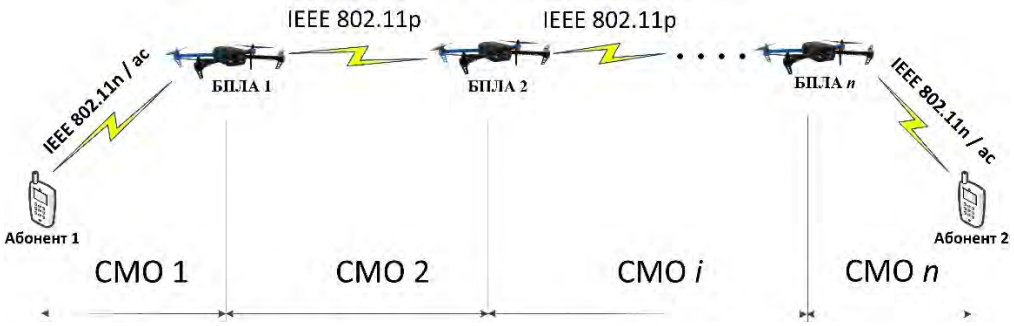


Рис. 3. Структура модели СМО летающей сети для передачи голоса

$$\overline{T} = \overline{T_1} + \sum_{j=1}^{N} \overline{T_j} + \overline{T_n}\ , \qquad (1)$$

где $\overline{T}$ – сумма среднего времени передачи на всех фазах, $\overline{T_1}$ – среднее время передачи в первой фазе (мс), $\overline{T_j}$ – среднее время передачи между ЛА (мс), $\overline{T_n}$ – среднее время передачи в последней фазе, N – количество БПЛА.

Согласно формулы (1) и модели СМО типа M/M/1 можно рассчитать количество БПЛА, которые смогут обеспечить время передачи голосового трафика между двумя абонентами с задержкой, не превышающей 100мс. Допускается, что времена доставки между абонентами и БПЛА одинаковы ($\overline{T_1} = \overline{T_n}$), и времена передачи между БПЛА также одинаковы. Для вычисления время передачи голоса в разных сценариях, предполагаем, что: для передачи голоса между абонентами и БПЛА используется технология IEEE802.11ac (со скоростью 650 Мбит/с). Связь между БПЛА предоставляется технологий IEEE802.11p (со скоростью 12 Мбит/с). ГБПЛА взаимодействуют друг с другом на базе технологии IEEE802.11p в супер-режим (IEEE802.11p*) со скоростью передачи 6 Мбит/с. БПЛА осуществляют полет в непосредственной близости к другим БПЛА в составе сети с постоянной скоростью (v); максимальное количество проходящих узлов (хопов) в каждой группе БПЛА (m = 5); средняя длина одного пакета 1000 байт. В рис. 4 (см. ниже), количество БПЛА задействованных для организации летающей сети у одноранговой модели (50 БПЛА) больше, чем у иерархической модели (41 ЛА). Однако, иерархическая модель в основном состоит

из ГБПЛА, что позволяет значительно увеличить область покрытия и осуществлять передачу голоса с сетевой задержкой не более 100мс.

Таким образом, в данной работе представлены модели взаимодействия БПЛА для летающих сетей экстренных служб: одноранговая модель и иерархическая модель. Показана возможность организации летающей сети и передачи голоса на базе технологии VoWi-Fi в условиях разрушенной инфраструктуры операторов связи. Согласно полученным результатам можно установить количество БПЛА для полного покрытия зоны стихийного бедствия в различных случаях, что может оказать существенную помощь при поиске и спасению пострадавших. Иерархическая модель представляет лучшие результаты, чем одноранговая, как с точки зрения экономии ресурсов, так и с точки зрения зоны радиопокрытия.

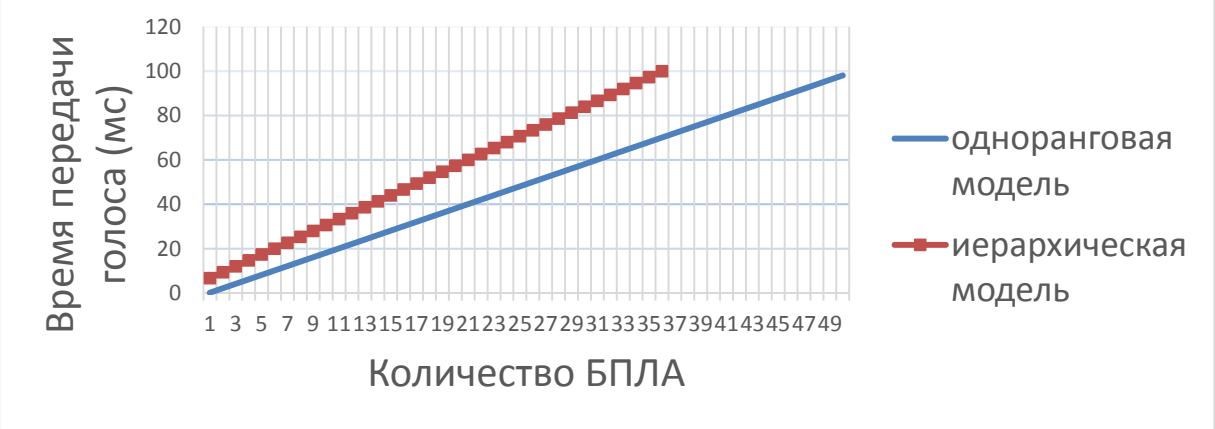


Рис 4. Сравнение двух моделей организации сети по времени передачи голоса в зависимости от количества БПЛА (IEEE 802.11ac)

Список используемых источников

1. Кучерявый А. Е., Владыко А. Г., Киричек Р. В., и др. Летающие сенсорные сети // Электросвязь. 2014. № 9. С. 2–5.

2. Koucheryavy A., Vladyko A., Kirichek R. State of the art and research challenges for public flying ubiquitous sensor networks / Lecture Notes in Computer Science (LNCS). 2015. Vol. 9247. PP. 299–308.

3. Sharma V, Song F, et al. Energy efficient device discovery for reliable communication in 5G-based IoT and BSNs using unmanned aerial vehicles // Journal of Network and Computer Applications. 97. 2017. PP. 79–95.

4. Ngongang S. F. M., Tadayon N., Kaddoum G. Voice over Wi-Fi: feasibility analysis. In Advances in Wireless and Optical Communications (RTUWO), IEEE. 2016. pp. 133–138.

5. Kulik V., Muthanna A., Pham V. D., Hakimov A., Kirichek R., Pirmagomedov R. The study of semantic gateway performance // Электросвязь. 2017. № 6. С. 69–73.

6. Jiang D., Chen Q., Delgrossi L. Optimal data rate selection for vehicle safety communications // In Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking. 2018. PP. 30–38.

7. Wang Q, Leng S, et al. An IEEE 802.11 p-based multichannel MAC scheme with channel coordination for vehicular ad hoc networks // IEEE Transactions on Intelligent Transportation Systems. 13 (2). 2012. PP. 449–458.

8. ITU-T Recommendation G.114. One-way transmission time. 2003.

9. Kirichek R., Paramonov A., Koucheryavy A. Swarm of public unmanned aerial vehicles as a queuing network // International Conference on Distributed Computer and Communication Networks. Communications in Computer and Information Science (CCIS). Vol. 601. 2015. PP. 111–120.

10. Kleinrock, L. Queueing systems, volume 2: Computer applications. New York: Wiley. Vol. 66. 1976. 576 p.

УДК 004.056
ГРНТИ 81.93.29

СРЕДСТВА ЗАЩИТЫ ОТ АТАК ТИПА ПЕРЕПОЛНЕНИЯ БУФЕРА НА ОС СЕМЕЙСТВА WINDOWS

В. Н. Диордица, А. Ю. Цветков

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

Современные операционные системы представляют достаточно обширный комплекс защитных средств от различного рода уязвимостей, однако существуют уязвимости, полная ликвидация которых не представляется возможной. Одной из таких уязвимостей является переполнение буфера. Критически опасная уязвимость, известная ещё с начала 70-х годов, активно эксплуатирующая злоумышленниками и сегодня.

В данной работе рассматриваются: проблемы уязвимости современных программ, исследование структуры компьютерной памяти, алгоритм атаки переполнения буфера, известные защитные механизмы и системы предотвращения атак переполнения.

информационная безопасность, переполнение буфера, защита операционных систем, компьютерная память, уязвимости приложений.

Переполнение буфера – одна из наиболее распространённых уязвимостей программного обеспечения, связанная с неправильным использованием памяти и отсутствием жёсткого контроля со стороны подсистемы программирования или операционной системы. Данная уязвимость была обнаружена ещё в 1972 году, но получила широкую известность только в 1994 г. после публикации Элисом Леви поэтапного введения в эксплуатацию переполнения буфера. Это не только привлекло всеобщее внимание

к данной уязвимости, но и сильно снизило порог вхождения. Уже спустя несколько лет переполнение буфера считалось доминирующей уязвимостью при атаке на удалённые хосты, так, например, больше половины выпусков CERT (*Computer Emergency Response Team site*) в 1998 и половина выпусков 1999 года связаны с переполнением буфера [1].

Повсеместное распространение высокоуровневых языков программирования выполняющихся поверх специальных программ (виртуальных машин) также не снизило актуальность атаки переполнением буфера. Данная уязвимость всё ещё остаётся критически опасной из-за большого количества библиотек написанных на C/C++ с использованием потенциально уязвимых функций.

Последствия эксплуатации уязвимости переполнения буфера часто сложно предсказать, однако в большинстве случаев последствия варьируются от раскрытия конфиденциальных данных до полной компрометации атакуемой системы [2].

Чтобы понять, как работает переполнение буфера нужно иметь необходимый минимум понятий об использовании процессами компьютерной памяти. В современных многозадачных операционных системах каждый процесс выполняется в собственном виртуальном адресном пространстве. Соответствие между виртуальным пространством адресов и физической памятью описывается с помощью таблицы страниц. Ядро создает и заполняет таблицы, а процесс обращается к ним при необходимости совершения манипуляций с памятью. Каждый процесс осуществляет операции со своим набором таблиц [3]. В адресном пространстве процесса выделяется место под различные данные, такие как: пространство ядра (*kernel space*), стек (*stack*), куча (*heap*), сегмент данных, сегмент текста, сегмент неинициализированных данных и т. д. Уязвимыми элементами являются стек, куча и область неинициализированных данных.

Переполнение буфера происходит, когда проверка выхода за границы не производится над данными, записываемыми в статический буфер. Если объем копируемых в стек данных превосходит размер буфера, компьютер продолжает перезаписывать стек до тех пор, пока не достигнет NUL-символа, переписывая другие значения в стеке и некоторые указатели, которые говорят программе, что делать дальше [4]. Такие указатели являются сохраненными значениями регистра EIP или SEH-указателей.

Когда данные перезаписывают один из сохраненных указателей инструкции, происходят интересные вещи. На некотором этапе после вызова функции процессор возвращается по адресу, сохраненному в одном из этих указателей и компьютер считает, что по этому адресу находится следующая инструкция. Обычно в данном случае адрес оказывается некорректным, что приводит к аварийному завершению программы. В Unix и Linux это приводит к тому, что операционная система посылает процессу сигнал SIGSEV.

Этот сигнал соответствует ошибке сегментации и сообщает процессу, что он пытается обратиться к несуществующей или запрещенной области памяти.

Используя инструментарий для отладки программ, а также зная адрес хранящий указатель на следующую исполняемую инструкцию, опытный злоумышленник может получить контроль над программой во время ее аварийного завершения и использовать ее привилегии и окружение для выполнения собственного кода в своих целях.

Несмотря на то, что проблему переполнения буфера так и не удалось решить до конца, работы в этом направлении всё ещё ведутся. В настоящее время выделяют несколько основных типов защиты памяти [5, 6, 7]:

1) Метод защиты на основе эталонных функций с защитой адреса возврата.
2) Метод защиты на основе проверочных значений.
3) Метод диверсификации.
4) Неисполняемая память.

Метод защиты с использованием эталонных функций. Этот метод основан на библиотеках, программно-реализующих «безопасный стек». Данный метод обеспечивает замену ограниченному набору уязвимых системных функций (таких как: *getc*(), *strcpy*(), *printf*(), и т. д.). Главный недостаток данного метода заключается в том, что он не заменяет уязвимые функции, а добавляет их безопасный аналог, таким образом безопасность приложений напрямую зависит от использования безопасных функций разработчиком.

Метод защиты на основе проверочных значений. Ключевым компонентом защиты, основанной на проверочных значениях, является поле canary word. Canary word это случайная последовательность байт встраиваемая в кадр стека между передаваемыми в функцию аргументами и сохранёнными значениями регистров. При попытке проведения атаки переполнения значение слова осведомителя перезапишется и при последующей проверке будет обнаружена попытка компрометации системы. Основу данного метода составляет высокая степень энтропии случайного значения слова осведомителя, так как в случае, если предсказание значения осведомителя возможно, сгенерировать последовательность перезаписывающую адрес возврата и сохраняющую значение осведомителя достаточно просто, что фактически сделает защиту бесполезной.

Метод диверсификации. Мера защиты, при использовании которой случайным образом изменяется расположение в адресном пространстве процесса важных структур данных, а именно образов исполняемого файла, подгружаемых библиотек, кучи и стека. Диверсификация не даст злоумышленнику узнать, по какому конкретно адресу размещаются структуры данных после переполнения, куда можно записать шелл-код. Таким образом диверсификация призвана сделать атаки переполнения бессмысленными.

Основой защиты данного механизма также является степень энтропии случайных значений адресов.

Неисполняемая память. Это защитный механизм, основанный на наборе программных и аппаратных технологий, позволяющих выполнять дополнительные проверки содержимого оперативной памяти и предотвращать запуск вредоносного кода. Использование неисполняемой памяти позволяет отразить целый класс атак. В частности, данный механизм позволяет блокировать вирусы и другие вредоносные программы, пытающихся выполнить свой код из областей системной памяти, резервированных для Windows и других авторизованных программ. Обнаружив, что программа использует системную память неправильно, средство защиты принудительно закрывает программу и выдает соответствующее сообщение. Недостаток данной технологии состоит в том, что для её функционирования необходимо устройство, поддерживающее её на физическом уровне.

Однако у всех вышеперечисленных средств защиты есть один недостаток. При компиляции приложения все перечисленные методы можно отключить, используя специальные флаги компиляции, таким образом злоумышленник может скомпилировать заранее уязвимую к переполнению программу и выдавать её за безопасную. Для компиляции уязвимого приложения служат флаги [8]:

1) (/GS-) – отключает стековые куки.
2) (/DYNAMICBASE:NO) – отключает использование ASLR.
3) (/NXCOMPAT:NO) – отключает использование DEP.
4) (/RTCu) – отключает проверку неинициализированных значений.

К счастью отключение почти всех перечисленных флагов отражается в заголовочной структуре скомпилированного PE файла, благодаря чему обнаружение уязвимых программ значительно упрощается. Информацию о состоянии флагов /DYNAMICBASE и /NXCOMPAT можно обнаружить в опциональном заголовке PE файла в структуре DllCharacteristics (рис. 1) [9].

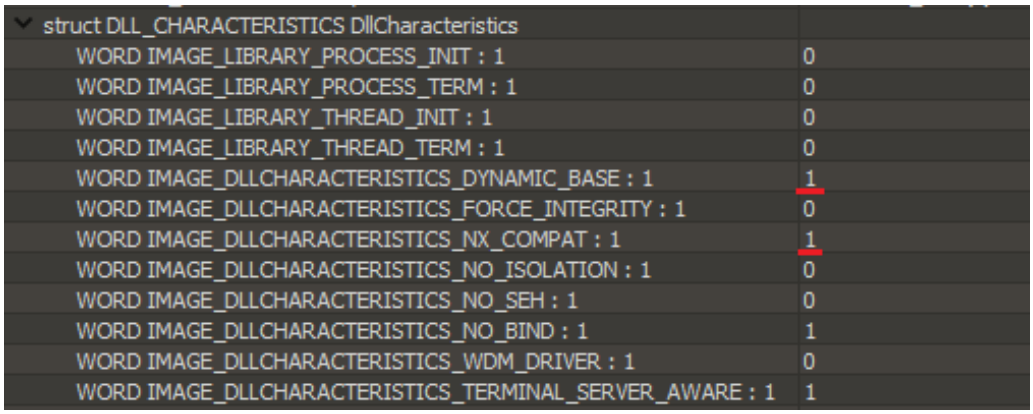


Рис. 1. Структура DllCharacteristics

Состояние флага GS получить сложнее, так как оно не отражается в PE заголовках, однако определить его можно по наличию константы ___security_cookie в секции .data (рис. 2) [10].

```
___security_cookie dd 0BB40E64Eh
```

Рис. 2. Константа ___security_cookie

В результате было принято решение написать простую программу-сканер выполняющую проверку PE структуры для детектирования уязвимых приложений (реализация интерфейса представлена на рис. 3).

В наше время уязвимость переполнения буфера потеряла былую популярность, во многом благодаря множеству механизмов противодействующих удалённой эксплуатации данной программной бреши. Однако данные механизмы не защищают систему от специально написанных и скомпилированных уязвимых программ, вследствие чего переполнение буфера всё ещё остаётся критически опасной уязвимостью программного обеспечения.

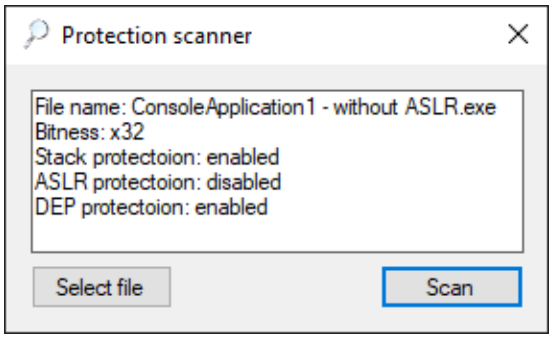


Рис. 3. Интерфейс сканера уязвимостей

Список используемых источников

1. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

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 (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 570–573.

3. Гельфанд А. М., Пестов И. Е., Катасонов А. И., Рязанцев К. С. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8. С. 91–97.

4. Крылов К. Ю., Ушаков И. А., Котенко И. В. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. 28–30 октября 2015 г. Материалы конференции. СПб.: СПОИСУ. 2015. С. 75–76.

5. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 657–662.

6. Application Protection Technologies in Windows Vista and Windows Server 2008 [Электронный ресурс]. URL: https://compress.ru/ (дата обращения 10.03.2019).

7. Stack overflow [Электронный ресурс]. URL: https://www.viva64.com/ (дата обращения 07.03.2019).
8. Visual studio compilation flags [Электронный ресурс]. URL: https://docs.microsoft.com/ (дата обращения 06.03.2019).
9. The structure of executable files Win32 and Win64 [Электронный ресурс]. URL: http://cs.usu.edu.ru/ (дата обращения 06.03.2019).
10. Buffer overflow [Электронный ресурс]. URL: http://www.codenet.ru/ (дата обращения 05.03.2019).

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

УДК 004.056
ГРНТИ 81.96

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ ЦЕЛЕЙ КИБЕРАТАК НА ОСНОВЕ НЕЙРОНЕЧЕТКИХ СЕТЕЙ

Е. В. Дойникова

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В статье рассматривается проблема прогнозирования целей кибератак. Описывается общий подход и предлагается модель прогнозирования с использованием нейронечеткой сети. Определяются различные классы целей атак. На основе системы метрик защищенности формируется набор признаков, характеризующих их. Описывается первичная реализация компонентов прототипа прогнозирования целей кибератак с использованием данной модели, а также результаты экспериментов.

кибератаки, нейронечеткие сети, цели кибератак, метрики защищенности.

В настоящее время наибольшую опасность для информационных систем представляют сложные целевые кибератаки. Ввиду того, что они обычно хорошо подготовлены за счет значительной фазы сбора информации, больших ресурсов, серьезных навыков исполнителей, способных хорошо замаскировать следы, их достаточно сложно обнаружить до момента достижения цели атаки. В работе предлагается подход к своевременному обнаружению целей кибератак, который объединяет несколько процессов, в том числе процесс корреляции информации безопасности для обнаружения инцидентов в системе; процесс определения метрик защищенности; процесс логического вывода с использованием онтологической модели; и процесс обучения нейронечеткой сети для выявления целей кибератак.

Процессы связаны между собой следующим образом. Процесс определения метрик защищенности основан на онтологической модели данных и метрик защищенности. Элементы данной онтологии ранее были представлены в [1] и [2]. Для определения целей кибератак выделим следующие основные взаимосвязанные сущности онтологии:

– Программно-аппаратное обеспечение, являющееся частью информационной системы, может быть целевым объектом для кибератаки. В качестве формата представления программно-аппаратного обеспечения используется стандарт CPE [3], его источником является база NVD [4]. В программно-аппаратном обеспечении могут быть уязвимости.

– Уязвимости программно-аппаратного обеспечения представляются в формате CVE [5]. Источником уязвимостей программно-аппаратного обеспечения является база NVD [4]. Уязвимости являются слабыми местами информационной системы и могут использоваться злоумышленниками для проведения кибератак. Для определения связи между сущностями «программно-аппаратное обеспечение» и «уязвимость» используется соответствующее поле записи CPE в NVD («уязвимости»).

– Слабые места информационной системы представляются в формате CWE [6]. Источником слабых мест программно-аппаратного обеспечения является база CWE [6]. Слабые места информационной системы могут использоваться злоумышленниками для проведения кибератак. Отметим, что введение данной сущности связано с тем, что кибератаки могут проводиться не только с использованием уязвимостей, а также с отсутствием прямой связи между записями уязвимостей в NVD и кибератаками, в то время как сущность «слабое место» и сущность «кибератака» связаны через соответствующее поле записи слабого места в базе CWE («связанные шаблоны атак»). Более подробно это описано в предыдущих исследованиях [7] и [8].

– Возможные кибератаки на информационную систему представляются в формате CAPEC [9]. Источником шаблонов кибератак является база CAPEC [9]. В предыдущем исследовании [1] были выделены следующие возможные цели кибератак: вызов, статус; политическая выгода; финансовая выгода; разрушение. Их связь с сущностями CAPEC в NVD определяется через свойство «последствия» (*Consequences*).

Для каждой выделенной сущности определен набор метрик защищенности, взаимосвязи между сущностями позволяют определить процесс вычисления сложных интегральных метрик на основе первичных метрик защищенности [10].

На следующем этапе процесс корреляции информации безопасности для обнаружения инцидентов в системе, а также процесс логического вывода с использованием онтологической модели, используются для формирования выборки исходных данных для обучения нейронечеткой сети,

то есть для сопоставления реальных значений первичных и интегральных метрик защищенности с целями кибератак.

И, наконец, на последнем этапе ведется обучение нейронечеткой сети для выявления целей кибератак на информационную систему, в зависимости от инцидентов безопасности, происходящих в реальном времени.

Таким образом, основными применяемыми в рамках подхода моделями является онтология данных и метрик защищенности, для определения признаков различных классов целей атак [10] и нейронечеткая сеть для выявления целей атак на основе обучающей выборки.

Проведенные на данный момент эксперименты позволяют выявить слабые места системы на основе имеющихся в ней уязвимостей, и, таким образом связать конкретную систему с атаками и возможными целями атак. Решение подобной задачи было необходимо ввиду достаточно большого количества уязвимостей, которые не связаны слабостями, что не позволяет, в свою очередь, связать их с конкретными шаблонами атак [7].

В качестве входных данных для обучения классификаторов была взята выборка уязвимостей из NVD, имеющих ссылки на слабые места CWE. В качестве признаков для обучения были взяты метрики уязвимостей CVSS [11], представленные в базе NVD. Использовались следующие методы классификации: *k*-ближайших соседей, дерево решений, случайный лес (реализованные на языке *Python* в рамках модуля *sklearn*). Наилучшие результаты (71,7 %) показал метод случайного леса. На следующем этапе планируется решить задачу выявления слабых мест системы на основе особенностей ее программно-аппаратного обеспечения; преобразовать онтологию в динамическую путем введения в нее сущности «инцидент безопасности»; и использовать нейронечеткую сеть для выявления целей кибератак на основе признаков инцидентов безопасности.

Работа выполнена при поддержке стипендии президента РФ (СП-751.2018.5).

Список используемых источников

1. Дойникова Е. В. Подход к прогнозированию и реагированию на кибератаки в индустриальном интернете вещей на основе нейронечётких сетей // Информационные технологии в управлении : материалы конференции. Санкт-Петербург. 2–4 октября 2018. СПб. : АО «Концерн «ЦНИИ «Электроприбор», 2018. С. 526–530.

2. Федорченко А. В., Котенко И. В., Дойникова Е. В., Чечулин А. А. Применение онтологического подхода для построения гибридного хранилища информации безопасности // SCM'2017, 24–26 мая 2017 г. Санкт-Петербург. Сборник докладов, том 2. Издательство СПбГЭТУ «ЛЭТИ», 2017. С. 55–58.

3. Common Platform Enumeration: Applicability Language Specification Version 2.3 [Электронный ресурс]. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7698.pdf

4. National vulnerability database [Электронный ресурс]. URL: https://nvd.nist.gov/

5. Common vulnerabilities and exposures. The Mitre Corporation website [Электронный ресурс]. URL: https://cve.mitre.org/

6. Common weakness enumeration. The Mitre Corporation website [Электронный ресурс]. URL: https://cwe.mitre.org/index.html

7. Дойникова Е. В., Федорченко А. В., Котенко И. В. Выявление слабых мест информационных систем для автоматического выбора защитных мер // Проблемы информационной безопасности. Компьютерные системы. 2018. № 3. С. 89–99.

8. Igor Kotenko, Andrey Fedorchenko, Elena Doynikova, Andrey Chechulin. An Ontology-based Hybrid Storage of Security Information // Information Technology and Control, No. 4, 2018. PP. 655–667.

9. Common attack pattern enumeration and classification. The Mitre Corporation website [Электронный ресурс]. URL: https://capec.mitre.org/index.html

10. Elena Doynikova, Igor Kotenko. Approach for determination of cyber-attack goals based on the ontology of security metrics // Proceedings of the MIST: Aerospace-2018. October 20, 2018, Krasnoyarsk, Russia. IOP Conference Series: Materials Science and Engineering (MSE), IOP Publishing, Vol.450. 2018. 7 p.

11. Common vulnerability scoring system. FIRST.org, Inc. website [Электронный ресурс]. URL: https://www.first.org/cvss/

УДК 621.391.6
ГРНТИ 49.44.31

ИСПОЛЬЗОВАНИЕ ОПТИЧЕСКИХ УСИЛИТЕЛЕЙ ДЛЯ ПОДДЕРЖАНИЯ КВАЗИСОЛИТОННОГО РЕЖИМА В ОПТИЧЕСКОМ ОДНОМОДОВОМ ВОЛОКНЕ С ПОТЕРЯМИ

С. Э. Доценко

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

Известно, что использование квазисолитонных режимов распространения импульсов, имеющих форму гиперболического секанса, позволяет увеличить протяженность и скорость передачи волоконно-оптической системы связи. Однако с увеличением расстояния квазисолитонный режим в одномодовых оптических волокнах с потерями разрушается. Для его поддержания могут использоваться дискретные оптические усилители, компенсирующие затухание на усилительных участках линейного волоконно-оптического тракта. Статья посвящена исследованию квазисолитонного режима работы в линейном тракте большой протяженности с несколькими усилительными участками и оптимальному выбору параметров этого тракта. Результаты теоретических исследований проверялись имитационным моделированием.

волоконно-оптические линии связи, солитоны, оптические усилители, оптическое волокно.

Теоретически существование солитонов в одномодовых оптических волокнах (ОВ) с аномальной хроматической дисперсией (ХД) без учета потерь может быть обосновано с помощью решения стандартного нелинейного уравнения Шредингера (НУШ) [1, 2]:

$$i\frac{\partial u}{dz}+\frac{1}{2}\cdot\frac{\partial^2 u}{\partial\tau^2}+|u|^2\cdot u=0,$$

где $u=N\cdot E_m/\sqrt{P_0\cdot Z_v}$ – нормированная комплексная амплитуда напряженности E_m электрического поля световой волны, распространяющейся по ОВ (огибающая импульса, которая на входе в ОВ равна 1); P_0 – пиковая мощность импульса, Вт; Z_v – волновое сопротивление среды (сердцевины ОВ), Ом; $N^2=L_D/L_{NL}$ – отношение дисперсионной $L_D=T_0^2/|\beta_2|$ длины к нелинейной $L_{NL}=1/(\gamma\cdot P_0)$ длине; β_2 – дисперсия групповых скоростей (ДГС), пс^2/км (при аномальной дисперсии $\beta_2<0$); γ – коэффициент нелинейности, 1/(Вт·км); $z=Z/L_D$ – нормированное расстояние; Z – расстояние, км; $\tau=T/T_0$ – нормированное внутриимпульсное время; T – время, отсчитываемое от середины импульса, пс; T_0 – полуширина импульса, пс.

Особое значение имеет решение для

$$N^2=\frac{L_D}{L_{NL}}=\frac{|\beta_2|}{P_0\cdot\gamma\cdot T_0^2}=1, \qquad (1)$$

получившее название фундаментального солитона (или солитона 1 порядка), который при распространении по ОВ без потерь не меняет свою форму. Этот эффект возникает вследствие баланса между ХД и фазовой самомодуляцией (ФСМ), т. е. при равенстве $L_{NL}=L_D$.

Фундаментальный солитон имеет огибающую напряженности электрического поля в форме гиперболического секанса и его распространение по ОВ без потерь описывается функцией [1]:

$$u(z,\tau)=\operatorname{sech}(\tau)\cdot\exp(i\cdot z/2).$$

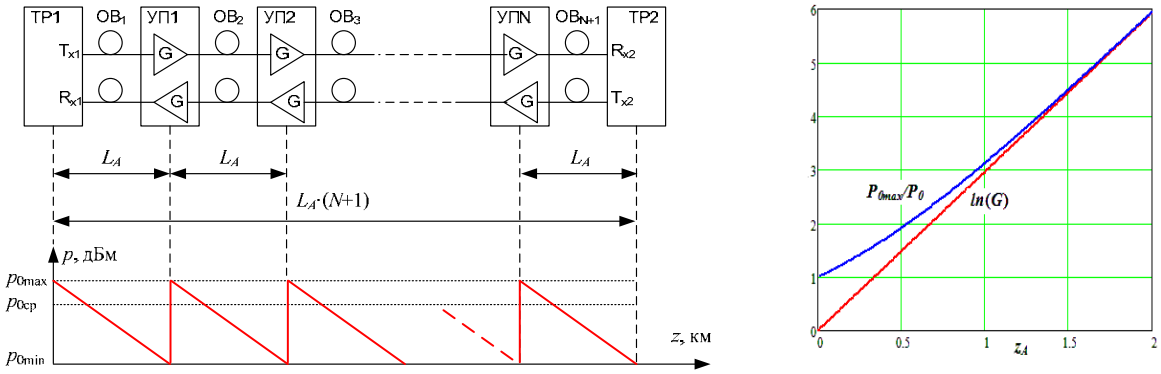
Из (1) можно определить соотношение между пиковой мощностью и длительностью солитона 1-го порядка [1]

$$P_0=|\beta_2|/(\gamma\cdot T_0^2)\approx 3{,}11\cdot|\beta_2|/(\gamma\cdot t_u^2),$$

где t_u – длительность секансного импульса на полувысоте по интенсивности.

В работах [3, 4, 5, 6], предназначенных для специалистов, работающих в области оптической связи, а также для студентов и аспирантов, обучающихся в вузах связи, систематизированы сведения об оптических солитонах и рассмотрены вопросы практического использования квазисолитонных режимов распространения сигналов в ВОСС. Данная работа посвящена более подробному исследованию процессов формирования и поддержания квазисолитонного режима в ВОСС с каскадным включением дискретных ОУ, которые восстанавливают форму и амплитуду солитонных импульсов. Качество связи в зависимости от расстояния оценивалось с помощью Q – фактора.

Структурная схема исследуемого линейного волоконно-оптического линейного тракта (ЛВОТ) приведена на рис. 1а. Она содержит оконечные пункты с транспондерами (ТР), усилительные пункты (УП) с эрбиевыми ОУ (EDFA). Протяженность усилительных участков одинакова и равна L_A.



а) б)

Рис. 1. Схема линейного тракта ВОСС с дискретными ОУ (а). Зависимости входной мощности и коэффициента усиления от относительного расстояния между ОУ (б)

Общая идея метода сохранения квазисолитонного режима распространения секансных импульсов по ОВ, который называют методом управления потерями, состоит в поддержании средней величины пиковой мощности $\overline{P}_0$ секансных импульсов, равной мощности фундаментального солитона P_0 при отсутствии потерь в ОВ. Поэтому, такие солитоны называют усредненными по длине. Для их существования необходимо, чтобы величина пиковой мощности $P_{0\max}$ на входе в ОВ каждого усилительного участка (УУ) существенно в k_g раз превышала мощность фундаментального солитона P_0. В [4] приведены выражения для расчета коэффициента усиления G дискретного ОУ и пиковой мощности $P_{0\max}$ на входе УУ в зависимости от относительного расстояния между ОУ $z_A = L_A / L_D$ и затухания на дисперсионной длине $\Gamma = \alpha \cdot L_D / 2$:

$$G = \exp\left(2 \cdot \Gamma \cdot z_A\right) \text{ и } P_{0\max} = P_0 \cdot k_g = P_0 \cdot \frac{G \cdot \ln(G)}{G - 1}. \quad (2)$$

На рис. 1б приведены зависимости требуемого коэффициента усиления ОУ и относительной мощности на входе УУ от относительной длины УУ, рассчитанные по (2).

В первом приближении при $L_A < L_D$ ($z_A < 1$) ослабленный и искаженный импульс динамически восстанавливает свою форму и амплитуду в эрбиевом ОВ оптического усилителя. Заметим, что расстояние L_A между дискретными ОУ должно быть максимально большим, чтобы минимизировать количество ОУ и стоимость ВОСС. Однако при больших значениях L_A происходит необратимое разрушение квазисолитонного импульса и возникает рассеянное излучение, которое накапливается в ЛВОТ от усилителя к усилителю до заметного уровня и ухудшает качество связи.

Для оценки реальных возможностей квазисолитонных ВОСС было проведено их моделирование. Исследования проводились для ВОСС на длине волны λ_0 = 1550 нм со скоростью передачи B = 10 Гбит/с, при скважности секансных импульсов q = 5 и полуширине T_0 = 11,34 пс (t_u = 20 пс). Было выбрано ОВ со смещенной дисперсией (DSF) со следующими параметрами: коэфициент затухания α = 0,2 дБ/км, ДГС β_2 = –2 пс^2/км, коэффициент нелинейности γ = 2,57 1/(Вт км), нелинейный показатель преломления n_2 = 26 10^{-21} м^2/Вт, эффективная площадь A_{ef} = 41 мкм^2. Были рассчитаны L_D = 64,3 км и P_0 = 6,05 мВт.

При моделировании распространения секансных импульсов в ОВ без потерь расчетная пиковая мощность оказалась не достаточной и была увеличена до 6,8 мВт. При этом был реализован истинно солитонный режим. Это доказывает таблица 1 и рис. 2а (см. ниже).

ТАБЛИЦА 1. Результаты моделирования процессов распространения секансных импульсов по ОВ типа DSF в ВОСС без усилителей

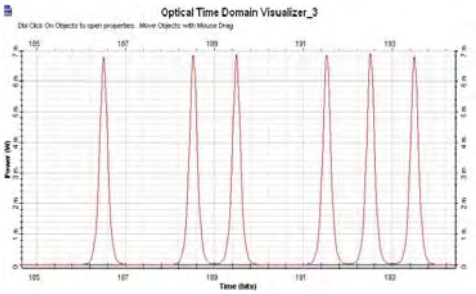
P_{ii}, мВт	l, км	0	100	200	500	1000	1300
6,05	P_{ml}, мВт	6,05	5,6	5,2	5,1	5,7	5,2
	t_u, пс	20	22	23	24	21	23
	Q	–	2649	8025	84	49	48
6,8	P_{ml}, мВт	6,8	6,8	6,8	6,8	6,8	6,8
	t_u, пс	20	20	20	20	20	20
	Q	–	2378	2258	2474	472	111

Исследования были продолжены для ОВ с потерями. Длины усилительных участков L_A принимались равными 32, 64, 77 км ($z_A = L_A/L_D$ = 0.5, 1, 1,2 соответственно). Рассчитанные по (2) коэффициенты увеличения энергии

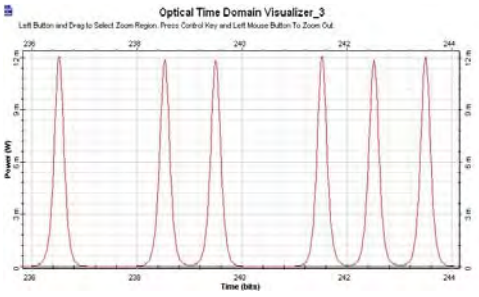
составили k_g = 1.92, 3.13, 3.67, а пиковые мощности P_0 = 13.04, 21.26, 25 мВт, соответственно (в третьем эксперименте, мощность была увеличена с 25 до 26 мВт). Результаты моделирования приведены в таблице 2.

ТАБЛИЦА 2. Результаты моделирования процессов распространения секансных импульсов по ОВ типа DSF в ВОСС с дискретными ОУ

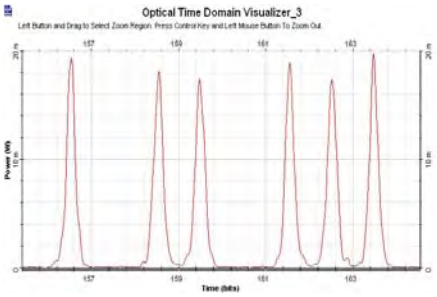
z_A	l, км	0	32,15	64,3	77	128,6	154	616	643	1232	1286
0,5	P_{ml}, мВт	13	13,2	13,3	–	13,1	–	–	12,4	–	12
	t_u, пс	20	19,7	20	–	20,1	–	–	20,8	–	20,9
	Q	–	354	225	–	186	–	–	71	–	64
1,0	P_{ml}, мВт	21	–	21,6	–	21,2	–	–	20,6	–	19,3
	t_u, пс	20	–	20	–	20,8	–	–	19,7	–	20,8
	Q	–	–	215	–	141	–	–	38	–	23
1.2	P_{ml}, мВт	26	–	–	26.6	–	25,5	24	–	25,5	–
	t_u, пс	20	–	–	20,2	–	21	21	–	19,1	–
	Q	–	–	–	174	–	117	24	–	12	–



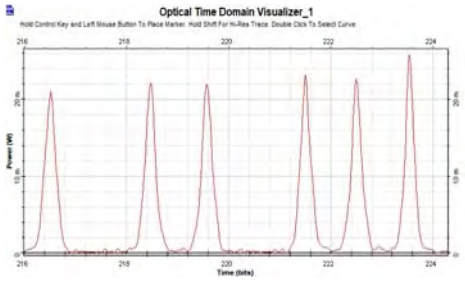
а)



б)



в)



г)

Рис. 2. Формы импульсов в ВОСС: без затухания 1300 км с P_0 = 6,8 (а); L_A = 32 км на выходе 40-го УУ 1286 км (б); L_A = 64 км на выходе 20-го УУ 1286 км (в); L_A = 77 км на выходе 16-го УУ 1232 км (г);

Из таблицы 2 видно, что при $L_A \leq L_D$ (L_A =3 2 и 64 км) квазисолитонный режим сохраняется и качество связи на достаточно больших расстояниях вплоть до Z = 1286 км остается высоким (Q > 64 и 23). Рис. 2б (для z_A = 0,5) подтверждает практически идеальное сохранение формы выходных импульсов. Рис. 2в (для z_A = 1) показывает, что формы выходных импульсов незначительно искажаются на больших расстояниях. При $L_A > L_D$ (L_A = 77км) качество связи на больших расстояниях остаётся высоким (Q = 12), но импульсы искажаться значительно (рис. 2г).

Список используемых источников

1. Агравал Г. Нелинейная волоконная оптика : пер. с англ. М. : Мир, 1996. 323 с.
2. Кившарь Ю. С., Агравал Г. П. Оптические солитоны. От волоконных световодов до фотонных кристаллов / Пер. с англ. под ред. Н. Н. Розанова. М. : ФИЗМАТЛИТ, 2005. 648 с.
3. Андреева Е. И., Былина М. С., Глаголев С. Ф., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Часть 1 // Труды учебных заведений связи. 2018. Т. 4. № 1. С. 5–11.
4. Андреева Е. И., Былина М. С., Глаголев С. Ф., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Часть 2 // Труды учебных заведений связи. 2018. Т. 4. № 2. С. 26–35.
5. Андреева Е. И., Былина М. С., Глаголев С. Ф., Доценко С. Э., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Часть 3 // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 5–6.
6. Андреева Е. И., Былина М. С., Глаголев С. Ф., Доценко С. Э., Чаймарданов П. А. Свойства временных оптических солитонов в оптических волокнах и возможность их использования в телекоммуникациях. Часть 4 // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 15–24.

Статья представлена научным руководителем, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 004.056
ГРНТИ 81.93.29

БЛОКЧЕЙН АУТЕНТИФИКАЦИЯ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

В. В. Добрянский, Д. В. Кушнир

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

Четвертая промышленная революция продолжает активно влиять на производственные системы, делая их более умными, взаимосвязанными, самоорганизующимися, децентрализованными и гибкими. Однако хорошие перспективы, прогнозируемые внедрением различных технологий для «Промышленности 4.0», сопряжены с различными проблемами, одна из которых – безопасность систем. Безопасность киберфизических систем имеет превалирующее значение, поскольку её компоненты активно взаимодействуют с физическим миром и нарушение безопасности может привести к различным технологическим катастрофам.

В данной работе предлагается модель системы управления подтверждением подлинности устройств, основанной на блокчейн технологии и автоматическом протоколе аутентификации с помощью TLS без участия PKI.

киберфизические системы, аутентификация, блокчейн, промышленность 4.0, безопасность.

Киберфизическая система (CPS) – это система, объединяющая физические и вычислительные компоненты в одну сеть, что позволяет им воспринимать, управлять и контролировать объекты в физическом мире. К таким компонентам можно, например, отнести промышленные машины, автоматизированные управляемые транспортные средства, различного вида роботов, датчики и т. д. [1]

Подобного рода системы относятся к критичным, поскольку содержат в себе большие объемы чувствительных данных, а также активно взаимодействуют с физическим миром. Поэтому реализация механизмов, обеспечивающих физическую, аппаратно-программную и сетевую безопасность в такой сети имеют первостепенное значение и в настоящее время ведутся активные работы по исследованию информационной безопасности в области киберфизических систем [2].

В данной статье предлагается система управления идентификацией, основанная на блокчейн технологии и автоматическом протоколе аутентификации с помощью TLS (*Transport Layer Security*) [3] без участия PKI (*Public Key Infrastructure*) [4] для обеспечения сетевой безопасности.

Сетевая безопасность строится на основе выполнения 3-х важных условий: обеспечение целостности, доступности и конфиденциальности. Широко распространенным механизмом, способным обеспечить выполнение данных условий, является система контроля доступа, состоящая из идентификации, аутентификации, авторизации, мониторинга и учёта. Важной частью такой системы является система управление идентификацией, поскольку она содержит в себе информацию об устройствах для проведения процесса аутентификации. Существующие сегодня механизмы управления учетными записями (*Active Directory*, PKI и т. п.) не способны удовлетворить требованиям «Промышленности 4.0», поскольку сильно зависят от вовлечения человека в процесс. Для повышения уровня автоматизации, система управления идентификацией должна быть безопасной, глобально доступной, доверенной и способной хранить большой объем данных.

В системе управления идентификацией необходимо определить идентификатор, который должен однозначно определять устройство. Выбранные атрибуты, образующие идентификатор, в данном случае будут являться совокупностью таких данных как: тип ключа, открытый ключ и серийный номер ключа. Открытый ключ является частью пары открытый/закрытый ключ, сгенерированной непосредственно на самом устройстве (остается храниться в аппаратном хранилище ключей). Открытого ключ в идентификаторе составляет 257 бит (длина сжатого ключа в биткоине) [5]. Поскольку различные устройства могут использовать разные алгоритмы для генерации ключей, то был добавлен атрибут Тип ключа длиной в 8 бит. Серийный номер может быть использован как вспомогательный параметр для идентификации устройства различным программным обеспечением и в случае ручной идентификации устройства системным администратором. Для данного поля был выбран размер 34 бита, что позволяет каждому производителю создавать 17,2 млрд. устройств. Если производитель превышает данное значение, то в блокчейне может быть создан новый идентификатор производителя с новым пулом серийных номеров. Также производитель может создавать иерархии в серийных номерах, чтобы предоставить информацию о типе устройства. Это может помочь администратору сети, сообщив ему, ищет ли он датчик или роботизированную руку.

На приведенном ниже рис.1 показан процесс обмена информацией между производителем, устройством и блокчейном.

В данном случае само устройство не взаимодействует с блокчейном – все действия осуществляют производителем. Он присваивает серийный номер изготовленному устройству, запрашивает у него открытый ключ и его тип, а затем отправляет данные в блокчейн.

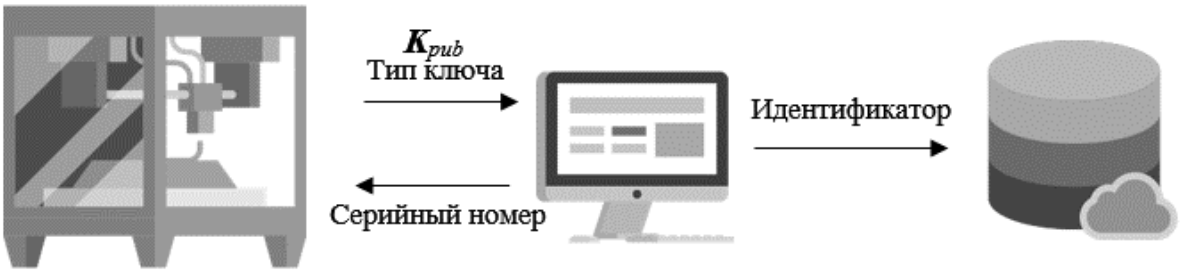


Рис. 1. Обмен информацией

Добавление идентификатора происходит через транзакцию в обмен на специальную монету. Помимо транзакций, содержащих идентификатор устройства, а также типа участника «Производитель», в нашей сети обозначены еще 2 вида ролей: «Майнер» и «Покупатель», и 4 вида транзакций:

– Транзакция с данными о личности участника блокчейна.
– Транзакция о передаче монет.
– Транзакция о передаче (продаже) идентификатора.
– Транзакция подтверждения покупки.

Также, помимо основной платы за транзакцию, в блокчейне действует система налогов и вознаграждения, которые защищают от попыток злоумышленника перегрузить сеть транзакциями [6].

Следующим необходимым шагом является проектирование протокола аутентификации, поскольку существующие сегодня протоколы на основе фрейморка EAP (*Extensible Authentication Protocol*) [7] не отвечают требованиям для работы в сети с высокой плотностью устройств.

В качестве основы для проектируемого протокола был выбрал протокол TLS, так как он является решением с открытым исходным кодом и предоставляет все необходимые механизмы для шифрования, аутентификации и проверки целостности.

Целью разрабатываемого протокола является проверка заявки на идентификацию, сделанной новым устройством, а также предоставление взаимной аутентификации между новым устройством и сервером аутентификации для защиты от нелегитимных серверов аутентификации, желающих перехватить устройство.

TLS использует базу данных сертификатов для проверки подлинности того, что только доверенные сертификаты будут авторизованы. База сертификатов содержит корневые сертификаты доверия для PKI. В разрабатываемом протоколе PKI был заменен блокчейн системой управления идентификацией и поэтому и в базе сертификатов не должно быть корневых сертификатов доверительного управления. Вместо этого протокол обновляет базу данных сертификатов на основе информации из блокчейна. Поэтому CPS устройства могу самостоятельно выпускать самоподписанные серти-

фикаты, которые должны храниться в отдельной (закрытой) базе сертификатов для того, чтобы исключить возможность влияния на другие системы в сети хранящие сертификаты.

Основными компонентами проектируемой системы аутентификации являются (рис. 2):

– Информационный сервер (производитель).
– Клиент (новое устройство).
– Сервер аутентификации (сетевой контроллер).
– Блокчейн.

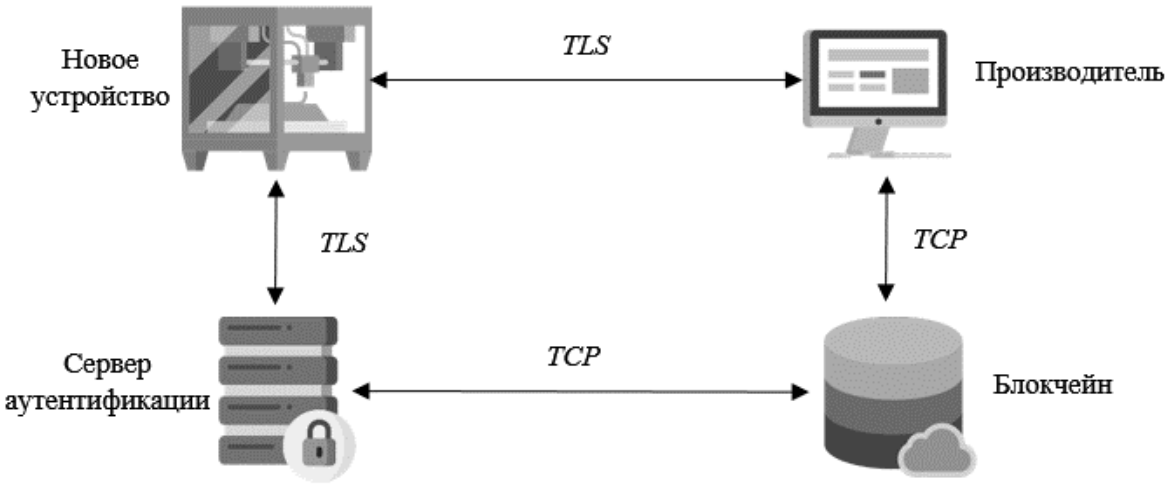


Рис. 2. Компоненты системы аутентификации

Процесс аутентификации начинается с момента подключения нового устройства к незащищенной сети (Это сеть, которая разворачивается поверх основной сети производителя. Может быть реализованы на основе виртуализации). В ходе этого процесса устройство пытается найти сетевой контроллер для установления соединения. Заранее устройство и контроллер не обладают информацией друг о друге. Новое устройство должно собрать информацию о контроллере и далее устанавливать соединение. Устройство запрашивает информацию от своего производителя о том, кто им теперь владеет, затем отправляет широковещательный запрос с просьбой ко всем сетевым контроллерам идентифицировать себя. После успешного подключения к сетевому контроллеру запускается проверка подлинности нового устройства.

В предложенной системе вовлеченность человека необходима лишь для организации процесса купли/продажи устройств, а процесс аутентификации не требует участия человека, благодаря чему он является автоматическим и масштабируемым. Такая система может способствовать активному внедрению развивающихся технологий «Промышленность 4.0».

Список используемых источников

1. Дзанни А. Киберфизические системы и разумные города [Электронный ресурс] // Как разумные устройства, датчики и исполнительные элементы поддерживают развитие IoT, 20.4.2015. URL: https://www.ibm.com/developerworks/ru/library/ba-cyber-physical-systems-and-smart-cities-iot/ba-cyber-physical-systems-and-smart-cities-iot-pdf.pdf (дата обращения 22.11.2018).
2. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.
3. . Венедюхин А. Ключи, шифры, сообщения: как работает TLS [Электронный ресурс] // tls.dxdt.ru. URL: https://tls.dxdt.ru/tls.html
4. Brian K. Windows Server 2008 PKI and Certificate Security Redmond, Washington: Microsoft Press, 2008. PP. 740.
5. Antonopoulos A. M. Mastering Bitcoin // 1th ed. Sebastopol, CA: O`Reilly Media, 2014. PP. 259.
6. Nakamoto S. Bitcoin: A Peer-To-Peer Electronic Cash System [Электронный ресурс] // bitcoin.org. URL: https://bitcoin.org/bitcoin.pdf (дата обращения 30.11.2018).
7. Википедия – сводная энциклопедия, Extensible Authentication Protocol [Электронный ресурс] // ru.wikipedia.org. URL: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol (дата обращения 05.12.2018).

УДК 004.732
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ УЛИЧНЫХ СЕТЕЙ WI-FI

Р. А. Дунайцев, Я. О. Колеватых

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

В статье рассматриваются особенности построения уличных сетей Wi-Fi. Приводятся экспериментальные данные по определению коэффициента затухания сигнала, обусловленного наличием зеленых насаждений между источником и получателем. Проводится сравнительный анализ программ для радиопланирования беспроводных сетей в части их применимости для планирования уличных сетей Wi-Fi, как то: возможности учета трехмерного рельефа местности и окружающей городской застройки, а также дополнительного затухания, создаваемого кронами деревьев и кустарников.

IEEE 802.11, outdoor Wi-Fi, беспроводная локальная сеть, радиопланирование.

Беспроводные локальные сети стандарта IEEE 802.11, также известные как Wi-Fi, прочно вошли в нашу жизнь. Их можно встретить дома

и в офисе [1], на территории университетов и общежитий [2, 3], на производстве [4] и в общественных местах [5, 6]. Традиционно технология Wi-Fi применяется для организации связи внутри помещений (*indoor* Wi-Fi) или для создания беспроводных каналов по методу «точка-точка» (*point-to-point*, PtP) или «точка-многоточка» (*point-to-multipoint*, PtMP). Однако в последние годы набирает популярность использование технологии Wi-Fi и для построения уличных сетей (*outdoor* Wi-Fi). Примером таких сетей являются муниципальные беспроводные сети, функционирующие во многих крупных городах разных стран [7].

Сегодня на рынке имеется целый ряд профессиональных программных продуктов, позволяющих выполнять радиообследование (*site survey*) и анализ характеристик действующих сетей Wi-Fi [8]. Кроме того, большинство подобных программ также может использоваться и для радиопланирования новых сетей Wi-Fi. Алгоритм работы с программой, будь то Acrylic WiFi Heatmaps, AirMagnet Planner, Ekahau Site Survey, iBwave Wi-Fi, TamoSoft TamoGraph Site Survey или VisiWave Site Survey, примерно один и тот же. На первом этапе в новый проект добавляется карта этажа или объекта. Затем производится калибровка карты. Далее создается модель окружения: на плане этажа или объекта указываются стены и другие препятствия на пути распространения радиосигналов, а также их свойства, влияющие на затухание или отражение сигнала. На заключительном этапе задаются требования к беспроводной локальной сети (требуемый уровень радиопокрытия и емкость сети), после чего программа посредством предиктивного моделирования определяет необходимое число точек доступа (ТД) и автоматически расставляет их на карте. По завершению этого процесса пользователь может просматривать и анализировать полученные результаты точно так же, как и в случае радиообследования уже действующей сети. Однако изучение вышеперечисленных программ показало, что ни одна из них не «умеет» работать с трехмерными картами местности, позволяющими учесть неровности рельефа и окружающую городскую застройку, что, разумеется, может быть крайне важно при планировании уличных сетей Wi-Fi. Напротив, данный функционал обычно присущ программным продуктам, предназначенным для планирования сотовых сетей. Примерами программ такого рода являются Altair WinProp, ATDI ICS telecom EV, Forsk Atoll и Ranplan Professional. Поэтому для радиопланирования сетей Wi-Fi на открытой и сильно пересеченной местности пристальное внимание следует обратить именно на данные продукты.

Если на распространение радиосигналов внутри помещений основное воздействие оказывают препятствия в виде стен, перекрытий и т. п., то на распространение радиосигналов в условиях уличной сети Wi-Fi, развернутой в городском парке или придомовой территории, будут оказывать

зеленые насаждения в виде деревьев и кустарников. Для определения коэффициента затухания радиосигнала, обусловленного наличием зеленых насаждений между источником и получателем, были проведены измерения по адресу Санкт-Петербург, ул. Белы Куна, д. 26. Эксперименты проводились летом, осенью и зимой, чтобы оценить влияние зеленых насаждений, сперва покрытых листвой, затем без листвы и в конечном итоге покрытых снегом (рис. 1). В качестве источника сигнала использовался мобильный телефон iPhone 7 Plus в режиме «модема», а в качестве приемника сигнала выступал ноутбук. Для определения мощности принимаемого сигнала использовалась программа Ekahau Site Survey, установленная на ноутбуке. Исследование проводились в частотном диапазоне 2,4 ГГц.

Рис. 1. Место проведения экспериментов (лето, осень, зима)

Схема исследования представлена на рис. 2. Эксперименты выполнялись на расстоянии 20 метров, стоя напротив соседних подъездов. Сперва проводилась серия из 10 измерений мощности принимаемого радиосигнала в условиях прямой видимости между источником и получателем, а затем – серия из 10 измерений с препятствием в виде зеленых насаждений между ними. Для каждой серии фиксировалось среднеарифметическое значение мощности сигнала в дБм.

Рис. 2. Измерения на открытом пространстве и с препятствиями в виде деревьев и кустарников, растущих между дорожками, ведущими к соседним подъездам

Полученные в ходе экспериментов результаты представлены в таблице. Для расчета коэффициента затухания при прохождении сигналом препятствия в 1 метр толщиной использовалась методика, описанная в [9]. Легко видеть, что даже отнюдь не густые зеленые насаждения приводят к ощути-

мому затуханию сигнала, которое обязательно следует учитывать при построении сетей Wi-Fi в парках и во дворах с большой плотностью деревьев и кустарников.

ТАБЛИЦА. Затухание сигнала при прохождении зеленых насаждений, расстояние 20м

Состояние зеленых насаждений и время года	Мощность радиосигнала в условия прямой видимости, дБм	Мощность радиосигнала с препятствием в виде зеленых насаждений, дБм	Затухание, обусловленное наличием препятствия в виде зеленых насаждений, дБ	Коэффициент затухания при прохождении зеленых насаждений, дБ/метр
С листвой, лето	–66	–74	8	0,40
Без листвы, осень	–66	–71	5	0,25
Под снегом, зима	м67	–73	6	0,30

Изучение программных продуктов для радиопланирования сетей Wi-Fi показало следующее. Acrylic Wi-Fi HeatMaps, AirMagnet Planner, iBwave Wi-Fi и VisiWave Site Survey позволяют задавать лишь всевозможные препятствия в виде стен, дверей и т. п. При этом невозможно указать области с повышенным затуханием сигнала (в частности, из-за зеленых насаждений). Ekahau Site Survey [10] и TamoSoft TamoGraph Site Survey [11] позволяют, помимо стен, дверей и т.п., задавать также области с повышенным затуханием.

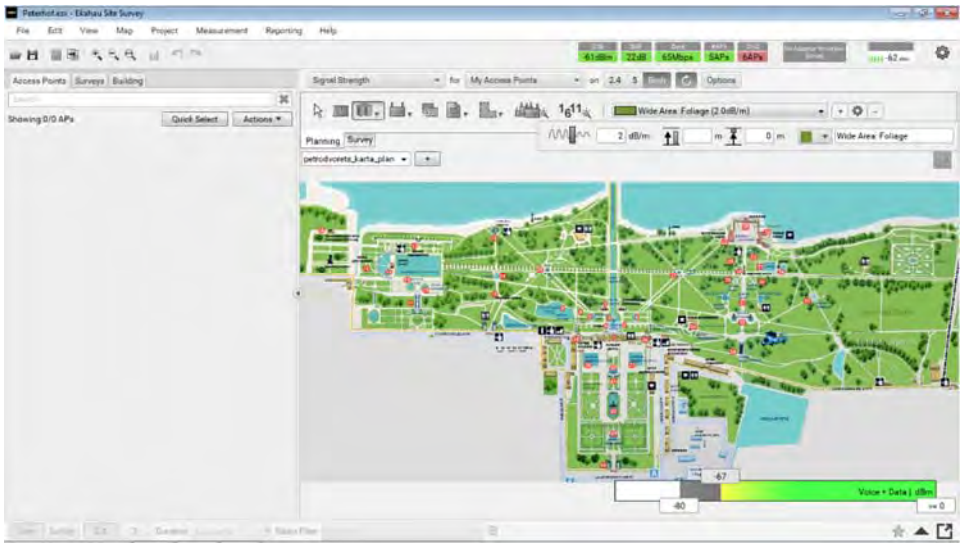


Рис. 3. Учет дополнительного затухания, создаваемого кронами деревьев и кустарников, при радиопланировании в программе Ekahau Site Survey

Например, затухание из-за зеленых насаждений (foliage) данные программы оценивают как 2 дБ на 1 метр (*Ekahau Site Survey* v9.2.5.260) и 1 или 3 дБ на 1 метр (*TamoSoft TamoGraph Site Survey* v5.0.227) в зависимости от плотности листвы и насаждений. Причем коэффициент затухания не зависит от используемого частотного диапазона (2,4 или 5 ГГц). Скриншоты соответствующих окон данных программ представлены на рис. 3 (см. выше) и 4. Таким образом, при радиопланировании уличных сетей Wi-Fi рекомендуется отдавать предпочтение именно этим программным продуктам.

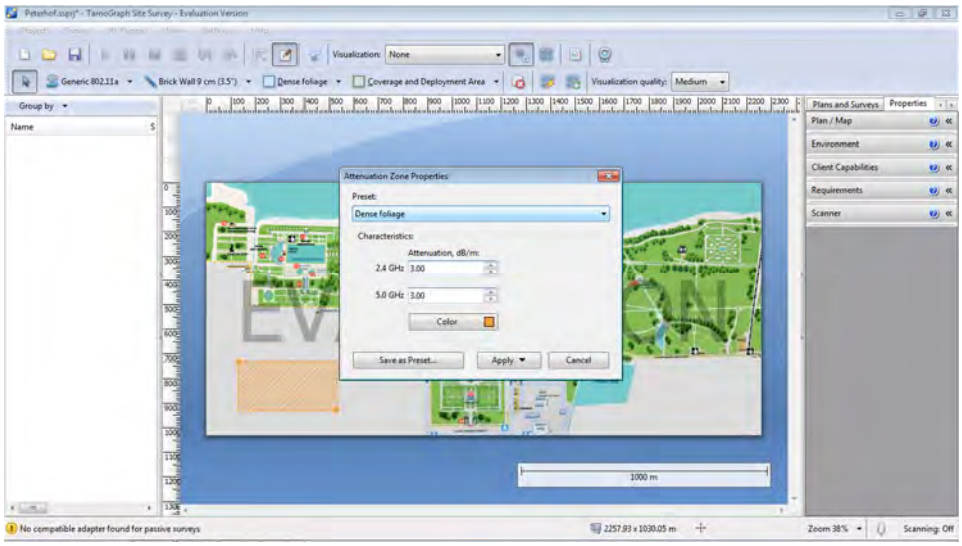


Рис. 4. Учет дополнительного затухания, создаваемого кронами деревьев и кустарников, при радиопланировании в программе TamoSoft TamoGraph Site Survey

Список используемых источников

1. Global Mobile Data Traffic Forecast Update, 2017–2022 [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.pdf (дата обращения 14.04.2019).

2. Дунайцев Р. А., Наумичева Д. А. Радиообследование общежития «Лесное» СПбГУТ // 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. 281–285.

3. Дунайцев Р. А., Тампио А. В. Радиообследование общежития «Рыбацкое» СПбГУТ // 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. 290–295.

4. Дунайцев Р. А., Короткин К. Ф. Радиообследование и радиопланирование беспроводных локальных сетей Wi-Fi // 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. 270–274.

5. Баландин И. А., Дунайцев Р. А. Радиообследование открытой городской Wi-Fi сети на Невском проспекте // 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. 83–88.

6. Дунайцев Р. А., Овчинникова П. А., Петренко А. С. Исследование характеристик сети Wi-Fi Петербургского метрополитена // 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. 332–336.

7. Municipal wireless network [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Municipal_wireless_network (дата обращения 14.04.2019).

8. Comparison of wireless site survey applications [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Comparison_of_wireless_site_survey_applications (дата обращения 14.04.2019).

9. Adjusting Wall Materials in Ekahau Site Survey [Электронный ресурс]. URL: https://www.openreality.co.uk/wp-content/uploads/2016/05/Adjusting-Wall-Materials-in-Ekahau-Site-Survey.pdf (дата обращения 14.04.2019).

10. Industry standard tool for designing, analyzing, optimizing and troubleshooting Wi-Fi Networks [Электронный ресурс]. URL: https://www.ekahau.com/products/ekahau-site-survey/overview/ (дата обращения 14.04.2019).

11. Планирование и обслуживание Wi-Fi сетей [Электронный ресурс]. URL: https://www.tamos.ru/products/wifi-site-survey/ (дата обращения 14.04.2019).

УДК 004.732
ГРНТИ 49.43.29

ОБ ОСОБЕННОСТЯХ РАДИООБСЛЕДОВАНИЯ СЕТЕЙ WI-FI

Р. А. Дунайцев, Н. А. Лебедева

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

Радиообследование сети Wi-Fi может проводиться в одном их двух режимов: непрерывном (continuous) и пошаговом (stop-and-go). Выбор режима, а также траектория обхода территории, на которой развернута сеть Wi-Fi, влияют на трудоемкость проводимого радиообследования и точность получаемых результатов. В статье проводится сравнительный анализ вышеуказанных режимов на примере беспроводной локальной сети СПбГУТ. На основе полученных данных даются рекомендации по проведению радиообследований сетей Wi-Fi в больших зданиях.

W-Fi, wireless site survey, беспроводная сеть, радиообследование, точка доступа.

Технология Wi-Fi широко используется дома и в офисе, в торговых и развлекательных центрах, в корпоративных и промышленных сетях, и, согласно многочисленным прогнозам, подобная тенденция сохранится в обозримом будущем. Помимо неоспоримых достоинств в виде отсутствия проводов, мобильности пользователей и легкости развертывания, сети Wi-Fi

имеют и ряд недостатков, как то: чувствительность к электромагнитным помехам и интерференции, препятствиям на пути распространения сигнала и т. д. В результате особое значение приобретает грамотное планирование беспроводной локальной сети, а также ее периодическая диагностика с целью своевременного обнаружения проблем и их оперативного устранения [1]. Wireless site survey – это комплекс мер по сбору и анализу информации о радиочастотной обстановке и особенностях территории на месте планируемой к развертыванию или уже действующей сети Wi-Fi. В русскоязычной литературе данный процесс известен как радиообследование, радиоразведка или радиоинспектирование. Таким образом, радиообследование сети Wi-Fi рекомендуется проводить [2, 3, 4, 5]:

– до развертывания с целью определения необходимого количества и типа точек доступа (ТД), используемых антенн, потенциальных источников радиопомех, а также возможных мест установки оборудования;

– сразу после развертывания, дабы удостовериться, что построенная сеть отвечает заявленным при планировании требованиям;

– периодически в процессе эксплуатации для выявления проблем в работе сети и выработке решений по улучшению ее функционирования, а также при необходимости модернизации или расширения сети.

Программы для радиообследования сетей Wi-Fi предусматривают два режима работы: непрерывный (*continuous*) и пошаговый (*stop-and-go*). В первом режиме необходимо отметить на карте обследуемой территории свое начальное местоположение, а затем медленно и, желательно, с постоянной скоростью двигаться по прямой. При смене направления движения необходимо отметить эту точку на карте. При остановке также следует указать свое текущее местоположение и остановить сканирование радиоэфира. В итоге все данные, собранные в процессе обхода территории, программа равномерно распределит между начальной и конечной точками маршрута. Естественно, чем ниже скорость движения, тем больше данных успевает собрать программа и тем точнее будут результаты последующего анализа. Во втором режиме требуется отметить на карте свое местонахождение и подождать, пока программа не закончит сбор данных, просканировав все выбранные радиоканалы. После этого можно свободно двигаться до следующей точки, где процесс повторяется заново. При этом траектория и скорость перемещения между соседними точками могут быть любыми. Преимуществом непрерывного режима является большее число измерений, которое успевает выполнить программа, и отсутствие необходимости постоянно отмечать на карте свое местоположение. Данный режим хорошо подходит для проведения измерений в длинных коридорах или на открытом пространстве. К недостаткам можно отнести погрешности в результатах, возникающие при неравномерном или слишком быстром движении. Напротив, достоинством пошагового режима является точная привязка собранных данных

к тому месту на карте, где фактически было произведено сканирование. Однако на выполнение радиообследования большой территории с той же точностью в пошаговом режиме обычно требуется больше времени. Как правило, оба эти режима можно успешно комбинировать, переключаясь между ними по мере необходимости в процессе радиообследования.

В настоящее время на рынке представлен довольно большой выбор программ для радиообследования и радиопланирования сетей Wi-Fi [6]. Рекомендации разработчиков по выполнению радиообследований во многом совпадают [7, 8, 9]. В частности, рекомендуется проводить тщательные измерения на всей территории исследуемого объекта, заходя, по возможности, во все помещения. Но что если такой возможности нет, а радиообследование провести необходимо? Подобная ситуация может возникнуть в условиях нехватки времени у проводящего обследование специалиста или из-за отсутствия доступа в закрытые помещения. Остается единственная возможность – провести радиообследование, пусть даже неполное и поверхностное, путем обхода коридоров и сбора данных лишь там. Согласно [7], радиообследование в коридорах следует проводить либо дважды, проходя сперва по одной стороне коридора, а затем по другой, либо двигаться от стены к стене по зигзагообразной траектории.

Данная статья посвящена анализу эффективности непрерывного и пошагового режимов на примере радиообследования, выполняемого в коридорах большого здания. Сравнивается трудоемкость процесса и точность получаемых результатов при различных способах прохождения коридоров.

Для выполнения экспериментов был выбран сегмент сети Wi-Fi Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПбГУТ), работающий во втором корпусе на пятом этаже. Такой выбор был не случайным. Во-первых, все ТД здесь имеют свой индивидуальный номер, присвоенный системным администратором, что позволяет легко их идентифицировать. Например, AP.5-15 – это ТД (*access point*, AP) под номером 15, работающая на пятом этаже. Во-вторых, приемопередающие антенны ТД являются выносными и их легко обнаружить на потолке (рис. 1). Таким образом, первым этапом в исследовании стало визуальное нахождение ТД на пятом этаже второго корпуса СПбГУТ. В результате осмотра помещений, удалось установить расположение 18 ТД (рис. 2). После этого стало возможным приступить к самому радиообследованию. Для этого была использована программа

Рис. 1. Антенны двухдиапазонных ТД на потолке второго корпуса СПбГУТ

Ekahau Site Survey [10], установленная на ноутбуке, и внешний двухдиапазонный Wi-Fi адаптер Linksys WUSB6300.

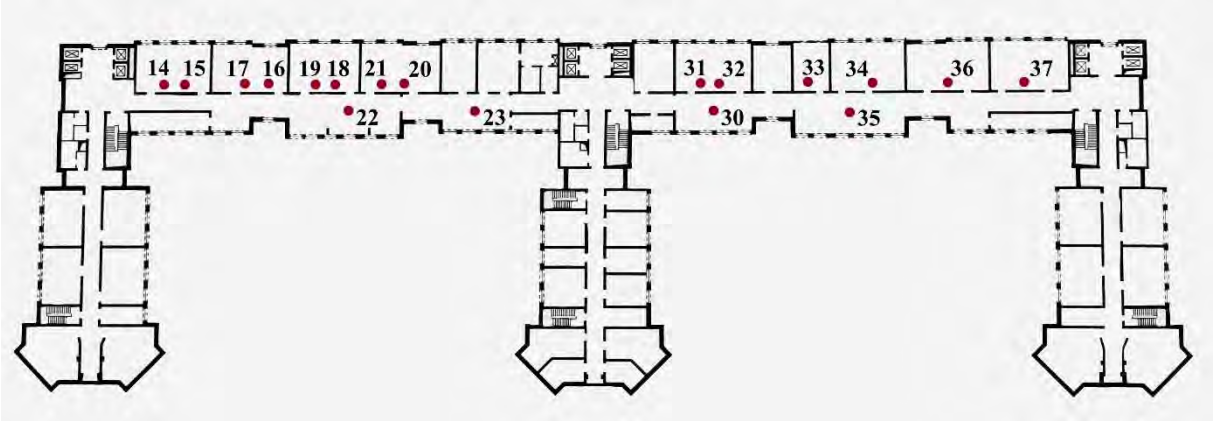
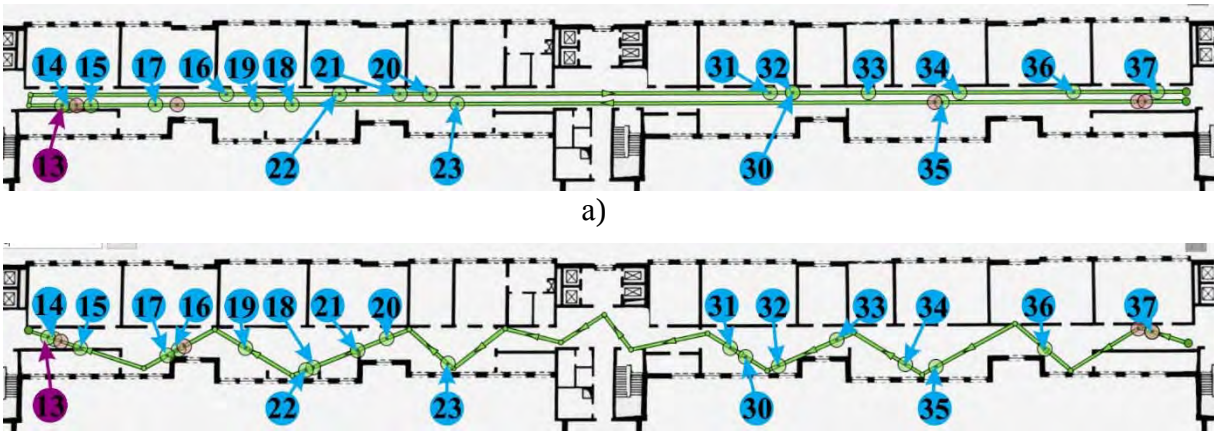


Рис. 2. Расположение ТД на пятом этаже второго корпуса СПбГУТ

Результаты радиообследования в непрерывном и пошаговом режиме представлены на рис. 3 и 4, соответственно. Легко видеть, что программе не только удалось определить все ТД, известные нам по рис. 2 (отмечены синим цветом), но и найти одну новую, не обнаруженную при визуальном осмотре этажа (отмечена на карте фиолетовым цветом, местоположение определенно приблизительно). К сожалению, как следует из рис. 3 и 4, программа не в состоянии верно расположить ТД вне маршрута обхода. Таким образом, для определения наилучшего способа проведения радиообследования, выполняемого в коридорах большого здания, были выбраны следующие критерии: количество обнаруженных ТД и точность определения их местоположения на этаже, а также затраченное на радиообследование время и пройденное при этом расстояние (см. табл.).



а)

б)

Рис. 3. Радиообследование в непрерывном (continuous) режиме
а) по прямой траектории, б) по зигзагообразной траектории

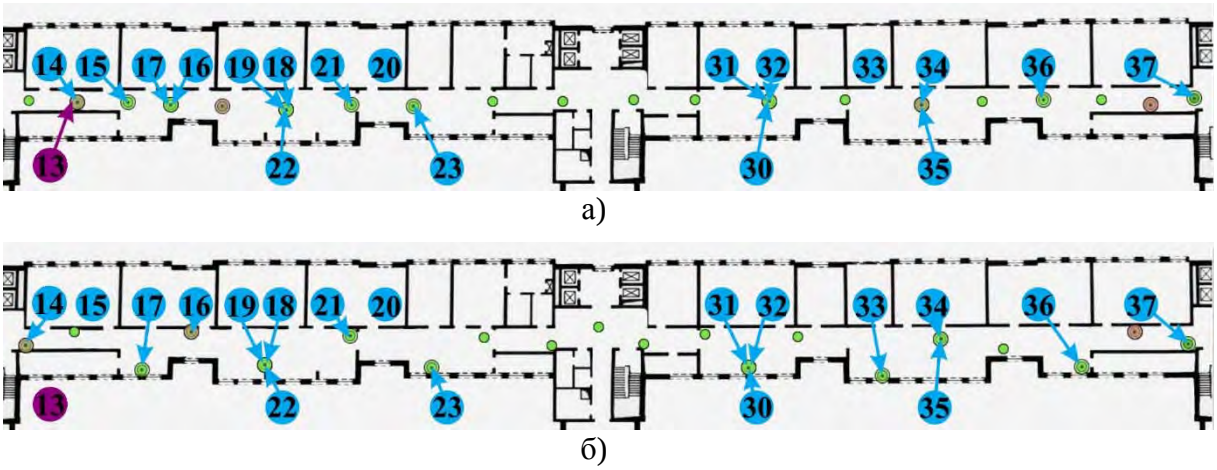


Рис. 4. Радиообследование в пошаговом (stop-and-go) режиме
а) по прямой траектории, б) по зигзагообразной траектории

Согласно таблице, в проведенном исследовании наилучшие результаты показал вариант обхода в непрерывном режиме, позволивший обнаружить все 19 ТД. По точности их расстановки на карте, а также по времени радиообследования и пройденному расстоянию, вариант с зигзагообразной траекторией обхода оказался значительно эффективнее, чем двойной обход по прямой. Пошаговый режим проявил себя хуже с обоими способами обхода. Следовательно, этот режим больше подходит для инспектирования небольших, тесно заставленных помещений, и для ликвидации «белых пятен», оставшиеся после радиообследования в непрерывном режиме.

ТАБЛИЦА. Результаты сравнительного анализа

Режим радиообследования и способ обхода	Количество обнаруженных ТД	Время обследования	Пройденное расстояние, м
Непрерывный режим, прямая траектория	19	11 мин. 47 сек.	285
Непрерывный режим, зигзагообразная траектория	19	7 мин. 9 сек.	163
Пошаговый режим, прямая траектория	17	5 мин. 24 сек.	140
Пошаговый режим, зигзагообразная траектория	16	6 мин. 36 сек.	160

Список используемых источников

1. О важности радиоразведки и радиопланирования при развертывании Wi-Fi сетей [Электронный ресурс]. URL: https://www.pcweek.ua/themes/detail.php?ID=148474 (дата обращения 13.04.2019).

2. Best Practices for Wireless Site Design [Электронный ресурс]. URL: http://www.nle.com/literature/Airmagnet_BestPractices-for_wireless_site_design.pdf (дата обращения 13.04.2019).

3. Wireless Site Survey Best Practices [Электронный ресурс]. URL: https://assets.te-quipment.net/assets/3/7/WhitePaper-WirelessSiteSurveyBestPractices.pdf (дата обращения 13.04.2019).

4. How To Do a Successful RF Site Survey [Электронный ресурс]. URL: https://www.metageek.com/inc/images/downloads/How-To-Do-A-RF-Site-Survey-Guide.pdf (дата обращения 13.04.2019).

5. Дунайцев Р. А., Короткин К. Ф. Радиообследование и радиопланирование беспроводных локальных сетей Wi-Fi // 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. 270–274.

6. Comparison of wireless site survey applications [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Comparison_of_wireless_site_survey_applications (дата обращения 13.04.2019).

7. Tips and hints: running a wireless site survey [Электронный ресурс]. URL: https://www.netspotapp.com/help/tips-and-hints-running-a-wireless-site-survey/ (дата обращения 13.04.2019).

8. Measurement point data acquisition type: Stop and Go, Continuous, and Real Time GPS [Электронный ресурс]. URL: https://www.acrylicwifi.com/en/blog/stop-and-go-continuous-gps/ (дата обращения 13.04.2019).

9. Site Survey Tool – TamoGraph [Электронный ресурс]. URL: https://www.tamos.ru/htmlhelp/tg/ (дата обращения 13.04.2019).

10. Wi-Fi Design, Wi-Fi Planning and Ekahau Site Survey Software, Wi-Fi Spectrum Analysis [Электронный ресурс]. URL: https://www.ekahau.com/ (дата обращения 13.04.2019).

УДК 654.078
ГРНТИ 49.46.33

СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ОПТИЧЕСКИХ СЕТЕЙ ДОСТУПА

А. С. Дюбов, А. П. Коваленко

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

В настоящее время оптические сети доступа являются наиболее динамично развивающимся сегментом рынка телекоммуникаций. Одним из характерных признаков постоянного развития рынка сетей доступа является из года в год совершенствующиеся технологии передачи данных и построения сетей, призванные удовлетворить растущие потребности пользователей. Если на транспортных сетях связи (магистральных линиях связи) переход на оптическое волокно идет полным ходом, то в оптических сетях доступа переход на оптическое волокно становится все ближе и ближе к конечному пользователю.

PON, FTTx, Active Ethernet, Micro SDH, перспективы развития оптических сетей доступа.

Оптические сети доступа сегодня

Можно с уверенностью сказать, что оптические сети доступа находятся в своей начальной фазе развития, что и делает их привлекательными и интересными как со стороны операторов связи, так и со стороны пользователей.

Архитектура построения оптических сетей доступа характеризуется степенью приближения оптического сетевого терминала к пользователю. Международный Союз Электросвязи дает следующую классификацию архитектуры построения оптических сетей доступа, показанной на рис. 1.

Рис. 1. Архитектуры построения оптических сетей доступа

Выбор архитектуры зависит от многих факторов, одним из главных является – плотность размещения абонентов на проектируемом участке сети. Как можно увидеть из рис. 1 все архитектуры построения оптических сетей доступа, характеризуются наличием распределительного участка с использованием медного кабеля. Не мало важным фактором является и использование конкретной базовой оптической технологии построения сети [1].

В последнее время на оптических сетях доступа наиболее часто используются три интегральные технологии:

– микросеть SDH (*Micro* SDH);

– активные сети Ethernet (*Active Ethernet,* AE);

– пассивные оптические сети (*Passive Optical Network,* PON).

Прогнозы потребностей скоростей и объемов трафика на абонентском участке

Современные телекоммуникационные сети в определенной манере также пытаются придерживаться следующего лозунга: «Быстрее, дальше, больше», что в свою очередь означает [2]:

1) постоянное стремление увеличить пропускную способность одного канала;

2) стремление увеличить протяженность регенерационного участка сети;

3) стремление увеличить общую емкость систем передачи с помощью различных методов уплотнения каналов.

Согласно исследованиям компании Cisco, в 2016 г. трафик в мобильных сетях в сравнении с 2015 г. вырос на 63 %. Если говорить в абсолютных значениях, то в конце 2016 г. он достиг уровня 7,2 эксабайт в месяц (в конце 2015 года эта цифра составляла 4,4 эксабайта). Чтобы все понимали, о какой цифре идет речь, напомним, что 1 эксабайт (Эбайт, ЭБ) равен 10^{18} байт, что соответствует одному миллиарду гигабайт (ГБ) или одному миллиону терабайт. Аналитики из Калифорнийского университета утверждают, что человечеству потребовалось 300 тысяч лет, чтобы создать первые 12 эксабайт информации, зато вторые 12 эксабайт были созданы всего за несколько лет, начиная с 2005 г.

Значительный рост трафика в ближайшие годы обусловлен передачей ультравысококачественных (UHD) 4K видеопотоков. Битрейт для 4K видеопотока составляет примерно 18 Мбит/с, что более чем в два раза больше битрейта HD-видео и в девять раз больше битрейта видеопотока стандартного разрешения SD – 720 на 576 точек. Прогнозируется, что к 2020 г., 40 % установленных ЖК-телевизоров будут поддерживать UHD (рис. 2).

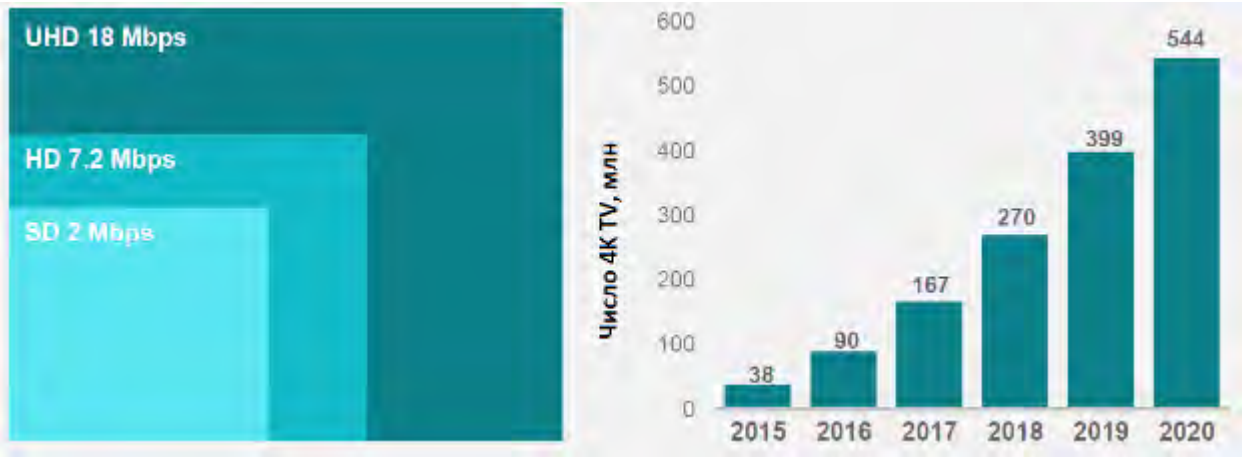


Рис. 2. Увеличение устройств с поддержкой видео 4K

Передача видеопотоков является также основной причиной роста трафика в мобильных сетях. В 2021 г. из 49 эксабайт данных, проходящих через мобильную сеть каждый месяц, 38 эксабайт принадлежат видеоконтенту. Начиная с 2012 г. видеопотоки составляют более половины мирового трафика в мобильных сетях.

Как видно из приведенных результатов, трафик в ближайшие годы будет увеличиваться довольно быстрыми темпами.

Возможные варианты дальнейшего развития

Одной из главных движущих сил, развивающих телекоммуникации, стала возможность предоставления услуг по передаче видеоконтента самыми разными способами [3].

Огромные финансовые потоки, хлынувшие в отрасль, начинают трансформировать мировую инфраструктуру, как в проводной, так и в беспроводной области. Аналитическая компания Insight Research попыталась предугадать дальнейшее развитие событий и описала три возможных варианта преобразований, ожидающих индустрию телекоммуникаций:

1. Сети продолжают развиваться равномерно, ни одна из технологий связи не уходит с рынка.

2. Сети глобально и повсеместно преобразуются к использованию решений на базе интернет.

3. Сети, в основной своей массе, становятся беспроводными и тотально всеохватывающими.

Аналитики полностью отдают себе отчет в том, что, скорее всего, ни один из этих вариантов «в чистом виде» не будет реализован никогда. Но задача данного прогноза и не состоит в попытке предугадать будущее.

Главная цель – показать основные тенденции, которые будут очень сильно влиять на телекоммуникации всего мира в самое ближайшее время. Иначе говоря, данное исследование должно помочь в построении планов и разработке аналитических прогнозов на будущее.

В первом варианте обычная телефония продолжает сохранять твердые позиции на рынке, полностью уступив IP-телефонии в бизнесе только внутрикорпоративную связь. Интернет будет считаться слишком небезопасным местом, чтобы использовать его для комплексной маршрутизации телефонного трафика.

Приложения будут требовать от глобальной сети все большей полосы пропускания, но VoIP останется исключительно «нишевой» услугой. Широкополосный доступ на базе оптоволокна будет становиться все более распространенным и поддерживать все виды коммуникаций.

Кабельные компании будут продолжать активное продвижение оптоволокна для подключения домашних пользователей, но постепенно начнут

уделять все большее внимание и предприятиям. Беспроводные виды доступа получат некоторое развитие, обеспечат определенное увеличение скоростей передачи данных, но все еще будут серьезно отставать по большинству характеристик от проводных видов связи.

Во втором варианте развития событий общественная телефонная сеть, выделенные услуги связи вида «точка-точка» и широковещательное обслуживание полностью перебираются в интернет. Весь голосовой поток будет преобразовываться в цифровой вид, пакеты данных будут передаваться через общественные линии интернет, а специальные системы будут следить за приоритетом передаваемого трафика, чтобы минимизировать помехи на чувствительных ко времени задержки приложениях.

Все местные, национальные и международные сети преобразованы к виду, обеспечивающему передачу исключительно IP-пакетов.

Стремление к рациональному использованию ресурсов приведет к тому, что каждое здание будет подключено только одним кабелем (разумеется, оптоволоконным), по которому будут осуществляться все виды коммуникаций. Внутри здания еще долгое время будет оставаться разводка медным кабелем. Эфирное телевидение исчезнет полностью, вытесненное IPTV. Все базовые станции беспроводных видов связи подключены непосредственно к IP-сетям. Не будет никакой разницы между WiMax, Wi - Fi, сотовой связью или домашними радиотелефонами, поскольку все устройства, в конечном счете, будут только IP-терминалами.

Полоса пропускания, предоставляемая WiMax, превысит все известные проводные виды связи, а телефонные столбы будут использоваться только для установки антенн и подачи постоянного питания беспроводному оборудованию. Доступ в интернет будет только беспроводным, а интернет-терминалы станут одним из видов беспроводной связи.

Кабельное телевидение почти полностью атрофируется, уступив место цифровому беспроводному широковещательному ТВ на базе как спутников, так и наземных систем трансляции, с практически неограниченными возможностями по индивидуальному заказу контента. При этом использование оптоволокна было бы достаточно существенным, поскольку передача трафика на большие расстояния беспроводными способами неэффективна и нецелесообразна.

Перспективные решения развития ВОСП

Дальнейшее развитие ВОСП, по мнению специалистов, будет происходить в двух основных направлениях.

Первое – разработка и внедрение в сетях различного назначения новых волоконно-оптических технологий, направленных на повышение эффектив-

ности ВОСП. На линиях дальней связи основное внимание по-прежнему будет уделяться повышению скорости передачи информации, увеличению длины регенерационных участков и повышению надежности. Широкое распространение получат промежуточные оптические усилители и методы волнового мультиплексирования. Доминирующей особенностью развития волоконно-оптических технологий в местных и локальных сетях будет приближение ОВ к конечному пользователю сети (абоненту).

Рост потребности в новых видах информационного обслуживания индивидуальных абонентов, а также совершенствование и постоянное снижение стоимости аппаратуры и средств коммутационной техники готовят окончательный переход сетей доступа на ОВ. Ведущая роль в этом процессе принадлежит сети Internet. По оценкам средний объем потока информации в расчете на одного пользователя сети увеличивается ежегодно в восемь раз. Постоянно появляются новые виды услуг. Это выдвигает повышенные требования к скорости передачи информации в сетях доступа, удовлетворить которые можно только с помощью ОВ.

Второе направление развития ВОСП это создание линий передачи, в которых используются нелинейные свойства ОВ, обеспечивающие солитонный режим распространения. Импульс лазерного луча состоит из набора волн, несколько отличающихся по частоте. При распространении этого импульса по ОВ в линейном режиме низкочастотные волны обгоняют высокочастотные, и форма импульса изменяется. В нелинейном режиме работы ОВ высокочастотные волны «догоняют» низкочастотные. Происходит самосжатие импульсов и формирование оптических солитонов, которые характеризуются замечательным свойством распространяться без изменения формы и длительности. В таких ВОСП можно достичь скорости передачи, равной десяткам гигабит в секунду при длине регенерационного участка до 1000 км.

Список используемых источников

1. Архитектура оптических сетей доступа FTTH (Fiber-to-the-Home) [Электронный ресурс]. URL: https://www.cisco.com/c/dam/global/ru_ru/assets/downloads/cisco_ftth_ architecture.pdf (дата обращения 22.02.2019).

2. Cisco прогнозирует почти 11-кратный рост мирового трафика мобильной передачи данных с 2013 по 2018 гг. [Электронный ресурс]. URL: https://infocity.az/2014/02/cisco-прогнозирует-почти-11-кратный-рост-мир/ (дата обращения 28.03.2019).

3. Три варианта развития мировых телекоммуникаций [Электронный ресурс]/ URL: https://nag.ru/articles/reviews/15578/tri-varianta-razvitiya-mirovyih-telekommunikatsiy.html (дата обращения 11.01.2019).

УДК 004.057.4
ГРНТИ 20.53.23

ВОЗМОЖНОСТИ MPLS-TP И ИНТЕГРАЦИЯ С SDN СЕТЯМИ

В. С. Елагин, И. Н. Иванов

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

Сеть MPLS была разработана для передачи различного вида трафика в 2001 году. Основной идеей при создании MPLS ускорить передачу пакетов через механизмы маршрутизации. По истечении времени операторы связи, эксплуатирующие MPLS, заметили, что базовому MPLS не хватает механизмов контроля и управления. В 2009 г. Международным Союзом Электросвязи и инженерным советом интернета был предложен новый протокол MPLS-TP, который устранял недостатки и удовлетворял желания операторов. С развитием виртуализации и появлением технологии программно-конфигурируемых сетей, возникла потребность объединить две передовые технологии MPLS-TP и SDN, для транспортных сетей оператора.

MPLS-TP, SDN, peer-to-peer, OpenFlow, таблица потоков.

MPLS-TP – Multi-Protocol Label Switch Transport Profile, предназначен для использования в качестве технологии сетевого уровня в транспортных сетях. Стандартизацией с 2009 года занимаются две организации: ITU-T и IETF. В концепции MPLS-TP лежит принцип псевдоканалов и близость к технологии SDH.

Основной задачей MPLS-TP является: упрощение сценариев применения MPLS с уменьшением затрат на оборудование, эксплуатацию и обслуживание. Основные улучшения MPLS-TP:

1. Совершенствование и ограничение плоскости пересылки MPLS.
2. Плоскость управления может быть, как статической, так и динамической.
3. Расширенная функциональность OAM.

Рассмотрим подробнее каждую плоскость.

В контексте MPLS-TP, плоскость управления – это механизм, используемый для автоматической настройки LSP в сетевом домене с коммутацией пакетов. Использование протокола плоскости управления является необязательным в MPLS-TP. Некоторые операторы могут предпочесть сконфигурировать LSP и PW с использованием системы управления сети таким же образом, как это использовано SONET/SDH. В этом случае протокол IP или маршрутизация не используются. И наоборот, возможно использовать

динамическую плоскость управления с MPLS-TP, чтобы LSP и PW устанавливались сетью с использованием G-MPLS и LDP соответственно [1].

Чтобы улучшить возможности сетевого транспорта, в MPLS-TP настроены несколько элементов MPLS.

– NO LSP Merge: архитектуры на основе MPLS позволяют объединять LSP для пакетов, проходящих по одному и тому же маршруту, что помогает повысить эффективность транспортировки трафика, но приводит к потере информации о головном узле LSP. Эта информация головного узла важна для предоставления расширенных возможностей OAM, которые желают поставщики услуг.

– Нет выталкивание внешней метки MPLS на предпоследнем шаге, разрешенное в сетях на основе MPLS.

– Нет балансировки нагрузки: ECMP – это механизм пересылки для маршрутизации пакетов по нескольким путям одинаковой стоимости для достижения почти равного распределения нагрузки на линии. Однако этот механизм приводит к проблемам с устранением неполадок, поскольку фактический путь клиента варьируется между пакетами.

– Двунаправленный LSP: этот элемент позволяет сетям на основе MPLS-TP эмулировать классические транспортные сети - передавать и принимать по одному и тому же пути через сеть. Это упрощает операции для двунаправленного соединения, что также улучшает производительность из-за уменьшенной дисперсии задержки пакета.

Функция OAM и возможность обеспечения живучести для сетевых ретрансляторов MPLS-TP предназначены для снижения сложности работы сети, связанной с мониторингом и управлением эксплуатационными характеристиками сетевого трафика, управлением отказами и защитным переключением [2].

SDN – программно-конфигурируемая сеть. В основе концепции SDN лежит, отделение уровня управления сетью от устройств передачи данных таких как, маршрутизаторы и коммутаторы. Движущей силой SDN является OpenFlow. OpenFlow – протокол реализующий управление процессами обработки данных. OpenFlow работает между маршрутизаторами и SDN – контроллером

В сердце OpenFlow лежат таблицы потоков (далее *FlowTable*). В FlowTable хранится информация о действиях, которые необходимо совершить с данным пакетом, о заголовках PDU (контрольные поля) и поля со статистикой (рис.).

Контрольные поля содержат в себе информацию о входном порте и о том какие протоколы используются на различных уровнях, после транспортного уровня идут сообщения OpenFlow.

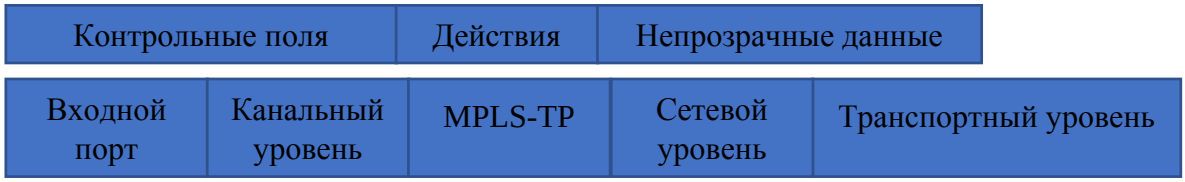


Рисунок. Структура FlowTable

С использованием расширения MPLS-TP для OpenFlow. В структуре FlowTable в контрольном поле, появляется новая запись – MPLS-TP.

Последовательность следующих друг за другом таблиц потоков с определенным набором инструкций называется конвейером. С использованием расширения MPLS-TP соответственно появляются новые таблицы потоков. Теперь в конвейере имеются таблицы потоков, которые содержат действия, которые необходимо выполнить для метки: вложить, поменять, удалить [3].

ТАБЛИЦА. Изменения в OpenFlow

Новые Match Fields	Новые действия OpenFlow MPLS-TP
MPLS_L2_PORT	PUSH_CW
MPLS_TYPE	POP_CW_OR_ACH
ALLOW_VLAN_TRANSLATION	PUSH_L2_HDR/POP_L2_HDR

Рассмотрим новые таблицы потоков.

1. MPLS L2 Port Flow Table, эта таблица служит для обеспечения QoS и OAM, она представляет собой логический входной интерфейс.

2. MPLS Type Flow Table. Таблица сопоставляет поле MPLS_TYPE для направления пакетов в разные таблицы пересылки. В эту таблицу встраиваются правила пересылки программно-аппаратным путем. Контроллер не может добавлять, удалять и изменять правила в этой таблице. На основании этой таблицы определяется таблица потоков ACL.

3. Policy ACL Flow Table. Эта таблица предоставляет действия по фильтрации безопасности на основании политик ACL. Если нету правил ACL, то пакет будет обработан для пересылки с помощью групповой записи или записей указанных в наборе действий.

4. MPLS L2 VPN Label, в этой записи указывается действие, которое необходимо выполнить:

a. Вставить заголовок Ethernet в кадр.

b. Толкнуть MPLS метку.

c. Установить значение метки, на метку PW.

Также в этой таблице содержатся действия для полей MPLS: TTL и TC (не всегда).

5. MPLS Tunnel Label 1. Этот тип записи необходим для проталкивания другой MPLS метки и установки значения метки для LSP.

6. MPLS Interface, необходим для установки MAC-назначения и MAC-источника и идентификатор VLAN для пересылки пакета на LSR.

7. MPLS L2 SWAP Label. Необходим для обновления полей TTL и MPLS_TC.

Количество таблиц потоков MPLS-TP может варьироваться от одного до двух, в зависимости от того граничный это маршрутизатор или нет.

В заключение можно сказать, что применение технологий MPLS-TP и SDN, позволит снизить затраты на эксплуатационное обслуживание и администрирование в транспортных операторских сетях, взаимодействующих между собой по принципу точка-точка.

Список используемых источников

1. RFC 6215 MPLS Transport Profile User-to-Network and Network-to-Network Interfaces.

2. ITU-T Recommendation G.8121.2/Y.1372.2 OAM.

3. Расширение MPLS-TP протокола OpenFlow [Электронный ресурс]. URL: https://www.opennetworking.org/wp-content/uploads/2017/07/MPLS-TP-OpenFlow-Protocol-Extensions-for-SPTN-1-0.pdf (дата обращения 18.02.2019).

УДК 004.7 (004.942)
ГРНТИ 49.37.29

ИССЛЕДОВАНИЕ ТРАФИКА В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ НА НАЗЕМНОМ ТРАНСПОРТЕ

В. С. Елагин, В. В. Илларионов

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

Сети передачи данных на наземном транспорте приобретают все большую популярность благодаря тому, что пользователи получают возможность доступа к сети Интернет в условиях персональной мобильности, будучи доступной и бесплатной для каждого пассажира.

сессия, трафик, сеть, часы наибольшей нагрузки (*ЧНН*).

Одним из основных показателей, характеризующих работу сети передачи данных, является их трафик, учет и визуализация которого осуществляется с помощью ряда программных средств (*zabbix, nagios, graphana*).

Рассматривая подобную сеть в рамках городского наземного транспорта, к вышеуказанному показателю добавляется распределение сессий по их длительности.

Следует отметить, что статистические данные были получены с BRASS сервера.

На основании полученных данных могут быть сделаны выводы о факторах, которые определяют активность пользователей, а также определить вектор дальнейшего развития сетевой инфраструктуры в целом.

Прежде чем перейти к непосредственному анализу распределений необходимо схематично отобразить и описать архитектуру сети передачи данных на наземном транспорте (рис. 1).

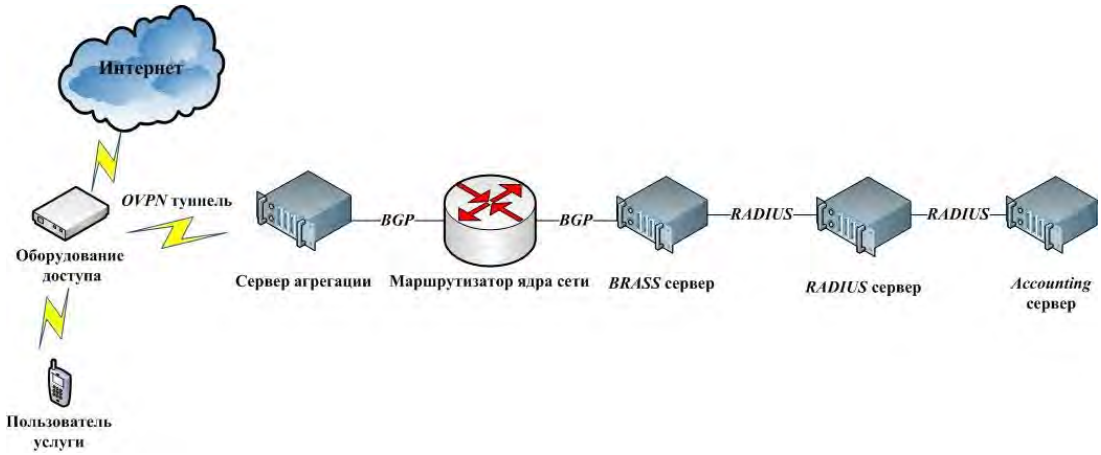


Рис. 1. Архитектура сети передачи данных на наземном транспорте

Основные составляющие архитектуры:

Оборудование доступа – блок Incarnet ViX [1].

Сервер агрегации – сервер, который имеет в своем составе множество сценариев управления маршрутизацией.

Маршрутизатор ядра сети – промежуточный маршрутизатор, который отвечает за передачу трафика по транспортной сети провайдера.

BRASS – сервер, отвечающий за выдачу IP-адреса абоненту и аутентификацию [2].

RADIUS – специализированный сервер основными задачами которого является авторизация и аутентификация абонента [2].

Accounting сервер – отвечает за сбор статистики по абонентским сессиям.

Поэтапно представим общую схему предоставления услуги доступа к сети Интернет по Wi-Fi на наземном транспорте:

1. Абонент подключается к оборудованию доступа выбрав в качестве Wi - Fi сети определенный SSID.

2. Далее происходит DHCP запрос к BRASS серверу.

3. BRASS сервер выдает абоненту IP-адрес по DHCP и производит запрос к RADIUS серверу.

4. После прохождения авторизации абоненту доступен выход в Интернет.

5. По окончании сеанса связи BRASS посылает RADIUS серверу подтверждение об окончании сессии для определенного абонента.

Анализ количества сессий за день (*31.12.2018*)

Для того чтобы выявить характер изменения данного показателя и установить его закономерность потребуется выделить количество сессий длительность которых превысила 23 минуты из общего количества сеансов связи меньшей длительности.

По причине того, что графики распределений сессий меньшей длительности отличаются лишь незначительно было решено произвести дальнейший анализ на основании графика, показанного на рис. 2.

Абсолютный пик сеансов связи приходится на 16:00 – в это время большинство пассажиров направляются за покупками. Затем график линейно убывает.

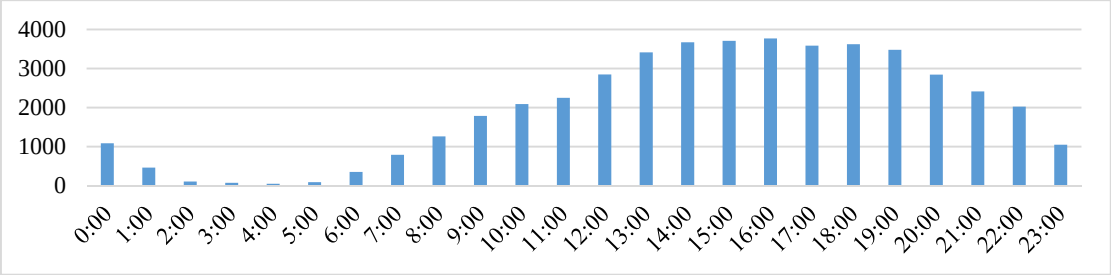


Рис. 2. Количество сессий длительностью более 23 минут

Минимум в 4:00 обусловлен тем, что большинство единиц наземного транспорта находятся в парке. Количество сессий в этом время не равно 0, что связано с тем, что некоторые автобусы развозят обслуживающий персонал, а также находятся на специальных (ночных) маршрутах.

Следует отметить, что съем статистики был произведен в нерабочий день, о чем свидетельствуют отсутствие утреннего и вечернего пика в ЧНН 8:00 и 18:00–19:00 соответственно.

Внешний вид графика, показанного на рис. 3 схож с графиком распределения Пуассона [3]. Это подтверждает гипотезу о том, что распределение сессий в выходные дни подчиняется закону Пуассона.

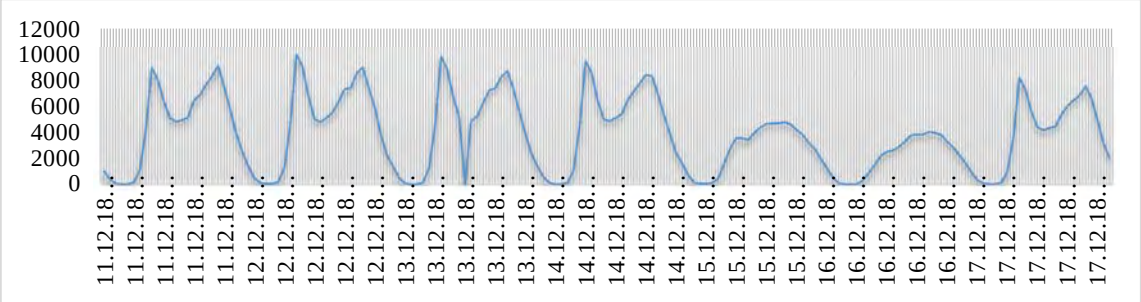


Рис. 3. Количество сессий длительностью более 23 минут
за период с 11.12.2018 по 17.12.2018

Анализ количества сессий за неделю (*11.12.2018–17.12.2018*)

Аналогично ранее рассмотренному периоду выделим из общего количества сеансов связи – сессии длительность которых превысила 23 минуты (рис. 3).

Зафиксирована просадка сессий в выходные дни (15.12.2018–16.12.2018), т. к. падает общее количество людей, подключающихся к сети (количество подключенных пользователей к сети Wi - Fi приведено на рис. 4).

Необходимо отметить, что 13.12.18 в 12:00 фиксировалось 0 сессий, рассматриваемой длительности: причиной их отсутствия являются ошибки при сборе статистики.

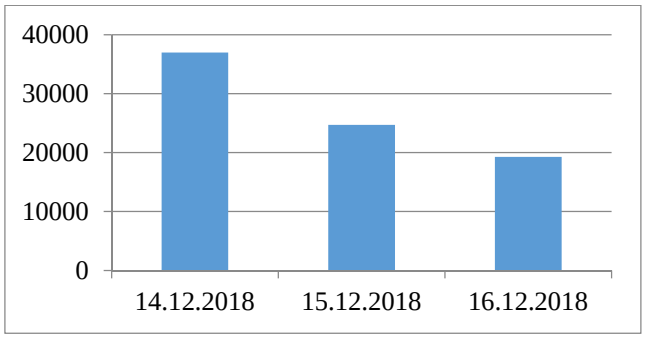


Рис. 4. Количество подключений в период с 14.12.2018 по 16.12.2018

Чтобы провести сравнение в качестве точек выборки были взяты ЧНН: 8:00, 18:00, 19:00. Количество сеансов связи за период с 14.12.2018 по 16.12.2018 приведены в таблице.

Рассмотрим динамику изменения сессий относительно рассматриваемого периода: 14.12.2018 в 8:00 – 9504, а в это же время 15.12.2018 – 2783, что в 3,41 раза меньше чем в будний день, а 16.12.2018 – 1525 – в 6,23 раза меньше в сравнении с 14.12.2018.

ТАБЛИЦА. Количество сессий более 23 минут с 14.12.2018 по 16.12.2018

Число/Время	8:00	18:00	19:00
14.12.2018	9504	8466	8360
15.12.2018	2783	4641	4230
16.12.2018	1525	3986	3845

Как уже ранее отмечалось, график распределения сессий в выходные дни схож с графиком распределения Пуассона. Покажем динамику распределения сессий 14.12.18 (пятница) и 15.12.18 (суббота) соответственно (рис. 5).

Сравнив графики распределения в выходной и будний день можно прийти к выводу, что в рабочий день гипотеза о том, что распределения сессий подчиняются закону Пуассона, не подтверждается. Об этом также свидетельствуют характерные пиковые значения в ЧНН в 8:00 и 18:00–19:00, свойственные графику сеансов связи за 14.12.18.

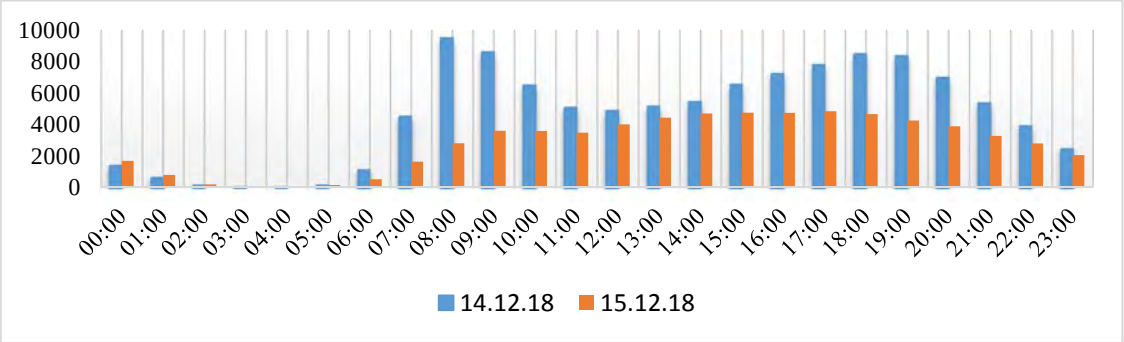


Рис. 5. Динамика распределения сессий в будний и выходной день

На основании вышеизложенной информации можно утверждать о том, что распределение сеансов связи в будний день подчиняется двумодальному закону [3].

Анализ количества сессий за месяц (*01.12.2018–31.12.2018*)

Произведем отбор только тех сессий длительность которых была более 23 минут в рамках рассматриваемого периода времени (рис. 6, см. ниже)).

По графику, изображенному на рис. 6 прослеживается тенденция аналогичная недельной выборке: в выходные и праздничные дни график схож с распределением Пуассона, а в рабочие дни появляются характерные пиковые значения в ЧНН, которые указывают на то, что распределение сессий подчиняются двумодальному закону.

Следует подчеркнуть тот факт, что в последнюю неделю декабря было 6 рабочих дней, что подтверждается количеством распределений сессий в эти дни на графике.

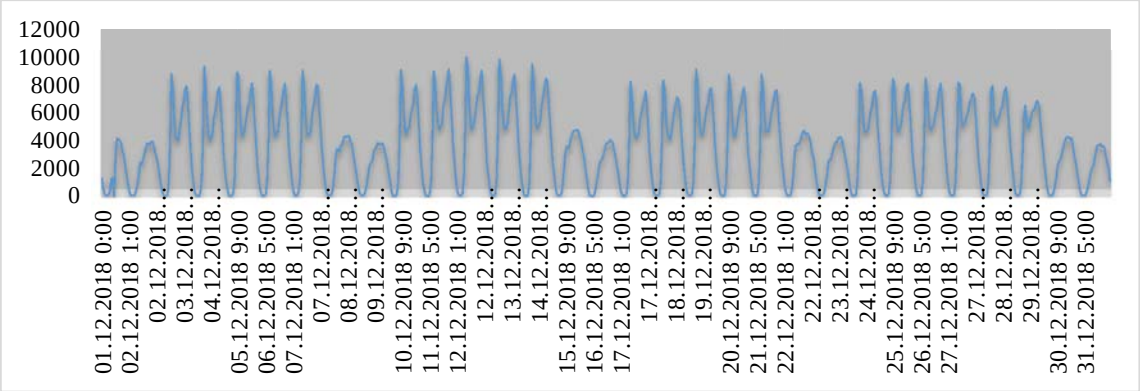


Рис. 6. Количество сессий длительностью более 23 минут
за период с 01.12.2018 по 31.12.2018

Общие выводы

Основываясь на результатах проведенного исследования, было установлено, что в рабочие дни пиковые значения сеансов связи были зафиксированы в ЧНН (8:00, 18:00–19:00), минимум сессий наблюдался в 4:00.

На основании вышеуказанной информации можно сделать вывод о том, что наибольшая нагрузка на сеть передачи данных на наземном транспорте приходится в ЧНН в рабочие дни, когда большинство людей добирается на работу или возвращается с нее.

Также было установлено, что распределение сессий в выходные и праздничные дни подчиняется закону Пуассона, а в рабочие напротив двумодальному. Дальнейшие исследования будут направлены на поиск соответствующего распределения, для построения математической модели загрузки рассматриваемой сети передачи данных.

Список используемых источников

1. Маршрутизатор Incarnet ViX [Электронный ресурс]: Сайт компании Incarnet. URL: http://incarnet.ru/multikanalnii_marshrutisator_dlya_avtomobilej_incarnet_vix/ (дата обращения 09.01.2019).

2. Олифер В. Г. Основы сетей передачи данных : учебное пособие. М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. 219 с. Б. ц.

3. Вентцель Е. С. Теория вероятностей : учебное пособие для вузов, 6-е изд. стер. М.: Высш. шк., 1999. 576 с.

УДК 004.057.4
ГРНТИ 49.33.29

АНАЛИЗ ПРИМЕНЕНИЯ ПРОТОКОЛА MPTCP ДЛЯ УСЛУГ ШИРОКОПОЛОСНОГО ДОСТУПА В МОБИЛЬНЫХ СЕТЯХ

В. С. Елагин, Ю. А. Невзоров

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

В данной статье предлагается решить прикладную задачу по организации канала связи для мобильного абонента с уровнем QoS необходимым для организации трансляции аудио и видео трансляции с минимальной задержкой и с максимальным уровнем качества, при нахождении абонента в условиях плотной городской застройки, без использования дорогостоящего сетевого или спутникового оборудования, при высокой загрузке сетевой инфраструктуры операторов подвижной связи.
MPTCP, TCP, агрегация данных, субпотоки.

В ситуациях, когда количество пользователей, желающих занять линий больше, чем доступно ресурсов, пропускная способность уже установленных соединений существенно уменьшается. А если учесть статистику средней скорости организации канала на территории РФ, неравномерность распределения частот между операторами и сложности с развёртыванием сетей, то становится очевидным, что необходимый уровень QoS для решения указанной задачи практически отсутствует.

Изучены средства обеспечения QoS за счёт организации многопоточного доступа с использованием агрегации каналов и маршрутов.

Исходя из условий поставленной задачи, предлагается обеспечить необходимый QoS за счёт организации многопоточного доступа в сеть Internet с использованием MultiPath TCP (MPTCP) [1].

MPTCP позволяет одновременно использовать несколько IP-адресов/интерфейсов с помощью модификации TCP, которая представляет собой обычный интерфейс TCP для приложений, и в то же время распространяет данные по нескольким потокам. Преимущества этого протокола включают лучшее использование ресурсов, лучшую пропускную способность и более плавную реакцию на сбои.

Избыточность, предлагаемая Multipath TCP, обеспечивает обратное мультиплексирование ресурсов и, таким образом, увеличивает пропускную способность TCP до суммы всех доступных каналов канального уровня вместо использования одного, как того требует простой TCP. Кроме того, Multipath TCP обратно совместим с обычным TCP.

Данная технология может быть применена как в проводных, так и в мобильных решениях, не требующая дополнительного лицензирования и соглашения с оператором.

MultiPath TCP (MPTCP) – это реализация одновременного использования нескольких IP-адресов/интерфейсов с помощью модификации TCP, которая представляет собой обычный интерфейс TCP для приложений, и в то же время распространяя данные по нескольким потокам.

Избыточность, предлагаемая Multipath TCP, обеспечивает обратное мультиплексирование ресурсов и, таким образом, увеличивает пропускную способность TCP до суммы всех доступных каналов канального уровня вместо использования одного, как того требует простой TCP.

Multipath TCP особенно полезен в контексте беспроводных сетей – использование Wi-Fi и мобильной сети является типичным вариантом использования. В дополнение к увеличению пропускной способности от обратного мультиплексирования, каналы могут быть добавлены или удалены по мере того, как пользователь, например, перемещается или выходит из зоны покрытия, не нарушая сквозного TCP-соединения. Таким образом, проблема передачи каналов связи осуществляется путем абстракции в транспортном уровне без каких-либо специальных механизмов на уровне сети или линии связи. Функциональность передачи обслуживания может быть реализована на конечных точках передачи данных, не требуя специальных функций в подсетях – в соответствии с принципом сквозного доступа в Internet.

Multipath TCP также обеспечивает преимущества производительности в средах центров обработки данных. В отличие от соединения каналов Ethernet с использованием протокола LACP, Multipath TCP может сбалансировать одно TCP-соединение на нескольких интерфейсах и достичь очень высокой пропускной способности.

MPTCP отлично подходит для агрегации каналов мобильных сетей за счёт своей гибкости. Он не требует настроек для собственного функционирования на промежуточных узлах, что делает его передачу возможной почти везде. Все современные телефоны уже являются многомаршрутными устройствами, так как обладают как минимум двумя радиоинтерфейсами. Так как большинство сетей, сервисов и услуг основаны на оригинальном протоколе TCP, MPTCP способен улучшить доступ к ним.

В мобильной индустрии данный протокол начал использоваться для быстрого перехода из сети Wi-Fi в сотовую сеть, и наоборот. Устанавливая и поддерживая два соединения одновременно, мобильное устройство могло использовать только одно, однако при ухудшении состояния используемой сети устройство автоматически переключалось на другую.

Однако в сентябре 2013 года в Южной Корее был запущен коммерческий проект GIGAPATH. При помощи агрегации данных из сотовой и Wi-

Fi сети, MPTCP позволял достичь мобильным устройствам теоретического предела скорости в 1,17 Гбит/с [2].

MPTCP работает на транспортном уровне и должен быть прозрачным для более высоких и более низких уровней. Он является набором дополнительных возможностей поверх стандартного TCP. Протокол устроен таким образом, чтобы быть применимым наследуемыми приложениями без необходимости внесения каких-либо изменений в код (рис. 1).

Рис. 1. Сравнение стеков протоколов TCP и MPTCP

– Для приложений, не работающих с MPTCP, протокол будет вести себя как протокол TCP. Продвинутые реализации могут обеспечить дополнительное управление приложениями, работающими с MPTCP. Приложение начнёт работу как обычно с формирования TCP-сокета. Процедура управления MPTCP и работа протокола зависит от конкретной программной реализации.

– Соединение MPTCP устанавливается аналогично обычному TCP-соединению.

– При доступности дополнительных маршрутов создаются дополнительные TCP-сессии, называемые «субпотоками». Они комбинируются с существующими сессиями, которые представляют собой отдельные соединения приложений. Создание дополнительной TCP-сессии осуществляется, например, между адресом А2 компьютера А и адресом Б1 компьютера Б.

– MPTCP идентифицирует несколько маршрутов при условии наличия у компьютера нескольких адресов. Комбинации этих адресов позволяет сформировать дополнительные маршруты.

– Формирование и конфигурирование субпотоков осуществляется с помощью метода управления маршрутами.

– MPTCP добавляет порядковые номера уровня соединения, чтобы при получении осуществить сборку сегментов, доставляемых по разным маршрутам с разными задержками.

– Субпотоки завершаются как регулярные TCP-соединения, посредством четырехтактного диалога FIN. MPTCP-соединение завершается с помощью флага FIN.

В роли пользовательского оборудования UE может выступать смартфон, планшет, ноутбук или любое другое устройство, требующего высокоскоростного широкополосного доступа с необходимым QoS (рис. 2). Связь с компьютером может быть осуществлена через любой доступный интерфейс (LAN, WiFi, USB) не требующий дополнительных настроек, так как транспортом служит стандартный протокол, поддерживаемый интерфейсами UE и компьютера. Связующим звеном между мобильным абонентом через сети мобильных операторов и запрашиваемым ресурсом становится второй сервер со стабильным широкополосным подключением к сети Internet, способный принимать пакеты MPTCP и демультиплексируя, пересылать их по стандартному протоколу TCP запрашиваемому ресурсу. Такая схема позволит использовать MPTCP для доступа к любым доступным ресурсам Internet через стандартный TCP.

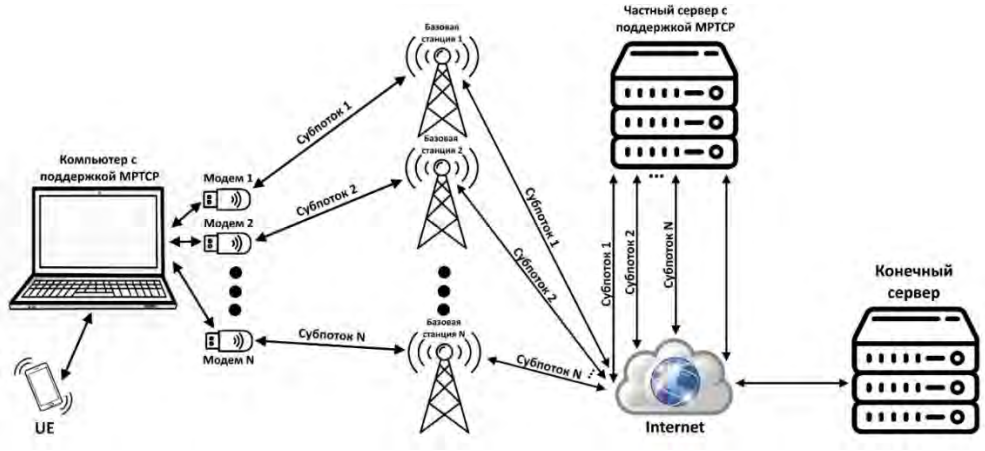


Рис. 2. Двухсерверная модель многопоточного доступа

В качестве компьютера может выступать любое устройство, способное устанавливать соединение по протоколу MPTCP и имеющее необходимое количество интерфейсов для подключения к сетям разного типа (LAN, Wi-Fi, LTE). Фактически компьютер выполняет функции сервера и обозначен таким образом, для лучшего разделения стороны абонента и конечного ресурса.

Модем в нашем случае, это одно устройство с двумя и более радиомодулями или два и более независимых модемов необходимых для обеспечения физического подключению к БС оператора. Для организации ШПД на базе MPTCP количество радиоинтерфейсов должно быть два и более, причём, чем больше одновременно будет установлено соединений, тем более высокой будет помехозащищённость и скорость передачи данных по каналу. Количество агрегированных уникальных каналов должно быть конечным. При определении количества одновременных подключений,

необходимо исходить из принципа разумной достаточности и число модемов предлагается принять равным количеству операторов, работающих в конкретном регионе тем более, что некоторые используют для предоставления услуг одни и те же физические БС, разделяя абонентов только на уровне авторизации и учёта трафика. Помимо агрегации каналов модемы могут использовать такую технологию, как MIMO. К сожалению, операторы сотовой связи на территории Российской Федерации не поддерживают технологию выше 2×2 MIMO.

Вторым сервером может выступать любое оборудование имеющее доступ к сети Internet и предоставляющее необходимую услугу или сервис, и имеющее поддержку протокола MPTCP. Фактически функции сервера аналогичны компьютеру и обозначен он, таким образом для лучшего разделения стороны абонента и конечного ресурса.

Инициализация соединения начинается с обмена SYN, SYN/ACK, ACK для каждого маршрута, подобно протоколу TCP (рис. 3). В каждом пакете содержится опция MP_CAPABLE, декларирующая способность отправителя работать с MPTCP, а также содержащая ключи отправителя и получателя. Данная опция используется только для первого субпотока, инициализации соединений в последующих субпотоках проводится без MP_CAPABLE.

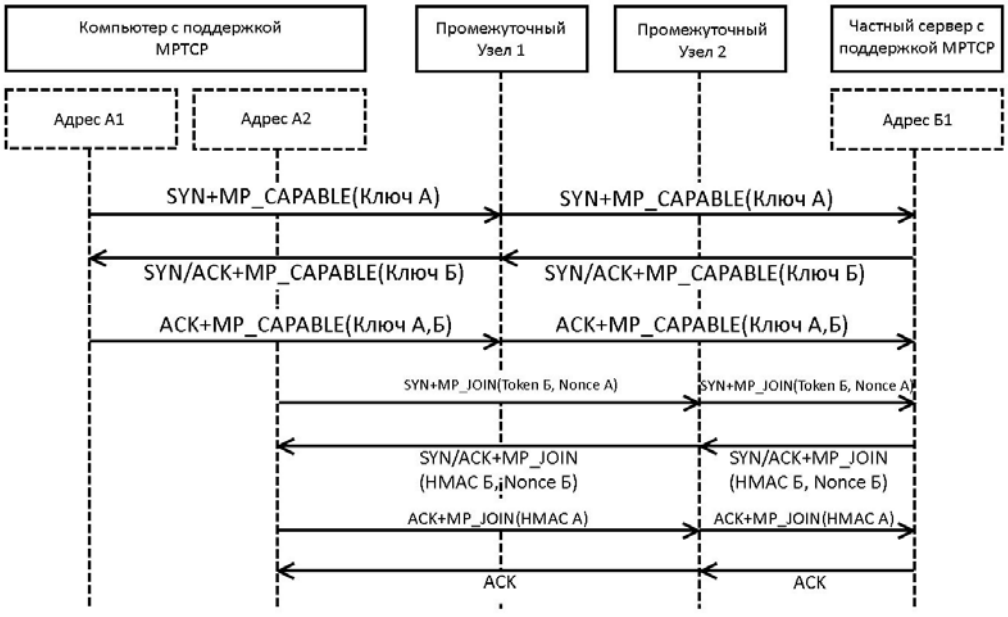


Рис. 3. Алгоритм установления соединения для двухсерверной модели

Далее формируется новый субпоток с помощью обмена SYN и опции MP_JOIN, содержащей маркер для конечного сервера и случайное число от компьютера. После это следует SYN/ACK с опцией MP_JOIN, содержа-

щей ключ HMAC и случайное число от конечного сервера. После этого компьютер отправляет ACK с опцией MP_JOIN, содержащей его HMAC. После этого следует ответ ACK от сервера.

Процедура инициализации субпотока может быть повторена при наличии дополнительных адресов у компьютера.

Конечный сервер может не поддерживать протокол MPTCP, в таком случае ответ SYN/ACK вернётся без опции MP_CAPABLE. В таком случае будет инициализировано регулярное соединение TCP.

Однако, ответ SYN/ACK может вернуться без дополнительной опции и из-за несовместимости с промежуточным узлом. Опять же, в таком случае будет инициализировано регулярное соединение TCP.

При уже установленном MPTCP соединении может возникнуть ошибка при инициализации субпотока. Так как соединение с сервером уже установлено, а сервер, поддерживающий MPTCP, отвечает на запрос SYN + MP_JOIN без данной опции, причиной ошибки является промежуточный узел. В этом случае инициализация субпотока не может быть завершена, и он закрывается с помощью команды RST.

Изучив средства организации многопоточного доступа с использованием агрегации каналов и маршрутов был проработан один из возможных вариантов решения прикладной задачи по организации канала связи для мобильного абонента с уровнем QoS необходимым для организации трансляции аудио и видео трансляции с минимальной задержкой и с максимальным уровнем качества, при нахождении абонента в условиях плотной городской застройки, без использования дорогостоящего сетевого или спутникового оборудования, при высокой загрузке сетевой инфраструктуры операторов подвижной связи (например, во время проведения массовых мероприятий).

Организация многопоточного доступа в сеть Internet с использованием MultiPath TCP (MPTCP) позволяет одновременно использовать несколько IP-адресов/интерфейсов с помощью модификации TCP, и в то же время распространяет данные по нескольким потокам. Очевидными преимущества этого протокола является лучшее использование ресурсов, лучшая пропускную способность и более плавная реакция на сбои.

Избыточность, предлагаемая Multipath TCP, обеспечивает обратное мультиплексирование ресурсов и, таким образом, увеличивает пропускную способность TCP до суммы всех доступных каналов канального уровня вместо использования одного, как того требует простой TCP.

Список используемых источников

1. Ford A., Raiciu C. Architectural Guidelines for Multipath TCP Development / RFC 6182, 2011. 28 p.

2. Bagnulo, M. Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses / RFC 6824, 2013. 64 p.

УДК 004.51
ГРНТИ 81.93.29

ОБЗОР МЕТОДОВ ЧЕЛОВЕКО-МАШИННОГО ВЗАИМОДЕЙСТВИЯ В СИСТЕМАХ ПРОТИВОДЕЙСТВИЯ СОМНИТЕЛЬНОЙ И НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ

К. Н. Жернова, М. В. Коломеец, А. А. Чечулин

Санкт-Петербургский институт информатики и автоматизации Российской Академии Наук

В различных системах противодействия сомнительной и нежелательной информации могут использоваться различные способы представления результатов и человеко-машинного взаимодействия с полученной информацией. Данные методы используются для управления данными и осуществления таких операций как фильтрация и акцентирование определенных областей данных для пользователя. В работе будут рассмотрены основные способы человеко-машинного взаимодействия, применяемые в таких программно-аппаратных средствах противодействия сомнительной и нежелательной информации как системы родительского контроля, системы определения репутации информационного ресурса и системы классификации веб-ресурса. В работе также производятся их сравнительный анализ и рекомендации по использованию.

человеко-машинное взаимодействие, информационная безопасность, системы противодействия сомнительной и нежелательной информации, пользовательские интерфейсы, графический пользовательский интерфейс, текстовый пользовательский интерфейс.

В настоящее время возрастает количество передаваемой информации, а также всевозможных способов её передачи [1]. Таким образом, возрастает важность противодействия сомнительной и нежелательной информации. Появляются программные средства, которые фильтруют поступающую информацию, классифицируют web-ресурсы и оценивают их репутацию. Большая популярность этих средств повысила актуальность проблемы человеко-машинного взаимодействия в данной области.

Подобные программные средства можно разделить на несколько групп: системы родительского контроля, системы определения репутации информационных ресурсов, системы классификации веб-ресурсов. Данные виды программного обеспечения (далее ПО) обычно фокусируют внимание пользователя на определённых данных и фильтруют запускаемые программы и/или информационные ресурсы по различным признакам. Эти группы ПО будут рассмотрены ниже.

Системы родительского контроля

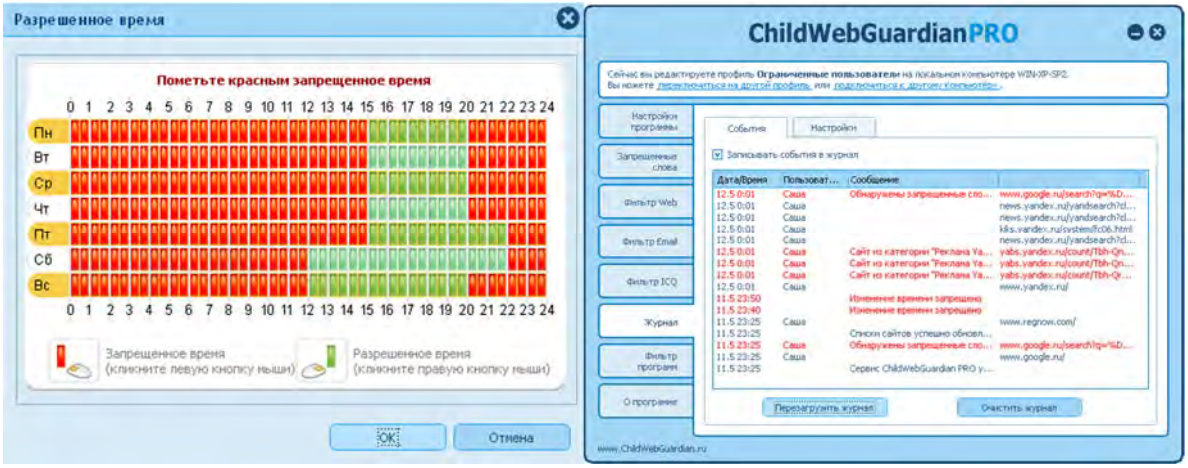
Такие системы предназначены для фильтрации информации, поступающей к несовершеннолетнему, а также контроля над тем, какие сайты, информационные ресурсы он посещает и какие программы запускает. ПО родительского контроля оснащены богатым набором функций, таких как контроль времени использования Интернета, контроль запуска игр, настройка списков запрещённых сайтов, геолокация и перехват сообщений. Однако с точки зрения человеко-машинного взаимодействия и визуализации информации особенный интерес представляет разнообразная фильтрация (web-ресурсов, разрешённых программ, разрешённых почтовых адресов и т. д.) и способ выдачи обработанной информации пользователю.

В качестве примера систем родительского контроля рассматривались программы ChildWebGuardian PRO [2], ESET Parental Control [3].

Фильтрация. Фильтрация чаще всего происходит по определённым словам, встречающимся на web-ресурсах. Также существует возможность заблокировать определённые адреса страниц и номера мессенджеров. В процессе настройки и эксплуатации ПО ChildWebGuardian PRO пользователь может переключаться между вкладками «Запрещённые слова», «Фильтр Web», «Фильтр Email», «Фильтр программ» и «Журнал». Запрещённые слова выделяются галочками в чекбоксах, web-страницы, электронные адреса и номера ICQ записываются вручную.

Акцентирование определённых областей данных. Разрешённое время использования тех или иных программ задаётся с помощью интерактивной диаграммы (рис. 1, а), при этом сами программы выбираются в диалоговом окне. Время, проведённое в различных приложениях, может иметь визуализацию тепловой карты (например, в приложении ESET *Parental Control*). Наиболее важными данными являются события, связанные с попытками нарушения заданных правил, по этой причине они выделяются красным цветом (рис. 1, б). Таким образом, человеко-машинное взаимодействие осуществляется как на графическом, так и на текстовом уровне. В данном случае использованы простые визуальные модели (тепловая карта и выделение текста цветом).

Рекомендации. С целью повышения наглядности полученных результатов и облегчения работы с ними можно ввести в подобные системы подходящие визуальные модели. Например, по собранной статистике посещённых сайтов строить круговую диаграмму, выражающую процентное соотношение различных категорий просмотренных сайтов.



а) б)

Рис. 1. Интерфейс ПО Child Guardian Pro [2]:
интерактивная диаграмма разрешённого времени (а), журнал событий (б)

Системы определения репутации информационных ресурсов

Репутационные системы часто имеют вид веб-сайтов, которые показывают время создания домена, местоположение IP-адреса, пользовательский рейтинг доверия и репутацию сайта. Анализ исследуемого сайта проводится на основе таких технологий как каталоги поисковых систем (например, каталоги Яндекс), Safe Brousing (сервис Google) и т. п. Также многие системы определения репутации используют сеть Web of Trust, которая формирует репутацию ресурсов на основе пользовательских отзывов.

Фильтрация. Поисковые системы также предлагают свои собственные сервисы для проверки сайтов. Google Safe Browsing, Яндекс.каталог. В данном случае со стороны пользователя не требуется никаких действий: поисковые системы понижают рейтинг недоверенных сайтов, и эти сайты просто не появляются на первой странице выдачи. Некоторые браузеры, например, FireFox или Opera, имеют специальные расширения для определения репутации сайта (рис. 2).

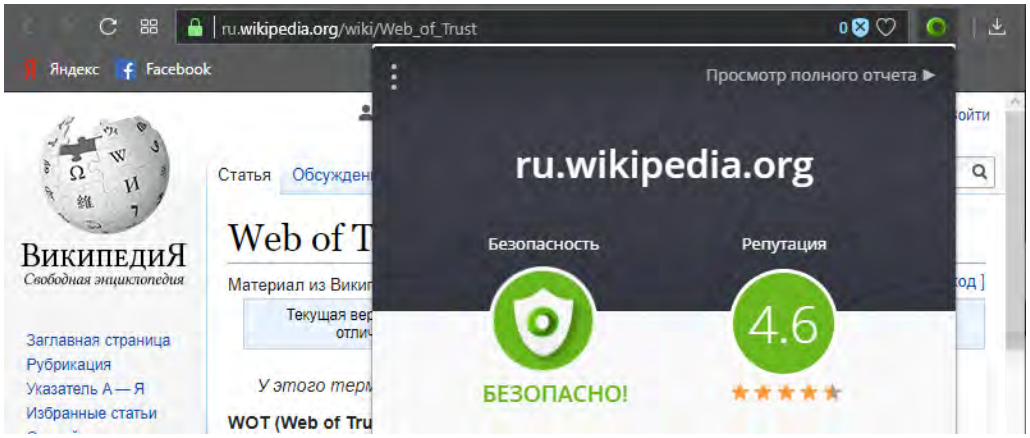


Рис. 2. Интерфейс расширения Web of Trust для браузера Opera

Акцентирование определённых областей данных. В специальное поле вводится адрес сайта, уровень доверия указывается в баллах (на основе голосов), используются интуитивно понятные цветовые обозначения: низкий уровень доверия обозначается пиктограммой красного цвета, при высоком уровне доверия пиктограмма становится зелёной. Некоторые антивирусные программы проверяют адреса сайтов после ввода ссылки в соответствующее поле и нажатия кнопки запуска проверки.

Рекомендации. Очевидный недостаток системы на основе Web of Trust – возможность искусственно понизить или повысить рейтинг определённого web-ресурса путём оставления нужного количества отрицательных/положительных отзывов. Такие системы как Яндекс.каталоги и фильтрация в Google более надёжны, так как основаны на более объективных признаках: дата создания, посещаемость, уникальность контента, правильность ссылок и т. д. Расчёт репутации web-ресурса по таким объективным признакам повысит надёжность системы.

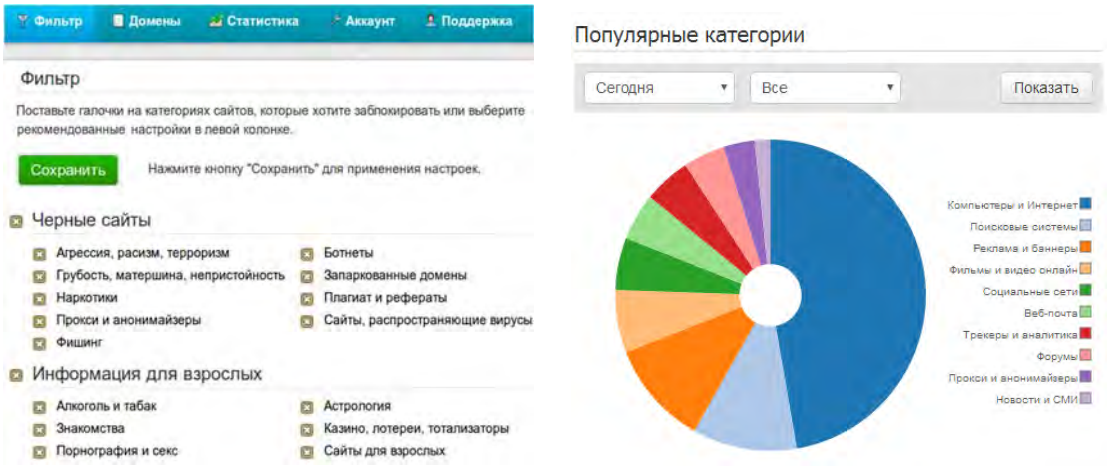
Системы классификации веб-ресурсов

Классификация интернет-ресурсов может осуществляться с помощью различных программных средств. Например, в рассмотренных ранее системах родительского контроля сайты классифицировались и фильтровались по запрещённым словам. Классификация производилась на простой основе («Игры», «Спорт», «Социальные сети» и т. д.). Также классификация сайтов выполняется с помощью таких программных средств информационной безопасности как SkyDNS и Kaspersky Endpoint Security. Эти приложения позволяют ограничить доступ пользователей к веб-ресурсам с определённым содержанием.

Фильтрация. Kaspersky Endpoint Security разделяет сайты по следующим категориям [5]: «для взрослых», «программное обеспечение, аудио, видео», «алкоголь, табак, наркотические и психотропные вещества», «насилие», «нецензурная лексика», и т. д. При этом некоторые категории могут пересекаться друг с другом. SkyDNS разделил сайты на большие группы («чёрные сайты», «информация для взрослых», «пожиратели трафика», «пожиратели времени», «прочие сайты»), внутри каждой из которых находятся более мелкие подгруппы (рис. 3а). Как в Kaspersky Endpoint Security, так и в SkyDNS взаимодействие осуществляется путём отметки чекбоксов напротив необходимых пунктов. Можно заблокировать всю категорию полностью, поставив галочку в соответствующий чекбокс, либо выбирать аналогичным образом определённую тематику.

Акцентирование определённых областей данных. Обработанные статистические данные могут быть представлены в виде графиков и диа-

грамм (рис. 3б). Однако, по таким графикам сложно оценить реальное процентное соотношение разных групп просмотренных сайтов. Например, очевидно, что сайты, посвящённые компьютерам и интернету, более популярны, чем новостные ресурсы. Однако сложно определить количественную разницу между социальными сетями и сайтами по аналитике.



а) б)

Рис. 3. Интерфейс ПО SkyDNS:
фильтрация в SkyDNS (а), визуализация полученной информации (б) [4]

Рекомендации. Следует создать унифицированную классификацию, сделать единые правила составления подобных классификаций с одинаковыми или сходными названиями групп, при разработке приложений использовать похожие дизайнерские решения в целях повышения удобства использования продукта.

Выводы

Каждое из рассмотренных программных средств обладает графическим интерфейсом, что делает работу интуитивно понятной. Однако, во многих приложениях слабо выражена визуализация обработанных данных. По этой причине в некоторых случаях всё ещё приходится осуществлять визуальный поиск необходимых данных, что усложняет работу с приложением.

Также каждое приложение обладает собственным набором критериев фильтрации и классификации, что усложняет переход пользователя с одного приложения на другое.

Работа выполнена при частичной финансовой поддержке РНФ (проект 18-11-00302).

Список используемых источников

1. Коломеец М. В., Чечулин А. А., Котенко И. В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Т. 5. №. 42. С. 232-257.

2. Сетевые возможности ChildWebGuardian PRO [Электронный ресурс]: Интернет фильтр ChildWebGuardian PRO, 2016. URL: http://childwebguardian.ru/network/index.html (дата обращения 09.02.2019).

3. Protect your family with ESET Parental Control [Электронный ресурс]: ESET Parental Control, 2008. URL: https://www.eset.com/us/parental-control/ (дата обращения 10.02.2019).

4. Блокировка сайтов по категориям [Электронный ресурс]: SkyDNS – Безопасный интернет для вашего дома и бизнеса, 2010. URL: https://www.skydns.ru/skydns-rukovodstvo-3/ (дата обращения 15.02.2019).

5. Категории веб-контроля в Kaspersky Endpoint Security 10 для Windows [Электронный ресурс]: Лаборатория Касперского, 2019 URL: https://support.kaspersky.ru/11971 (дата обращения 20.02.2019).

УДК 004.421
ГРНТИ 28.23.37

СЕМАНТИЧЕСКАЯ СЕГМЕНТАЦИЯ СИНТЕТИЧЕСКИХ ИЗОБРАЖЕНИЙ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ АРХИТЕКТУРЫ U-NET

А. А. Зарубин, Е. В. Каляшов, А. Р. Коваль, А. В. Тарлыков

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

В статье исследуется вопрос использования свёрточной нейронной сети на основе архитектуры U-Net для семантической сегментации объектов разных классов на изображениях в условиях произвольной фоновой составляющей. Рассмотрены вопросы подготовки обучающего набора с использованием синтетических данных, описан процесс обучения нейронной сети, приведены результаты моделирования.

свёрточная нейронная сеть, семантическая сегментация, обучение, подготовка данных.

В ходе работы исследовалась возможность использования свёрточной нейронной сети на основе архитектуры U-Net [1] для семантической сегментации изображений объектов поверх неизвестного фонового изображения. В качестве целевых изображений объектов выступали проекции трёхмер-

ных объектов летательных аппаратов, получаемые с использованием специально разработанного программного обеспечения [2], настроенного для проецирования от одного до четырёх различных объектов на каждое изображение, параллельно приложение обеспечивало построение бинарных масок фона и отдельных масок для изображения каждого объекта. В дальнейшем маски были объединены в массивы NumPy [3], где на маску конкретного класса отводился один соответствующий бит в каждом элементе массива. При использовании массива типа uint8 появляется возможность работы с восемью масками одновременно, что соответствует классу фона и семи классам объектов. При этом обеспечивается возможность сопоставлять каждому пикселю тестового изображения несколько классов путём одновременного выставления нескольких бит в единичное состояние.

Процесс генерация обучающих изображений и масок всех классов производился с использованием следующих типов объектов – A6M2N, BOEIN707, EA_6B, FW3FL, BUCCANE, HARR, KA25. В качестве фона было использовано 27 изображений облаков, земли и строений, при генерации использовалась аугментация фонов – отражения, деформации, вариации цвета [4]. Указанным образом для обучения сети были подготовлен обучающий набор изображений с проекциями летательных аппаратов семи классов, для каждого изображения количество проекций варьировалось, все проекции в рамках одного изображения смещались друг относительно друга на случайные расстояния. Полученный таким образом совокупный обучающий набор составил 16 000 изображений, из них 14 400 изображений использовалось для обучения и 1 600 – для проверки (рис. 1).

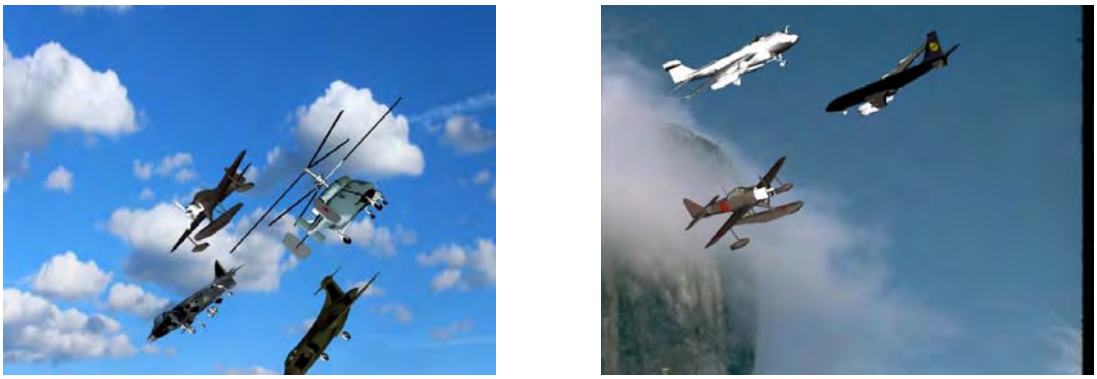


Рис. 1. Пример изображений, использовавшихся для обучения

Базовая архитектура сети U-Net была доработана для поддержки изображений необходимого размера (1024×768 пикселей) и модифицирована таким образом, чтобы на выходе вместо одиночной бинарной маски получить требуемый набор масок для всех классов. Для этого финальный свёрточный слой был настроен на выдачу восьми выходных каналов. Обучение прово-

дилось в течение 15 эпох, в качестве функции подобия выступал коэффициент Дайса [5] – отношения истинных и предсказанных масок объектов для каждого изображения из обучающего набора. Результаты сегментации на нескольких вариантах тестового набора приведены в таблице.

ТАБЛИЦА. Качество сегментирования (к-т Дайса),
1 –исходный тестовый набор, 2 – набор с удалением наложения объектов
и пустых изображений, 3 – набор с альтернативными фоновыми изображениями

Тестовый набор	Минимальное	Максимальное	Среднее	Стандартное отклонение
1	0,358	1,0	0,956	0,270
2	0,543	0,998	0,971	0,177
3	0,894	0,998	0,982	0,050

Примеры сегментации представлены на рис. 2. Можно отметить, что основные проблемы с неверной классификацией наблюдались при сегментации объектов с наложенными проекциями, пример подобных ошибок приведён на рис. 3, результаты проверки на тестовом наборе с исключением пересечений в проекциях также приведены в таблице. Следует отметить, несмотря на неверную классификацию в местах пересечения проекций, отделение объектов от фона выполняется качественно и соответствует контуру объекта.

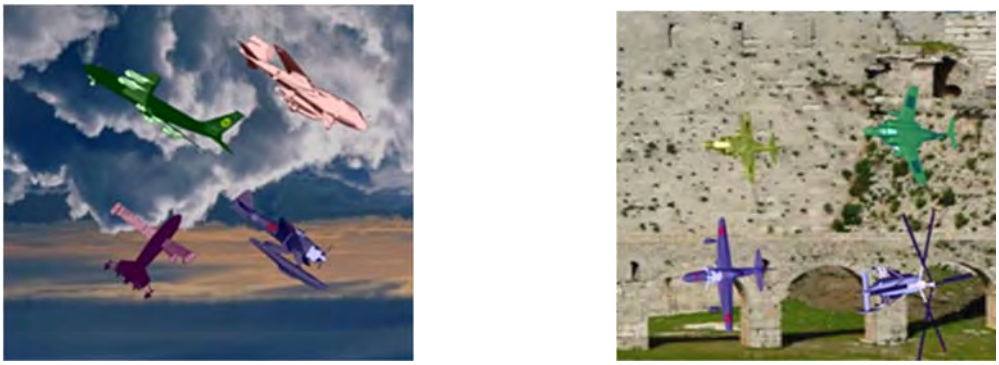


Рис. 2. Пример сегментации изображений с базовыми фонами

В качестве оценки наличия пересечения объектов и причисления части пикселов к нескольким классам был предложен следующий подход. Из предсказанной маски (по всем классам) отбирается класс с наибольшим количеством предсказанных пикселей (за исключением фона) и классы, для которых количество предсказанных пикселей превышает 5 % от количества для максимального класса. Все полученные классы считаются значимыми и для них попарно производится расчёт коэффициента Дайса. Значе-

ние коэффициента более 0,05 является признаком наложения соответствующих объектов, когда наблюдается неверная классификация части пикселей. В случае качественной сегментации значение коэффициента не превышают величины 0,001. С использованием данного подхода, появляется косвенный способ оценки пересечений без использования оригинальных масок, что позволяется анализировать качество сегментации не только синтетических кадров, но и реальных, для которых зачастую отсутствуют точные маски объектов.

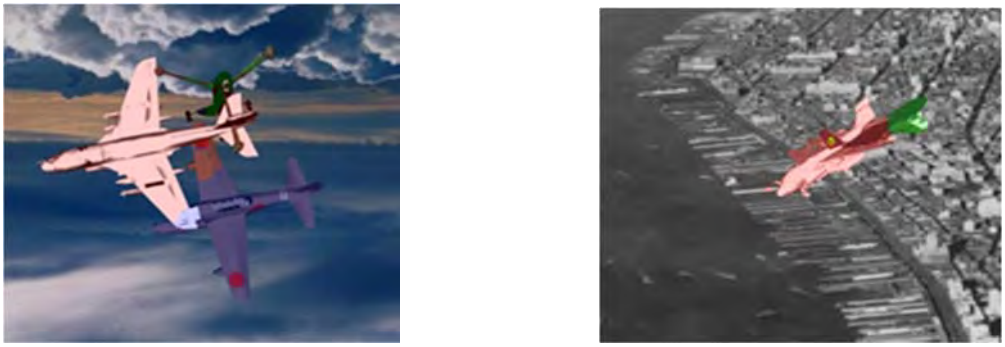


Рис. 3. Пример сбоя классификации при наложении объектов

В качестве отдельного эксперимента был дополнительно подготовлен тестовый набор с фоновыми изображениями, не использовавшимися при обучении. Оценки качества сегментации приведены в таблице (набор №3), пример сегментации приведён на рис. 4.

Рис. 4. Пример сегментации изображений с альтернативными фонами

Подавая на вход сети реальные изображения с объектами неизвестных классов (рис. 5) можно видеть, что, потеряв способность правильно классифицировать объекты (подобные класс отсутствовал на этапе обучения) сеть, тем не менее, достаточно качественно выделяет класс фона или, иными словами, сегментирует объекты поверх класса фон.

На том же рис. 5 можно видеть пёстрые маски для неверно сегментированных объектов, что можно трактовать как наличие пересечений известных сети классов. Данная ситуация хорошо диагностируется предложенным выше подходом с расчётом показателя пересечений, что позволяет в автоматическом режиме определять сбой сегментации.

Рис. 5. Сравнение изображения и выделенных масок для случая реального изображения

Полученные результаты позволяют сделать вывод, что использование архитектуры U-Net для семантической сегментации вполне оправданно, но в ряде случаем архитектура может потребовать ряд доработок.

Список используемых источников

1. Olaf Ronneberger, Philipp Fischer, Thomas Brox. U-Net: Convolutional Networks for Biomedical Image Segmentation [Электронный ресурс]. Электрон. текстовые дан. 2015. Режим доступа: https://arxiv.org/abs/1505.04597, свободный. Загл. с экрана. Яз. англ.

2. Каляшов Е. В., Савельева А. А., Тарлыков А. В. Использование синтетических данных для обучения нейронной сети классификации летательных аппаратов // 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.432–437.

3. NumPy [Электронный ресурс]. Электрон. дан. 2018. Режим доступа: http://www.numpy.org/, свободный. Загл. с экрана. Яз. англ.

4. Aysegul Dundar, Ignacio Garcia-Dorado. Context Augmentation for Convolutional Neural Networks [Электронный ресурс]. Электрон. текстовые дан. 2017. Режим доступа: https://arxiv.org/abs/1712.01653, свободный. Загл. с экрана. Яз. англ.

5. Sørensen–Dice_coefficient [Электронный ресурс]. Электрон. дан. 2018. Режим доступа: https://en.wikipedia.org/wiki/Sørensen–Dice_coefficient, свободный. Загл. с экрана. Яз. англ.

УДК 004.725.7
ГРНТИ 49.33.01

ИСПОЛЬЗОВАНИЕ МОДЕЛЬНЫХ СЕТЕЙ ДЛЯ СОКРАЩЕНИЯ СРОКОВ ПРОЕКТИРОВАНИЯ

М. В. Захаров, Р. В. Киричек, Е. А. Сафронова, К. А. Тимец

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

Значительную часть времени проектирования комплексов телекоммуникационного оборудования занимает процесс конфигурации самого оборудования согласно требованиям ТЗ. Для сокращения времени конфигурации оборудования и, соответственно, сроков проектирования, предлагается использовать модельные сети для эмуляции разрабатываемых виртуальных комплексов телекоммуникационного оборудования с возможностью выгрузки файлов конфигурации. В качестве среды для эмуляции рассматривается эмулятор EVE-NG.

модельные сети, проектирование сетей связи, EVE-NG.

Проектирование – процесс определения архитектуры, компонентов, интерфейсов и других характеристик системы или её части. В области телекоммуникаций зачастую производится проектирование как отдельных сетевых узлов – комплексов технических средств, так и целых сетей или их отдельных сегментов.

При проектировании значительную часть времени опытно-конструкторских и пуско-наладочных работ занимает процесс конфигурации самого оборудования согласно требованиям, изложенным в ТЗ [1, 2]. Часто бывает так, что сотрудники раньше не сталкивались с тем оборудованием, с которым необходимо работать в рамках выполнения НИР и ОКР. Поэтому после получения оборудования прежде чем приступать к его конфигурации согласно требованиям ТЗ некоторое время тратится на его изучение. Часто бывает так, что сроки НИР и ОКР затягиваются в результате срыва сроков поставки оборудования или внесения корректировок в ТЗ со стороны заказчика.

Для сокращения времени конфигурации оборудования, а значит и сроков проектирования, авторами предлагается использовать модельные сети для эмуляции разрабатываемых комплексов телекоммуникационного оборудования с возможностью выгрузки файлов конфигурации [3].

В качестве среды для эмуляции рассмотрим эмулятор EVE-NG [4, 5]. EVE-NG (*Emulated Virtual Environment – Next Generation*) – это свободно распространяемая мульти-вендорная многопользовательская платформа,

которая позволяет эмулировать в виртуальной среде различные типы сетевого оборудования: маршрутизаторы, коммутаторы, устройства безопасности и многое другое. Свободно распространяемая версия EVE-NG Community Edition позволяет эмулировать до 63 экземпляров оборудования одновременно, что вполне достаточно для эмулирования даже достаточно больших проектов. EVE-NG обеспечивает эмуляцию оборудования различных типов большого числа производителей: Juniper, Extreme, Fortinet, HP, Checkpoint, Palo Alto, Arista, Alcatel, Citrix, а также нескольких операционных систем – MS Windows, Linux.

В качестве эксперимента авторами была разработана виртуальная модельная сеть, представляющая собой упрощенную телекоммуникационную инфраструктуру структурированной кабельной системы типового здания. Для построения сети была выбрана классическая древовидная топология. В сети представлены следующие узлы: персональные компьютеры пользователей (PC-1 – PC-N1), коммутаторы доступа (уровень L2) и маршрутизатор уровня ядра (L3). Топология разработанной виртуальной сети представлена на рис. 1.

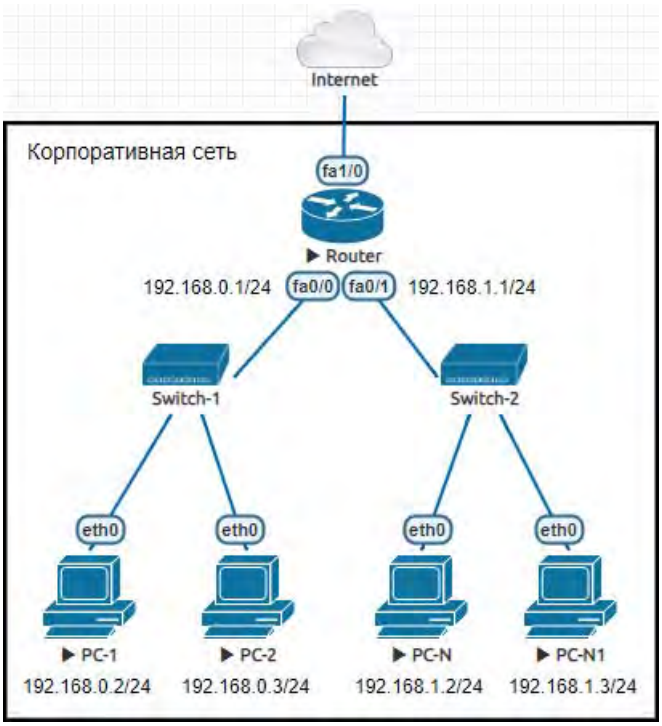


Рис. 1. Топология телекоммуникационной инфраструктуры СКС

Разработанная топология является упрощенной, реализация дополнительных сервисов (VPN, ACL, NAT и т. д.) не производилась, т. к. главной целью исследования была проверка возможности эмуляции сетевого оборудования, а также – возможность экспорта конфигурации для её последующего использования на реальном оборудовании.

На рис. 2 показан экспорт конфигурации эмулируемого маршрутизатора из EVE-NG:

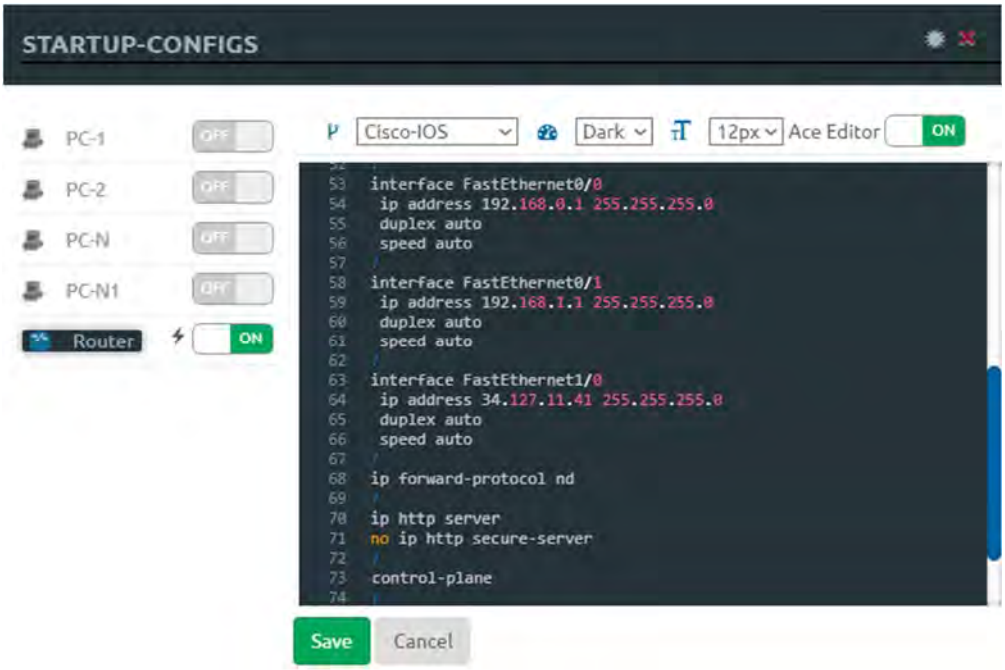


Рис. 2. Экспорт конфигурации

В результате проведенных исследований было установлено, что с помощью эмулятора EVE-NG возможно организовать подготовку персонала телекоммуникационной компании по работе с оборудованием требуемого производителя, а также использовать сконфигурированное в EVE-NG оборудование для экспорта файлов конфигурации. Полученные в результате работы конфигурационные файлы целесообразно использовать в процессе разработки телекоммуникационных сетей и/или комплексов телекоммуникационного оборудования с для сокращения сроков проектирования.

Список используемых источников

1. Семенов А. Б. Проектирование и расчет структурированных кабельных систем и их компонентов. М. : ДМК Пресс, М. : Компания АйТи, 2005.

2. Семенов А. Б. Проектирование и расчет структурированных кабельных систем и их компонентов. М. : ДМК Пресс; М. : Компания АйТи, 2010. 416+16 с.: ил.

3. Максан М. Полная и комплексная виртуализация сетевых функций // Вестник связи. 2016. № 1.

4. Захаров М. В., Киричек Р. В., Кучерявый А. Е. Виртуальные модельные сети на базе эмулятора UNETLAB // 72-я Всероссийская научно-техническая конференция, посвященная Дню радио. 2017. С. 183–185.

5. Захаров М. В., Киричек Р. В. Использование программного обеспечения EVE-NG для эмуляции телекоммуникационного оборудования при обучении студентов // 73-я Всероссийская научно-техническая конференция, посвященная Дню радио. 2018. С. 211–212.

УДК 004.056.5
ГРНТИ 50.41.27

ПОДХОД К АНАЛИЗУ БЕЗОПАСНОСТИ ПРОГРАММНОГО КОДА С ПОЗИЦИИ ЕГО ФОРМЫ И СОДЕРЖАНИЯ

К. Е. Израилов, И. М. Татарникова

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

В статье предлагается подход к исследованию уязвимостей программы, основанный на представлениях жизненного цикла последней, а также на философских категориях – форма и содержание. Выделяются статические и динамические свойства уязвимостей, полученные в результате анализа. Описываются предпосылки к возникновению качественно новых эффектов от взаимодействия нескольких уязвимостей в программе. Приводится пример одного из таких эффектов с позиции антропоморфизма, а именно «паразитизм» одной уязвимости над другой.

информационная безопасность, уязвимость, программный код, представление программы, жизненный цикл, антропоморфизм, форма, содержание.

Введение

В современном мире IT-технологии заняли прочное место, привнеся множество положительных эффектов практически во все сферы жизнедеятельности. Тем не менее, одной из негативных сторон технологии можно считать растущее из года в год количество нарушений информационной безопасности (ИБ), большая часть которых возникает по вине небезопасного программного обеспечения (ПО). Основная причина этого заключается в наличии уязвимостей в ПО, при этом как возникающих случайно, так и создаваемых злонамеренно. Результативное им противодействие требует использования основательной научной базы, которая на данный момент построена еще недостаточно. Критичность же реализации угроз вынуждает экспертов ИБ лишь создавать новые методы и средства противодействия уже существующим уязвимостям, оставаясь при этом в запаздывающем (а значит и мало результативном) состоянии перед новыми, постоянно возникающими и эволюционирующими уязвимостями.

Причиной такого медленного построения научной базы ИБ в аспекте уязвимостей ПО отчасти является то, что большинство научных исследований опирается на достаточно статические модели безопасности программного кода (исходного, машинного, байт-кода и др.), не касаясь динамических свойств уязвимостей в течении всей их жизни – возникновение,

развитие, мутация, исчезновение и пр. (например, [1, 2, 3]). В данной статье предлагается подход к рассмотрению уязвимостей на всем их жизненном пути, опираясь на философские категории Форма vs Содержание и абстрагируясь тем самым от конкретных реализаций уязвимостей в программном коде.

Представления программы

Поскольку уязвимость, как сущность, не может существовать вне программного кода, то для исследования ее жизненного цикла необходимо рассмотреть процесс разработки ПО, в котором она в некоторый момент появляется. Так, с точки зрения авторов [4], любая программа от своего зарождения до конечной реализации последовательно проходит через следующие представления: Идея – образ будущей программы у ее создателя; Концептуальная модель – абстрактная модель программы с основными понятиями и их взаимосвязью; Архитектура – схема деления программы на структурные элементы и пути их реализации; Алгоритмы – деление на подпрограммы с описанием логики их работы с помощью формализованных алгоритмов; Исходный код – реализация алгоритмов подпрограмм на заданном языке программирования; Ассемблерный код – описание алгоритмов подпрограмм на языке инструкций процессора исполнения; Машинный код – бинарное представление программы в виде инструкций процессора; Файл образа (иногда отсутствует) – бинарное представление программы в виде файла-контейнера для развертывания на устройстве.

Необходимо отметить, что предложенное деление на представления верно только для случая разработки ПО на императивных языках программирования с получением инструкций реального процессора исполнения (а, например, не байт-кода для виртуальной машины).

Категории Формы и Содержания

Для последующего исследования представлений применим к ним философские категории Формы и Содержания следующим образом – под первой будем понимать базовые элементы для описания программы в каждом представлении (например, язык программирования), а под второй – саму *суть* программы в этом представлении (например, код программы на языке программирования).

Анализ особенностей и закономерностей предложенных представлений программы позволяет сделать следующие выводы. Во-первых, по мере прохождения представлений, программа переходит от человеко-ориентированной формы (Идея) к машинно-ориентированной (Код). Во-вторых, мощность Формы (по аналогии с множествами характеризующая количество

ее элементов) убывает. Так, для описания Идеи, Форма представления сопоставима с разговорным языком, Алгоритмы имеют более формализованный вид и существенно меньший размер, а текст Исходного кода программы состоит из элементов языка программирования и пользовательских названий. В-третьих, противоположно Форме, мощность Содержания будет расти. Так, Идея может быть описана в нескольких предложениях, программа разбита на множество Алгоритмов подпрограмм с фразами в их элементах, а Исходный код опишет каждый элемент Алгоритма в виде множества строк кода. И, в-четвертых, Содержание программы не меняется от перехода между представлениями – то есть оно в конечном (Машинный код, Файла образа) и начальном (Идеи) представлении совпадает. Это, в том числе, обосновывает возможность и обратного преобразования представлений с сохранением Содержания – так называемый *реверс-инжиниринг*; для этого, в частности, предназначены авторский метод и прототип программного средства [5, 6, 7].

Безопасность программы

Применим выводы, сделанные по предложенным представлениям программы, в аспекте возможных нарушений ИБ. Во-первых, уязвимость может появиться в любом из представлений программы, кроме первого, являясь дефектом Содержания представления в его Форме (Идею можно считать идеальной, не содержащей уязвимостей, поскольку именно такое Содержание изначально и задумывал создатель). С этой точки зрения уязвимостью, появившейся в некотором представлении, можно считать различие Содержаний этого (N) и предыдущего (N–1) представления; естественно, их Формы будут различны. Во-вторых, уязвимость в представлении N, являясь частью его Содержания, остается и во всех последующих представлениях (N+1, N+2, …). И, в-третьих, поскольку мощность Содержания программы в процессе разработки увеличивается, то мощность части Содержания уязвимости также будет расти.

Исходя их вышесказанного можно сделать следующий важный вывод (Вывод): уязвимость, появившаяся в одном из начальных представлений, будет иметь существенно б***о***льшую мощность Содержания в конечном представлении программы. А исходя из очевидной сложности и нелинейности преобразований между представлениями, эта уязвимость окажется в некотором смысле *размазанной* по конечному представлению. В качестве одного из значимых примеров этого можно привести высокоуровневую уязвимость в Архитектуре программы [8] – выбор устаревшего механизма защиты, которая в Машинном коде будет представлять из себя использование множества устаревших библиотек и алгоритмов защиты, слабых к атакам.

Интереснейшим с научной и практической точек зрения является изучение различных эффектов взаимодействия уязвимостей, находящихся в одной программе. При этом, если их взаимодействие в общем представлении, в котором они были созданы, достаточно хорошо прогнозируемо (например, два слабых архитектурных модуля защиты приведут к приблизительно удвоенному ослаблению защиты и в представлении Машинного кода), то создание уязвимостей в каждом из представлений может давать непредсказуемые эффекты ИБ при выполнении готовой программы. Причина этого как раз следует из предыдущего Вывода – одна уязвимость в раннем представлении может иметь вид множества элементов Содержания, разбросанных по конечному представлению, часть из которых в совокупности с элементами других уязвимостей приведет к качественно новым эффектам, не проявляющимся в случае отдельных уязвимостей. При этом эффекты могут иметь как положительный (синергетический), так и отрицательный (дисинергетический) суммарный эффект. Необходимо отметить, что подобная ситуация достаточно распространена для всей IT-сферы [9, 10].

Приведем пример взаимодействия двух уязвимостей, эффект которого с позиции антропоморфизма (аналогично [11]) может быть назван термином «паразитизм» – отношение в живой природе между организмами паразита и хозяина (первый использует второго в качестве источника питания и/или среды обитания, возлагая на него регуляцию своих отношений с внешней средой). Предположим, в представление Архитектуры внесена случайная уязвимость, заключающаяся в периодической широковещательной рассылке «мусорных» сетевых пакетов во внешнюю сеть – угрозу ИБ от реализации уязвимости можно считать несущественной. Также, в исходный код внесена злонамеренная уязвимость, которая компрометирует пароли пользователей путем их перехвата и добавления к телу произвольного сетевого пакета (предположим, код уязвимости не имеет прав для непосредственной отправки пакета на адрес злоумышленника) – угроза ИБ в этом случае хотя и более существенна, однако только для случая взаимодействия программы с внешней сетью. И если по отдельности эти уязвимости могут себя никак не проявить, то их взаимодействие в конечном представлении приведет к эффекту паразитизма – вторая уязвимость, используя первую, будет отправлять во внешнюю сеть перехваченные пароли; последние очевидно могут быть перехвачены злоумышленником, что будет критично для ИБ.

Естественно, возможны и иные формы взаимодействия уязвимостей, приводящие как к нейтральному, так и к положительному влиянию на безопасность программы.

Заключение

Анализ процесса разработки ПО и жизненного цикла программ, а также применение к ним категориального деления на Форму и Содержание позволил сделать ряд выводов, описывающих статические и динамические свойства уязвимостей. Это дает возможность рассматривать последнюю не просто, как часть программного кода (зачастую определяемую субъективно экспертом ИБ), а в качестве элемента множества, имеющего определенную точку рождения, динамику развития и эффекты взаимодействие с элементами других уязвимостей.

И хотя предложенный подход еще далек от конкретной практической реализации и применения в интересах обеспечения ИБ, тем не менее его уже можно считать шагом на пути формализации этой важнейшей области, а значит и потенциального построения крепкой научной базы.

Список используемых источников

1. Шудрак М. О., Золотарев В. В. Модель, алгоритмы и программный комплекс автоматизированного поиска уязвимостей в исполняемом коде // Труды СПИИРАН. 2015. № 5 (42). С. 212–231.

2. Торшенко Ю. А. Модель и метод обнаружения уязвимостей на начальных этапах промышленного проектирования программного продукта : дисс. ... канд. техн. наук: 05.13.19 / СПб., 2008. 104 с.

3. Цыганенко Н. П. Статический анализ кода мобильных приложений как средство выявления его уязвимостей // Труды БГТУ. №6. Физико-математические науки и информатика. 2015. № 6 (179). С. 200–203.

4. Buinevich M., Izrailov K., Vladyko A. The life cycle of vulnerabilities in the representations of software for telecommunication devices // 18th International Conference on Advanced Communications Technology (ICACT-2016). 2016. PP. 430–435.

5. Буйневич М. В., Израилов К. Е. Метод алгоритмизации машинного кода телекоммуникационных устройств // Телекоммуникации. 2012. № 12. С. 2–6.

6. Буйневич М. В., Израилов К. Е. Автоматизированное средство алгоритмизации машинного кода телекоммуникационных устройств // Телекоммуникации. 2013. № 6. С. 2–9.

7. Израилов К. Е., Покусов В. В. Утилита для поиска уязвимостей в программном обеспечении телекоммуникационных устройств методом алгоритмизации машинного кода. Часть 3. Модульно-алгоритмическая архитектура // Информационные технологии и телекоммуникации. 2016. Т. 4. № 4. С. 104–121.

8. Израилов К. Е. Архитектурные уязвимости программного обеспечения // Шестой научный конгресс студентов и аспирантов СПбГИЭУ (ИНЖЭКОН-2013): сборник тезисов докладов научно-практической конференции факультета информационных систем и экономике и управлении «Инфокоммуникационные технологии и математические методы». 2013. С. 35.

9. Покусов В. В. Синергетические эффекты взаимодействия модулей системы обеспечения информационной безопасности // Информатизация и связь. 2018. № 3. С 61–67.

10. Буйневич М. В., Покусов В. В., Израилов К. Е. Эффекты взаимодействия обеспечивающих служб предприятия информационного сервиса (на примере службы пожарной

безопасности) // Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2018. № 4. С. 48–54.

11. Бабенко Л. К., Катаргин Д. А. Обнаружение мутации уязвимостей в программном обеспечении // Информационное противодействие угрозам терроризма. 2014. № 23. С. 81–84.

УДК 004.7
ГРНТИ

ПРОБЛЕМЫ БЕЗОПАСНОСТИ И СОВМЕСТИМОСТИ В IoT

М. Н. Иманкул

Казахский агротехнический университет им. С. Сейфуллина

IoT-решения повышают эффективность и безопасность и обеспечивают принятие решений в реальном времени. Их реализацию тормозит нехватка архитектурных шаблонов, описывающих протоколы связи с учетом конкретных отраслей. С внедрением IoT возрастают проблемы с кибербезопасностью, так как каждое новое подключение физического устройства к IoT-сети может стать источником угрозы безопасности.

пограничные вычисления, блокчейн, информационная безопасность, Интернет вещей.

IoT (Internet of Things) – концепция сети, состоящей из устройств, способных взаимодействовать между собой и с внешней средой. Чтобы концепция заработала, нужны: повсеместное распространение скоростного/дешевого Интернета, обеспечение всех устройств уникальными сетевыми адресами, удешевление/снижение размеров датчиков, появление программных и аппаратных средств, способных автоматически обрабатывать огромные потоки данных в реальном времени (РВ). Без внедрения компонентов IoT любая компания вскоре станет неконкурентоспособной.

Развитие электронных устройств и инфраструктуры информационного взаимодействия (Интернета) дает эффективные решения для высоко адаптивных, обучаемых, растущих систем взаимодействия человека с физическими вещами и логическими объектами. В IoT используются разнообразные по формату и содержанию структуры данных, которые в хронологическом порядке наращивают цифровую динамичную систему описания транзакций IoT.

База IoT включает большое число различных датчиков, систем беспроводного доступа, аппаратно-программных средств обработки, распределения, хранения данных. Из 28 млрд подключенных устройств (в 2021 г.) 1,5 млрд будет приходиться на IoT-подключения. Количество «вещей», подключенных к Интернету, резко увеличится с крупным всплеском, предсказанным после 2020 г., когда 5G обеспечит IoT необходимыми сетевыми ресурсами, которые позволят решить весь спектр задач, возлагаемый на IoT (структурирование передачи типов данных от разных устройств с различными приоритетами и скоростью и др.). 5G – когнитивная сеть, включающая в себя потенциальные ресурсы, обеспечивающие ее функциональность (элементы ментальной деятельности, функции мониторинга, сбора информации, исполнительные устройства и др.). Стандарт 5G обеспечивает улучшенную защиту данных, высокие энергоэффективность, более широкую полосу пропускания. Ключевыми факторами/тенденциями, которые повлияют на IoT в ближайшей перспективе, будут [1]: инновации и конкурентноспособность; бизнес-модели; стандартизация и кибербезопасность; беспроводные технологии.

Разработчики IoT-приложений должны использовать данные от множества развернутых датчиков, вычислительных устройств и хранилищ данных. Так как ключевой особенностью IoT служит «размытие границ» между потребительским и индустриальным полями, то полноценный проект для IoT лежит в потребительской и индустриальной плоскости одновременно. Интернет вещей вовлекает во взаимодействие не только мобильные и стационарные устройства, не только физические вещи и алгоритмы, но и обычных людей, социальные группы, производства, бизнесы. Сбой в цепи транзакций на любом этапе и на любом субъекте может привести к неожиданным последствиям. Поэтому требуется особого вида и информационного уровня риск-менеджмент [2].

Недостаток существующей архитектуры Интернета – отсутствие встроенных механизмов безопасности. Кибербезопасность – одна из критических проблем IoT. Приборы IoT создают сложную среду управления, их огромное количество потребительского класса не имеет достаточной безопасности. Основными опасностями для них служат DDoS (*Distributed Denial of Service*)-атаки и вирусы, глубоко проникающие внутрь самых безопасных промышленных объектов, нанося существенный ущерб.

В Cisco считают, что, новый интернет-протокол Named Data Networking (NDN, сетевой протокол именованных данных), служащий одним из способов реализации сетей, ориентированных на передачу контента (*Content-Centric Networking,* CCN) и дающий доступ к данным независимо от того, где они находятся, позволит решить многие актуальные проблемы распределения контента, обеспечения масштабируемости, мобильности и безопасности [3].

Блокчейн может служить платформой координации действий субъектов IoT, безопасность которой злоумышленники могут скомпрометировать только в том случае, если захватят контроль над большинством устройств («атака 51 %»). Взломать блокчейн практически невозможно, однако приложения, построенные на платформе блокчейна, к сожалению, не настолько защищены. Но блокчейн, работающий под управлением интеллектуального алгоритма, сможет обнаружить факт атаки и автоматически включить защитные механизмы [4]. В частности, DNS (*Domain Name Service*) на базе блокчейна позволяет избегать блокировок интернет-ресурсов, а также различного рода DDoS-атак.

Нерешенные проблемы безопасности служат самым большим препятствием на пути к промышленности 4.0. Поэтому следует соблюдать принцип сквозной информационной безопасности (ИБ), который рекомендован для всех ИТ-продуктов и услуг и состоит в закладывании ИБ на начальной стадии проектирования продукта или услуги и в ее поддержке вплоть до завершения их жизненного цикла [5].

Слабые стороны безопасности могут оставаться неоткрытыми в течение длительных периодов времени. Поэтому требуются инструменты сетевого анализа для повышения защиты. В частности, эта проблема может решаться с помощью тестера широкополосной радиосвязи R&S®CMW500 с опцией анализа безопасности IP-соединения R&S®CMW-KM052. Модуль отчетности R&S®CMW-KM052 анализирует и регистрирует связанные с безопасностью параметры трафика данных для мобильных устройств и модулей IoT в реальном времени, а также предоставляет ИТ-специалисту инструмент для определения соответствия мобильного устройства, используемого в деловых целях, внутренним политикам безопасности. Это позволяет разработчикам обнаруживать и закрывать пробелы в безопасности на ранней стадии процесса проектирования.

По мере возрастания числа подключенных к Интернету приборов объем генерируемых и хранимых данных значительно увеличится. Для поддержки этих устройств требуется обработка данных в РВ. Поэтому вопрос обработки данных служит еще одной проблемой. Где она должна происходить – в облаке, на границе сети или непосредственно в самом устройстве? Многие компании для управления собственными ИТ используют как локальные дата-центры, так и дистанционные облачные услуги. В перспективе IoT будет немыслим без облачных технологий хранения значительных массивов информации, без интенсивного анализа больших данных, без широкого цифрового потока регистрируемых фактов, событий и состояний.

Однако сегодня не все предприятия пользуются облачными услугами (особенно те, что имеют дело с конфиденциальными данными и озабочены защитой информации). Также не все каналы передачи данных достаточно производительные для выполнения требований в режиме реального

времени. Некоторые задачи обработки данных будут выполняться на границе сети за счет инфраструктуры. Пограничные вычисления – метод оптимизации вычислительных систем методом переноса обработки данных на границу сети вблизи источника данных, что снижает трафик между датчиками и дата-центром. Сотовые шлюзы станут неотъемлемой частью пограничных вычислений.

Перемещение зеттабайтных объемов данных, генерируемых подключенными предприятиями, автомобилями и др., может привести к появлению множества проблем в традиционных облачных инфраструктурах [6]. Передача в облака громадных массивов данных, их обработка, формирование управляющих воздействий и их доставка за разумное время требуют огромной высокой производительности облачных ресурсов и сверхширокой полосы пропускания от сетевой инфраструктуры, что сопряжено с гигантскими затратами.

Ценность продуктов из IoT-сферы составляет информация, которую собирают «умные» устройства, превращая данные в сведения и в руководство к действию. Множественность данных с нескольких устройств и приложений одновременно (или даже с нескольких приложений на одном и том же устройстве) даст высокоинформативный поток, который может быть использован для удовлетворения частных/коллективных интересов.

Как сделать разные платформы и устройства от разных производителей обратно совместимыми и при этом защититься от риска утечки данных или их несанкционированного (нецелевого) использования? Разработками гибридных инструментов для совместимости с разными типами устройств и платформами для них занимаются: Samsung SmartThings и Apple HomeKit для решений по смарт-домам; Dash и Mojio для интеллектуального управления машинами; Validic и Jawbone UP – в сегменте контроля состояния здоровья [7].

Устройства IoT работают с низкими и все снижающимися внутренним напряжением и взаимодействуют между собой с помощью беспроводных сетей с низким энергопотреблением. Преднамеренные электромагнитные помехи, имеющие мощность, превышающую существующие стандарты электромагнитной совместимости, способны нарушить работу устройств IoT или привести к повреждению цифровых устройств [8].

Сегодня существует более 400 платформ IoT. Многие платформенные решения управления подключениями CMP (*Connectivity Management Platforms*) позволяют наращивать стоимость с целью расширения возможностей платформ обеспечения работы приложений AEP (*Applicatiom Enablement Platform*) и DEP (*Data Exchange Platform*) и гарантируют высокоинтегрированную функциональность для разработчиков и пользователей IoT-приложений [9].

Разнообразие объектов и информации обуславливает необходимость выработки общих принципов построения глобальной сети взаимодействия в рамках IoT. При таком разнообразии не обойтись и без определенных регуляторов. Сети и датчики должны быть объединены под управлением единых стандартов. На текущий момент отсутствуют единые стандарты в сфере кибербезопасности IoT-устройств. Стандартизация в области IoT-технологий и IoT-устройств будет способствовать дальнейшему насыщению рынка технологий IoT.

Проблема стандартизации действительно важна для IoT, и не только в части закрепления формата и способа обмена пакетами данных между вещами. Ключевым является регулирование интерфейсного, функционального и целевого общения любых вещей и объектов. Множество условий, обязательств, прав, возможностей, ограничений, которые должны быть реализованы в рамках технологий IoT, ждут своей очереди, чтобы быть четко формализованными в удобной форме и в разумном содержании [10]. Большинство из требований, предъявляемых к участникам IoT-общения, важны для устойчивости системы транзакций, её предсказуемости и целостности. Жесткие регламенты, четкие стандарты, общепризнанные схемы (цепочки), приемлемые политики, безопасные формы составляют систему стандартизации IoT-технологий [10].

IoT-устройства относительно просты и дешевы. Добавление полупроводниковых элементов и батарей питания в устройства ограничило их срок службы. Если раньше некоторые бытовые приборы могли работать десяток лет, то теперь их срок службы сократился в 2–3 раза. Также большинство современных электронных устройств не предполагает замены, а в некоторых случаях и подзарядки батарей [11].

Современные технологии и модернизация беспроводных сетей вполне смогут обеспечить массовое внедрение IoT, осталось решить отдельные проблемы совместимости протоколов и безопасности.

Список используемых источников

1. Подключаемость как элемент Интернета вещей // Зарубежная электронная техника. 2018. № 10 (6659). С. 20–21.

2. Сегменты Интернета вещей: общие принципы. URL: https://habr.com/post/300608/ (дата обращения 01.03.2019).

3. Ганьжа Д. Станцию IPv6 Интернет проследует без остановок // Журнал сетевых решений/LAN. 2018. № 04. URL: https://www.osp.ru/lan/2018/04/13054568/ (дата обращения 01.03.2019).

4. Танг Динх, Ми Тай. Искусственный интеллект и блокчейн: идеальная пара // Открытые системы. СУБД. 2018. № 04. URL: https://www.osp.ru/os/2018/04/13054611/ (дата обращения 01.03.2019).

5. Восков Л. Как решается проблема безопасности Интернета вещей? URL: https://thequestion.ru/questions/401180/kak-reshaetsya-problema-bezopasnosti-interneta-veshei/ (дата обращения 01.03.2019).

6. Чернобровцев А. Стандартизация туманной инфраструктуры // Журнал сетевых решений/LAN. 2018, № 4. URL: https://www.osp.ru/lan/2018/04/13054572/ (дата обращения 01.03.2019).

7. Перспективы развития «интернет вещей» до 2020 года. URL: http://1234g.ru/novosti/479-internet-veshchej-k-2020-godu (дата обращения 01.03.2019).

8. Преднамеренные электромагнитные помехи как недооцененная угроза Интернету вещей // Зарубежная электронная техника. 2018. № 10 (6659). С. 32.

9. Обработка данных как элемент Интернета вещей // Зарубежная электронная техника. 2018. № 12 (6661). С. 34–37.

10. Сегменты Интернета вещей: общие принципы. URL: https://habr.com/post/300608/ (дата обращения 01.03.2019).

11. Internet of Trash Things: какие проблемы принесет «Интернет вещей». URL: https://nag.ru/articles/article/102131/internet-of-trash-things-kakie-problemyi-prineset-internet-veschey-.html (дата обращения 01.03.2019).

УДК 004.421
ГРНТИ 28.23.37

СЕГМЕНТАЦИЯ РЕАЛЬНЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ, ОБУЧЕННОЙ НА СИНТЕТИЧЕСКИХ ДАННЫХ

Е. В. Каляшов, А. А. Савельева, А. В. Тарлыков

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

В статье рассмотрен метод обучения свёрточной нейронной сети с использованием синтетических обучающих данных для задачи попиксельной сегментации реальных объектов на видеоизображении. Затронуты вопросы генерации данных, процессов обучения и оптимизации сети, работы с видеоизображением. Приведены примеры применения обученной сети для качественных фотоснимков и кадров видеопотока низкого разрешения.

свёрточная нейронная сеть, обучение, синтетические данные, сегментация.

В статье рассмотрена задача попиксельной сегментации изображений летательных аппаратов для систем оптического наблюдения. Подобные системы характеризуются практически произвольной ориентацией и положением наблюдаемого объекта в поле зрения системы. При обучении нейронной сети для решения задачи в таких условиях требуется наличие большого

набора заранее размеченных данных, что является определённой проблемой – отсутствием размеченных с необходимой точностью видеоматериалов, тем более – в свободном доступе. В ходе решения задачи предлагается использовать специально подготовленные синтетические данные – проекции трёхмерных компьютерных моделей летательных аппаратов, сгенерированные специальным программным обеспечением [1]. Используя набор параметров, программный комплекс обеспечивает генерацию набора обучающих изображений – проекций летательных аппаратов и пиксельных масок, соответствующих каждой проекции, поверх различных фонов (рис. 1, 2).

Рис. 1. Пример проекций летательных аппаратов на фоне неба

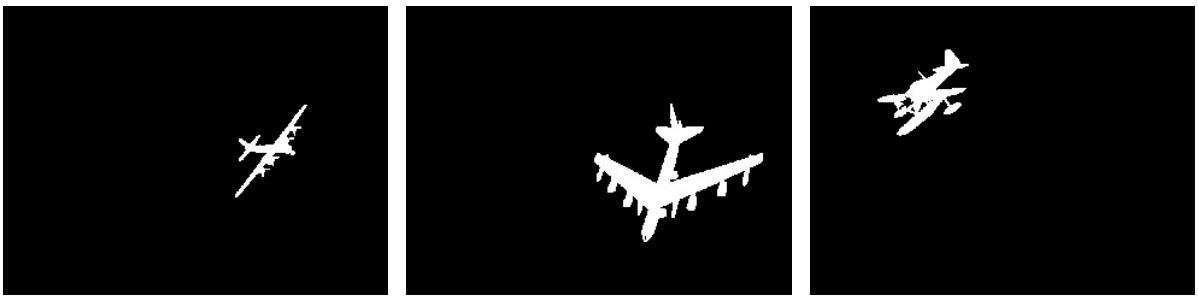


Рис. 2. Пример бинарных масок, соответствующих примеру на рис. 1

В ходе начального обучения был использован набор проекций и масок, полученный для 3-х моделей самолётов, общее количество проекций – 9000 изображений разрешением 1024×768 пикселей, дополнительно было использовано 7 различных изображений фона. Сети ставилась задача сопоставить поданному на вход изображению верную маску. Точность сопоставления определялась с использованием коэффициента Дайса (*Dice coefficient* [2]**)**. В ходе обучения использовалась аугментация обучающего набора – фильтрация, изменение яркости и насыщенности [3].

В качестве основы для построения архитектуры нейронной сети использовался подход, предложенный авторами сети U-Net и использовавшейся для сегментирования медицинских снимков [4]. Архитектура базовой сети была доработана для работы с изображениями и масками необходимого разрешения, использованными в работе.

Обучение полученной сети производилось в течение 15 эпох. Размер батча при обучении составлял 4 изображения и ограничивался памятью GPU вычислителя. Кривая значений функции потерь в ходе обучения приведена на рис. 3.

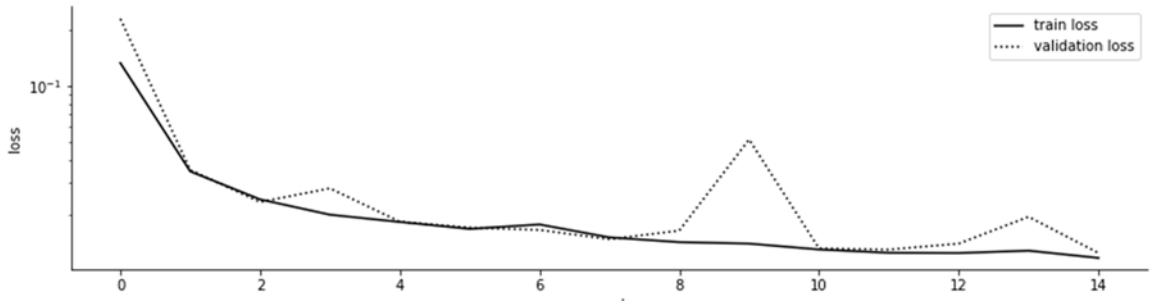


Рис. 3. Кривая значений функции потерь в процессе обучения

Можно заметить достаточно низкое значение ошибки в конце процесса обучения. И действительно, визуальная проверка качества сегментации на тестовом наборе это подтвердила. В качестве дальнейшего шага был проведён эксперимент с подачей на вход обученной сети реальных изображений – фотографий с объектами различного масштаба и кадров видео потока парада Победы. По результатам предсказания маска объекта накладывалась поверх изображения в полупрозрачном виде.

Качество сегментации оценивалось визуально и показало высокий результат для качественных изображений реальных объектов (рис. 4), ошибка практически сопоставима с усреднённой ошибкой на тестовом наборе синтетических данных.

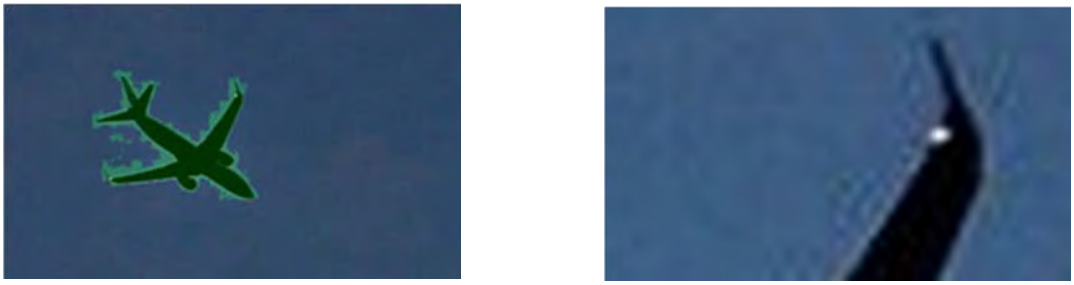
а) б)

Рис. 4. Пример сегментации: а) видеоряде парада; б) качественной фотографии

Что касается кадров видео потока, то результирующая ошибка оказалась существенно выше (рис. 4). Данный факт можно объяснить широким рядом факторов: сильным разбросом в масштабе летательных аппаратов на видео, плохой фокусировке изображения, нестационарным состоянием

воздушного слоя на линии съёмки (следствие пролёта большого количества летательных аппаратов).

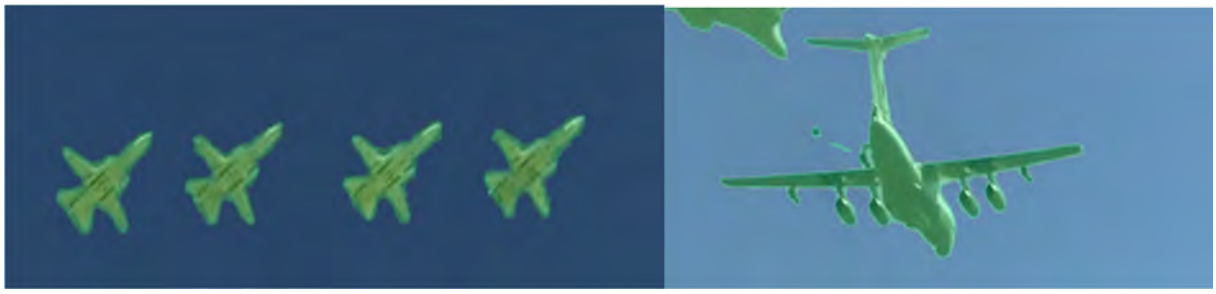
Также необходимо отметить, что при использовании изображений низкого качества, например, в формате jpeg с большим сжатием, качество сегментации резко ухудшалось, что объясняется артефактами сжатия на изображениях (рис. 5).



а) б)

Рис. 5. Пример: а) сегментации изображения с артефактами сжатия; б) соответствующий увеличенный фрагменты исходного изображения

В качестве борьбы с низким качеством сегментации видеоряда парада, было произведено дообучение сети на наборе отдельных кадров парада с высоким качеством исходной сегментации (хорошая фокусировка, удовлетворительный масштаб объектов). Был подготовлен набор обучающих данных количеством 834 кадра, дообучение проводилось в течение 5 эпох, применялась аугментация набора – горизонтальное и вертикальное отражение, масштабирование, изменение яркости и насыщенности изображений. Результатом дополнительного обучения стало резкое увеличение качества сегментации на подавляющем большинстве кадров видеоряда, что можно видеть на примере, представленном ниже (рис. 6).



а) б)

Рис. 6. Пример сегментации на кадрах видеопотока после дообучения сети

Таким образом, подход с использованием синтетических данных для сегментации изображений с помощью нейронных сетей является достаточно мощным средством для решения подобных задач. Тем не менее,

для удовлетворительной сегментации изображений, значительно отличающихся по параметрам от обучающего набора, может понадобиться дополнительное обучение на выборке из целевого набора. При этом подготовку обучающих масок можно выполнить самой сетью, с последующим ручным отбором. Такой подход позволяет экономить время и значительно повысить качество сегментации.

Список используемых источников

1. Каляшов Е. В., Савельева А. А., Тарлыков А. В. Использование синтетических данных для обучения нейронной сети классификации летательных аппаратов // 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.432–437.

2. Sørensen–Dice_coefficient [Электронный ресурс]. Электрон. дан. 2018. Режим доступа: https://en.wikipedia.org/wiki/Sørensen–Dice_coefficient, свободный. Загл. с экрана. Яз. англ.

3. Aysegul Dundar, Ignacio Garcia-Dorado. Context Augmentation for Convolutional Neural Networks [Электронный ресурс]. Электрон. текстовые дан. 2017. Режим доступа: https://arxiv.org/abs/1712.01653, свободный. Загл. с экрана. Яз. англ.

4. Olaf Ronneberger, Philipp Fischer, Thomas Brox. U-Net: Convolutional Networks for Biomedical Image Segmentation [Электронный ресурс]. Электрон. текстовые дан. 2015. Режим доступа: https://arxiv.org/abs/1505.04597, свободный. Загл. с экрана. Яз. англ.

Статья представлена проректором по информатизации СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 004.421
ГРНТИ 28.23.37

ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ОРИЕНТАЦИИ ЛЕТАТЕЛЬНОГО АППАРАТА С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

Е. В. Каляшов, А. В. Тарлыков, А. А. Швидкий

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

В статье рассматривается задача определения углов ориентации объектов на видеоизображении с использованием нейронных сетей. Описан процесс обучения свёрточных нейронных сетей различных архитектур с использованием синтетических обучающих данных. Рассмотрены вопросы генерации обучающего набора данных и различных

вариантов обучения. Приведены результаты тестирования при различных способах обучения и на различных модельных примерах.

свёрточная нейронная сеть, обучение, регрессия, подготовка данных.

Рассмотрим задачу определения углов ориентации летательного аппарата на основании изображения, полученного от системы оптического наблюдения. Такие системы характеризуются большим диапазоном возможных ориентаций и положений летательного аппарата в исходном кадре. Для решения подобной задачи с использованием нейронной сети необходимо обеспечить процесс обучения с достаточным объёмом тренировочных данных. Что, в случае определения параметров летательного аппарата по изображению, требует наличия достаточно большого набора проекций аппарата с различной ориентацией и соответствующим набором параметров, описывающих ориентацию на каждом изображении. Построить подобный обучающий набор на основе фотографирования и протоколирования параметров является невыполнимой задачей. В ходе работы использовались свободно доступные компьютерные трёхмерные модели соответствующих летательных аппаратов. Специально разработанное программное обеспечение предоставляло возможность чтения трёхмерных моделей в форматах 3ds и obj, ориентацию моделей в необходимом диапазоне углов наклона и построение двумерных проекции [1].

Для подготовки обучающего набора данных в ходе работы была использована модель самолёта FA5 (рис.), модель подавалась на вход специального программного обеспечения со следующими параметрами: количество проекций – 160 000 изображений разрешением 320×240 пикселов, фоны – 2 изображения аналогичного разрешения. Контролируемые параметры – смещение объекта в кадре по осям X и Z, углы ориентации относительно осей Y (перпендикулярно изображению, по направлению взгляда) и Z (вертикально вверх), масштаб объекта. Масштаб нормировался на единицу, что соответствует площади прямоугольника, обрамляющего вертикальную проекцию объекта и равной 30 % от площади всего изображения. Величина смещения составляла 25 % от размера обрамляющего прямоугольника и также нормировалась на ±1.

Рисунок. Модель самолёта FA5, использованная в работе

В ходе работы для проведения экспериментов были использованы следующие широко распространённые базовые архитектуры нейронных сетей: VGG19 [2], Inception_v3 [3], ResNet50 [4]. В сети было внесено следующее изменение: отделены оконечные слои, отвечающие за классификацию изображений, и заменены на новые, предназначенные для решения задачи регрессии параметров, описывающих ориентацию летательного аппарата. Для свёрточной части сетей исходно использовались веса, полученные обучением на наборе данных ImageNet [5] для задачи классификации изображений [6].

Для ускорения процесса обучения и уменьшения совокупного времени, необходимого для проведения экспериментов, был использован подход с предварительной генерацией промежуточных признаков свёрточными частями исходных сетей на основе обучающего набора. Через сети были пропущены изображения обучающего набора и результаты обработки были сохранены для непосредственного использования в качестве входных данных при обучении регрессионных слоёв сетей. Подобный подход является достаточно распространённой практикой и позволяет сильно сократить время обучения результирующей нейронной сети за счёт непосредственного использования большей части слоёв, заранее обученных на выделение ключевых элементов поданного на вход сети изображения. Для повышения результирующей точности остаётся возможность дальнейшего обучения всей сети на исходном наборе данных, включая в обучение и часть свёрточных слоёв, но данный подход требует повышенных вычислительных ресурсов и значительного времени.

Для оценки возможностей нейронной сети первоначально использовался набор данных с двумя фиксированными фоновыми изображениями и пятью параметрами – смещениями по осям X, Y, углами ориентации относительно осей Y и Z в диапазоне ± 1,5 рад и масштабом в диапазоне 0,3–1. В дальнейшем, с целью большего приближения условий эксперимента к реальным, был использован обучающий набор с 7 фоновыми изображениями и их аугментацией [7] в процессе генерации проекций. В таких условиях сеть показала существенное увеличение ошибки. По результатам обучения были получены следующие результаты на тестовом наборе данных (табл. 1, см. ниже).

Одним из факторов, сильно влияющих на величину ошибки, является количество оцениваемых параметров и их разброс. В данном случае таким параметром, оказывающим сильнейшее влияние, является положение модели в кадре. Тем не менее, не уменьшая общности, данный параметр можно исключить из предсказываемого набора – в большинстве случаев существует возможность предварительной обработки тестового кадра с целью обнаружения центра оцениваемого объекта и подачи на вход сети центри-

рованного изображения. Небольшие относительные сдвиги можно компенсировать путём использования аугментации на этапе обучения, сдвигая модель в фиксированных границах.

ТАБЛИЦА 1. Ошибка на тестовом наборе. Обучающие наборы: №1 – два фоновых изображения, №2 – семь фоновых изображений с аугментацией

Обучающий набор	Тип сети	Углы, рад.	Положение, %	Масштаб, %
1	VGG19	0,051	3,1	1,5
	Inception v3	0,099	6,2	2,6
	ResNet50	0,160	5,5	2,4
2	VGG19	0,202	13,7	5,2
	Inception v3	0,196	14,6	4,9
	ResNet50	0,202	9,5	3,8

С целью проверки данной гипотезы на модель были наложены ограничения в процессе генерации обучающих данных – были исключены смещения объекта, масштаб был ограничен диапазоном 0,8–1, максимальные отклонения углов ориентации относительно оси X составили ± 1 рад, оси Y – ± 1,2 рад, оси Z – ± 1,5 рад. Можно заметить, что набор предсказываемых параметров был расширен включением ориентации относительно оси X. Размер обучающего набора изображений был также сокращён и составил 80 000 изображений. Результаты обучения приведены в таблице 2. Дополнительно был проведён эксперимент с построением ансамбля лучших сетей для повышения качества предсказания. Значения, предсказанные всеми сетями ансамбля, усреднялись и использовались как результирующие. Результаты представлены в таблице 2.

ТАБЛИЦА 2. Ошибка на тестовом наборе при ограничении определяемых параметров

Тип сети	Угол отн. оси X, рад	Угол отн. оси Y, рад	Угол отн. оси Z, рад.	Масштаб, %
VGG19	0,032	0,029	0,039	1,9
Inception v3	0,035	0,028	0,037	1,7
ResNet50	0,044	0,037	0,051	2,0
Ансамбль	0,028	0,020	0,029	1,3

Можно отметить сильное уменьшение результирующей ошибки после исключения сдвига модели в поле кадра. Также необходимо выделить результат использования ансамбля сетей – как можно видеть из таблицы 2, результирующая ошибка в случае ансамбля существенно ниже.

С целью проверки возможности улучшения результатов был дополнительно опробован другой подход – дообучение всей сети с использованием

очень малых скоростей обучения. В качестве отправной точки в свёрточную часть сети были загружены веса ImageNet, в регрессионную – веса, полученные на предыдущем этапе обучения. В данном случае большое значение для успешного обучения имеет подбор оптимизатора. Удовлетворительным выбором для всех трёх типов сетей оказался оптимизатор Adam со скоростью обучения 1×10^{-5}. Результаты представлены в таблице 3.

ТАБЛИЦА 3. Ошибка на тестовом наборе.

Тип сети	Углы, рад	Положение, %	Масштаб, %
VGG19	0,025	1,4	0,9
Inception v3	0,024	1,9	1,1
ResNet50	0,028	2,1	1,1
Ансамбль	0,016	1,2	0.6

Заметно явное уменьшение величины ошибки в сравнении с результатами из таблицы 1 (для второго обучающего набора). Следует отметить очевидный минус такого подхода – свёрточная часть сети не может быть использована для общего выделения признаков, для каждого вида самолетов должна использоваться отдельная сеть. Также данный подход требует больших вычислительных ресурсов и значительных затрат времени.

Таким образом, предложенные подходы продемонстрировали достаточно высокую точность определения параметров ориентации объекта. Тем не менее, следует отметить, что результаты обучения сети на определённом типе объектов часто неприменимы к другому типу, что требует дополнительного обучения сети на всех необходимых типах объектов или использования раздельных сетей для различных типов объектов. Возможный конвейер обработки изображения может строиться следующим образом – выделение объекта сегментирующей сетью, классификация объекта, выбор на основе классификатора подходящей регрессионной сети, определение параметров объекта регрессионной сетью.

Список используемых источников

1. Каляшов Е. В., Савельева А. А., Тарлыков А. В. Использование синтетических данных для обучения нейронной сети классификации летательных аппаратов // 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.432–437.

2. Karen Simonyan, Andrew Zisserman. Very Deep Convolutional Networks for Large-Scale Image Recognition [Электронный ресурс]. Электрон. текстовые дан. 2015. Режим доступа: https://arxiv.org/abs/1409.1556, свободный. Загл. с экрана. Яз. англ.

3. Christian Szegedy, Wei Liu and others. Going Deeper with Convolutions [Электронный ресурс]. Электрон. текстовые дан. 2014. Режим доступа: https://arxiv.org/abs/1409.4842, свободный. Загл. с экрана. Яз. англ.

4. Kaiming He, Xiangyu Zhang, Shaoqing Ren, Jian Sun. Identity Mappings in Deep Residual Networks [Электронный ресурс]. Электрон. текстовые дан. 2016. Режим доступа: https://arxiv.org/abs/1603.05027, свободный. Загл. с экрана. Яз. англ.

5. ImageNet [Электронный ресурс]. Электрон. дан. 2016. Режим доступа: http://www.image-net.org/, свободный. Загл. с экрана. Яз. англ.

6. Keras code and weights files for popular deep learning models [Электронный ресурс]. Электрон. дан. 2018. Режим доступа: https://github.com/fchollet/deep-learning-models, свободный. Загл. с экрана. Яз. англ.

7. Aysegul Dundar, Ignacio Garcia-Dorado. Context Augmentation for Convolutional Neural Networks [Электронный ресурс]. Электрон. текстовые дан. 2017. Режим доступа: https://arxiv.org/abs/1712.01653, свободный. Загл. с экрана. Яз. англ.

Статья представлена проректором по информатизации СПбГУТ, кандидатом технических наук, доцентом А. А. Зарубиным.

УДК 654.152
ГРНТИ 49.33.29

ОПТИМИЗАЦИЯ СИММЕТРИЧНОГО КАБЕЛЯ УВЕЛИЧЕННОЙ ПРОТЯЖЁННОСТИ ПО ЭКОНОМИЧЕСКОМУ КРИТЕРИЮ

Е. В. Кандзюба

Московский технический университет связи и информатики

Осуществлена оптимизация конструкции 2-парного симметричного кабеля «длинного» Ethernet. В качестве критерия оптимизации предложена модель использующая эквивалентность цены использованных при производстве кабельного изделия материалов и площади их сечения в конструкции кабеля.

кабельный тракт, волновое сопротивление, рабочее затухание, оптимизация.

При построении сетей доступа и информационных систем объектов недвижимости могут применяться оптические и симметричные электропроводные кабели. Использование последних, несмотря на меньшую дальность передачи, обеспечивает ряд преимуществ, в т. ч. возможность дистанционного питания терминального оборудования. В таких условиях актуальным

представляется отработка такой конструкции этих изделий, которая обеспечивает увеличение дальности действия по сравнению с типовыми для кабелей СКС значениями [1].

Цель работы – определение основных конструктивных параметров симметричного тракта увеличенной протяжённости. При дальнейшем рассмотрении используются следующие ограничения:

– Тракт выполняется в 2-парном варианте, что достаточно для достижения скорости 100 Мбит/с.

– Диаметр токопроводящей жилы (ТПЖ) витой пары может быть увеличен свыше тех 0,64 мм, которые указаны как предельные стандартами ISO/IEC 11801 и ANSI/TIA 568-2C.

Рис. 1. Структура затрат на реализацию 4-парного кабеля

– В качестве прототипа для сравнения привлекается типовая 4-парная конструкция с диаметром ТПЖ 0,52 мм и структурой затрат на отдельные укрупнённые компоненты, приведённые на рис. 1.

Ранее было установлено, что основным средством наращивания предельной протяжённости тракта «длинного» Ethernet является снижение коэффициента затухания линейного кабеля [2].

$$\alpha l = 8{,}69\left(\frac{R_{\text{п}}}{2Z} + \frac{GZ}{2}\right), \qquad (1)$$

где $R_{\text{п}}$ – полное сопротивление провода витой пары; Z – волновое сопротивление; G – проводимость изоляции.

Анализ формулы расчёта коэффициента затухания неэкранированного кабеля (1) показывает, что эта задача может быть решена двумя путями:

1. Снижение активного сопротивления кабеля R_0.

2. Увеличение его волнового сопротивления Z.

Из независимости этих подходов следует возможность их комбинации для достижения наилучшего результата [3].

Зависимость волнового сопротивления Z от геометрических размеров кабеля определена в [4]:

$$Z = \frac{120}{\sqrt{\varepsilon_r}} \ln\left(\frac{a}{d} + \sqrt{\left(\frac{a}{d}\right)^2 - 1}\right), \text{дБ} \qquad (2)$$

где a – расстояние между осями жил, d – диаметр жилы, ε_r – относительная диэлектрической проницаемость (для полиэтилена ε_r = 1,9–2,3).

В результате упрощения (2) можно выразить, как:

$$Z = \frac{120}{\sqrt{\varepsilon_r}} \ln\left(\frac{2a}{d}\right) \quad , \text{дБ} \tag{3}$$

Рабочее затухание витой пары при условии отсутствия согласования сетевых интерфейсов по входу выходу [3]:

$$\mathrm{A_p} = \alpha l + 40 \lg\left(\frac{R+Z}{2\sqrt{RZ}}\right), \text{дБ} \tag{4}$$

где α – коэффициент затухания (1); R = 100 Ом – входное и выходное сопротивление приёмника и передатчика сетевого интерфейса; Z – волновое сопротивление линейного кабеля.

Сложность исходного выражения (4), дающего плоскость решений для возможных значений диаметров ТПЖ и изолированной жилы, не даёт критерия для выбора конкретного решения.

Стандартные по ISO/IEC 11801 [5] кабели U/UTP содержат 4 пары. Возможность отказа от соблюдения стандарта в линиях Long Ethernet [2] с учётом применения 100-мегабитных сетевых интерфейсов позволяет сократить количество пар до двух. Полученный выигрыш направляется на наращивание волнового сопротивления и снижение активного сопротивления, что даёт выигрыш по α.

Таким образом, в качестве критерия для выбора оптимального решения предложено ценовое равенство расходных материалов, используемых при производстве кабеля.

Для дальнейших расчётов привлекаются модели рис. 2.

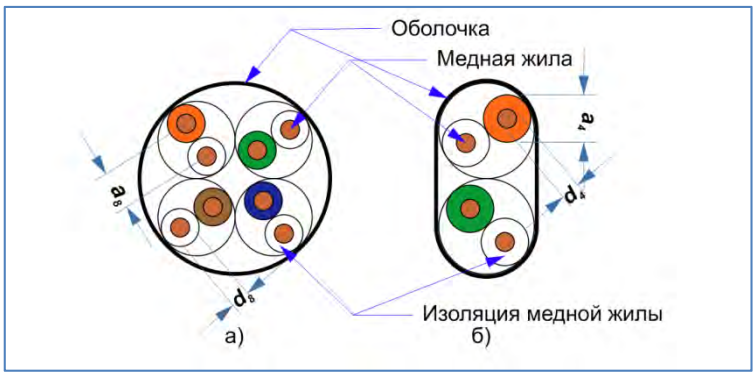


Рис. 2. Модели кабеля. а) прототип; б) оптимальный

Предельное значение для Z ограничено значением, при котором: $S_8 = S_4$, где S_i – стоимость кабельной продукции.

В производимых на сегодня кабелях стоимость внешней изоляции составляет 10 % от цены конечного продукта. Для упрощения дальнейших расчётов нею можно пренебречь.

Критерием эквивалентной стоимости кабеля модели а) к модели б) является площадь сечения используемых в кабеле материалов.

Формула для расчёта эквивалентных кабелей при $n = 8$ и $n = 4$**:**

$$S_{м8} + \frac{c_и}{c_м} S_{и8} = S_{м4} + \frac{c_и}{c_м} S_{и4}, \quad (5)$$

где $S_{мi}$,$S_{иi}$ – площади сечения: м – меди, и – изоляции жилы, i = 4 или 8, $c_{мi}$,$c_{иi}$ – ценовые коэффициенты площадей.

Физический смысл ценового коэффициента заключается в том, что после умножения его на объём используемого материла получается ценовая доля материала в стоимости конечного продукта, в данном случае кабеля. Цена любого многокомпонентного продукта вычисляется как сумма стоимостей, входящих в него компонентов:

$$\mathrm{Cost}_{total} = \sum_{i=1}^{n} \rho_i Price_i V_i, \text{ руб.} \quad (6)$$

где ρ – плотность материала кг/м^3; V – объём материала м^3; *Price* – цена материла за килограмм; Cost_{total} – конечная стоимость товара.

Из (6) получена формула расчёта ценовых коэффициентов для меди и полиэтилена:

$$c_i = \frac{\rho_i * Price_i}{\mathrm{Cost}_{Total}}, \quad (7)$$

Применяемые далее значения являются справочными и равны: $\rho_м$ = 8900 кг/м3 – для меди, $\rho_м$ = 920 кг/м3 – для полиэтилена. Цена на медь взята из котировок на бирже LME.Copper, USD за тонну: 6144,3038; курс USD по данным ЦБ РФ из 66,0628 руб.

Для конструкций категории 5*e* справедливо использовать фактический ценовой вклад в процентном выражении в себестоимость конечного продукта: медь = 75 %, полиэтилен = 15 %. Используя значения процентного вклада и (6) составлено равенство, с помощью которого вычислена цена на полиэтилен при которой соблюдается равенство (5).

$$\mathrm{Cost}_{total} = \frac{\rho_м Price_м V_{8м}}{0{,}75} = \frac{\rho_и Price_и V_{8и}}{0{,}15} = \frac{\rho_м Price_м V_{4м}}{x} = \frac{\rho_и Price_и V_{4и}}{y}.$$

Используя (7) и информацию о процентном вкладе материалов получено отношение ценовых коэффициентов на основании формул расчёта площадей сечения для каждого материала:

$$\frac{c_и}{c_м} = \frac{0{,}2d8^2}{a8^2 - d8^2}, \quad (8)$$

Подстановка (8) в (5) и использование известных геометрических размеров кабеля *U/UTP*, d = 0,51 мм, a = 1,0 мм, даёт зависимость геометрических размеров для жилы модели б):

$$a_4 = 3{,}64\sqrt{0{,}67 - {d_4}^2}, \text{при } d_4 \le a_4 \qquad (9)$$

где: d_4 – диаметр медной жилы, a_4 – диаметр изолированной жилы для модели б) рис. 2.

Выражение (9) определяет область возможных значений для радиуса медной жилы у кабеля модели б): $d_4 \in (0{:}0{,}78)$.

Трансцендентное выражение для нахождения коэффициента затухания (1) не позволяет решить задачу поиска минимального значения α в аналитическом виде с удобным для практической работы результатом.

Преобразование функции (3) методом Тейлора с использованием (9) даёт упрощённую формулу для расчёта волнового сопротивления для кабеля модели б):

$$Z = 79 \cdot (3{,}7 - 2{,}6 * d_4 - 0{,}6 * {d^2}_4)\,, \text{Ом} \qquad (10)$$

Использование первых трёх членов разложения даёт погрешность (10) относительно (2) в 4 %, что достаточно для дальнейших расчётов.

Для расчёта полного сопротивления ТПЖ с учётом влияния вихревых токов использована аппроксимированная методом Тейлора формула из [4]. Первые два члена разложения обеспечивают точность вычисления в 3%.

$$R_{\text{п}} = R_0\left(3{,}77d + \frac{0{,}26}{\sqrt{f}}\right) \cdot \sqrt{f}\,, \text{Ом} \qquad (11)$$

$$R_0 = \frac{8 \cdot k \cdot \rho}{\pi \cdot d_4^2} \cdot l, \text{Ом} \qquad (12)$$

где R_0 – сопротивление ТПЖ постоянному току, ρ = 0,0175 Ом*мм^2/м – удельное сопротивление меди, k = 1,02– коэффициент укрутки.

Применение вышеописанного метода аппроксимации для формулы расчёта ёмкости [6] даёт упрощённое выражение для расчёта проводимости изоляции. В реальных кабелях проводимость, обусловленная утечкой тока в силу несовершенства диэлектрика $G_0 << G$, поэтому ней можно пренебречь:

$$G = \left(\frac{2{,}47}{(3{,}7 - 2{,}6 \cdot d_4 - 0{,}6 \cdot {d^2}_4)}\right) \cdot f \cdot l \cdot 10^{-7}, \text{См/м} \qquad (13)$$

где l – длина кабеля, f – частота сигнала.

В результате подстановки в (1) выражений (10), (11) и (13) и последующие упрощения имеют результатом выражение коэффициента затухания через частоту и диаметр ТПЖ.

$$\alpha = 8{,}69 \cdot 10^{-5} \cdot f - \frac{1{,}56 \cdot 10^{-2} \cdot \sqrt{f}}{d_4(d_4(d_4 + 4{,}34) - 6{,}17)}. \qquad (14)$$

Минимальное значением α на интервале допустимых значений находится через решение следующего дифференциального уравнения:

$$\frac{d}{dd_4}\alpha(d_4, f) = \frac{\sqrt{f}(4{,}67 \cdot 10^{-2}\, d_4^2 + 1{,}35d_4 - 9{,}6)}{d_4^2(-d_4^2 - 4{,}33d_4 + 6{,}17)^2} = 0. \qquad (15)$$

Решение (15) сводится к решению квадратного уравнения:

$$4{,}67 \cdot 10^{-2}\, d_4^2 + 1{,}35d_4 - 9{,}6 = 0, \qquad (16)$$

В результате решения (16) получено два значения для d_4, одно из которых противоречит физическому смыслу решаемой задачи.

Коэффициент затухания принимает минимальное значение при d_4 = 0,59 мм. На основании (10) волновое сопротивление при найденном значении диаметра ТПЖ: – Z(0,59) = 154 Ом, что отличается от значения Z согласно (2) на 1,3 %.

Учитывая, что полученное значение для волнового сопротивления отличается от нормированного для стандартного кабеля значения в 100 Ом, расчёт рабочего затухание произведён с применением (4) и (10).

Для проверки полученых результатов использовался классический математиче-ский аппарат работ [7, 8].

Сравнение поведения функции рабочего затухания согласно классической модели и модели, предложенной в статье показано на рис. 3.

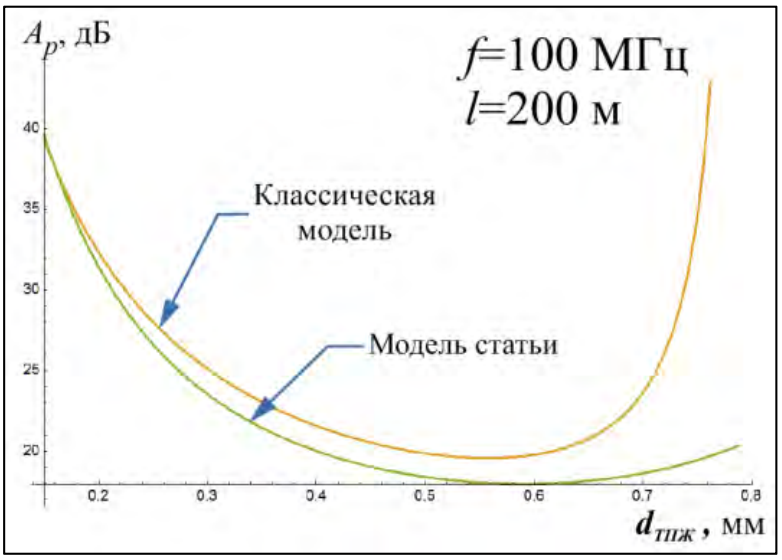


Рис. 3. График рабочего затухания

Наилучшие результаты по рабочему затуханию обеспечивает кабель с диаметром ТПЖ 0,59 мм при диаметре с изоляцией 2,06 мм с волновым сопротивлением 155 Ом (табл.).

ТАБЛИЦА. Рабочее затухание и волновое сопротивление в зависимости от протяженности тракта при d_4 = 0,59 мм

***L*, м**	***Z*,** Ом (статья)	***Z*,** Ом (классич.)	A_p дБ (статья)	A_p дБ (классич.)
150	155	148	14,1	14,9
200	155	148	18,6	19,7
250	155	148	23,2	24,5
300	155	148	27,8	29,4

Примечание: Оценка A_p для f = 100 МГц.

Пропорция ценового вклада материалов в кабеле длинного Ethernet меняется с типовых для 4-парных изделий 0,75 : 0,15 для меди: изоляции до соответственно 0,43:0,46 без учёта стоимости защитной оболочки.

Список используемых источников

1. Семенов А. Б., Кандзюба Е. В. Перспективы увеличения протяженности симметричного кабельного тракта систем цифрового видеонаблюдения // Перспективные технологии в средствах передачи информации. Материалы 12-й международной научно-технической конференции. Т. 1. / Владимирский государственный университет. Владимир : ВлГУ, 2017. С. 215–218.

2. Семёнов А., Кандзюба Е., Руденко В. «Длинный» Ethernet – дальше, дальше и дальше // Первая миля. 2017. № 7. С. 32–36.

3. Кандзюба Е., Семёнов А., Предельное затухание витой пары с повышенным волновым сопротивлением // Первая миля. 2018. № 8. С. 42–46.

4. Семёнов А. Б. Классические структурированные кабельные системы. М. : Горячая линия-Телеком, 2016. 462 с

5. ISO/IEC 11801-1:2017 Information technology – Generic cabling for customer premises – Part 1: General requirements // International standard. Edition 1.0. 2017. 160 p.

6. Семёнов А. Б., Стрижаков С. К., Сунчелей И. Р. Структурированные кабельные системы, 5-е изд. М. : Компания АйТи, ДМК Пресс, 2014. 640 с.

7. Андреев В. А., Портнов Э. Л., Кочановский Л. Н. Направляющие системы электросвязи. Том 1. М. : Горячая линия-Телеком, 2011. 422 с.

8. Кулешов В. Н. Теория кабелей связи: учебник. М. : Государственное издательство по вопросам связи и радио, 1950. 419 с.

Статья представлена научным руководителем, доктором технических наук А. Б. Семёновым.

УДК 004.5
ГРНТИ 49.40.49

ИССЛЕДОВАНИЕ ТРАФИКА ПРИЛОЖЕНИЙ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

З. С. Канивец, В. А. Кулик, М. А. Маколкина

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

Темой исследования в данной статье являются характеристики трафика приложений Дополненной реальности. В статье описывается архитектура программно-аппаратного комплекса. С помощью разработанной архитектуры была создана модельная сеть, на базе которой был исследован трафик, создаваемый различными приложениями ДР. На основе полученных данных были сделаны выводы об общем характере трафика приложений Дополненной реальности.

дополненная реальность, AR, анализ трафика.

Введение

Дополненная реальность – среда, дополняющая физический мир, где виртуальные объекты проецируются на реальное окружение. Процесс отображения объектов ДР в большинстве случаев представлен следующим образом: оптический сканер устройства снимает изображение объекта в реальном мире; программное обеспечение, установленное на устройстве, проводит анализ полученного изображения, сопоставляя полученную информацию с информацией о подходящем видимом дополнении; объединяет реальное изображение с его дополнением и выводит его на устройство визуализации.

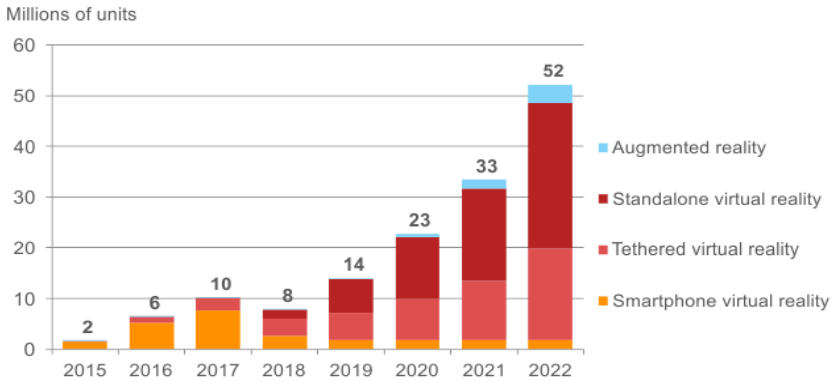


Рис. 1. Мировые поставки устройств с VR/AR, млн шт.

В последние годы технологии, связанные с Виртуальной и Дополненной реальностью, активно развиваются и начинают играть далеко не последнюю роль во многих сферах жизни человека – от обучения и медицины до строительства и сферы развлечений. Долгое время популярность технологий, связанных с VR/AR, возрастает. Уже сейчас заметен переход от простых приложений и девайсов VR/AR для смартфонов к более сложным и дорогим технологиям (рис. 1) [1, 2].

В настоящее время трафик, связанный с приложениями Виртуальной и Дополненной реальности, занимает значительную долю от всего трафика, передаваемого в сети. Причём зачастую требования к сетевым характеристикам у данных приложений достаточно высоки. Именно поэтому исследование и анализ такого трафика представляет особую ценность для дальнейшего развития современных сетевых технологий.

Перехват и анализ трафика

Пока что доля сферы развлечений в данной области превалирует. Поэтому в качестве приложений, сбор и анализ трафика которых описан в данной статье, используются игры, включающие в себя технологии Дополненной реальности [3, 4]:

1) Pokemon GO – многопользовательская ролевая мобильная игра, элементы которого игрок может просматривать в режиме ДР, используя камеры и гироскоп на своём мобильном устройстве.

2) SketchAR – приложение, с помощью которого пользователь видит виртуальное изображение на поверхности, на которую планирует перевести рисунок.

3) Ghost Snap AR Horror Survival – игра с элементами ДР.

Для перехвата трафика был использован программно-аппаратный комплекс (рис. 2).

Рис. 2. Структура программно-аппаратного комплекса

Так как реализация сервера AR – достаточно сложная задача, было решено ограничиться перехватом трафика, поступающего на смартфон с внешних серверов игр. Для этого был организован сетевой мост – ПК, который через один сетевой интерфейс подключается напрямую к ССОП, а через второй сетевой интерфейс к ПК подключается Wi-Fi роутер. Данные, передаваемые смартфоном по беспроводной сети во время игровой сессии, перехватываются с помощью Wireshark.

При анализе полученных данных рассматривались такие показатели, как задержки, пропускная способность и джиттер.

Полученные результаты отражены в таблице.

ТАБЛИЦА. Результаты исследования

Приложение	Среднее значение интервалов между пакетами, мс	Пропускная способность, байт/с	Джиттер, мс
Pokemon GO	186,75	431869,49	10,00
SketchAR	164,13	8596,98	25,10
Ghost Snap AR Horror Survival	410,76	3884,50	13,02

Также на рис. 3–5 представлены графики вероятностного распределения трафика. По ним можно заметить, что данное распределение достаточно точно соответствует экспоненциальному распределению. Подобного рода распределение свойственно другим видам трафика, полученным от платформ и программ, передающих данные в режиме реального времени. Из вышесказанного можно сделать вывод о том, что данные от исследуемых приложений должны доставляться на устройство клиента с максимально возможной скоростью.

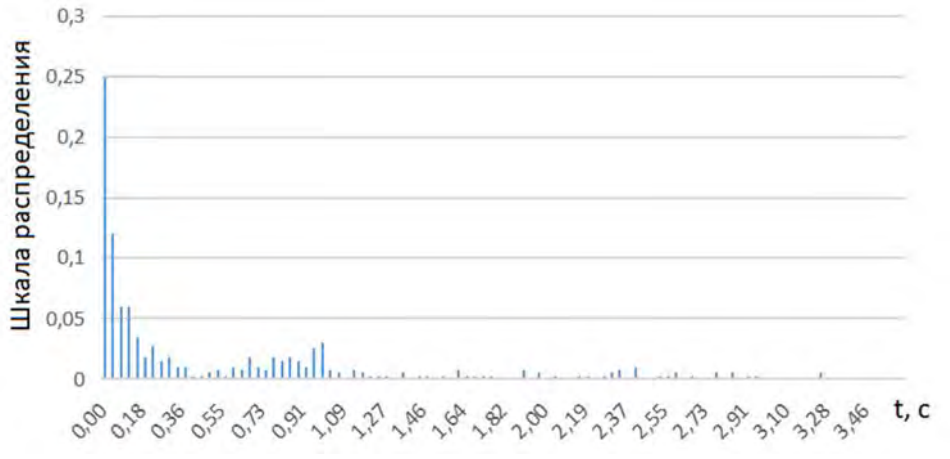


Рис. 3. График вероятностного распределения для приложения Pokemon GO

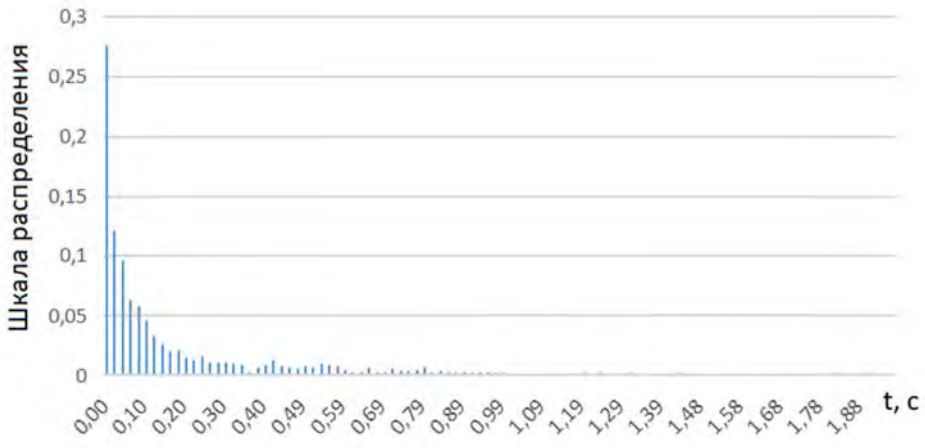


Рис. 4. График вероятностного распределения для приложения SketchAR

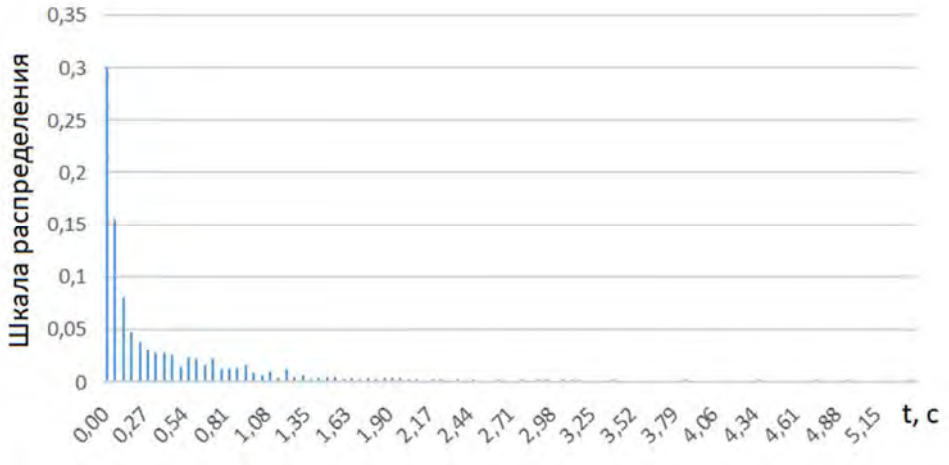


Рис. 5. График вероятностного распределения для приложения Ghost Snap AR Horror Survival

Вывод

В данной статье были получены результаты по задержке, джиттеру и пропускной способности для трёх приложений, включающих в себя технологию Дополненной реальности.

По результатам сравнения среднего значения интервалов между поступлениями сообщений для исследуемых приложений видно, что наибольшее значение соответствует приложению Ghost Snap AR Horror Survival. Это можно связать с полученными значениями пропускной способности. Наименьшее значение джиттера соответствует приложению Pokemon GO, так как для него наиболее важно стабильное качество связи.

Результаты из статьи в дальнейшем будут использованы в ходе подготовки выпускной квалификационной работы и разработки имитационной модели для исследования генерации трафика Дополненной реальности.

Список используемых источников

1. Тельтевская В. А., Зеленов В. В., Шустов Н. И., Кулик В. А., Киричек Р. В., Маколкина М. А. Идентификация устройств Интернета Вещей с помощью технологий дополненной реальности // Информационные технологии и телекоммуникации. 2017. Т. 5. № 4. С. 64–70.
2. Маколкина М. А., Окунева Д. В., Кулик В. А., Тельтевская В. А., Щербак А. С., Киричек Р. В. Исследование взаимодействия приложений дополненной реальности с облачными сервисами «1С» // Электросвязь. 2017. № 12. С. 31–35.
3. Маколкина М. А., Парамонов А. И., Кучерявый А. Е. Характеристики сетей связи и приложения дополненной реальности // Проблемы техники и технологий телекоммуникаций (ПТиТТ-2016). Первый научный форум «Телекоммуникации: теория и технологии» ЗТ-2016. 2016. С. 137–138.
4. Маколкина М. А., Парамонов А. И., Гоголь А. А., Кучерявый А. Е. Распределение ресурсов при предоставлении услуги Дополненной реальности // Электросвязь. 2018. № 8. С. 23–30.

УДК 004.491
ГРНТИ 50.41.27

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ РЕАЛИЗАЦИИ ROOTKIT

К. С. Кирилова, А. Ю. Цветков

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

С развитием и распространением информационных технологий нельзя не заметить, что вместе с ними распространяются и свойственные им угрозы. Например, с вредоносными программами нередко сталкиваются и пользователи, и администраторы компьютерных систем. В данной статье рассматриваются вредоносные программы для UNIX-подобных систем типа руткит уровня ядра, а также способы, которые могут ими использоваться для того, чтобы оставаться незаметными в атакуемой системе. Кроме того, руткиты уровня ядра по сравнению с прикладными программами имеют некоторые особенности, на которые также обращено внимание.

linux, модули ядра, анализ вредоносных программ, руткиты.

Понятие Rootkit появилось в мире UNIX, где под этим термином понимается набор утилит или специальный модуль ядра, которые злоумышленник устанавливает на взломанной им компьютерной системе сразу после получения прав суперпользователя. Иногда под руткитом понимают утилиту, предназначенную для получения этих прав, но в данной работе рассматриваются руткиты с первой точки зрения [1].

Руткит, как правило, содержит хакерский инструментарий (снифферы, сканеры) и троянские программы, замещающие основные утилиты UNIX. Он позволяет хакеру закрепиться во взломанной системе и скрыть следы своей деятельности путём сокрытия файлов, процессов, сетевых соединений. Также руткит может выполнять функции бэкдора.

Первые программы, скрывающие присутствие злоумышленника в системе, появились в мире UNIX в 1989 г. в виде пользовательских программ, изменяющих системные логи (тогда файлы `/etc/utmp`, `wtmp` и `lastlog`) так, что команды `who`, `w` и `last` не позволяли его обнаружить [2].

Поскольку в данной статье рассматриваются руткиты-модули ядра, необходимо обратить внимание на некоторые особенности работы модулей, не свойственные пользовательским приложениям.

Привилегии модулей ядра в операционной системе

Операционные системы (ОС) обычно имеют свою иерархическую структуру, свои логические уровни управления. Программы более высокого логического уровня (кольца) управления активно используют программы более низкого уровня (рис. 1). При этом, чем ниже логический уровень программ, тем большими привилегиями они обладают. Поэтому сбои в этих программах могут привести к более тяжелым последствиям, и степень их защиты должна быть выше.

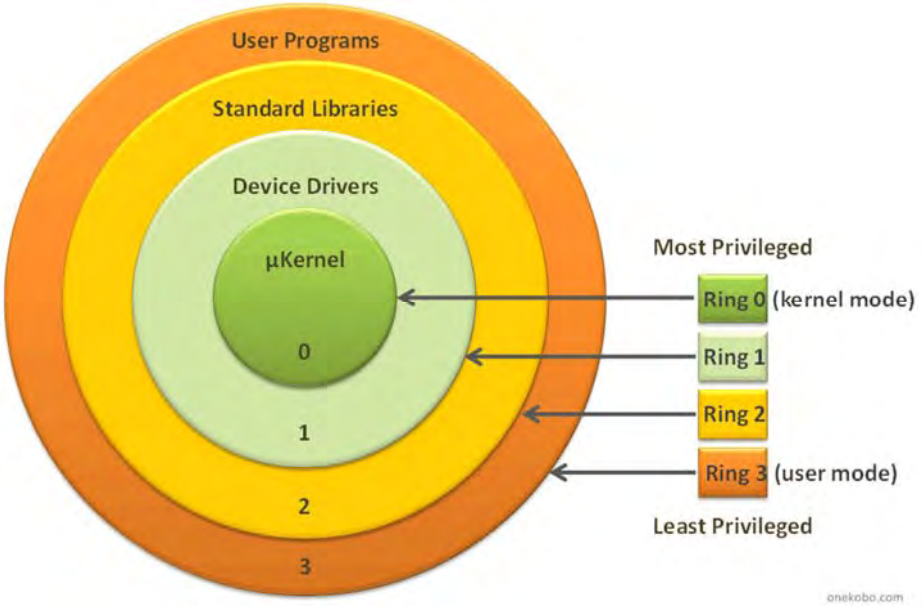


Рис. 1. Уровни привилегий ОС

Модуль ядра Linux – это скомпилированный двоичный код (объектный файл), который вставляется непосредственно в ядро Linux, работая таким образом в кольце 0. Здесь код исполняется без каких-либо проверок, но зато

с доступом к любым ресурсам системы. В настоящий момент широко используются загружаемые модули ядра (*Loadable Kernel Modules*, LKM), которые позволяют расширить функционал ядра, не переписывая и не перекомпилируя его целиком. Модули хранятся в `/lib/modules` и имеют расширение `.ko`. Список загруженных модулей находится в `/proc/modules`.

Важным для понимания работы модулей является понятие символьной таблицы ядра (*Kernel Symbol Table*). Её можно найти в `/proc/kallsyms` или в файле `System.map` (в разных дистрибутивах может находиться по разным путям). Каждая запись в псевдофайле `kallsyms` представляет экспортируемый (публичный) символ (например, функцию) ядра, который может быть использован загружаемым модулем. Туда же экспортируются все символы загружаемых модулей, и так модуль может быть обнаружен.

Кроме этого, существует внутренний неэкспортируемый список ядра. При загрузке модуля ядро добавляет его в этот список и исключает при выгрузке. Все операции, требующие перебора загруженных модулей, так или иначе сводятся к итерации ядром этого внутреннего общего списка. Если в этом внутреннем списке модуля нет, то считается, что он не загружен, и его, соответственно, нельзя выгрузить.

Так как модули ядра позволяют модифицировать само ядро, они широко используются для создания руткитов, поскольку наличие самых высоких привилегий в ОС позволяет использовать низкоуровневые функции ядра и с их помощью эффективно скрываться в атакованной системе. Ниже рассмотрены некоторые механизмы, которые могут использоваться вредоносными модулями ядра Linux для скрытия своего присутствия в системе.

Троянские программы

Изначально руткиты работали в пространстве пользователя. Они содержали троянские версии стандартных утилит, таких как `ps`, `ls`, `top` и `netstat`, модифицированных так, чтобы в выводе не отображалась информация о работающем рутките. Однако, поскольку при их использовании изменяются файлы на диске, такие руткиты могут быть обнаружены при сравнении контрольных сумм заменённых программ.

Перехват таблицы системных вызовов и таблицы прерываний

Некоторые руткиты способны скрываться с помощью перехвата таблицы системных вызовов ОС `sys_call_table`, в которой находятся функции, экспортируемые ядром. Сама эта таблица ядром не экспортируется, и один из самых простых способов её найти – парсинг `System.map`.

После того, как эта таблица найдена, выключается защита от записи, т. к. изначально она находится в режиме read-only. Для этого изменяется содержимое регистра CR0 [3].

Теперь можно перехватить обработчик операции чтения файла /proc/modules и сделать так, что любые нужные строки (например, содержащие данные о рутките) не будут выводиться, или изменить функцию чтения каталогов на собственную, которая не будет отображать файлы руткита.

Перехват таблицы векторов прерываний (*Interrupt Descriptor Table*, IDT), хранящей указатели на обработчиков прерываний, схож с перехватом таблицы системных вызовов и также позволяет руткиту использовать собственный обработчик, но работает на более низком уровне и позволяет изменять не только поведение системных вызовов, но и, к примеру, добавлять собственные обработчики исключений.

Например, в Linux прерывание 0×80 вызывается для обработки любого системного вызова. Руткиту, работающему в режиме ядра, не представляет большой сложности заменить запись в таблице прерываний по индексу 0×80 на собственный обработчик.

Патчинг VFS

Следующим механизмом, используемым руткитами режима ядра, является патчинг виртуальной файловой системы (*Virtual FileSystem*, VFS). VFS – уровень абстракции, лежащий между файловой системой и пользовательскими приложениями, предоставляющий последним единообразный доступ к различным файловым системам. Таким образом, изменяя функции-обработчики для VFS, можно изменить механизмы доступа к любым файловым системам, скрывая и файлы, и процессы, так как, согласно философии UNIX, «всё есть файл».

Кроме того, в VFS могут быть скрыты файлы руткита. При этом они по-прежнему хранятся на диске, но информация о них в физической файловой системе будет отсутствовать, а, чтобы эти файлы не были перезаписаны, сектора, в которых они находятся, помечаются как «bad sector». В таком случае эти файлы нельзя будет обнаружить, даже если просматривать содержимое диска с другого компьютера.

Direct Kernel Object Manipulation

Один из наиболее интересных механизмов получил название Direct Kernel Object Manipulation (DKOM) [4]. Основа этого метода, как следует из названия, строится на манипуляции с внутренними структурами ядра, поскольку загружаемый модуль имеет доступ к памяти ядра. Достаточно сложный и изощренный руткит может изменять объекты прямо в памяти.

К примеру, изменяемым объектом может быть внутренний список модулей, содержащий все модули, загруженные в систему. Ядро LINUX содержит массив структур `task_struct`, описывающих модули. В каждой структуре-описателе есть поле `list`, являющееся элементом связного

списка, посредством которого данный модуль линкуется в общий список модулей ядра (внутренний список ядра, упоминавшийся ранее).

Сокрытие модуля не представляет особых сложностей: необходимо просто исключить соответствующий элемент из этого списка. После этого скрываемый модуль не будет отображаться в выводе `lsmod`, и при попытке выгрузить его командой `rmmod` отобразится сообщение о том, что модуль не загружен и выгрузить его нельзя; при этом он будет выполняться в системе.

Другой задачей, решаемой с помощью DKOM, является скрытие запущенных процессов. В структуре `task_struct` содержатся указатели на `prev_task` и `next_task`. Чтобы скрыть процесс, необходимо удалить его из списков, содержащих `prev_task` и `next_task`, аналогично тому, как удаляется запись о модуле из общего списка модулей ядра. Но в этом случае нужно помнить, что планировщик задач пробегает по списку структур `task_struct`, чтобы рассчитать «добростность» (goodness) процесса и решить, выделять ли ему время для выполнения. Если процесс убран из этого списка, то планировщик не знает о его существовании, и процесс повиснет. Чтобы такого не происходило, нужно ещё и изменять логику работы планировщика, что усложняет исходную задачу.

Заключение

Рассмотрены основные методы, которые используются руткитами в Linux-системах. Исторически первый из них – внедрение троянских версий стандартных программ – достаточно легко обнаруживается и считается устаревшим методом. Он использовался руткитами пространства пользователя.

Напротив, работа руткита в пространстве ядра предоставляет широкие возможности скрыть своё присутствие в системе, поскольку в таком случае руткит обладает намного большими привилегиями в системе при взаимодействии с ядром. Такие способы, как перехват таблиц системных вызовов и прерываний, изменение работы VFS и манипулирование внутренними структурами ядра требуют некоторых знаний об устройстве ядра и его взаимодействии с модулями, они сложнее в реализации, но такие руткиты труднее обнаружить в атакованной системе [5].

Тем не менее, прежде, чем руткит-модуль получит такие широкие права в системе и начнёт работать в режиме ядра, его необходимо установить. Для этого нужны права суперпользователя, полученные, вероятно, с использованием каких-то уязвимостей других программ или эксплойтов, и это уже другая задача [6].

Список используемых источников

1. Raúl Siles Peláez. Linux kernel rootkits: protecting the system's "Ring-Zero" [Электронный ресурс] // SANS Institute. GIAC Unix Security Administrator. 2004. URL : https://www.giac.org/paper/gcux/243/linux-kernel-rootkits-protecting-systems-ring-zero/105411 (дата обращения 15.12.2018).
2. Hiding out under UNIX [Электронный ресурс] // Phrack Magazine. 1989. URL : http://phrack.org/archives/issues/25/6.txt (дата обращения 15.12.2018).
3. Hiding with a Linux Rootkit. Exploit development [Электронный ресурс]. URL : https://0x00sec.org/t/hiding-with-a-linux-rootkit/4532 (дата обращения 15.12.2018).
4. Jamie Butler. Direct Kernel Object Manipulation [Электронный ресурс]. URL : https://www.blackhat.com/presentations/win-usa-04/bh-win-04-butler.pdf (дата обращения 15.12.2018).
5. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика «РИ-2016»: материалы конференции. 2016. С. 168–169.
6. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

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

УДК 004.7
ГРНТИ 49.33.35

МЕТОДЫ ПРИМЕНЕНИЯ СЕТЕВОЙ СТЕГАНОГРАФИИ ДЛЯ ПЕРЕДАЧИ ИДЕНТИФИКАТОРОВ В ГЕТЕРОГЕННЫХ СЕТЯХ СВЯЗИ

Р. В. Киричёк, Д. Ю. Мицковский

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

В современном мире информация является самым распространённым ресурсом, обладающим, порой, огромной ценностью. Разумеется, для организации связи в сложных системах соединений между множеством пользователей необходима отлаженная, надёжная система, которая позволит обеспечить надёжную передачу данных между пользователями, а также её полную конфиденциальность, в случае необходимости. С появлением более мощной вычислительной техники стеганографические методы защиты данных становятся всё более актуальными, но они зачастую предполагают доступ к исходным данным. В случае отсутствия такого доступа эта задача решается путем применения методов сетевой стеганографии.

сетевая стеганография, заголовок пакета, RSTEG-стеганография, флаги.

Несмотря на то, что криптография до сих пор остаётся популярным методом защиты информации, большие успехи в разработке мощных вычислительных устройств (квантового компьютера, в частности) ставят под вопрос перспективы развития традиционной криптографии, ввиду необходимости разработки принципиально новых и более сложных алгоритмов из-за недостаточной надёжности уже устаревших методов. Актуальность проблемы подтверждают многочисленные исследования, направленные на нахождение перспективных альтернативных методов сохранения конфиденциальности информации [1]. На фоне данной проблемы всё более перспективным является сравнительно простой метод скрытия информации, называемый стеганографией. Стеганография в узком смысле – это семейство методов обработки данных, которое позволяет при сохранении высокого качества этих данных обеспечить невозможность (или хотя бы сложность) обнаружения самого факта присутствия спрятанной дополнительной информации нелегитимными пользователями [2]. То есть теперь злоумышленник не может украсть информацию по той причине, что не может найти её и не знает, где она может быть. Это значит, что для обеспечения безопасности не нужно применять какие-либо алгоритмы для шифрования данных, а нужно спрятать исходные данные так, чтобы при просмотре их не было видно человеку или программе и, таким образом, безопасно передать информацию получателю, знающему, где находятся данные. Такой метод обеспечения безопасности данных менее трудоёмкий. Однако чаще всего прямого доступа к данным, которые необходимо доставить от отправителя к получателю, нет. В таких случаях прибегают к методам сетевой стеганографии, которые, в частности, рассматриваются в статье [3]. В этой статье кратко рассматриваются принципы методов сетевой стеганографии и раскрываются их практические аспекты применения (эффективность, сложность реализации и т. д.). Авторы статьи делают упор на более детальное рассмотрение самых популярных методов сетевой стеганографии, такие как модификация заголовка (на примере протокола IPv4), а также RSTEG-стеганография.

Так как исходные данные недоступны для изменения, стеганограмма будет внедряться в «контейнеры», в которые эти данные упаковываются для транспортировки, а именно в сетевые блоки данных протоколов сетевой модели OSI. Блок содержит полезную нагрузку (данные, которые нужно передать) и служебные данные в заголовке и хвосте блока. Как хвост, так и заголовок могут использоваться для внедрения стеганограммы, но чаще для этого используют заголовок, ведь хвост часто содержит данные для проверки целостности пакета. Заголовок состоит из полей, значения которых

влияют на передачу блока. Исходя из задачи, необходимо найти поля, в которых при изменении служебных параметров не наблюдалось бы влияние на процесс передачи блока. Сперва рассмотрим метод модификации заголовка на примере протокола IPv4, который находится на сетевом уровне модели OSI. Единицей данных на этом уровне считается пакет данных. Задачей протокола, помимо передачи пакетов данных, является обработка и фрагментация пакетов для их передачи по сети с меньшим размером пакетов данных. Процесс внесения стеганограммы упрощается за счёт того, что пакеты независимы друг от друга и влияние на правильную работу протокола при внесении стеганограммы минимально (хотя и могут быть упорядочены с помощью поля идентификатора, о чём будет рассказано ниже).

Рассмотрим функции полей заголовка и попробуем найти те поля, изменение которых не повлияет на общую передачу данных. Поле «Идентификатор» или ID (рис. 1) используется в случае передачи нескольких пакетов для того, чтобы собрать упорядоченные фрагменты данных. Это значит, что необходимость в нём отпадает, если данные можно впоследствии упорядочить на стороне получателя, либо если данные передаются в одном сетевом пакете.

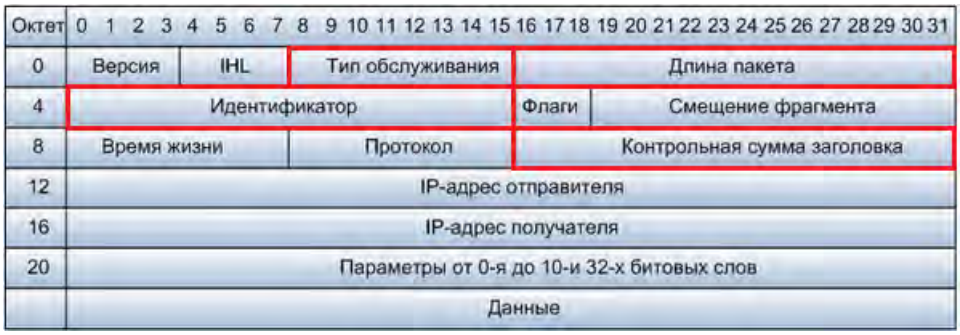


Рис. 1. Структура пакета IPv4

Данное поле занимает 16 бит, а это значит, что потенциально могут быть использованы 2 байта для передачи информации. Альтернативным вариантом будет использование поля «Длина пакета». Это поле не влияет на сам процесс передачи данных (только если не производится проверка размера пакета) и это поле позволяет внести значения от 20 до 65535 (ограничения размера пакета в байтах), что также даёт приблизительно 16 бит, но указание размера важно для отделения заголовка от данных, так что использовать это поле опасно, да и для передачи данных оно подойдёт слабо, поскольку допустимыми могут быть значения поля только от 5 до 15. Другим вариантом является использование поля «Тип обслуживания» (ToS). Часто пакету не требуется задавать особый приоритет, поэтому чаще всего это поле не используют, а значение по умолчанию соответствует 0. Это зна-

чит, что поле ToS можно использовать для помещения в него стеганограммы, а это даёт ещё 8 бит. «Контрольная сумма» в случае протокола IP вполне может подойти для внедрения данных, поскольку функции контроля целостности данных берут на себя другие уровни модели OSI и это поле редко задействуется, что даёт ещё 16 бит. Подводя итог анализу можно сделать вывод, что потенциально можно использовать поля длины пакета, ID, ToS и даёт 16 + 16 + 8 + 16 = 56 бит для передачи данных, что является неплохим результатом.

Теперь рассмотрим сетевую стеганографию на примере протокола TCP (спецификация RFC 793). Протокол TCP находится на транспортном уровне модели OSI. Единицей данных на этом уровне считается сегмент данных. Протокол TCP предоставляет ещё одну возможность для внедрения стеганограмм. При использовании TCP выполняет повторный запрос данных в случае потери этих данных или их искажения. Суть состоит в том, чтобы в сообщении, пересылаемом повторно, отправлять не те данные, что были в первичном сегменте, а те данные, которые необходимо скрыть. При отправке сегмента данных отправляется значение флага SYN, а получатель в случае удачной доставки сегмента отправляет сегмент назад к отправителю с установленным флагом ACK, указывающим, что поле номера подтверждения задействовано. Отправитель определяет факт получения сегмента с установленным флагом ACK как подтверждение того, что получатель получил SYN от TCP клиента (рис. 2а).

а) б)

Рис. 2. а) подтверждение передачи данных; б) RSTEG-стеганография

В случае, если получатель не получает сегмент данных, либо получает данные и отправляет подтверждение ACK, но оно не доставляется отправителю, то через определённое время (*Timeout* или задержку, не являющейся постоянной и зависящей от определённых условий, что в данном контексте не имеет особой важности, процесс выбора оптимального времени задержки описан в спецификации RFC 793) отправитель, не получив ACK, отправляет

сегмент данных повторно и цикл повторяется. Именно в момент повторной отправки данных можно поместить стеганограмму. Для этого сначала отправляется сегмент без стеганограммы. Получатель не отправляет подтверждение и через некоторое время отправитель производит повторную передачу данных, но с уже вложенной стеганограммой. Получатель вновь не отправляет подтверждение и отправителем снова передаётся сегмент данных без стеганограммы, уже на которую получатель отправит подтверждение (рис. 2б). Такую стеганограмму сложнее обнаружить, чем если бы осуществлялась простая модифицировался заголовка сегмента, поскольку сложно отследить такую передачу данных, ведь она маскируется её удачной передачей исходного сегмента без стеганограммы. Именно этот метод стеганографии и называют RSTEG-стеганографией (Retransmission steganography method – метод стеганографии повторной передачи). У этого метода стеганографии также есть уязвимость, заключающаяся в самом механизме этого метода. При помещении стеганограммы искусственно создаётся «обрыв» передачи, что само по себе является внештатной ситуацией, т. е. она не является частой. Однако частое повторение передачи скрытых сообщений с использованием механизма повторного отправления данных может вызвать нежелательные подозрения. Более того, слишком частые передачи стеганограмм могут вызвать определённую задержку передачи в связи с ожиданием отклика получателя.

Как можно заметить, отсутствие доступа к содержимому отправляемых данных не является преградой для осуществления передачи скрытых сообщений. Напротив, существует множество методов реализации данной задачи. Однако также можно сделать вывод, что не существует метода сетевой стеганографии, который делает передачу полностью скрытой. Любое изменение значения поля заголовка или изменение привычного хода передачи сообщения при желании всё же можно отследить. Эти методы работают тогда, когда не возникает повода обращать на какой-либо процесс особо пристальное внимание, т. е. необходимо оставить впечатление «обыденности» происходящего процесса передачи и не создавать частых ситуаций, которые обычно не происходят при передаче сообщений (частое повторение отправления того же сообщения, частые задержки передачи и т. д.). При использовании любого из методов стеганографии нужно соблюдать осторожность и не использовать только один метод, а комбинировать несколько из них. Так сложнее отследить факт маскировки передачи, ведь чаще вызывает подозрение не сама внештатная ситуация, а её частое повторение.

В статье было рассмотрено применение стеганографических методов защиты данных в случае отсутствия доступа к исходным данных путем применения методов сетевой стеганографии. На примере заголовка протокола IPv4 рассматривались возможные варианты внедрения стеганограммы

в процесс передачи данных. В дальнейших работах будут представлены результаты натурного эксперимента по маркировке трафика идентификаторами архитектуры цифровых объектов (DOA) внедренные в структуру пакетов на основе методов, представленных в статье, а также исследований в статье [4].

Список используемых источников

1. Дошина А. Д., Михайлова А. Е., Карлова В. В. Криптография. Основные методы и проблемы. Современные тенденции криптографии // Современные тенденции технических наук: материалы IV Междунар. науч. конф. (г. Казань, октябрь 2015 г.). Казань : Бук, 2015. С. 10–13.

2. Коржик В. И., Небаева К. А., Герлинг Е. Ю., Догиль П. С., Федянин И. А. Цифровая стеганография и цифровые водяные знаки : монография в 2 ч. / под общ. ред. проф. В. И. Коржика; СПбГУТ. СПб., 2016. 226 с.

3. Пескова О. Ю., Халабурда Г. Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи // Известия ЮФУ. Технические науки. 2012. № 12. С. 167–176.

4. Аль-Бахри М. С., Киричек Р. В., Бородин А. С. Архитектура цифровых объектов как основа идентификации в эпоху цифровой экономики // Электросвязь. 2019. № 1. С. 12–22.

УДК 004.7
ГРНТИ 49.33

МЕТОДЫ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ НА БАЗЕ АРХИТЕКТУРЫ ЦИФРОВЫХ ОБЪЕКТОВ

Р. В. Киричёк, Д. О. Реутова

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

Технология дополненной реальности на сегодняшний день является одной из самых перспективных направлений в сфере информационных технологий. Её стремительное развитие влечет за собой увеличение количества цифровых объектов, что в свою очередь ставит вопрос проблемы их идентификации. В данной статье рассмотрен возможный метод идентификации объектов дополненной реальности на базе архитектуры цифровых объектов.

DOA, цифровой объект, дополненная реальность, архитектура.

С каждым днем количество и разнообразие электронных устройств растёт, также, как и количество цифровых объектов, благодаря набирающей популярность технологии дополненной реальности. Многие крупные компании считают ее одной из самых перспективных направлений в IT-сфере, способную сделать жизнь людей более удобной. Дополненная реальность или «расширенная реальность» – это технология, дополняющая реальный мир цифровыми данными, которые можно увидеть с помощью электронных устройств. На сегодняшний день основной сферой применения дополненной реальности является развлечения и реклама, но ее можно встретить и во многих других областях, начиная от отображения информации об объектах вокруг через экран мобильного телефона, например, отзывы о ресторанах или историческая справка о местной достопримечательности, до создания реалистичных тренажеров для обучения врачей. Технология дополненной внедряется повсеместно, так как любой процесс или деловая активность только выигрывает от визуального наложения слоев дополнительной информации. Это приводит к тому, что возникает необходимость создать механизмы идентификации цифровых объектов – сущностей дополненной реальности, а также механизмы проверки их достоверности [1, 2].

Согласно терминам и определениям Международного союза электросвязи Интернет вещи бывают физические и виртуальные. Объекты дополненной реальности – это виртуальные интернет вещи, которые однозначно должны быть определены с помощью идентификаторов.

Выбор системы идентификации является важной задачей для разработки реестра цифровых объектов. Системы DOA, URI, XRI, IRI позволяют идентифицировать любой виртуальный или реальный объект в сетях связи общего пользования, независимо от наличия или отсутствия у него сетевого интерфейса. Чего нельзя сказать о системах, использующих аппаратные решения, например, IPv4 + MAC, IPv6, EMEI и другие. Кроме того, необходимо отметить, что не все существующие системы идентификации объектов отвечают требованиям развития сетей связи вследствие их гетерогенности.

Оптимальная система идентификации определяется следующими требованиями [3,4]:

– способность отвечать на множественные запросы;
– обеспечение различных уровней доступа;
– удаленная база данных;
– отсутствие динамических элементов и метаданных в идентификаторах.

Таким требованиям удовлетворяет система идентификации DOA. Архитектура цифровых объектов (*Digital Object Architecture*, DOA) – логическое расширение архитектуры Интернета, которое учитывает необходимость поддержки управления информацией в более широком смысле,

чем просто передача информации в цифровой форме из одного места в другое [5]. DOA предусматривает долгосрочное хранение информации, которой безопасно пользоваться и обмениваться. Архитектура определяет три основных компонента – систему резолюции, систему репозитория и систему реестра. Для взаимодействия перечисленных элементов в рассматриваемой архитектуре реализовано два служебных протокола: протокол системы резолюции IRP и протокол систем репозитория и реестра DOIP [6].

Базовым элементом взаимодействия этих систем является цифровой объект. В системе DOA каждый цифровой объект имеет уникальный и постоянный цифровой идентификатор – DOI (*Digital Object Identificator*), с помощью которого можно найти этот объект и получить о нём информацию [7, 8, 9].

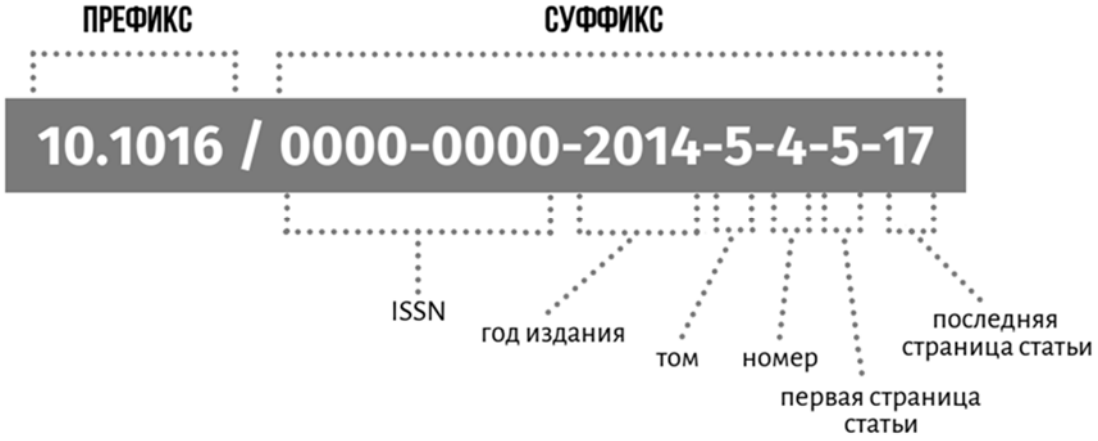


Рис. 1. Цифровой идентификатор

Структура идентификатора соответствует двухуровневой системе. На примере идентификатора, можно увидеть, что: первая часть – префикс, по которому определяется локальный регистр LHR, вторая часть – суффикс – однозначно идентифицирует конкретный объект (рис. 1).

Основные компоненты DOA [7, 8, 9]:

Система реестра представляет собой хранилище, в котором находятся метаданные о цифровых объектах, но не сама цифровая информация, что позволяет управлять доступом к объектам. Метаданные, находящиеся в реестре, могут управляться одной или несколькими системами репозиториев. Реестр также используется для регистрации цифровых объектов и для извлечения сведений о ранее зарегистрированном объекте (место, свойства, авторы, обладатели прав и т. п.) по его идентификатору. Доступ к этой системе осуществляется средствами протокола DOIP.

Система репозитория хранит цифровые объекты, а также управляет ими, включая перемещение цифровых объектов между репозиториями с сохранением всех метаданных. Система не требует от пользователя знания

технологий хранения цифровых объектов, обеспечивая тем самым долгоживущий механизм для доступа к цифровым объектам. Доступ к системе разрешен с помощью протокола DOIP.

Система резолюции отвечает за присвоение уникальных идентификаторов информации в цифровой форме, структурированной как цифровые объекты; преобразовывает идентификатор в актуальную информацию о соответствующем цифровом объекте. Информация о состоянии хранится в виде цифрового объекта. Быстрое разрешение обеспечивается протоколом IRP.

Данная система состоит из двух уровней резолюции:

– GHR – global handle registry (глобальный реестр);

– LHR – local handle registry (локальный реестр).

При установке локального сервиса создается пара ключей. Публичный отправляется в GHR (частный хранится в LHR), а сервису выделяется префикс и права на изменение записей.

На рис. 2 представлена концептуальная модель функционирования архитектуры цифровых объектов для идентификации объектов дополненной реальности.

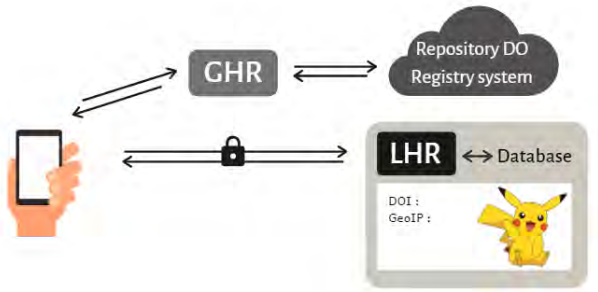


Рис. 2. Концептуальная модель функционирования архитектуры цифровых объектов для идентификации объектов дополненной реальности

Взаимодействие компонентов модели можно описать следующей последовательностью действий:

1) Клиент отправляет запрос на получение информации об объекте в глобальный регистр, с помощью имеющегося открытого идентификатора DOI.

2) Данный запрос обрабатывается GHR, после чего он отправляет запрос в систему реестров, затем в репозиторий, где находится информация о LHR отвечающего за запрашиваемый цифровой объект.

3) Данная информация отправляется пользовательскому устройству, которое устанавливает защищенное соединение с LHR, при помощи алгоритмов ассиметричного шифрования;

4) После обработки данного запроса LHR находит данные об объекте в базе данных и отправляет пользовательскому устройству.

Для исследования параметров функционирования рассматриваемого подхода в пакете Anylogic была разработана имитационная модель, которая описывала процесс разрешения идентификатора верхним уровнем GHR и следующим уровнем работы системы LHR.

На рис. 3 элемент *clients* соответствует источнику заявок на разрешение идентификаторов, поступающих от устройств. Элементы GHR_*buffer* и *GHR* имитируют глобальный реестр, который состоит из буфера заявок и сервера обработки идентификатора. GHR принимает поступившие заявки и равновероятно отправляет на конкретный локальный регистр – LHR (LHR_buffer_1, LHR_1), который конфигурируется непосредственно локальными администраторами.

Рис. 3. Имитационная модель процесса разрешения идентификатора на базе DOA

По результатам серии компьютерных экспериментов с имитационной моделью были получены гистограммы, представленные на рис. 4 (см. ниже). Согласно предварительной оценке следует, что реестр GHR является самым загруженным участком обработки заявок, а значит необходимо исследовать вопросы оптимизации алгоритмов работы с запросами во избежание отказов обслуживании при поступлении новых идентификаторов.

В статье были рассмотрены методы идентификации объектов дополненной реальности на базе архитектуры цифровых объектов, а также составные функциональные элементы DOA: система репозитория, система реестра и система резолюции. Была разработана имитационная модель DOA, которая описывает разрешение идентификаторов и проведены эксперименты.

В заключении, стоит отметить, что DOA является предпочтительной системой для идентификации объектов дополненной реальности, так как удовлетворяет предъявляемым требованиям и позволяет выявлять фальсификацию идентификатора за счет сопоставления различных параметров объекта дополненной реальности, занесенных как метаданные на сервере LHR. Основываясь на результатах компьютерных экспериментов можно сказать, что текущая инфраструктура системы требует дальнейшего масштабирования и распределения для того, чтобы быть способной выдерживать большие нагрузки и минимизировать время разрешения поступающих запросов.

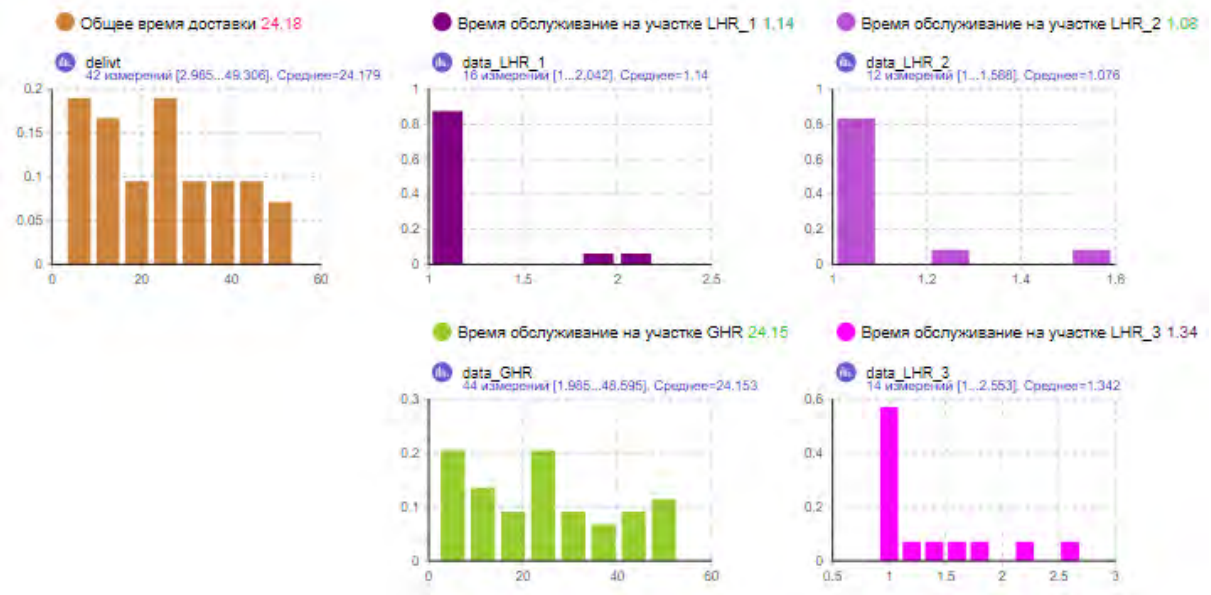


Рис. 4. Измерение времени обработки заявки на GHR и LHR

Список используемых источников

1. Цифровая идентификация объектов: технология и не только; под ред. М. А. Медриша. М. : Научное обозрение, 2016. – 28 с.

2. Данилов К. Н., Кулик В. А., Киричек Р. В. Исследование методов идентификации и аутентификации устройств интернета вещей // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 49–57.

3. Аль Бахри М. С., Киричек Р. В., Сазонов Д. Д. Моделирование системы идентификации устройств интернета вещей на базе архитектуры цифровых объектов // Труды учебных заведений связи. 2019. Т. 5. № 1. С. 42–47.

4. Аль-Бахри М. С., Киричек Р. В., Бородин А. С. Архитектура цифровых объектов как основа идентификации в эпоху цифровой экономики // Электросвязь. 2019. № 1. С. 12–22.

5. Michele Nitti, Virginia Pilloni, Giuseppe Colistra, Luigi Atzori. The Virtual Object as a Major Element of the Internet of Things: a Survey.

6. DONA Foundation. URL: https://www.dona.net/handle-system

7. Al-Bahri M., Ateya A. A., Muthanna A., et al Combating Counterfeit for IoT System based on DOA // Proceedings of the 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) 2018, St. Petersburg, Russia, November 5-9, 2018. IEEE, 2018. PP. 338–342.

8. Al-Bahri M., Yankovsky A., Borodin A., Kirichek R. Smart System Based on DOA and IoT for Products Monitoring and Anti-counterfeiting // 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC). IEEE, 2019. PP. 25–31.

9. Al-Bahri M., Yankovsky A., Borodin A., Kirichek R. Testbed for Identify IoT Devices Based on Digital Object Architecture // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Proceedings of 18th International Conference, NEW2AN 2018, and 11th Conference, ruSMART 2018, St. Petersburg, Russia, August 27–29, 2018. Cham: Springer, 2018. PP. 129–137.

УДК 004.7
ГРНТИ 49.33.29

АРХИТЕКТУРА ЦИФРОВЫХ ОБЪЕКТОВ КАК ПОДХОД К ИДЕНТИФИКАЦИИ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Р. В. Киричек, Д. Д. Сазонов

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

Проведен анализ возможности построения системы идентификации устройств интернета вещей на базе архитектуры цифровых объектов Предложена модель системы резолюции идентификаторов цифровых объектов Handling System как системы массового обслуживания. Выполнен оптимизационный эксперимент и получена конфигурация, позволяющая сократить время на разрешение идентификатора. Предложены пути возможного улучшения алгоритмов с целью сокращения времени на разрешения идентификатора.

интернет вещей, архитектура цифровых объектов, идентификация цифровых объектов, Handle System, система массового обслуживания.

В современном обществе значительную часть рынка технических систем занимает Интернет Вещей. Данные устройства находят место во многих областях, начиная от простого бытового использования, медицины и заканчивая применением в военных целях. По приблизительным оценкам, число устройств IoT составляет порядка 28 миллиардов и это цифра с каждым годом растет. Для обеспечения корректной и быстрой работы с огромным потоком информации от таких устройств требуется наличие надежной системы адресации и идентификации.

Основные особенности идентификации для Интернета Вещей [1, 2, 3, 4, 5, 6]:

– различный жизненный цикл устройств;

– взаимоотношение объектов интернета вещей с другими сущностями, не входящими в данную систему;

– требования к обеспечению механизмов защиты;

– возможность расширения системы идентификации до огромного числа устройств;

– прозрачность системы адресации и независимость от сети;

– гибкий и эффективный механизм резолюции идентификаторов.

На сегодняшний день существуют несколько подходов для построения системы идентификации устройств интернета вещей [1, 2]. Одним из возможных решений является построение системы идентификации на базе архитектуры цифровых объектов DOA (*Digital Object Architecture*).

Важной частью архитектуры DOA является система резолюции (*Handling System*). Каждому цифровому объекту в описываемой архитектуре ставится в соответствие уникальный идентификатор цифровых объектов – DOI (*Digital Object Identificator*). Данный идентификатор остается постоянным и не зависит от состояния цифрового объекта. Система резолюции связывает идентификатор с информацией о цифровом объекте [1, 2, 7].

Классическая система Handling является двухуровневой [1, 2]. Первым уровнем резолюции является глобальный реестр (GHR). Вторым уровнем является набор локальных реестров (LHR). Схематически архитектура представлена на рис. 1.

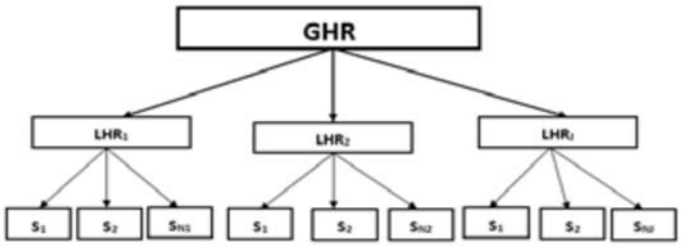


Рис. 1. Структура Handling System

Идентификатор DOI состоит из префикса и суффикса. Префикс позволяет установить сведения о локальном реестре цифрового объекта. Данное соответствие префикса и информации об администраторе хранится в глобальном реестре. Суффикс однозначно идентифицирует конкретный объект, и данная информация, связывающая суффикс с конкретным объектом хранится в локальном реестре.

Для того, чтобы охарактеризовать эффективность системы резолюции идентификаторов в архитектуре DOA, рассмотрим систему Handling как СМО (систему массового обслуживания).

В качестве системы СМО было решено взять модель с экспоненциальным распределением времени обслуживания заявок и экспоненциальным распределением времени между поступления заявок [5]. В качестве времени работы системы был выбран промежуток в 200 с.

Модель СМО была построена путем анализа существующей реализации системы резолюции [1, 4, 7]. В реализации Handling System используется не один GHR сервер, а несколько серверов, принадлежащих так называемым администраторам верхнего уровня MPA (*Multi-Primary Administrators*), контролируемых DONA Foundation [1, 2, 8]. Была установлена

инфраструктура серверов GHR и определена средняя задержка на разрешение запроса [9]. Все MPA сервера эквивалентны между собой, запрос на разрешение поступает последовательно на все сервера и анализируется первый полученный ответ [7, 9]. В таблице представлены характеристики серверов MPA, используемые в качестве GHR.

ТАБЛИЦА. Характеристики серверов MPA

MPA	IP адрес	Средняя задержка на разрешение, мс
Америка	132.151.20.9; 38.100.138.153; 38.100.138.131; 132.151.20.9; 2001:550:100:6::138:153; 2001:550:100:6::4; 132.151.1.179	243.548
Швейцария	156.106.193.160	71.33
Китай	119.90.34.34	473.583
Китай	47.90.103.77	410.693
Тунис	41.231.118.2	82.510
Германия	134.76.30.197	44.356
Саудовская Аравия	86.111.195.107	318.450
Кения	196.12.152.22	258.450

На рис. 2 приведена разработанная в пакете Anylogic модель СМО.

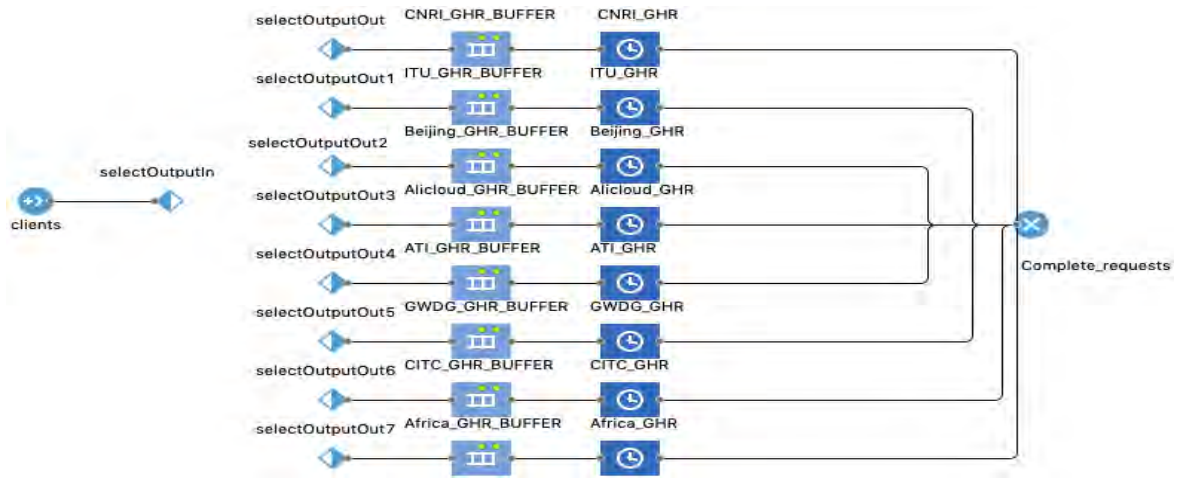


Рис. 2. Модель СМО

Каждый сервер MPA представляет собой набор из буфера заявок и сервера обработки идентификатора. Количество каналов в сервере обработки соответствует количеству серверов каждого конкретного MPA, приведенных в таблице.

Основными параметрами, влияющими на работу подсистемы резолюции Handling, являются величина сетевой задержки для поступающего запроса, скорость обработки этого запроса серверами и количество каналов обработки. Основным характеристикой для данной системы является среднее время разрешения одного запроса. Данное время будет зависеть как от конфигурации системы, так и от интенсивности нагрузки. На рис. 3 показана зависимость среднего времени разрешения идентификатора от интенсивности поступающих запросов при текущей конфигурации системы. Параметр λ является параметром экспоненциального распределения времени между поступлениями запросов.

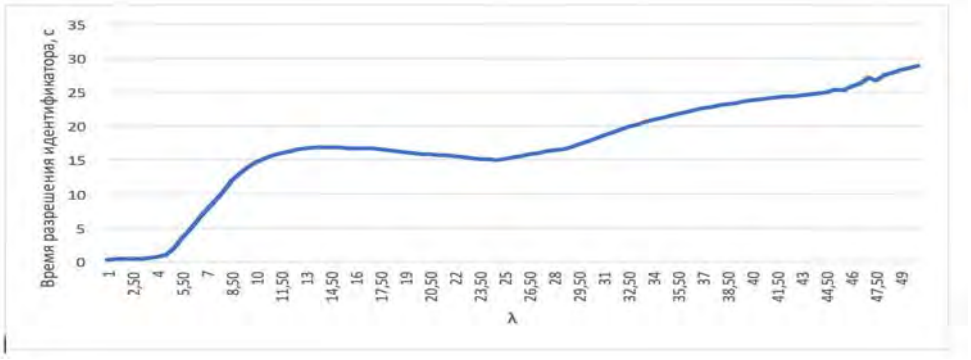


Рис. 3. Зависимость времени разрешения от интенсивности запросов

Как видно из рис. 3, с ростом интенсивности нагрузки увеличивается и среднее время разрешения одного идентификатора, причем при больших нагрузках это время доходит до 30 секунд, что достаточно много для реальных приложений.

Проведем оптимизационный эксперимент, направленный на установление наиболее подходящей инфраструктуры GHR серверов при текущей конфигурации временных задержек с целью снизить среднее время разрешения идентификатора. Основным параметром для оптимизации будет количество серверов GHR, используемых каждым из MPA. Время разрешения не более 1 сек. Оптимизационный эксперимент установил наиболее подходящее число серверов GHR: 7, 10, 1, 10, 10, 10, 10, 10. На рис. 4 показана кривая зависимости времени разрешения от интенсивности при конфигурации серверов, взятых в результате оптимизационного эксперимента.

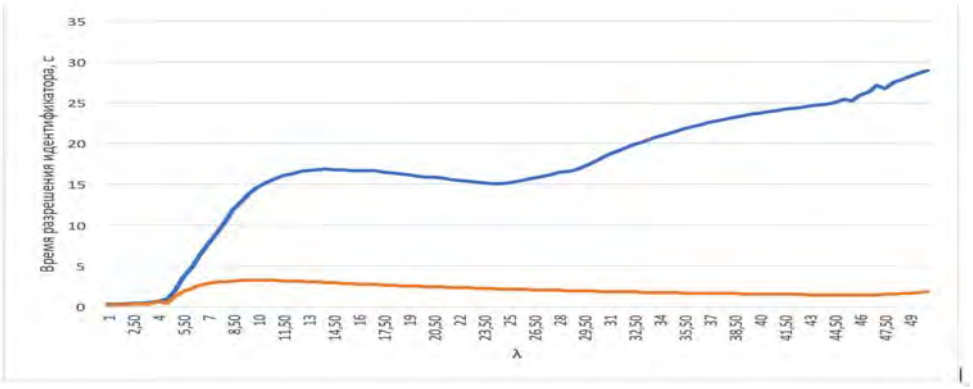


Рис. 4. Время разрешения запроса от интенсивности нагрузки при оптимальной конфигурации

По зависимости на рис. 4 видно, что при такой конфигурации серверов GHR, разрешение идентификатора в системе происходит гораздо быстрее. Прирост в скорости достигает 15 раз на максимальной интенсивности нагрузки.

Основываясь на результатах моделирования системы можно сделать выводы о том, что текущая инфраструктура системы Handling требует масштабирования и распределения для того, чтобы быть способной выдерживать большие нагрузки и минимизировать время разрешения поступающих запросов. Особенно актуально это при использовании системы Handling в задачах, связанных с идентификацией устройств интернета вещей [1, 3, 4].

Помимо инфраструктурного расширения существующей системы доработки нужно вести и в программной части Handling system. В результате анализа открытого исходного кода библиотеки, предоставляемой Handling.net [8] было установлено, что при отправке запроса на разрешение идентификатора к серверам GHR не производится предварительного анализа времени сетевой задержки до каждого из серверов. Каждый сервер из списка, приведенного в таблице, опрашивается в случайной последовательности и анализируется первый полученный ответ. Такая реализация несомненно сказывается на общем времени разрешения идентификатора. Поэтому требуется дальнейшая модификация исходного с целью создания функционала сортировки и выбора серверов GHR в зависимости от сетевой задержки от клиентского устройства.

Список используемых источников

1. Белявский Д. М., Дарбинян С. С., Засурский И. И., Казарьян К. Р., Левова И. Ю., Харитонов В. В. Цифровая идентификация объектов: технология и не только: монография. М. : Научное обозрение, 2016. 252 с.

2. Kirichek R. , Kulik V., Koucheryavy A. False clouds for Internet of Things and methods of protection // 18th International Conference on Advanced Communication Technology (ICACT). 2016. PP. 201–205.

3. Аль-Бахри М С., Киричек Р. В., Бородин А. С. Архитектура цифровых объектов как основа идентификации в эпоху цифровой экономики // Электросвязь. 2019. № 1. С. 12–21.

4. Тельтевская В. А., Зеленов В. В., Шустов Н. И. и др. Идентификация устройств интернета вещей с помощью технологий дополненной реальности // Информационные технологии и телекоммуникации. 2017. Т. 5, № 4. С. 64–70.

5. Тхаи Н. З. Удаленные вычисления через Web-сервер Matlab как система массового обслуживания // Вестник ИрГТУ. 2012. № 4 (63). С. 25–31.

6. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.

7. Handle.Net Registry. http://www.handle.net/index.html

8. DONA Foundation. https://www.dona.net/handle-system

9. Handle.Net Software. http://www.handle.net/download_hnr.html

УДК 004.7
ГРНТИ 49.33.29

АНАЛИЗ ТЕХНОЛОГИЙ СЕТЕЙ СВЯЗИ 2030

Р. В. Киричек, М. В. Склярова

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

Концепция Сети связи 2030 была анонсирована в июле 2018 года в Международном Союзе Электросвязи и представляет набор технологий и приложений не вошедших в описание сетей связи 5G/IMT-2020. В статье рассмотрены возможности развития технологий к 2030 году в различных сферах жизнедеятельности. Отдельно рассмотрены требования, которые будут предъявляться к новым к Сетям связи 2030: высокая скорость передачи данных, ультрамалые сетевые задержки, новые методы обработки массивов данных и др.

Интернет вещей, Тактильный Интернет, задержка.

Развитие сетей в 2030+ годах является интересной темой как для пользователей, так и для разработчиков. Для начала рассмотрим предпосылки перехода к Сетям связи 2030, а именно концепцию Интернета вещей. В Интернете можно найти много определений и характеристик концепции, но в основном, под Интернетом Вещей понимается единая сеть, объединяющая объекты реального и виртуального мира [1, 2].

Следовательно, это не просто устройства, которые объединены между собой беспроводными и проводными каналами связи и подключенные к сети Интернет, а более тесная интеграция реального и виртуального миров, в котором общение происходит в любое время, в любом месте и в любых сочетаниях.

Предполагается, что «вещи» будут принимать участие в бизнесе, социальных и информационных процессах. «Вещи» будут «общаться» между собой без постороннего вмешательства и будут способны перестроить жизнь общества. Роб ван Краненбург представляет Интернет вещей как четырехслойный пирог [1]:

1 уровень: Все объекты проходят идентификацию.

2 уровень: Обслуживание потребностей пользователя (например, «умный дом»).

3 уровень: Концепция «умного города».

4 уровень: Сенсорная планета.

Концепция Интернета вещей предполагает значительное увеличение беспроводных подключений, что натолкнуло исследователей на создание сетей связи пятого поколения 5G/IMT-2020, которые бы учитывали потребности по межсетевому взаимодействию устройств. Прогнозируется, что к 2030 году предельное число Интернет вещей составит 50 трлн. За счёт сверхплотных сетей на *n*-й площади можно будет обслуживать большое количество абонентов, что в свою очередь позволяет строить сложные иерархии сети. Помимо сверхплотности для сетей будущего необходима ультрамалая задержка.

С появлением ультрамалых задержек будут развиваться новые приложения, которые еще пару лет назад можно было отнести к научной фантастике: наносети, голограммы, телепортация и т. д. [3].

Концепция Тактильного Интернета вытекает из концепции Интернета вещей, только вместо взаимодействия двух машин, взаимодействовать будут машина и человек [4, 5, 6]. Концепция Тактильного Интернета опирается на то, что время, которое затрачивается на обработку пакета очень мало, а сетевая задержка при передаче информации составит 1 мс, что позволит передавать тактильные ощущения.

Исходя из этого, можно предположить, что появится приложение «Телеприсутствие». Суть заключается в создании аватара, который будет воспроизводить действия человека, который им управляет. Появятся новые типы взаимодействия: Human-to-Avatar (H2A), Avatar-to-Human (A2H), Avatar-to-Avatar (A2A) [3].

Аватар – это находящийся далеко от пользователя, разумный терминал сети, который оснащен различными манипуляторами, способен перемещаться по желанию человека и получать информацию с помощью сенсоров. Оператор управляет аватаром и его движениями «синхронизировавшись» с ним, автоматика формирует команды (оператора) и затем через канал связи (сотовой, спутниковой и т. п.) заставляют его двигаться [8].

Такие роботы-аватары помогут исследовать места, в которых человеку сложно или невозможно находиться, например, морские глубины или территории с повышенной радиацией.

Использование наносетей к 2030 году будет все больше внедряться в повседневную жизнь, а сами нановещи увеличат плотность сетей. В смартфоны могут быть встроены микро-спектрометры, к этому приводит прогресс в области спектроскопии. С помощью такого нововведения можно быстро получить спектрограмму и анализ, а значит, можно проводить анализы продуктов, чтобы убедиться в их качестве.

Голография, как настоящее трехмерное изображение согласно прогнозов обретет популярность к 2030 году.

Фундаментальные принципы голографии.

Согласно определения, голография – это особый фотографический метод, при котором сначала с помощью лазера регистрируются, а затем восстанавливаются максимально приближенные к реальным 3D-изображения. При освещении лазером голограммы формируют точный 3D-клон объекта и копируют его свойства.

Может существовать 2 типа голографической коммуникации:

1. Создание голограммы недалеко от дисплея после передачи реального 3D объекта с помощью мощных локальных вычислений.

2. Создание голограммы традиционным способом в отправляющей конечной точке, а затем ее передача по сетям.

Рабочим способом сейчас является первый вариант передачи, так как он предъявляет меньшие требования к возможностям сети, в то время как, второй вариант будет осуществлен, если возможности сети будут расширены.

Потенциальные требования к сети:

– Пропускная способность.

Динамический голографический тип коммуникации может потребовать на сотни или даже тысячи полос больше, по сравнению с требованиями для передачи 2D изображений. Например, для передачи изображения человека в полный рост (около 180 см) может потребоваться пропускная способность сети, превышающая 1 Тбит/с.

– Задержка.

Для изучения голографии обычно принимается от 30FPS (кадров в секунду) до 60FPS, а для проведения эксперимента может потребоваться 120FPS.

– Архитектура сети.

Огромный размер данных и низкая задержка могут сгенерировать требования для инновационной архитектуры [4].

На рис. 1 представлена экспериментальная схема для создания интерактивных голограмм. Учёные применяли лазеры, зеркала и камеры для создания вокселей – небольших пучков света, из которых можно создавать трёхмерные, интерактивные голограммы, которые способны реагировать

на человеческие прикосновения. Специалисты из Digital Nature Group пропускали фемтосекундный лазер через устройство, известное как пространственный световой модулятор и группу линз, направляя его на сканер Гальвано. Сканер направляет луч – ещё через две линзы – на зеркало, дабы показать окончательную форму вокселей. Технология получила название «Fairy Lights» («Сказочные огни») [9].

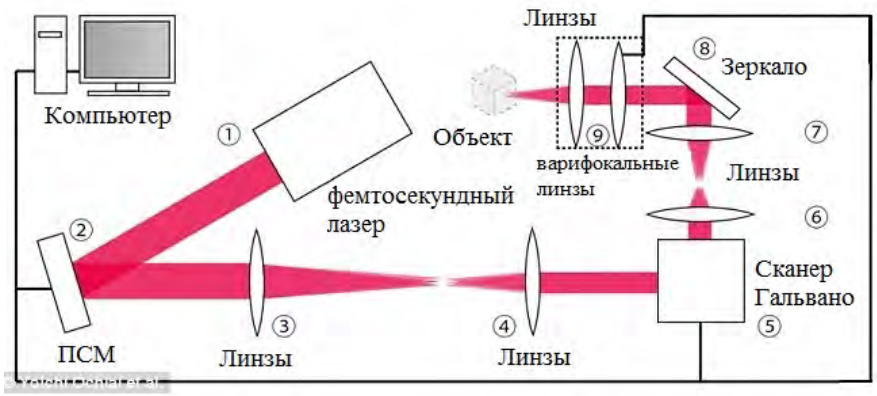


Рис. 1. Создание голограммы. Технология «Сказочные огни»

Развитие медиа услуг стремится к использованию всех органов чувств, чтобы предоставить пользователям наиболее полное общение. Развитие медиа услуг представляет собой постепенный переход от текста к голограмме через изображение, звук, видео, виртуальную реальность, причем с этим добавляется пункт «чувствительности»: смотреть, слышать, трогать, чувствовать на вкус, чувствовать запах. На данный момент мы получаем информацию через зрение и слух, но когда-нибудь эти возможности будут расширены и в пункте «Голограмма» уже будут доступны все возможные восприятия. На рис. 2. представлен процесс переходы к новым медиа услугам в привязке к органам чувств, которые будут использоваться для восприятия.

Рис. 2. Процесс переходы к новым медиа услугам в привязке к органам чувств

На рис. 3 представлены предполагаемые требования к сетевым параметрам необходимые для воплощения в жизнь таких технологий будущего, как голограммы.

Рис. 3. Предполагаемые требования к сетевым параметрам, Необходимые для передачи голограмм

Одним из методов достижения параметров сети, которые позволят реализовать сервисы в Сетях связи 2030 являются системы передачи данных на базе прогнозирования поведения трафика [7].

Принцип действия компенсирующих систем заключается в получении будущих значений управляющих или тактильных данных на основе некоторого промежутка предыдущих и их использовании вместо действительных значений, когда сигнал не был получен в нужный момент времени из-за длительности распространения, потери, искажения, либо был дублирован (рис. 4).

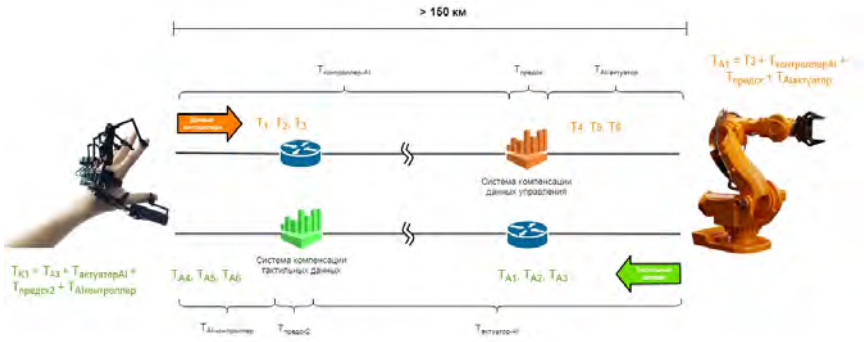


Рис. 4. Принцип действия компенсирующих систем

Такие системы возможно использовать при любой частоте передачи команд, но они ограничены вычислительной мощностью оборудования, удаленностью исполнителя и требуемой точностью [6].

Подытожив, можно сделать вывод, что Сети связи 2030 будут сверхплотными сетями с ультрамалыми задержками и приобретут новые характеристики благодаря развитию технологий в области сетей и систем. Такие сети будут полезны для пользователей, а также смогут привнести большой вклад в новые научные исследования.

Список используемых источников

1. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : «Любавич», 2011.
2. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.
3. Кучерявый А. Е., Бородин А. С., Киричек Р. В. Сети связи 2030 // Электросвязь. 2018. № 11. С. 29–33.
4. The Tactile Internet. Technology Watch report. Geneva : ITU-T, 2014. 24 p.
5. Кучерявый А. Е., Маколкина М. А., Киричек Р. В. Тактильный Интернет. Сети связи со сверхмалыми задержками // Электросвязь. 2016. № 1. С. 44–46.
6. Кучерявый А. Е., Выборнова А. И. Тактильный Интернет / Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Междунар. науч.-техн. и науч.-метод. конф. : сб. науч. ст. СПбГУТ. СПб., 2016. Т. 1. С. 6–11.
7. Владимиров С. С., Кучерявый А. Е. Механизм компенсации задержек для приложений Тактильного Интернета // Электросвязь. 2018. № 3. С. 62–67.
8. Алексей Бойко. Аватары // Аватары – Классификация роботов по-конструкции – Телеприсутствие. Роботы телеприсутствия. 2016. URL: http://robotrends.ru/robopedia/avatary (дата обращения 27.03.19).
9. Редакция Mediasat. Технологии. // Ученые используют лазеры для создания 3D-голограмм, к которым можно прикоснуться. 2015. URL: http://mediasat.info/2015/07/02/3d-holograms/ (дата обращения 30.03.19).

УДК 004.75
ГРНТИ 49.37.29

МОДЕЛИ ВЗАИМОДЕЙСТВИЯ БЕСПИЛОТНОГО АВТОТРАНСПОРТА С ИНФРАСТРУКТУРОЙ VANET ДЛЯ ОРГАНИЗАЦИИ СЕТЕВОЙ ПОДДЕРЖКИ

Р. В. Киричек, Е. Д. Филин

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

Развитие технологий, связанных с беспилотными автомобилями и инфраструктурой для беспилотного транспорта, способствует появлению новых моделей и методов

их взаимодействия. В этой связи, целесообразно рассмотреть и провести анализ текущих мировых исследований в данном направлении работ. В статье приведен обзор существующих технологических решений для организации беспилотного движения транспортных средств.

беспилотный автомобиль, Connected and Autonomous Vehicle (CAV), Vehicular Cloud (VC), Vehicle-to-Everything (V2X).

Беспилотный автомобиль – как объект критической информационной инфраструктуры

С появлением концепции Сети 2030 появилось виденье новых приложений и сервисов, которые могут быть реализованы на основе таких сетей [1]. Одним из новых приложений концепции Сети 2030 является беспилотный автотранспорт, именно его повсеместное внедрение диктует совершенно новые требования к сетевой инфраструктуре, а также взаимодействие со всеми элементами инфраструктуры Умного города.

В настоящее время наблюдается активное развитие тематики беспилотного автомобилестроения. Практически каждый автомобильный концерн разрабатывает концепты или прототипы легковых автомобилей, автобусов и тяжелых грузовых автопоездов. При анализе подходов по разработке таких автомобилей можно выявить одну особенность – на текущий момент беспилотный автомобиль ориентируется в пространстве самостоятельно. Самостоятельность заключается в сборе данных с датчиков, расположенных на автомобиле, и анализе на бортовом компьютере, с последующей выдачей управляющих команд на систему руления, торможения и пассивной безопасности.

В марте 2018 года произошел первый зарегистрированный случай гибели человека, когда автомобиль в беспилотном режиме стал виновником смерти человека. Анализ ДТП показал, что беспилотный автомобиль распознал человека, но алгоритмы решили не выдавать команду на торможение [2]. Типовая структура современного беспилотного автомобиля, состоящая из лидаров, радаров и видеокамер, не позволяет обеспечить абсолютную безопасность дорожного движения, так как не происходит взаимодействия с окружающими элементами инфраструктуры, что значительно снижает безопасность и возможность заранее предвидеть опасности на пути движения. Требуется дублирование функций бортового компьютера, чтобы исключить вероятность столкновения беспилотного автомобиля в случае отказа бортового компьютера.

Обзор публикаций по тематике беспилотного автотранспорта показывает, что в данной области ведется исследовательская работа над созданием решений и теоретических моделей в области взаимодействия Connected

and Autonomous Vehicle (CAV) и иными компонентами технической инфраструктуры, то есть автомобилей, поддержка функционирования которых будет проводиться на базе сети связи.

Возможность взлома систем беспилотного автотранспорта с целью совершения террористических актов, прекращения функционирования транспортной инфраструктуры и иных действий, способствующих угрозе национальной безопасности, является реальностью будущего, в связи с чем одной из определяющих задач, стоящих при создании систем беспилотного автотранспорта, является обеспечение безопасности функционирования систем, входящих в транспортную инфраструктуру будущего. С 1 января 2018 года в России вступил в силу Федеральный закон от 26.07. 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», который регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации целях ее устойчивого функционирования при проведении ее отношении компьютерных атак. Исходя из чего, транспортные системы беспилотного автотранспорта, следует относить к элементам критической информационной инфраструктуры.

Обзор моделей взаимодействия CAV

Основой сети обмена данными между беспилотными автомобилями и сетевой инфраструктурой является беспроводная ad-hoc-сеть, представляющая собой децентрализованную беспроводную сеть, не имеющую постоянной структуры. Автомобильные самоорганизующиеся сети (VANET) представляют собой радиосети со случайными мобильными абонентами, реализующих децентрализованное управление при отсутствии опорных узлов [3, 4, 5]. Основные задачи, решаемые VANET – организация безопасности и комфорта всех участников дорожного движения. Различают следующие основные системы, позволяющие взаимодействовать друг с другом: V2V, V2I, V2P, V2G, V2D и V2X [5]. Основной особенностью таких сетей является то, что автомобиль является генераторам трафика, а при рассмотрении беспилотного автотранспорта автомобиль можно рассматривать как генератор и приемник трафика.

Система «транспортное средство – транспортное средство» (*Vehicle-to-Vehicle*, V2V) обеспечивает автоматизированный обмен информацией между CAV. V2V-система предупреждает водителей об опасности фронтальных, боковых и задних столкновений с другими транспортными средствами, уведомлений об неисправностях дорожных средств и неудовлетворительного состояния дорожного покрытия и необходимости оказания помощи при аварии.

Система «транспортное средство – инфраструктура» (*Vehicle-to-infrastructure*, V2I) позволяет CAV обмениваться информацией с объектами интеллектуальной транспортной системы (ИТС) – светофорами, дорожными знаками переменной информации, спутниковой маршрутной навигации. VANET считается одной из составляющих интеллектуальной транспортной системы (ИТС), основной задачей которой является организация информационного обмена между транспортным средством и элементами технической инфраструктуры [6].

Система «транспортное средство – пешеход» (*Vehicle-to-pedestrian*, V2P) предназначена для обмена информацией с мобильными телекоммуникационными средствами пешеходов, находящимися поблизости.

Система «транспортное средство – электросеть» (*Vehicle-to-grid*, V2G) подразумевает подключение электромобилей в общую энергосеть для подзарядки автомобилей и возвращать ее обратно, продавая излишки электроэнергии.

Система «транспортное средство – устройство» (*Vehicle-to-device*, V2D) используется для обмена информацией с иными техническими средствами, такими как мобильные устройства водителя или пассажиров. Примером данного типа взаимодействия является приложение «Volvo on Call», выполняющего следующие функции [7]:

– Определение местонахождения автомобиля.
– Запуск стояночного обогревателя.
– Управление журналом поездок.
– Блокирование/разблокирование дверных замков.
– Дистанционная диагностика состояния автомобиля.

В 2018 году компании Huawei, Bosch и Vodafone провели испытания систем интеллектуальной мобильной телефонии на базе 5G/IMT-2020, позволяя машинам проводить обмен информацией друг с другом. Каждый автомобиль, используя Wi-Fi и сотовую передачу данных в радиусе 300 метров отправляет по тысяче сигналов в секунду, сообщая о своей скорости, траектории движения торможении, срабатывании ESP, подушек безопасности [8].

Система «транспортное средство – X» (*Vehicle-to-everything*, V2X) является универсальной, и позволяет организовывать взаимодействие между автомобилем и иными техническими компонентами дорожной инфраструктуры.

Для обеспечения безопасности дорожного движения бортовой компьютер должен обрабатывать большое количество информации с наименьшей задержкой, для чего необходим рост вычислительной мощности [7]. Согласно данным Bosch, за один километр пути каждая камера автономного

автомобиля собирает 100 Гб информации. Чтобы оперативно работать с таким массивом данных, NVIDIA создала Drive Pegasus – суперкомпьютер для машин с автопилотом, который совмещает высокую производительность (320 трлн операций в секунду) с высокой энергоэффективностью (1 трлн операций за 1 Вт.) [8].

По прогнозам компании Intel, объем трафика, который должен выгружаться сеть для анализа в реальном времени – 4000 Гб в сутки на один беспилотный автомобиль. Эта цифра формируется, исходя из следующих значений:

– Радар – 10–100 кб/с.
– GPS/GLONASS – 50 кб/с.
– Лидар – 10–70 Мб/с.
– Видеокамеры – 20–40 Мб/с.

Согласно технического отчета компании Huawei, круговая сетевая задержка при взаимодействии сетевой инфраструктуры поддержки с беспилотным автомобилем должна составлять не более 20 мс, что диктует необходимость многоуровневой системы обработки данных на базе распределенной облачной инфраструктуры.

В публикации [9] описаны рассмотрены два важных вопроса применения Big Data, а именно, передача информации в VANET и их использование для улучшения работы системы. Для того, чтобы не передавать весь внушительный объем информации по каналам связи, существует возможность производить обработку всех сохраненных данных для извлечения наиболее важных и дальнейшей их передачи в Vehicular Cloud для проведения анализа.

В публикации [10] рассмотрена архитектура Cloud-Based Vehicular network, состоящая из Vehicular Cloud, Roadside Cloud и Central Cloud. В Vehicular Cloud транспортные средства распределяют вычислительные ресурсы, организуют хранение между собой. Roadside Cloud необходимо для организации вычислений и обмена информацией между элементами придорожной инфраструктуры и автомобилями. Central Cloud предназначено для организации вычислений и обмена информацией с серверами через Интернет, и по сравнению с RSU имеет гораздо больше вычислительных ресурсов, и используется для сложных вычислений, хранения больших данных и глобальных решений.

Вывод

Проведение исследований в области сетевого взаимодействия беспилотного автотранспорта с инфраструктурой VANET является актуальной и востребованной задачей. Главные вопросы, которые необходимо решить – как увеличить скорость обработки информации, уменьшить задержки

и обеспечить при этом защиту от всевозможных атак на беспилотный автотранспорт.

Список используемых источников

1. Кучерявый А. Е., Бородин А. С., Киричек Р. В. Сети связи 2030 // Электросвязь. 2018. № 11. С. 29–33.

2. Беспилотник Uber сбил насмерть пешехода из-за настроек автопилота [Электронный ресурс]. URL: https://www.vedomosti.ru/technology/news/2018/05/08/768916-bespilotnik-uber-sbil (дата обращения 27.01.2019).

3. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : «Любавич», 2011.

4. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.

5. Ярцев С. В. Исследование и разработка моделей и методов распределения широковещательного трафика в сетях VANET : диссертация канд. техн. наук: 05.12.13 / Ярцев Сергей Викторович. Санкт-Петербург, 2018. 42 с.

6. Савельев И. С., Иконников И. В., Савыкина О. А. VANET – современные автомобильные коммуникации // Научно-практический электронный журнал Аллея Науки. 2018. № 1 (17). С. 25–29.

7. Поддержка Volvo Cars. URL: https://support.volvocars.com/. (Дата обращения 20.01.2019)

8. Автопилот – что нового? [Электронный ресурс]. URL: https://motor.ru/reports/autopilotovich.htm (дата обращения 18.01.2019).

9. Nan Cheng, Feng Lyu, Jiayin Chen, Wenchao Xu, Haibo Zhou, Shan Zhang, Xuemin (Sherman) Shen. Big Data Driven Vehicular Networks. 04.2018.

10. Rong Yu, Member, IEEE, Yan Zhang, Senior Member, IEEE, Stein Gjessing, Senior Member, IEEE, Wenlong Xia, Student Member, IEEE, Kun Yang, Senior Member, IEEE. Toward Cloud-based Vehicular Networks with Efficient Resource Management. 2013.

УДК 623.61
ГРНТИ 49.33.35

МЕТОД ПОВЫШЕНИЯ УСТОЙЧИВОСТИ СИСТЕМЫ УПРАВЛЕНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ ЗАЩИТЫ ТЕХНОЛОГИЧЕСКОГО ТРАФИКА

Ю. В. Ковайкин, П. В. Лебедев, О. Д. Прокофьев

Военная академия связи имени Маршала Советского Союза С. М. Буденного

В статье рассматриваются теоретические аспекты построения систем управления сетью, модель взаимодействия управляющей и управляемой систем, способы

управления криптомаршрутизаторами построенными по двухсегментной архитектуре, а также технические предложения по совершенствованию системы управления сети передачи данных путем защиты технологического трафика.

сеть передачи данных, криптомаршрутизатор, технологический трафик, двухсегментная архитектура.

Возрастающие потребности по предоставлению разнообразных услуг (речь, видео, передача данных и т. д.) высокого качества, предъявляют все возрастающие требования к устойчивому функционированию сетей передачи данных (СПД), а также к системе управления сетью. В разы возрастает циркуляция технологической информации, необходимой для решения задачи надежного функционирования СПД. В современных сетях передачи данных, команды управления телекоммуникационным оборудованием открытого сегмента, с центра мониторинга и управления сетью (ЦМУС) на управляемые узлы, передаются в открытом виде с использованием общепринятых протоколов (SNMP, Telnet и т. д.), что создает предпосылки нарушения надежности функционирования сети. Противник имеет возможность осуществить перехват команд управления телекоммуникационным оборудованием открытого сегмента и их модификацию, тем самым нарушить устойчивое функционирование сети передачи данных в целом, включая передачу конфиденциального трафика из закрытого сегмента.

Для мониторинга и управления сетью наиболее эффективным является иерархический подход построения СПД, так как он позволяет создать наиболее устойчивую структуру сети и более рационально распределить ресурсы. В иерархической сети при установке сети заранее выделяются один или несколько компьютеров, управляющих обменом данных по сети и распределением ресурсов. Также достоинством иерархической сети является более высокий уровень защиты данных [1].

На основе полученных результатов анализа построения СПД, системы управления сетью разработаны предложения по совершенствованию системы управления сети передачи данных путем защиты технологического трафика, заключающиеся в защите команд управления оборудованием СПД, путем организации специального управляющего «туннеля», при помощи криптомаршрутизатора построенного по двухсегментной архитектуре.

Конструктивно изделие, исполненное в двухсегментной архитектуре, представляет собой моноблок, в корпус которого вмонтирована двухсегментная объединительная плата; на базе каждого из ее сегментов собран универсальный вычислительный процессор [2, 3].

На рис. 1 приведена общая функциональная схема изделия, исполненного в двухсегментной архитектуре. Группы устройств, входящие в состав изделия, объединены в следующие функциональные блоки:

– блок обеспечения функционирования и управления изделием (БФУ),
– блок наружной маршрутизации (БНМ),
– блок внутренней маршрутизации (БВМ),
– блок криптографической обработки (шифратор) (БКО).

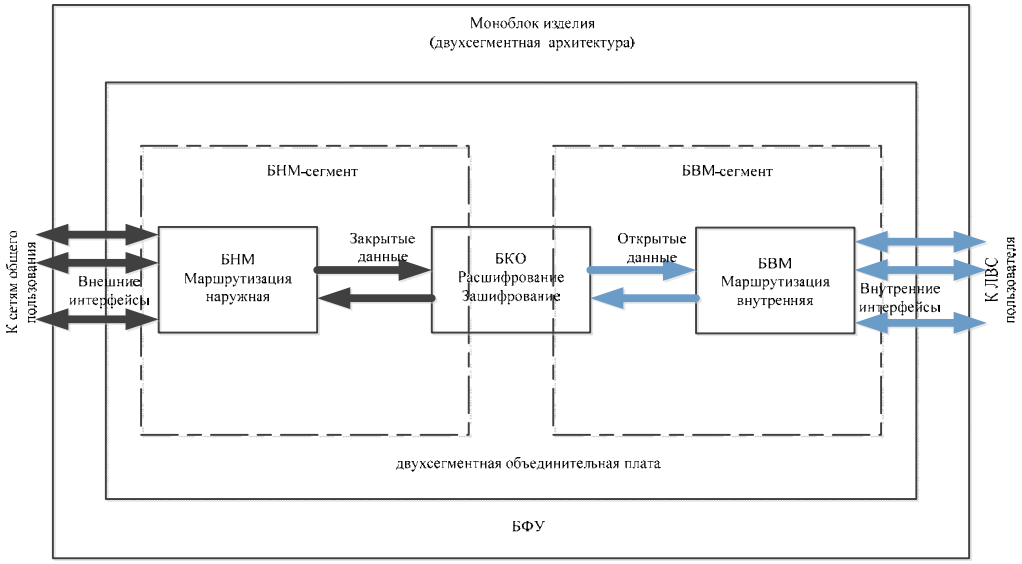


Рис. 1. Общая функциональная схема изделия (двухсегментная архитектура)

БФУ содержит следующие компоненты, обеспечивающие работу изделия:

– блок электропитания внутренних устройств;
– двухсегментную объединительную плату;
– технические средства локальной консоли управления изделием – клавиатуру, видеомонитор и устройство попеременного подключения консоли к тому из УВП, который в настоящий момент требует управляющих действий обслуживающего персонала.

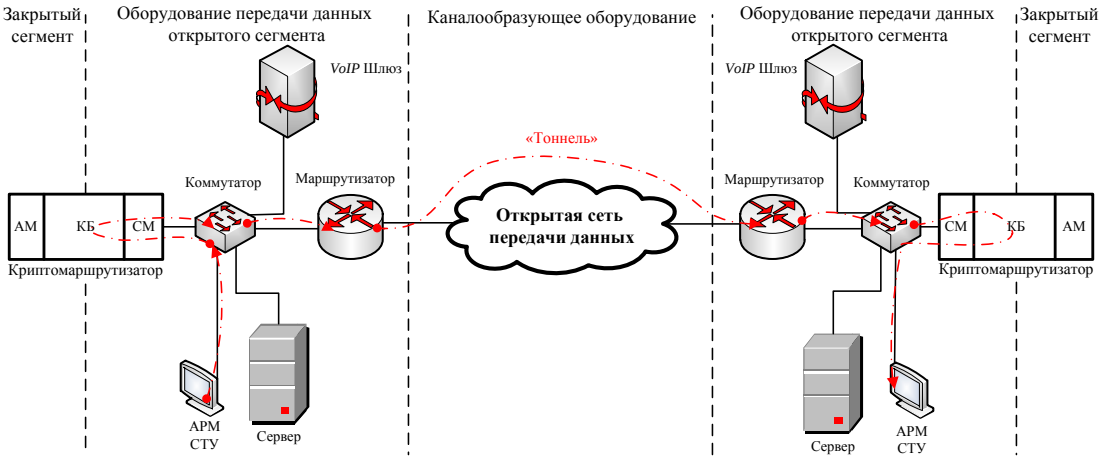
БНМ и БВМ обеспечивают маршрутизацию IP-потоков данных в подключенных к маршрутизатору сетях внешнего или внутреннего сегментах ЗСПД соответственно.

БКО, физически соединяя разделенные сегменты БВМ и БНМ, обеспечивает информационное взаимодействие между ними с надлежащим уровнем надежности, осуществляя при этом криптографическую обработку проходящих через него потоков данных. БКО выполняет все необходимые криптографические операции как по обработке потоков канала данных, так и по обработке потоков канала управления.

Управляющее изделие может удаленно (по защищенному каналу управления) получить объединенную базу параметров управляемого изделия, модернизировать ее и затем передать измененную конфигурацию на удаленное управляемое изделия.

На основе анализа архитектур систем управления сетью, систем управления сетями связи, порядка функционирования системы управления сетями связи была выявлена проблемная область по недостаточной защите, а в ряде случаев отсутствию защиты управляющей (технологической) информации, предназначенной для настройки телекоммуникационного оборудования СПД. Это создает предпосылки к воздействию на нее противника (перехват, модификация и т.п.), и тем самым к нарушению устойчивого функционирования СПД и показывает актуальность вопроса защиты управляющей информации и необходимость разработки предложений по внесению изменений в организацию управления сетью передачи данных [4].

Одним из способов решения поставленной задачи является применение существующих средств криптографической защиты информации (криптомаршрутизаторов) построенных по двухсегментной архитектуре, путем защиты управляющего трафика, с помощью организации специального управляющего «туннеля». Для описания разработанных предложений рассмотрим существующую схему построения СПД, представленную на рис. 2.



АМ – абонентский маршрутизатор;
КБ – блок криптографической обработки;
СМ – сетевой маршрутизатор;
АРМ СТУ – автоматизированное рабочее место сервера технологического управления;

Рис. 2. Схема построения СПД на основе защиты технологического трафика

Для защиты управляющей (технологической) информации, передающейся с автоматизированного рабочего места (АРМ) администратора ЦМУС к серверу технологического управления подчиненного узла, предлагается использовать следующий алгоритм взаимодействия:

1. Управляющая информация с АРМ администратора через коммутатор, поступает на сетевой маршрутизатор.

2. Для повышения системы защиты управляющего трафика на сетевом маршрутизаторе должна быть настроена система фильтрации входящего

трафика. Должно быть дано разрешение на прохождение команд управления только с IP-адреса АРМ сервера технологического управления (СТУ) ЦМУС (т.е. фильтрация по IP-адресам на сетевом уровне), только по протоколу TCP (фильтрация на транспортном уровне), а также с указанием конкретного порта прикладной службы, например: Telnet, SNMP и т. д. (фильтрация на прикладном уровне).

3. Пройдя систему фильтрации, технологические параметры поступают на криптоблок (КБ), где происходит их шифрование и помещение в туннель управления. КБ должен быть настроен таким образом, чтобы разрешать помещать в туннель только датаграммы поступающие с АРМ администратора сети.

4. Зашифрованные данные поступают снова на сетевой маршрутизатор в качестве исходящего трафика. Так же, как и для входящих команд управления на маршрутизаторе должны быть настроены три уровня фильтрации (на сетевом, транспортном и прикладном уровнях), и далее «закрытый» управляющий трафик передается на управляемый узел через внешнюю сеть.

5. При установлении соединения между сетевыми маршрутизаторами управляющего и управляемого изделий организуется криптографически защищенный канал управления. Весь телекоммуникационный обмен между управляющими и управляемыми изделиями при реализации рассмотренного алгоритма выполняется по криптографически защищенным каналам, причем шифрование выполняется на ключах канала управления.

6. Управляемый сетевой маршрутизатор принимает закрытую информацию, которая проходит через систему фильтрации, и передает ее на криптоблок.

7. Приемный криптоблок настраивается таким образом, что производит обработку входящего трафика, полученного только от ЦМУС. Получив закрытую информацию, осуществляет необходимые криптографические преобразования и передает открытую управляющую информацию сетевому маршрутизатору.

8. На сетевом маршрутизаторе информация, пройдя систему фильтрации трафика, через внешние интерфейсы поступает на сервер технологического управления.

Конфигурация оборудования должна быть настроена таким образом, чтобы запретить обратное прохождение команд управления от управляемого узла на ЦМУС.

Управляющее изделие может удаленно (по защищенному каналу управления) получить объединенную базу параметров управляемого изделия, модернизировать ее и затем передать измененную конфигурацию на удаленное управляемое изделие.

Данный алгоритм работы поддерживают принятые на снабжение криптомаршрутизаторы, что позволит, внеся незначительные изменения в программное обеспечение (ПО), повысить надежность функционирования СПД, путем криптографической защиты управляющей информации.

Предлагаемый способ защиты управляющей информации может найти практическое применение в сети передачи данных, что позволит защитить трафик управляющей (технологической) информации от воздействий противника и тем самым, повысить надежность функционирования сети в целом.

Список используемых источников

1. Бесков А. В., Ковайкин Ю. В., Лебедев П. В. Совершенствование системы управления сети передачи данных путем защиты конфигурационного трафика // Нейрокомпьютеры и их применение: Сборник трудов XVI Всероссийской научной конференции. Москва. 2018. С. 112–113.

2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. СПб. : Питер, 2010. 943 с.

3. Одоевский С. М. Инфокоммуникационные системы специального назначения : учеб. пособие. СПб. : ВАС, 2016. 437 с.

4. Бесков А. В., Ковайкин Ю. В., Кривошей О. И, Кирьянов А. С., Лебедев П. В. Направления развития системы связи ТЗУ с использованием средств криптографической защиты информации // Вопросы оборонной техники. 2018. инв. № 410. С. 18–21.

УДК 004.056
ГРНТИ 49.38.49

ИССЛЕДОВАНИЕ МЕХАНИЗМА ПРЕДОСТАВЛЕНИЯ ДОСТУПА К СЕРВИСУ IP-ТВ С ИСПОЛЬЗОВАНИЕМ RADIUS-СЕРВЕРА

М. М. Ковцур, А. В. Козьмян, Ю. В. Твердохлебова

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

Безопасность является одним из наиболее важных аспектов в сетях передачи данных. Для обеспечения контролируемого доступа к сети, авторизации и аутентификации пользователей часто используется AAA сервер. IP-TV – технология цифрового телевидения в сетях передачи данных по протоколу IP, новое поколение телевидения. Как правило, при организации трансляций IP-TV используется многоадресная рассылка трафика, а также аутентификация и авторизация респондентов. В исследовании рассматриваются клиентская авторизация для доступа к услуге IP-TV с использованием сервера RADIUS, представлена модель процесса авторизации.

авторизация, граф, IGMP, IP-TB, multicast, RADIUS.

IP-TV – это системы, в которых IP-протоколы сети Интернет используются для трансляции телевизионных программ и применяется пакетная передача данных [1]. Как правило, при организации вещания IP-TV используется многоадресная передача. Многоадресный трафик используется для потоковой передачи видео и доставляет видеоконтент неограниченному количеству подписчиков одновременно без перегрузки сети. При организации службы каждый канал представляется, как отдельная многоадресная группа. Для просмотра контента пользователь должен подписаться на группу, а по окончании просмотра - покинуть группу. Для присоединения или выхода из группы используется протокол IGMP (*Internet Group Membership Protocol*).

Модель исследуемой сети представлена на рис. 1 и состоит из IP-TV сервера, маршрутизатора, коммутаторов и M IP-TV клиентов, причем клиенты могут смотреть, как разные, так и одинаковые каналы.

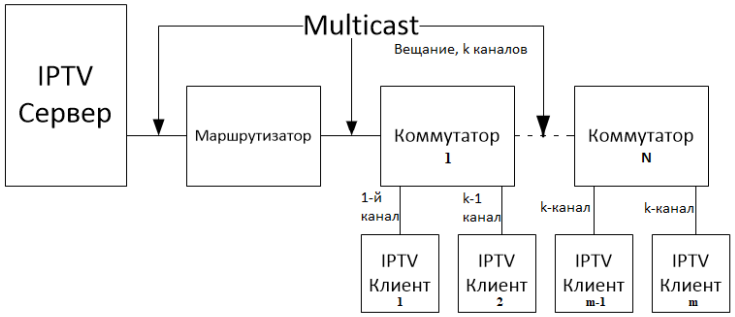


Рис. 1. Модель сети для предоставления услуги IP-TV

Одним из важных аспектов в организации IP-TV является авторизация пользователей при запросе канала. Для этой задачи можно использовать списки доступа IGMP [2], но этот подход требует обновления списков на оборудовании при изменении тарифного плана клиента. Наиболее популярными подходами являются использование медиа-шифрования и порталов IP-TV, а также применение RADIUS-авторизации для многоадресной рассылки. При использовании IP-TV портала оператор загружает специализированное программное обеспечение на оборудование клиента, но такой подход уменьшает количество поддерживаемого оборудования.

При внедрении IP-TV RADIUS-авторизации возникают дополнительные временные затраты, вызванные необходимостью коммутатора запросить разрешение для подключения в группу каждого отдельного клиента. Параметр RADIUS Timeout, который задает время ожидания коммутатором

ответа RADIUS Response от сервера, прежде чем признать попытку авторизации неудачной, также может оказать влияние на время получения доступа к услуге [3]. Все эти задержки влияют на время подключения канала [4].

Исследование посвящено оценке влияния параметров канала связи на скорость предоставления доступа к услуге IP-TV. Модель процесса авторизации клиента IP-TV представлена на рис. 2.

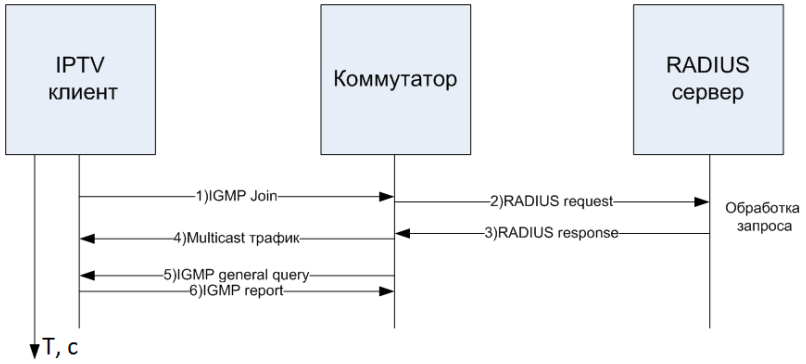


Рис. 2. Модель процесса авторизации клиента при доступе к услуге IP-TV

Пусть используется канал связи со следующими параметрами – задержка D_{dist}, вероятность битовой ошибки P_0, скорость C_{dist}.

Модель процесса авторизации пользователя представлена на рис. 3. Для оценки временных характеристик используются следующие параметры модели:

– время передачи запроса на доступ к услуге от клиента до порта коммутатора провайдера – T_{12} (мс);

– время обработки запроса пользователя коммутатором, зависит от оборудования – T_{23} (мс);

– время ожидания коммутатором ответа RADIUS Response от RADIUS-сервера – $T_{timeout}$ (с);

– время между повторными отправками запросов с коммутатора на RADIUS сервер – $T_{\text{повтор}}$(с);

– количество повторов сообщения RADIUS Request коммутатором $n_{\text{повтор}}$;

– задержка в канале связи – D_{dist} (мс);

– время доставки multicast-пакета от порта коммутатора до пользователя– T_{56} (мс);

– время кэширования multicast-потока на IP-TV клиенте пользователя T_{cash} (мс);

– размер пакета *AccessRequest* – N_{rqr} (бит);

– размер пакета IGMP – N_{rqi} (бит);

– размер пакета *AccessResponse* – N_{rs} (бит);

– размер пакета Multicast – N_m (бит);

– скорость канала связи – C_{dist} (Мбит/с).

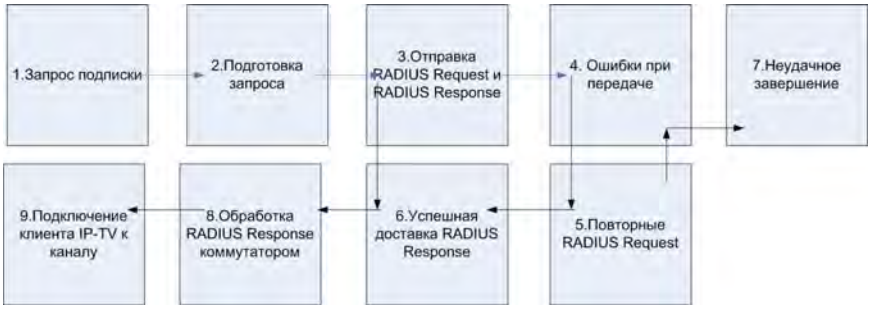


Рис. 3. Модель процесса авторизации клиента

Составим вероятностный граф, описывающий процесс авторизации пользователей для доступа к услуге IP-TV [5]. Граф представлен на рис. 4, где каждая ветвь соответствует переходу из одного состояния в другое согласно модели процесса авторизации клиента.

Нумерация вершин графа соответствует нумерации узлов рис. 3. Переход 1–6 соответствуют успешному завершению процесса авторизации, когда переход 1–7 означает возникновение ошибки. Переход 1–9 соответствуют доступу пользователя к услуге IP-TV.

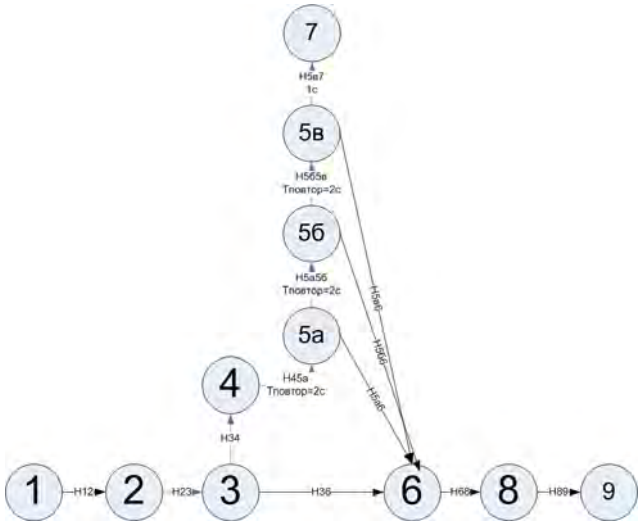


Рис. 4. Граф процесса авторизации клиента

Вероятность успешной передачи запроса авторизации от коммутатора к RADIUS-серверу будет иметь вид:

$$p_{36} = (1 - P_0)^{N_{rqr}},$$

где N_{rqr} – размер сообщения RADIUS Request в битах, P_0 – вероятность битовой ошибки в канале связи [6].

Тогда производящая функция ветви H_{36} имеет вид [7]:

$$H_{36} = p_{36} \times x^{T_{36}},$$

где:

$$T_{36} = D_{dist} + \frac{N_{rqr}}{C_{dist}}.$$

Аналогичным образом определяются другие производящие функции.

Ветвь неуспешного завершения процесса авторизации будет иметь вид:

$$H_B = H_{12} * H_{23} * H_{34} * (H_{45а} * H_{5а5б} * H_{5б5в} * H_{5в7}).$$

Ветвь успешного завершения процесса $T_{success}$ авторизации будет иметь вид:

$$H_A = H_{12} * H_{23} * (H_{36} + H_{34} * H_{45а} * \\ * [H_{56б} + \{H_{5а5б} * ([H_{5б5в} * H_{5в6}] + H_{5б6})\}]) * H_{68} * H_{89}.$$

Вычислим производящую функцию ветви успешного завершения протокола. Время успешного завершения $T_{success}$ будет иметь вид:

$$T_{success} = \frac{d}{dx} H_A(x).$$

Вероятность успешной авторизации пользователя для доступа к услуге IP-TV будет иметь вид [8]:

$$P_d = H_A(x = 1).$$

Дальнейшими задачами исследования являются количественная оценка таких показателей модели, как вероятность успешной авторизации пользователя, среднее время доступа к услуге, а также подтверждение полученных зависимостей путем выполнения эксперимента.

Список используемых источников

1. Герасимова В. В. Передача ТВ программ по IP-сетям // Теория и практика современной науки. 2016. № 7 (13). С. 96–100.

2. RFC 3376: Internet Group Management Protocol, Version 3 [Электронный ресурс]. URL: https://tools.ietf.org/html/rfc3376/ (дата обращений 16.03.2019).

3. RFC 2865: Remote Authentication Dial In User Service (RADIUS) [Электронный ресурс]. URL: http://www.rfc-base.org/rfc-2865.html/ (дата обращений 16.03.2019).

4. Гольдштейн Б. С., Елагин В. С., Сенченко Ю. Л. Протоколы AAA: RADIUS и DIAMETER. Серия «Телекоммуникационные протоколы». Книга 9. СПб. : БХВ-Петербург, 2014.

5. Никитин В. Н., Юркин Д. В. Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 42–46.

6. Ковцур М. М., Никитин В. Н., Юркин Д. В. Оценка вероятностно-временных характеристик защищенной IP-телефонии // Защита информации. Инсайд. 2012. № 4. С. 64.

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: сборник научных статей: в 4-х томах. 2017. С. 295–301.

8. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

УДК 004.056
ГРНТИ 19.31

РАЗРАБОТКА СИСТЕМЫ УЧЕТА ПОСЕЩАЕМОСТИ СТУДЕНТОВ МАСШТАБА ВУЗА

М. М Ковцур, П. Э. Луеке

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

Одной из наиболее распространенных задач в любой организации является отслеживание и постоянная проверка посещаемости своих сотрудников. Такие технологии, как RFID и веб-приложения, используются каждый день практически в каждой организации. В докладе описывается концепция системы учета посещаемости студентов с использованием веб-технологий и систем RFID. Основное внимание уделяется двум возможным подходам. Первый из них основан на веб-инфраструктуре, используя возможности клиент-серверных приложений с веб-аутентификацией. Второй - на технологиях RFID и беспроводной передачи данных. Для каждой реализации проводится полный анализ с сильными и слабыми сторонами с точки зрения безопасности, затрат и сложности внедрения. Определяются возможные атаки, направленные на систему.

учет посещаемости, RFID, веб приложение.

Учет посещаемости является важной и актуальной задачей для любой организации [1]. В работе представлена концепция системы учета посещаемости с использованием технологий RFID и веб-сервисов в рамках вуза. Выявлены потенциальные атаки, направленные на разрабатываемую систему.

Цель системы состоит в упрощении контроля посещаемости студентов в течение учебного года. Предложены два возможных подхода для реализации системы учёта посещаемости: веб-приложение и RFID терминал.

Первый подход состоит в разработке веб-приложения, позволяющего студентам войти в систему и тем самым зафиксировать посещение текущего занятия. Для входа в веб-приложение студенты могут использовать мобильные телефоны, планшеты и ноутбуки, подключенные к беспроводной сети университета. Студентам предоставляется доступ к веб-интерфейсу, а преподаватель имеет доступ к панели управление со всей статистикой, относящейся к студентам. Для обеспечения высокого уровня защиты вход преподавателя в систему может осуществляться с применением личных сертификатов. Сценарий работы системы представлен на рис. 1.

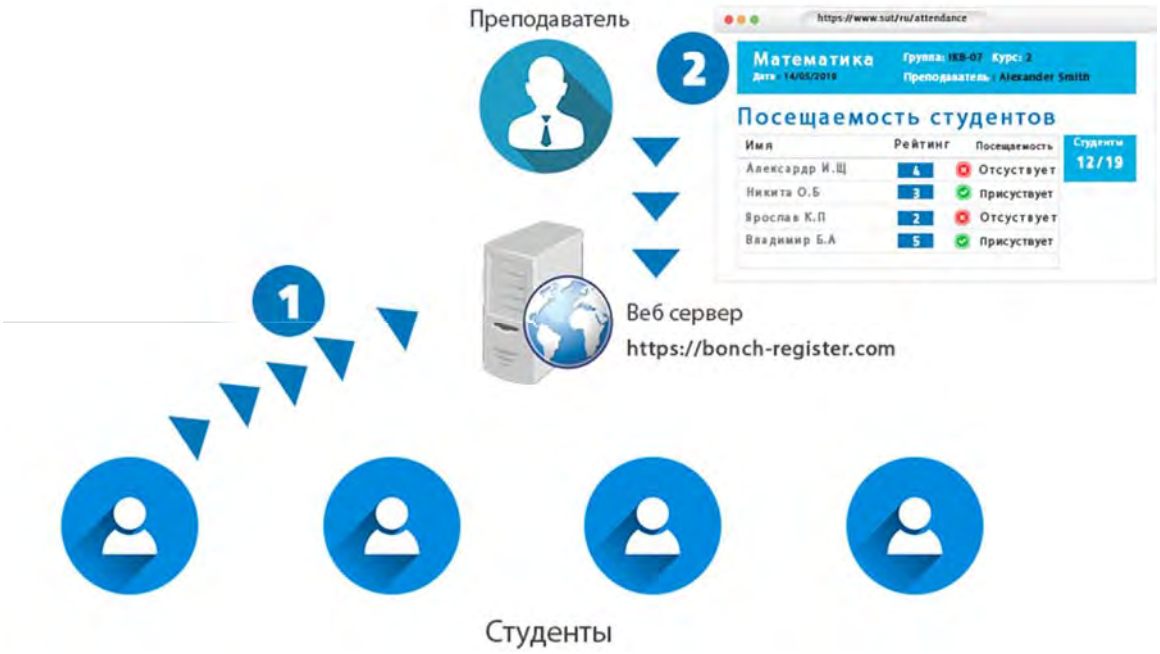


Рис. 1. Сценарий учета посещаемости через веб приложение

Важно учитывать расположение веб-сервера, которое может быть локальным или внешним по отношению к корпоративной сети. Локальный сервер подразумевает регистрацию только из сетевого периметра, а внешний сервер позволяет организовать доступ из любой сети. Система также может быть развернута в облачной инфраструктуре предприятия [2].

Для создания веб приложения используются такие технологии, как HTML, CSS, Javascript на стороне клиента, PHP и база данных MySQL на стороне сервера. Для обеспечения высокой масштабируемости могут также применяться NoSQL базы данных [3].

Второй подход требует разработки RFID-терминала сбора данных. Возможными компонентами такого терминала являются:

– платформа Arduino UNO;
– модуль Wi-Fi ESP, для HTTP запросов;
– LCD экран;
– RFID считатель;
– SD-карта в качестве хранилища.

Студенты приходят в аудиторию со своими пропусками и регистрируют их с помощью преподавательского мобильного RFID считывателя. Мобильное устройство считывает данные с карты и отправляет запрос с помощью модуля ESP на сервер. Серверная составляющая добавляет запись о посещении студента в базу данных и возвращает результат, который будет отображаться на экране терминала. Если в данный момент сеть недоступна, запись о посещении студента регистрируется в файле на SD-карте и будет синхронизирована с базой данных, когда сеть снова станет доступной.

Рис. 2. Сценарий учета посещаемости с использованием RFID устройства

Для обеспечения непрерывного функционирования системы необходимо проанализировать подходы обеспечения информационной безопасности решения [4]. Можно выделить несколько потенциальных нарушителей, которые могут выполнять атаки на систему: внутренние и внешние.

Внутренними нарушителями могут быть студенты или сотрудники. Выделены несколько возможных атак, которые могут реализовать эти нарушители:

– регистрация посещаемость из любой аудитории университета;

– регистрация отсутствующих студентов;

– модификация записей работниками, имеющими прямой доступ к базе данных.

Внешними нарушителями могут являться хакеры, которые пытаются получить информацию, осуществить доступ к системе или нарушить ее целостность. Они могут реализовать такие атаки, как: SQL-инъекции, XSS, перехват трафика, DDOS-атаки, выполнение кода сервера.

В соответствии с исследованиями компаний [5, 6, 7] в области информационной безопасности (*Kaspersky*, ESET, *BitDefender*), наиболее распространенные типы атак для взлома удаленных систем являются: DDOS атаки, подмена DNS кэша, сканирование портов, TCP desynchronization, SMB relay, ICMP атаки.

Для сокращения числа внутренних нарушений безопасности предлагается реализовать сбор информации о терминалах студентов. При регистрации студента в системе, кроме основной информации (имя, группа), также сохраняется дополнительная информация об устройстве пользователя, например, тип операционной системы, версия, язык по умолчанию. Вся эта информация учитывается при проверке посещаемости. При попытке сту-

дента зарегистрировать отсутствующего студента, информация об устройствах сравнивается, и сообщение об этих попытках отправляется на панель управление преподавателя. Другое решение – сравнение IP-адресов, с которых исходит регистрация.

Существует несколько коммерческих решений по организации контроля посещаемости. Среди них такие популярные системы, как Keka [8], greytHR [9] и Zoho people [10]. Была выполнена оценка стоимости развертывания этих систем для 1000 студентов. Результат представлен в таблице.

ТАБЛИЦА. Стоимость развертывания систем учета посещаемости для 1000 студентов

Система учета посещаемости	Стоимость развертывания системы, руб.
Keka	4 800 000
GreytHR	480 000
Zoho People	1 900 000

Из таблицы можно сделать вывод, что большинство существующих систем учета посещаемостью имеют высокую стоимость. По этой причине целесообразно разработать систему, имеющую невысокую стоимость, но решающую проблему автоматического контроля посещаемости.

Список используемых источников

1. Виткова Л. А., Герлинг Е. Ю., Головлёва Ю. А., Ковцур М. М. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга // 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. : СПб ГУТ, 2018. Т.2 С. 140–142.

2. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. Е. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуре // Информационная безопасность регионов России (ИБРР-2017): материалы конференции, Санкт-Петербург, 01–03 ноября 2017 г. С. 535–537.

3. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Овраменко А. Ю Гибридная модель базы данных NOSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1 (85). С. 46–54.

4. Цветкова А. Ю, Красов А. В. Разработка защищенных приложений: учебное пособие, СПбГУТ. СПб., 2013.

5. Распространённые атаки в соответствии с ESET [Электронный ресурс]. Режим доступа: https://support.eset.com/kb2907/, свободный. Загл. с экрана.

6. Top 5 most notorious cyberattacks [Электронный ресурс]. Режим доступа: https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/, свободный. Загл. с экрана.

7. Latest Virus Threats – Bitdefender Real-Time Virus Reporting [Электронный ресурс]. Режим доступа: https://www.bitdefender.com/resourcecenter/real-time-reporting/, свободный. Загл. с экрана.

8. Pricing – Keka HR and Payroll Platform [Электронный ресурс]. Режим доступа: https://www.keka.com/pricing/, свободный. Загл. с экрана.
9. GreytHR [Электронный ресурс]. Режим доступа: https://www.greythr.com/pricing/, свободный. Загл. с экрана.
10. Zoho People [Электронный ресурс]. Режим доступа: https://www.zoho.com/people/zohopeople-pricing.html, свободный. Загл. с экрана.

УДК 004.056
ГРНТИ 19.31

АНАЛИЗ ОСОБЕННОСТЕЙ ОРГАНИЗАЦИИ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СЕТЯХ КОЛЛЕКТИВНОГО ДОСТУПА СТАНДАРТА IEEE 802.11

М. М. Ковцур, М. С. Симанов

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

На сегодняшний день распространено использование беспроводных сетей семейства IEEE 802.11 для обеспечения коллективного гостевого доступа в Интернет. Число запущенных сетей увеличивается с каждым годом. В связи с этим, необходимо обратить особое внимание на организацию авторизации пользователей. В работе представлена классификация существующих способов авторизации пользователей в беспроводных сетях коллективного доступа, а также существующие решения. Сформированы рекомендации по выбору решения исходя из таких показателей, как время подключения пользователя, стоимости внедрения и эксплуатации, масштабов сети, окупаемости проекта. Также рассмотрена модель нарушителя и возможные атаки.

авторизация, гостевой доступ, Wi-Fi, беспроводные сети, IEEE 802.11.

Быстрое развитие и использование беспроводных сетей семейства IEEE 802.11 для обеспечения коллективного гостевого доступа в Интернет привело к ряду проблем, которые затрагивают как вопросы подключения новых пользователей, так и вопросы безопасности. Возможные уязвимости в таких сетях позволяют злоумышленникам получить доступ не только к личным данным пользователей, но и организовать наблюдение за ними [1]. Поэтому, на данный момент вопрос организации авторизации пользователей в беспроводных сетях коллективного доступа является актуальным.

Стоит отметить, что в Российской Федерации существует постановление Правительства № 758 и № 801, а также Федеральный закон № 97, которые обязывают организаторов доступа в интернет авторизовать пользователей их Wi-Fi сети [2]. После принятия этих нормативных актов, началось

внедрение в беспроводные сети коллективного доступа систем авторизации пользователей. Также, согласно прогнозам компании Cisco, Число публичных точек доступа Wi-Fi за период 2016–2021 гг. вырастет шестикратно, с 94 до 541,6 млн [3]. Наличие этих факторов обуславливает многообразие методов авторизации пользователей, а также готовых решений для каждого из них.

В рамках данной работы рассмотрим наиболее распространенные методы авторизации: по звонку, по короткому сообщению (СМС), по ваучеру. Первые два из них предполагают авторизацию через номер мобильного телефона клиента посредством входящего или исходящего звонка либо СМС – сообщения.

Схема организации авторизации пользователя представлена на рис. 1 и состоит из нескольких шагов. Клиент подключается к беспроводной сети и попадает на форму авторизации, где ему требуется ввести его номер мобильного телефона. Далее, пользователь либо получает СМС – сообщение на указанный номер, либо совершает исходящий звонок на шлюз. После этого происходит сверка полученных данных, и сервер доступа разрешает пользователю доступ в Интернет.

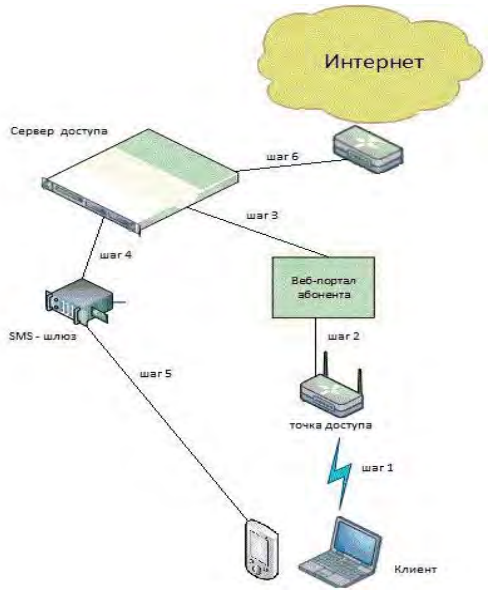


Рис. 1. Сценарий авторизации по звонку и СМС

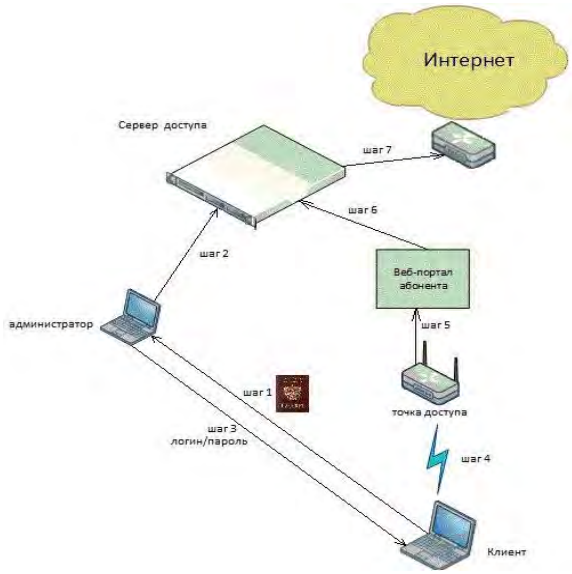


Рис. 2. Сценарий авторизации по ваучеру

Авторизация по ваучеру является аналогом авторизации по паспорту. В конечном итоге у администратора беспроводной сети будет храниться связка данных: паспортные данные клиента – логин/пароль – мак-адрес устройства (рис. 2). При данном методе пользователь должен получить ваучер при предъявлении своих паспортных данных сотруднику компании,

в котором установлена беспроводная сеть. Это время может сильно разниться в зависимости от загруженности сотрудников, а также от других различных факторов. Поэтому в данном исследовании учитываются оба варианта.

Одним из важных показателей для пользователя является время, затраченное на подключение к гостевой беспроводной сети.

Экспериментально были произведены замеры времени авторизации пользователей для T_1–T_{10} каждого из методов. Результаты измерений для T_1–T_{10} (с) для 10 попыток представлены в таблице 1.

ТАБЛИЦА 1. Оценка времени авторизации для каждого из методов

Методы	T_1	T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}
Звонок	55.26	52.77	52.44	54.98	48.65	50.02	53.17	55.14	49.26	51.00
СМС	51.56	46.25	49.63	50.17	46.73	49.62	51.03	48.74	45.12	45.77
Ваучер	37.49	34.31	35.17	33.52	34.86	36.15	34.44	33.92	37.08	35.37

Далее, по результатам измерений были определены средние значения времени авторизации пользователя, а также значения погрешностей $T_{\text{погр}}$ для каждого из методов авторизации [4]:

$$T_{\text{с}} = \frac{\sum_{i=1}^{n} T_i}{n}, \quad (1)$$

$$T_{\text{погр}} = \text{ŋ}\frac{\sqrt{\frac{\sum_{i=1}^{n}(T_i - T_{\text{с}})^2}{n-1}}}{\sqrt{n}}, \text{с} \quad (2)$$

где T_c – среднее арифметическое значение результатов измерений, T_i – каждое из значений измерения, n – число измерений, ŋ - коэффициент Стьюдента, равный 2?262, взятый из таблицы для 10 измерений.

Результаты оценки среднего времени подключения пользователя к гостевой сети представлены в таблице 2.

ТАБЛИЦА 2. Расчет среднего значения времени и погрешности

Методы авторизации	Среднее значение и погрешность
Звонок	52,27±1,68 (секунд)
СМС	48,46±1,65 (секунд)
Ваучер (с учетом полученных данных)	35,23±0,42 (секунд)
Ваучер (без учета полученных данных)	5–15 (минут)

В таблице 2 также дополнительно добавлен расчет времени авторизации по ваучеру с учетом временных затрат на получение логина и пароля пользователя.

Проанализировав таблицу 2, можно сделать вывод о том, что время авторизации по звонку и по СМС различаются минимально. Метод авторизации по ваучеру без учета временных затрат на получение логина и пароля является самым быстрым из всех остальных, представленных в исследовании.

Для каждого из исследуемых методов авторизации существует большое количество готовых сервисных решений. Все они очень похожи по функционалу и имеют приемлемую цену.

Готовые сервисные решения имеют стоимость в месяц 400–3000 рублей для каждого из методов авторизации. Тем самым, многие окупаются за первый же день работы беспроводной сети в заведении. Но наличие ежемесячной оплаты, а также передача данных о посетителях во внешние системы являются значительными недостатками в работе таких решений.

Готовые аппаратные решения, такие как Cisco ISE и Айдеко, работают без абонентской платы, но имеют довольно высокую стоимость: цена Айдеко начинается от 50000 рублей, а Cisco ISE от 140000 рублей [5, 6]. Также они могут работать только с определенным оборудованием.

В некоторых заведениях используется метод Wi-Fi авторизации через социальные сети. Однако, данный подход не соответствует требованиям Российского законодательства. Пользователь может воспользоваться подложной страницей в социальной сети, тем самым получит доступ к Интернету, обойдя авторизацию.

Первые решения Wi-Fi авторизации предполагали подмену DNS адресов. Нарушителю достаточно было прописать рабочие DNS адреса на своем устройстве, чтобы получить доступ к Интернету без прохождения процедуры авторизации [7]. В наше время такие решения либо уже не используются, либо используются крайне редко. На данный момент маршрутизатор, через который подключается клиент, отправляет на сервер авторизации запрос, содержащий MAC-адрес абонента. Сервер авторизации принимает решение об открытии или блокировке сессии, отправляя соответствующий ответ обратно маршрутизатору [8].

Также нарушитель может воспользоваться атакой «человек по – середине» с использованием сниффера, например, Wireshark. Так как при авторизации используется связка MAC-адрес и логин-пароль или IP-адрес и логин-пароль, злоумышленнику требуется подменить мак-адрес или IP-адрес своего компьютера. После того, как жертва покинет сеть, нарушитель может подключиться к сети с использованием перехваченных данных [9].

При исследовании различных методов авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11 можно заметить,

что самым быстрым методом является авторизация по ваучерам (с учетом полученного логина и пароля). Методы по звонку и по СМС имеют временные затраты одного порядка, но эти затраты существенно больше, чем при авторизации по ваучеру. Однако, если учитывать, что пользователь приходит в гостевую сеть организации с авторизацией по паспорту впервые, то подключение к Wi-Fi сети может занять довольно длительное время, которое варьируется в промежутке от 5 до 15 минут. В этом случае существенную роль сыграет скорость работы администратора организации, который осуществляет выдачу ваучеров согласно паспортным данным.

Анализируя готовые решения Wi-Fi авторизации, можно сделать вывод о том, что на рынке на сегодняшний день не обнаружено готовых решений авторизации без использования ежемесячных платежей и, одновременно, способных использовать бюджетное оборудование, которое могло бы использовать пользовательские СМС шлюзы.

Тем самым, становиться актуальным исследование, связанное с разработкой такого решения.

Список используемых источников

1. Александрова Е. С., Иванов Г. Н., Ковцур М. М. Анализ механизмов защиты Wi-Fi сетей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х томах. 2018. С. 47–51.

2. Федеральный закон и штрафы за публичный Wi-Fi в 2018 году по 97-ФЗ [Электронный ресурс]. Режим доступа: https://global-hotspot.ru/wi-fi-2018/

3. Cisco прогнозирует семикратный рост мобильной передачи данных за период 2016–2021 гг. [Электронный ресурс]. Режим доступа: https://www.cisco.com/c/ru_ru/about/press/press-releases/2017/02-09b.html

4. Савельев А. И., Фетисов И. Н. Обработка результатов измерений при проведении физического эксперимента / под ред. С. П. Ерковича. М. : Издательство МГТУ, 1990. 14 с.

5. Cisco identity services engine (ISE) [Электронный ресурс]. Режим доступа: http://www.cbs.ru/catalog/10252/

6. Документация Ideco UTM [Электронный ресурс]. Режим доступа: http://doc.ideco.ru/pages/viewpage.action?pageId=1278071

7. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи Multicast – трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

8. Александрова Е. С., Ковцур М. М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х томах. 2017. С. 24–28.

9. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

УДК 004.652
ГРНТИ 20.53.17

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НЕРЕЛЯЦИОННЫХ БАЗ ДАННЫХ

А. В. Козьмян, Ю. В. Твердохлебова, И. А. Ушаков

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

Статья посвящена сравнительному анализу наиболее популярных нереляционных баз данных на основе ряда оценочных критериев. Для исследования были выбраны Apache Cassandra, HBase и MongoDB, которые занимают лидирующие позиции согласно различным отраслевым тенденциям. Базы NoSQL специально созданы для определенных моделей данных и обладают гибкими схемами, что позволяет разрабатывать современные приложения. Базы данных NoSQL получили широкое распространение в связи с простотой разработки, функциональностью и производительностью при любых масштабах.

NoSQL, Apache Cassandra, HBase, MongoDB, производительность, базы данных.

В настоящее время невозможно представить работу какого-либо приложения без получения, обработки и записи определённого типа данных. Системы управления базами данных (СУБД) – это высокоуровневое программное обеспечение, работающее с низкоуровневыми API. Для решения различных проблем создавались новые виды СУБД (реляционные, NoSQL и т. д.), а также их новые реализации. В течение долгого времени центральное место в разработке приложений занимали реляционные базы данных, такие как Oracle, DB2, SQL Server, MySQL и другие. Однако в середине – конце 2000-х годов заметное распространение стали получать и другие модели данных, для обозначения которых был введен термин «NoSQL» [1, 2].

NoSQL – термин, обозначающий ряд подходов, направленных на реализацию хранилищ баз данных, имеющих существенные отличия от моделей, используемых в традиционных реляционных СУБД с доступом к данным средствами языка SQL. Термин применяется к базам данных, в которых решаются проблемы масштабируемости и доступности за счёт атомарности и согласованности данных [1, 2, 3].

В базах NoSQL для доступа к данным и управления ими применяются различные модели данных, в том числе документная, графовая, поисковая, с использованием пар «ключ-значение» и хранением данных в памяти [2, 3, 4]. Базы данных таких типов оптимизированы для приложений, например, мобильных, игровых, интернет-приложений, когда требуются гибкость

и масштабируемость с высокой производительностью и широкими функциональными возможностями, способность обеспечивать максимальное удобство использования [2, 3].

На сегодняшний момент существует большое количество реализаций нереляционных баз данных. Проведем сравнительный анализ наиболее популярных из них: Apache Cassandra, HBase и MongoDB.

Apache Cassandra хорошо масштабируемая высокопроизводительная распределенная база данных, предназначенная для обработки больших объемов данных на множестве серверов, обеспечивающая высокую доступность без единой точки отказа [5].

HBase распределенная нереляционная база данных, созданная на основе Google BigTable на языке Java. Разработана в рамках проекта Apache Hadoop и работает поверх HDFS, предоставляя возможности, сходные с BigTable [6].

MongoDB кроссплатформенная документно-ориентированная база данных, которая отказалась от традиционной таблично-ориентированной реляционной структуры в пользу документов json с динамическими схемами, делая интеграцию данных определенных типов проще и быстрее [7].

Все сравниваемые базы данных с открытым исходным кодом. Cassandra и HBase написаны на языке Java, в то время как MongoDB на C++. Cassandra и HBase предлагают модель хранения данных на базе семейства столбцов (*ColumnFamily*), что дает возможность организовывать хранение хэшей с несколькими уровнями вложенности. В таком хранилище данные хранятся в виде разреженной матрицы, строки и столбцы которой используются как ключи. Применением этого вида СУБД являются задачи, связанные с большими данными, с пониженными требованиями к согласованности данных. Это отличает ее от систем, хранящих данные только в связке «ключ-значение». Представителем таких систем является MongoDB. Это простейший вид хранилищ данных, использующий ключ для доступа к значению. Такие хранилища используются для хранения изображений, создания специализированных файловых систем, в качестве кешей для объектов, а также в системах, спроецированных с прицелом на масштабируемость [5, 6, 7].

MapReduce – это парадигма обработки данных для сжатия больших объемов данных в полезные агрегированные результаты. Например, в MongoDB сначала применяется фаза Map к каждому введенному документу. Эта функция выдает пары «ключ – значение», для тех ключей, которые имеют несколько значений, применяется фаза Reduce. Она собирает и сжимает агрегированные данные. Затем результаты хранятся в коллекции. Коллекция – это группа MongoDB документов, является эквивалентом таблицы в реляционных базах данных [3, 4].

Далее приведена таблица (табл.) со сравнительным анализом рассматриваемых баз данных [5, 6, 7, 8].

ТАБЛИЦА. Сравнительный анализ

	Cassandra	HBase	MongoDB
Описание	Хранилище типа Wide-column, основанное на идеях BigTable DynamoDB	Хранилище типа Wide-column, основанное на Apache Hadoop и идеях BigTable	Документоориентированная СУБД с открытым исходным кодом
Модель основной базы данных	Хранилище типа Wide-column	Хранилище типа Wide-column	Document store
Операционные системы	BSD, Linux, OS X, Windows	Linux, Unix, Windows	Linux, OS X, Solaris, Windows
Язык реализации	Java	Java	C++
Метод распределения	Sharding	Sharding	Sharding
Метод репликации	Выборочная репликация	Выборочная репликация	Master-slave репликация
Применение	Для больших наборов данных, которые требуют хранения с дружелюбным для пользователя интерфейсом	Лучше всего подходит для выполнения MapReduce функции на больших данных. При этом применяют стек HDFS/Hadoop	Применяется в случаях, когда требуются динамические запросы к базе данных, задание индексов и высокая производительность
Примеры использования	Веб-аналитика для обработки кликов в час, версий браузера, IP адресов, логирования транзакций и сбора данных со счетчиков	Поисковые движки. Анализ логов. Сканирование больших двухмерных невзаимосвязанных таблиц	Подойдет там, где нужна гибкость структуры и большие объемы данных. Высокопроизводительные распределенные интернет-приложения

Понимание зависимости поведения производительности базы данных NoSQL, такой как Apache Cassandra, от различных условий имеет решающее значение. Проведение формального подтверждения концепции (*proof of concept*) в среде, в которой будет работать база данных, является лучшим способом оценки платформ. Процессы POC, которые включают в себя важные контрольные показатели, такие, как рабочие конфигурации и параметры, ожидаемые нагрузки по данным и пользователям, дают как ИТ-специалистам, так и бизнес-заинтересованным сторонам глубокое понимание

рассматриваемых платформ и представление о том, как бизнес-приложения будут работать в производстве.

Независимая компания «End Point» провела сравнительные тесты баз данных Apache Cassandra, HBase и MongoDB на проверку скорости загрузки и чтения данных, а также комбинаций записи и чтения, что является типичными операциями для реальных приложений. Тестирование проводилось на Web сервере Amazone. На каждом стенде была установлена конфигурация, а также запущен скрипт для управления процессом измерения производительности, включая запись, настройку, вычисление параметров нагрузки и отправку команд клиентским узлам для запуска теста. Каждый тест начинался с пустой базы данных, клиенты загружали начальный набор случайно сгенерированных данных, после чего последовательно запускались тесты производительности [1]. Рассмотрим графики скорости чтения и загрузки информации в базы данных (рис. 1, 2 (см. ниже)). Каждая рабочая нагрузка отображена в виде вертикальной диаграммы. На вертикальной оси диаграммы изображено количество операций в секунду, на горизонтальной оси – количество узлов, используемых для тестирования рабочей нагрузки. Как видно из графиков, Cassandra во многих случаях превосходит своих главных конкурентов в области быстрой записи и чтения данных и обеспечения высокой производительности линейного масштабирования.

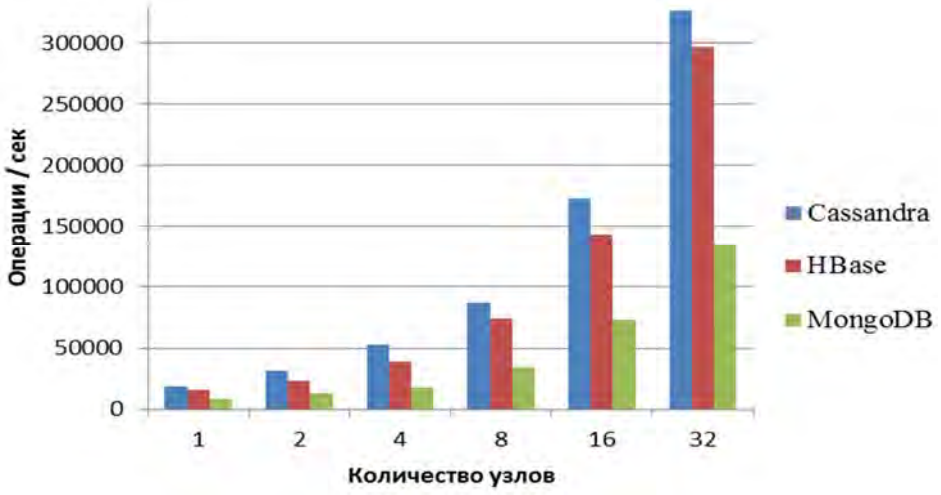


Рис. 1. График скорости загрузки данных

Такие архитектурные преимущества, как отсутствие единой точки отказа или гибкая масштабируемость между несколькими центрами обработки данных и облаком, не так важны, как обеспечение времени отклика, соответствующего высоким ожиданиям потребителей индустрии Web, IOT и мобильных приложений. Как показывают тесты, Cassandra во многих случаях превосходит другие исследуемые базы данных NoSQL в области быстрой записи и чтения [9].

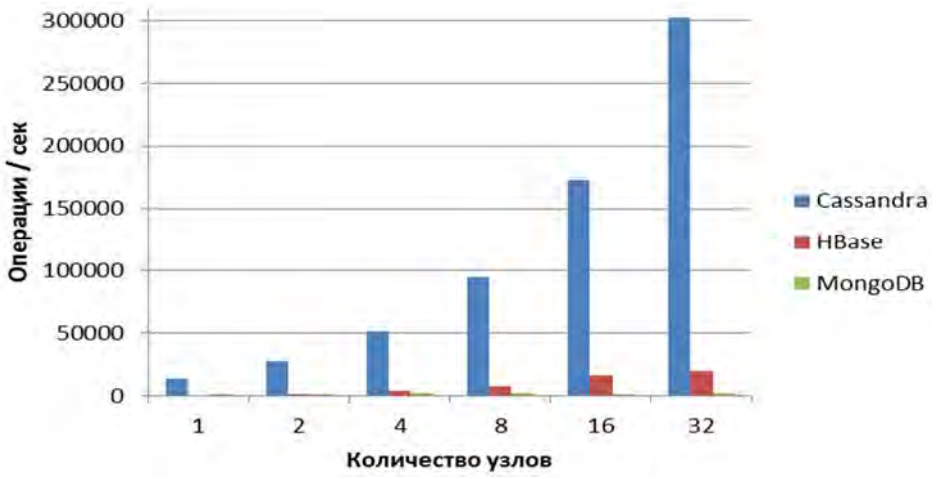


Рис. 2. График скорости чтения данных

Список используемых источников

1. Benchmarking top NoSQL databases [Электронный ресурс]. Режим доступа: https://www.datastax.com/apache-cassandra-leads-nosql-benchmark – (Дата обращения: 02.12.2018).

2. Котенко И. В., Ушаков И. А., Пелевин Д. В., Овраменко А. Ю. Гибридная модель базы данных NoSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1 (85). С. 46–54.

3. Ушаков И. А., Котенко И. В. База данных безопасности корпоративной сети: применение SQL и NOSQL технологий // Региональная информатика и информационная безопасность 2017. С. 254–255.

4. Котенко И. В., Ушаков И. А. Модели NOSQL баз данных для мониторинга кибербезопасности // 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. 498–501.

5. Eben Hewitt Cassandra – The Definitive Guide "O'Reilly Media, Inc.", 2015. – Computers. – PP. 267–279.

6. Lars George HBase – The Definitive Guide "O'Reilly Media, Inc.", 2016. – Computers. – PP. 34–59

7. Eelco Plugge, Peter Membrey, David Hows MongoDB Basics "O'Reilly Media, Inc.", 2014. – Computers. – PP. 154–158

8. Головлева Ю. А., Виткова Л. А., Ковцур М. М., Дмитриева Е. В. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 510–512.

9. Чмутов М. В., Ковцур М. М., Ушаков И. А., Пестов И. Е. Исследование действующей ИТ-инфраструктуры организации для последующего перехода к облачной архитектуры // Информационная безопасность регионов России (ИБРР-2017) : материалы конференции. 2017. С. 535–537.

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

УДК 004.056
ГРНТИ 81.93.29

Приглашенный доклад

МОДЕЛИ И АЛГОРИТМЫ РЕАЛИЗАЦИИ ВИЗУАЛЬНЫХ ИНТЕРФЕЙСОВ ДЛЯ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ НЕЖЕЛАТЕЛЬНОЙ, СОМНИТЕЛЬНОЙ И ВРЕДОНОСНОЙ ИНФОРМАЦИИ

М. В. Коломеец[1,2], А. А. Чечулин[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Модели визуализации позволяют построить графические структуры отображения данных таким образом, что пользователь может легко воспринимать информацию в сравнении с обычным табличным или текстовым представлением. Различные модели и алгоритмы визуализации в абстрактном графическом виде можно использовать при реализации систем противодействия информации, а именно в подсистемах поддержки и принятия решений. В работе рассматриваются модели и алгоритмы реализации визуальных интерфейсах в таких системах выявления и противодействия нежелательной, сомнительной и вредоносной информации как системы родительского контроля и системы классификации интернет ресурсов.

визуальная аналитика, противодействие информации, модели визуализации, информационная безопасность.

Для выявления и противодействия нежелательной, сомнительной и вредоносной информации используются системы принятия решений, которые позволяют классифицировать анализируемые данные и способствуют выработке контрмер [1]. Одним из способов анализа данных в таких системах является визуализация. В основе визуальной аналитики лежат модели визуализации [2] – концепции представления информации в графическом виде таким образом, что пользователь может легко воспринимать информацию в сравнении с обычным табличным или текстовым представлением. На основе данных моделей визуализации строятся визуальные интерфейсы, которые используются в системах поддержки и принятия решений.

Основными моделями визуализации [3, 4, 5] при проектировании интерфейсов аналитики являются: линейный графики, круговые диаграммы, столбчатые графики, матрицы и графики рассеивания, параллельные координаты, различные виды графов и карты деревьев.

Линейные графики и круговые диаграммы являются наиболее распространенными моделями визуализации. Чаще всего с их помощью визуализируют временные данные и данные отношений в процентном выражении. Линейные графики являются весьма гибким инструментом, за счет возможности задания видов линий (различные кривые или ломанные), и видов шкал (линейная, логаримфическая, относительная). В большинстве систем поддержки и принятия решений сипользуются именно эти два вида графиков (рис. 1).

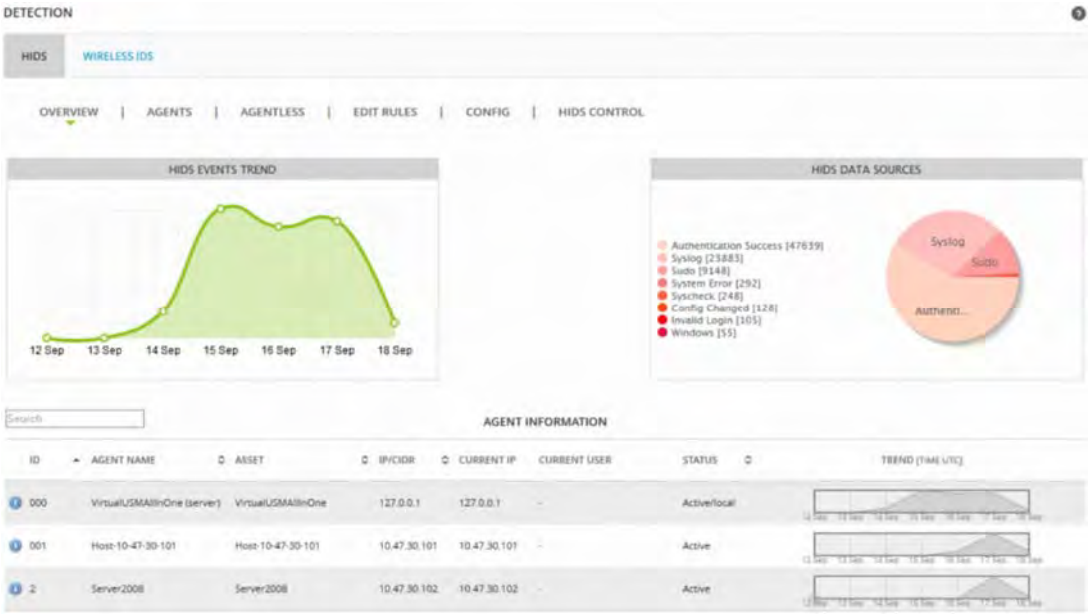


Рис. 1. Линейный график и круговая диаграмма в SIEM-системе OSSIM

Столбчатые графики используются, когда необходимо весьма точно сравнить несколько значений. В отличие от круговых графиков, где площади частей круга тяжело сравнивать, по высоте рядостоящих столбцов можно легко определить разницу между значениями. Основные виды столбчатых графиков это: вертикальные столбцы – стандартный вариант отображения (рис. 2 слева), сложенные столбцы – позволяет сравнивать сумму нескольких значений (рис. 2 в центре), и группы столбцов – позволяет оценивать дианмику значений по группам (рис. 2 справа).

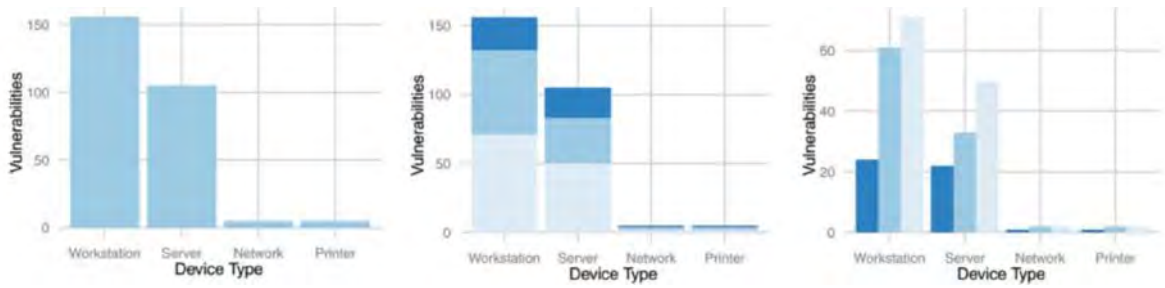


Рис. 2. Различные виды столбчатого графика

Матрицы и графики рассеивания используются для визуализации большого количества значений, которые могут сформировать определенный шаблон, описывающий их природу. При этом, данная модель отображать данные в двухмерном виде, трехмерном, треугольном (рис. 3), а также с различными шкалами (рис. 4).

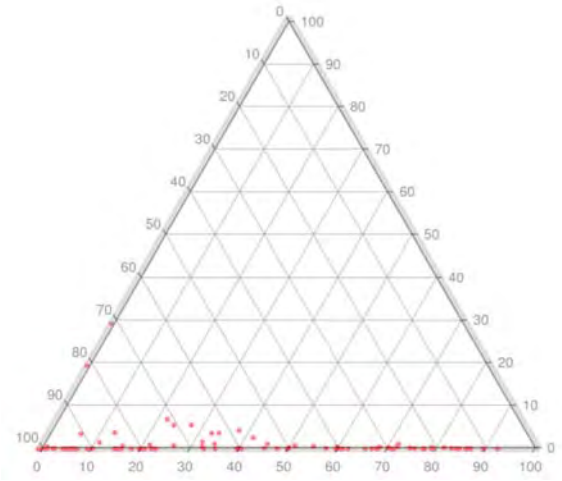


Рис. 3. Треугольная матрица рассеивания пакетов трафика различных типов

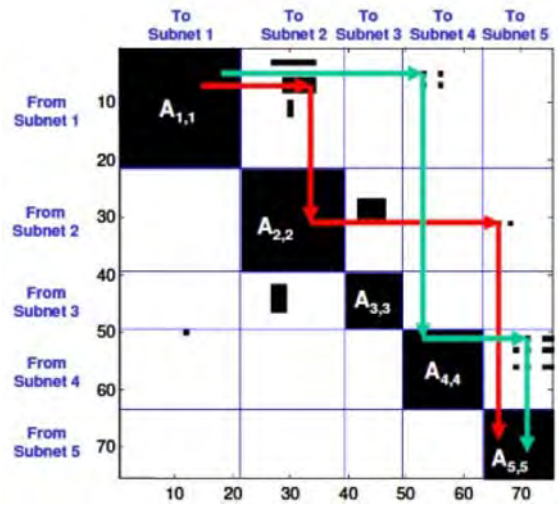


Рис. 4. Матрица уязвимостей подсетей с нелинейной шкалой. Пути отображают маршруты злоумышленника

Параллельные координаты (рис. 5) используются для визуализации многомерных данных. Каждого значение объекта привязывается к шкале, а сам объект отображается ломанной. Данным способом удобно анализировать общие свойства множества объектов.

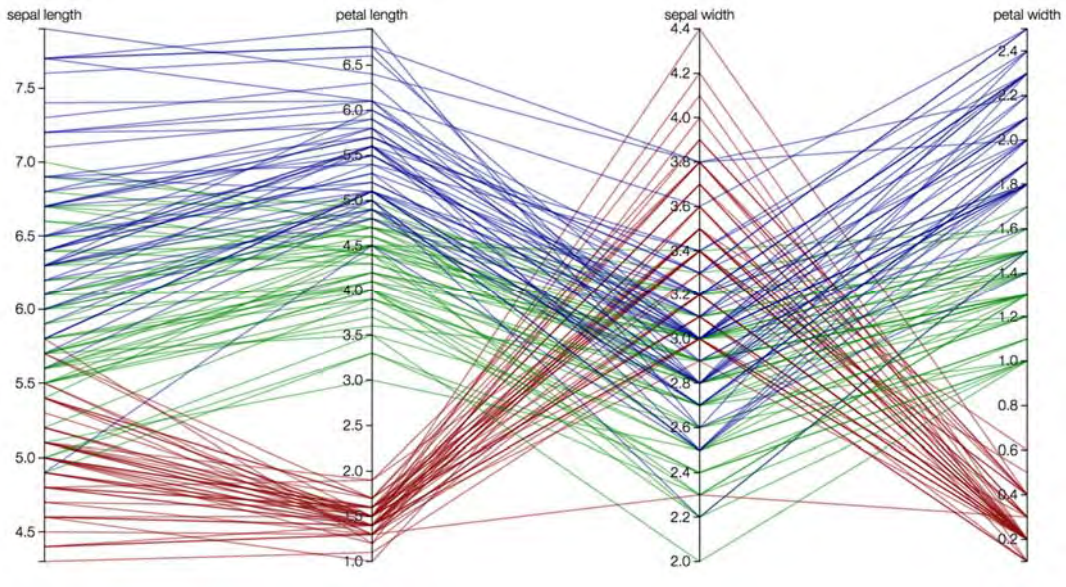


Рис. 5. Параллельные координаты

Графы используются при анализе топологий и отношений между элементами. При этом их можно задавать в различных видах: в виде силовой отрисовки, радиальные, круговые, использовать различные методы кластеризации и т. д. Отдельно можно выделить карты деревьев – модель визуализации, которая позволяет весьма эффективно отображать метрики дерева при помощи вложенных друг в друга прямоугольников. В данной модели прямоугольники потомки вкладываются в прямоугольники предки, что позволяет анализировать как метрики листьев дерева, так и целых ветвей.

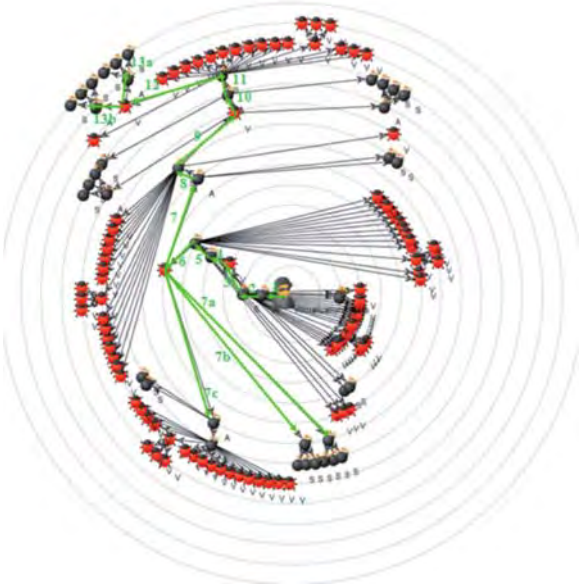


Рис. 6. Представление графа в радиальном виде

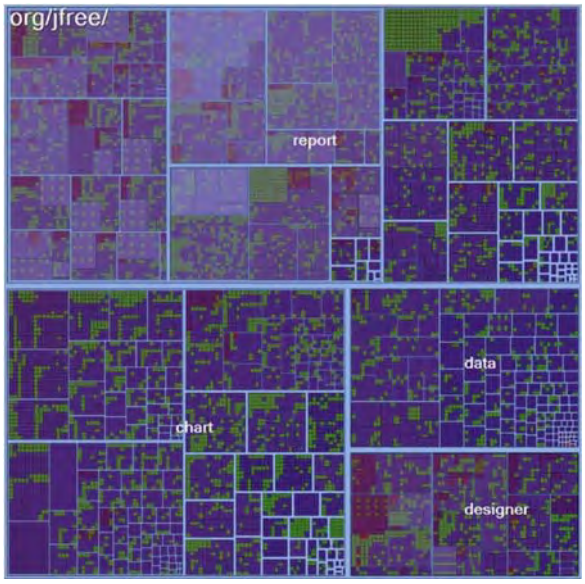


Рис. 7. Представление дерева в виде карты деревьев

Использование данных моделей визуализации при проектировании визуальных интерфейсов анализа информации позволит повысить качество и скорость принятия решений в системах выявления и противодействия нежелательной, сомнительной и вредоносной информации.

Работа выполнена при финансовой поддержке РНФ-18-11-00302.

Список используемых источников

1. Коломеец М. В., Левшун Д. С. Требования, предъявляемые к визуализации данных в интересах выявления и противодействия нежелательной и сомнительной информации // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24–26 октября 2018 г. : материалы конференции. СПб. : СПОИСУ. 2018. С. 144–146.

2. Коломеец М. В., Чечулин А. А., Котенко И. В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 42. С. 232–257.

3. Коломеец М. В., Чечулин А. А., Дойникова Е. В., Котенко И. В. Методика визуализации метрик кибербезопасности // Изв. вузов. Приборостроение. 2018. Т. 61. № 10. С. 873–880. DOI: 10.17586/0021-3454-2018-61-10-873-880.

4. Maxim Kolomeec, Andrey Chechulin and Igor Kotenko. Methodological Primitives for Phased Construction of Data Visualization Models. Journal of Internet Services and Information Security (JISIS), Vol.5, No.4, November 2015. PP. 60–84.

5. Jacobs J., Rudis B. Data-driven security: analysis, visualization and dashboards. – John Wiley & Sons, 2014.

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МОДЕЛЕЙ И СИСТЕМ ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ СОБЫТИЙ ДЛЯ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н. А. Комашинский, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

В работе проанализированы существующие модели и системы параллельной обработки событий информационной безопасности. Рассмотрены возможности и оценки результативности параллельной обработки данных с целью обнаружения компьютерных воздействий на основе функционального подхода. Опираясь на результаты проведенного анализа, представлена спецификация основных этапов процесса параллельной обработки событий и схема их реализации в составе системы обработки событий информационной безопасности.

информационная безопасность, параллельная обработка событий безопасности, компьютерная атака, функциональный подход, анализ событий безопасности.

Введение

В настоящее время много внимания уделяется обеспечению безопасности информации как в крупных учреждениях и компаниях, так и в средних и малых организациях. Защищаемые объекты имеют различные уровни доступа, всевозможные варианты развертывания вычислительных сред и разнообразные топологии сетевого взаимодействия. Задача обеспечения информационной безопасности с помощью средств обнаружения и предотвращения атак усложняется, в том числе за счет стремительного роста числа пользователей и разнообразия типов устройств, использования облачных

технологий и многократного увеличения объема и скорости передачи и обработки информации [1, 2, 3].

Одним из классов средств, позволяющих обеспечивать безопасность систем любого уровня и набора устройств, являются системы параллельной обработки событий информационной безопасности. Преимущество данных решений заключается в гибкости применения и возможности большого расширения вычислительных мощностей, в зависимости от решаемой задачи и объемов обрабатываемых данных [4].

Работа посвящена анализу существующих моделей и систем параллельной обработки событий информационной безопасности. Данный анализ производился за счет изучения научно-технической литературы, включающей описания как отдельных методов выявления компьютерных аномалий, так и особенностей реализации компонентов обработки событий в конкретных решениях открытых продуктов данного класса. Кроме того, в работе также ставится цель спецификации основных этапов процесса параллельной обработки событий и представления схемы их реализации в составе системы обработки событий информационной безопасности.

Релевантные работы

К настоящему времени предложены различные методики обработки разнородных данных, а также рассмотрены возможные схемы, описывающие сам процесс выявления компьютерных инцидентов. Вместе с развитием данной тематики публиковались работы, посвященные системам параллельной обработки событий безопасности.

В [5] описывается система обнаружения вторжений, которую представляет система Snort. Перехваченные сетевые пакеты анализируются с помощью фреймворка для распределенных приложений Hadoop, который использует технологию анализа больших данных. Для анализа используется система управления базами данных Apache Hive, позволяющая выполнять запросы, агрегировать и анализировать данные, хранящиеся в Hadoop. Задача работы оптимизировать систему так, чтобы осуществить оповещения о вероятности атаки на соседние узлы, когда количество аномальных сетевых пакетов от определенного источника превышает некоторое конкретное число.

Чтобы охватить большее количество сетевых сообщений, в [6] построена экспериментальная распределенная система обнаружения вторжений с использованием Hadoop, распределенной файловой системы HDFS и нескольких рабочих узлов. В работе реализована распределенная система Snort, собирающая оповещения от распределенных серверов после обработки с помощью модели вычислений MapReduce, что существенно уско-

ряет процесс обработки событий безопасности. Практические эксперименты данной системы имеют высокие результаты производительности при работе нескольких узлов в кластере Hadoop.

Работа [7] посвящена улучшению точности и производительности алгоритма «Случайного леса» при его параллельном выполнении на платформе реализации распределённой обработки Spark. Дается описание алгоритма, включая извлечение обучающей выборки, построение деревьев решений и объединение их в лес. Предлагается подход к уменьшению размерности для высоко-размерных данных, в которых экземпляры (или записи) содержат достаточно большое количество признаков. Данный подход базируется на выделении значимых признаков на основе вычисления показателей энтропии обучающего подмножества и каждого рассматриваемого признака, а также оценки рассчитанных величин.

В [8] используется распределенная система корреляции событий для организации широкомасштабной системы мониторинга безопасности. В работе делается упор на мониторинг DNS-запросов для выявления вредоносных доменов. Настроив DNS-зонд на рекурсивном DNS-сервере сети компании, все соответствующие DNS-запросы и ответы сети собираются без избыточности данных. Зонд DNS предлагаемой системы настроен в соответствии с пассивной архитектурой DNS ISC. Ответы DNS, адресованные рекурсивному DNS-серверу, регистрируются, и информация извлекается из пакетов DNS. Каждый наблюдаемый домен, вместе с извлеченной информацией, хранится в масштабируемой базе данных Apache Cassandra для определения степени вредоносности домена.

В [9] предлагается приложение для автоматического анализа логов журналов. Выделены две причины недостаточной производительности: некоторые части еще обрабатываются последовательно; во время извлечения признаков, из которых извлекается нужная информация из логов, выполняется несколько проходов входных данных, которые хранятся на диске. Производительность недостаточна, поскольку для выбора подходящих параметров требуется несколько часов обучения. Это напрямую связано с тем фактом, что Hadoop используется только для извлечения соответствующих функций из логов, в то время как уменьшение размерности с использованием анализа главных компонентов и обучения нейронной сети выполняется последовательно.

Для реализации алгоритма на параллельной системе его можно представить в виде последовательности групп операций как описано в [4]. Необходимо, чтобы отдельные операции в каждой группе можно было выполнять одновременно на имеющихся в системе устройствах. Операции алгоритма разбиты на группы, а множество групп упорядоченно так, что каждая операция любой группы зависит либо от начальных данных, либо от результатов выполнения операций, находящихся в предыдущих

группах. Каждая группа операции называется ярусом, а число таких ярусов – высотой параллельной формы. Максимальное число операций в ярусах (число привлекаемых процессов в ярусах) – шириной параллельной формы. Для эффективного распараллеливания процесса стремятся к увеличению загруженности системы процессоров и отысканию параллельной формы с заданными свойствами.

Общие принципы работы системы

Учитывая большое и постоянно возрастающее число событий безопасности, наиболее острая проблема параллельной обработки – обеспечение масштабируемости вычислительной системы. Вариант решения этого вопроса, согласно рассмотренным системам – использование инфраструктуры, позволяющей распределять обрабатываемые данные на отдельные рабочие узлы, связанные между собой. Принцип работы данной схемы формально похож на алгоритм работы модуля MapReduce. Основная идея MapReduce заключается в использовании большого кластера машин, называемых рабочими, для параллельного выполнения простых вычислительных задач с использованием только операций Map и Reduce. Первым шагом на этапе Map является разбиение входных данных на маленькие блоки, затем параллельно обрабатывается каждый блок разными рабочими узлами. На этапе Reduce подмножество рабочих узлов выполняет операцию получения входящих данных от рабочих узлов, которые завершили выполнение операции Map. На рис. приведена схема работы архитектуры MapReduce.

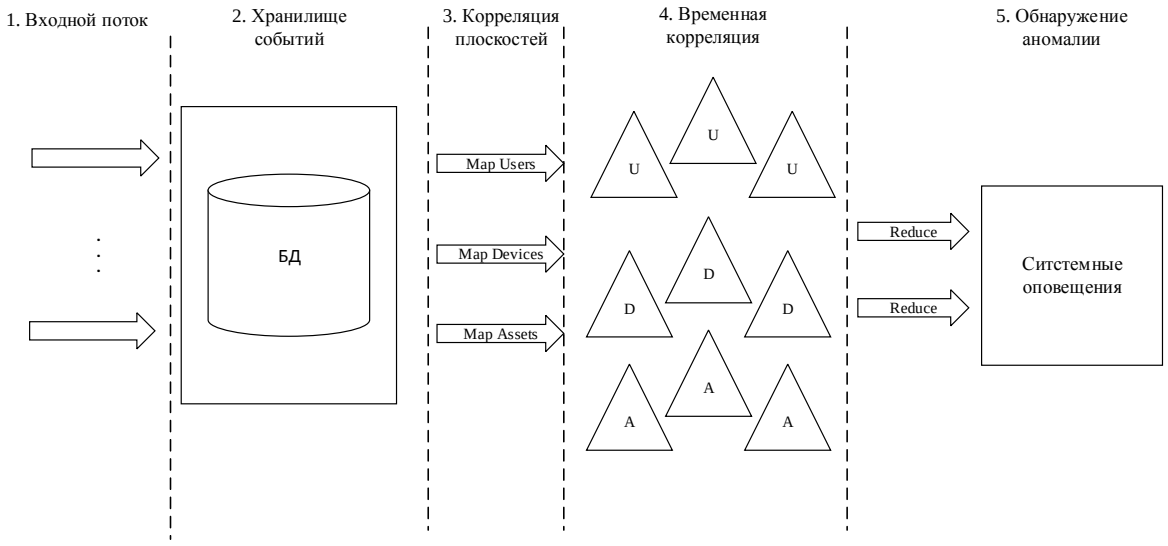


Рисунок. Распределенное вычисление с помощью MapReduce

Правила обработки выглядят следующим образом: *map*(*sensor, event*) → *list*(*goal, event*), *reduce*$_1$(*list*(*goal, event*)) → *list*(*goal, set*(*event*)), *reduce*$_2$(*goal, set*(*event*)) → *list*(*goal, alert desc*). На первом этапе события собираются из всех источников,

таких как сетевые сенсоры, системы логирования, системы безопасности периметра и др. Если платформа обработки не успевает за скоростью генерации событий, они сохраняются в течение предварительно определенного периода времени и затем передаются в вычисление MapReduce. Следующая операция $reduce_1$ обрабатывает входные данные (цель, событие) парами и выводит список задач и наборов всех событий, относящихся к связям в этой задаче. Наконец, последняя операция сокращения $reduce_2$ применяется для каждой задачи, а набор событий, принадлежащих ее связям и выходные данные представляют собой список с задачей и всеми описаниями предупреждений, найденными при запуске алгоритма обнаружения вредоносной активности. Выход последней операции уменьшения передается в систему оповещения, которая в конечном итоге решает, является ли активность вредоносной или нет. Операции *map* и $reduce_1$ представляют связную шаговую конструкцию в крупномасштабных вычислениях. Все алгоритмы обнаружения, которые работают со связанными событиями, обрабатываются в операции $reduce_2$. Следует обратить внимание, что этот модульный подход достаточно гибок и позволяет использовать любой алгоритм обнаружения, который принимает в качестве входных данных все связанные элементы. Более конкретно, операция $reduce_2$ может быть заменена любым алгоритмом, который выполняет обнаружение связанных аномалий, объемный анализ, сигнатурный анализ, проверку политики безопасности, анализ последовательности событий.

Заключение

В работе описаны основные подходы к построению систем мониторинга безопасности сетей, основанные на реализации параллельной потоковой обработки данных о событиях безопасности. Рассмотренные модели и системы параллельной обработки включают компоненты, ответственные за сбор, хранение, нормализацию и анализ, а также визуализацию данных. Также стоит отметить, что для хранения данных следует использовать специализированные распределенные файловые системы [10], что повышает надежность хранения и оперативность обработки запросов к данным. Дальнейшие исследования планируется проводить в направлении совершенствования системы мониторинга сетевой безопасности за счет повышения скорости обращений к блокам данных файловой системы.

Работа выполнена при частичной финансовой поддержке РФФИ (*проекты 16-29-09482, 18-07-01369, 18-07-01488, 18-37-20047, 18-29-22034, 18-37-20047*) *и бюджетной темы 0073-2019-0002.*

Список используемых источников

1. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах // Труды СПИИРАН. 2016. Вып. 4 (47). С. 5–27.
2. Котенко И. В., Степашкин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды Института системного анализа Российской академии наук. 2007. Т. 31. С.126–207.
3. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 1 (24). С. 21–40.
4. Бугрова И. Г., Демьянович Ю. К. Алгоритмы параллельных вычислений и программирование. Курс лекций. СПбГУ. С. 19–22.
5. Prathibha P. G., Dileesh E. D. Design of a Hybrid Intrusion Detection System using Snort and Hadoop // International Journal of Computer Applications. India. 2013. PP. 1–6.
6. Cheon J. J., Choe T.-Y. Distributed Processing of Snort Alert Log using Hadoop // International Journal of Engineering and Technology. 2013. PP. 1–7.
7. Chen J., Li K., et al. A Parallel Random Forest Algorithm for Big Data in a Spark Cloud Computing Environment // IEEE Transactions on Parallel and Distributed Systems. 2016. PP. 919–933.
8. Marchal S., Jiang X., et al. A Big Data Architecture for Large Scale Security Monitoring // IEEE International Congress on Big Data. 2014. PP. 56–63.
9. Koutsoumpakis G., Spark-based Application for Abnormal Log Detection // Department of Information Technology, Uppsala University. Sweden. 2014. PP.12–29.
10. Котенко И. В., Саенко И. Б., Кушнеревич А. Г. Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей интернета вещей // Труды СПИИРАН. 2018. Вып. 4 (59). С. 5–30.

УДК 004.056
ГРНТИ 81.93.29

МОДЕЛЬ СИСТЕМЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ С ИСПОЛЬЗОВАНИЕМ СИГНАТУРНЫХ МЕТОДОВ С УЧЕТОМ ТЕХНОЛОГИИ БОЛЬШИХ ДАННЫХ

Н. А. Комашинский, И. В. Котенко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

На основе анализа различных классов параметров современных информационных систем предлагается модель обнаружения вредоносной активности с помощью сигнатурных методов. В данной модели специфицированы способы повышения эффективности обработки больших потоков трафика в высокоскоростных сетях передачи данных

с целью обнаружения паттернов вредоносной активности. Сигнатурные методы представлены правилами Snort и адаптированы под обработку входных данных с использованием технологии больших данных. Представлен разработанный прототип системы обнаружения и проведена предварительная оценка показателей его производительности.

аномальная активность, трафик, Snort, сигнатурные методы, сенсор, большие данные, Hadoop.

Введение

Извлечение данных из сетевого трафика для анализа и выявления аномалий становится серьезной исследовательской проблемой из-за возрастающих объемов передаваемой информации по каналам связи. Кроме того, часто в трафике содержатся неструктурированные данные. В то же время злоумышленники постоянно совершенствуют способы получения доступа к сети или компьютерной системе [1, 2]. К основным категориям компьютерных атак и вредоносной активности, относятся: сканирование, отказ в обслуживании (DoS), несанкционированный удаленный доступ к сети, повышение привилегий и т. д. [3, 4]. Для решения проблем, связанных с обнаружением атак и вредоносной активности, в работе предлагается модель системы, основанной на использовании сигнатурных методов и технологии больших данных для анализа и извлечения данных из большого объема сетевого трафика.

Модель

Инфраструктура для работы с большими данными рассмотрена на примере Hadoop. Два главных компонента Hadoop – это MapReduce и Hadoop Distributed File System (HDFS) [5]. MapReduce – модель программирования и программная среда, впервые разработанная Google для параллельной обработки. HDFS – распределенная файловая система, предназначенная для хранения большого объема данных. Эти компоненты могут обрабатывать большие объемы данных на кластере из обычных компьютерных машин. Более того, есть несколько инструментов поверх Hadoop, которые можно эффективно использовать для обработки большого количества данных. Среди них – Apache Hive, являющаяся системой управления базами данных на основе платформы Hadoop, которая позволяет выполнять запросы, агрегировать и анализировать данные, хранящиеся в HDFS [5].

В статье рассматривается система, которая сможет обрабатывать и анализировать большие объемы трафика на предмет обнаружения компьютерных атак и аномалий. Архитектура предлагаемой системы состоит из шести

модулей: (1) модуль сбора данных, (2) модуль передачи и хранения информации, (3) модуль конвертации, (4) модуль интеллектуального анализа, (5) модуль преобразователя правил Snort, (6) модуль отчетов.

Модуль сбора данных предназначен для сбора данных сетевого трафика, выявленных системой обнаружения вторжений (*Intrusion Detection System*, IDS) Snort. Затем информация о сетевом трафике сохраняется в базе данных сетевого трафика. Кроме того, системный администратор может настроить мультисенсор IDS Snort для сбора данных трафика с различных источников.

Модуль передачи и хранения информации используется для передачи информации о предупреждениях из базы данных сетевого трафика в Hive с помощью приложения Sqoop. Однако база данных в Hive должна быть создана до того, как информация о предупреждении будет передана в хранилище.

Модуль конвертации предоставляет конечному пользователю пользовательский интерфейс для выбора атрибутов каждой из таблиц из базы данных в Hive для предварительной обработки данных, которая обрабатывается методом интеллектуального анализа данных. После этого отбирается информация о данных для хранения в HDFS.

Модуль интеллектуального анализа предназначен для обработки данных сетевого трафика. Кроме того, он позволяет конечному пользователю осуществлять выбор подходящего метода интеллектуального анализа данных (кластеризация, классификация, ассоциация и т. д.) Результат интеллектуального анализа данных сохраняется в HDFS.

В модуле преобразователя правил Snort результаты предыдущей процедуры преобразуются в правила IDS Snort. Затем они сохраняются в базе данных правил IDS Snort. Кроме того, этот модуль также имеет функцию проверки уникальности.

Модуль отчетов предоставляет панель мониторинга для отслеживания результатов информации о предупреждениях из IDS Snort, которая обнаруживает компьютерные атаки и аномальную активность. Кроме того, он суммирует события и выдает сообщения системному администратору для того, чтобы спрогнозировать типы реализуемых атак.

Оценка производительности

Для оценки производительности представленной системы сравнивалось среднее время ответа на запрос по обработке сетевого трафика в среде Hadoop.

В данной системе использовалась IDS Snort версии 2.9.11, установленная в операционной системе CentOS Linux версии 7. Для хранения инфор-

мации о предупреждениях использована СУБД MySQL. Технические характеристики машины, на которой установлена IDS Snort: процессор Intel Core (i7) 3770 3,40 ГГц, 16 ГБ ОЗУ DDR3, жесткий диск SATA емкостью 1 ТБ, гигабитный Ethernet-контроллер Intel 82579LM.

Узлы Hadoop, входящие в кластер, оснащены процессором Intel Xeon 3,10 ГГц E3-1220 V3, 16 ГБ оперативной памяти DDR3, жестким диском SATA емкостью 1 ТБ и гигабитным Ethernet-контроллером Intel I210. Каждый узел в кластере Hadoop подключен через один гигабитный Ethernet-контроллер к базовому коммутатору. Для управления кластером Hadoop использовался Ambari версии 2.7.3.

Для обнаружения необработанных данных сетевого трафика написаны правила Snort [6], представленные в таблице 1.

ТАБЛИЦА 1. Правила Snort для необработанных данных сетевого трафика протоколов передачи данных

№	Правило Snort
1.	alert tcp any any -> any any (msg: “Detect TCP Protocol”; \ sid: 10000001)
2.	alert icmp any any -> any any (msg: “Detect ICMP Protocol”; \ sid: 10000002)
3.	alert tcp any any -> any any (msg: “Detect UDP Protocol”; \ sid: 10000003)
4.	alert IP any any -> any any (msg: “Detect IP Protocol”; \ sid: 10000004)

Эти правила определяют любой источник и любой IP-адрес назначения и любой порт соответственно. Кроме того, в правилах Snort определены уникальные номера (от sid: 10000001 до sid: 10000004). С помощью команд *snort -N -r inside.tcpdump/outside. tcpdump -c /etc/snort/ snort.conf* можно обнаруживать файл *.tcpdump* с оповещениями безопасности в хранилище базы данных MySQL.

Данные сетевого трафика, отобранные по признакам правил Snort, заносятся в специальную базу данных для дальнейшей обработки.

В таблице 2 и рис.1 приведены количественные показатели записей, приведенных в таблице базы данных по выбранным протоколам, обработанные в среде Hadoop. Полученные результаты позволяют увидеть нагрузку на систему обнаружения атак – в конечном итоге в базу данных запишется примерно 50 млн событий, которые нужно оперативно и безошибочно обработать.

ТАБЛИЦА 2. Зависимость количества записей в базу данных от количества циклов передачи трафика

№ цикла	Протоколы			Общее количество
	ICMP	TCP	UDP	
1	1 574	4 227 430	604 862	4 833 866
2	3 274	6 685 252	631 116	7 319 642
3	9 446	11 877 418	1 456 660	13 343 524
4	14 814	18 396 576	2 790 082	21 201 511
5	23 390	23 593 634	3 954 824	27 571 887
6	42 972	28 995 980	5 690 622	34 730 504
7	47 843	39 224 567	7 267 294	46 544 627

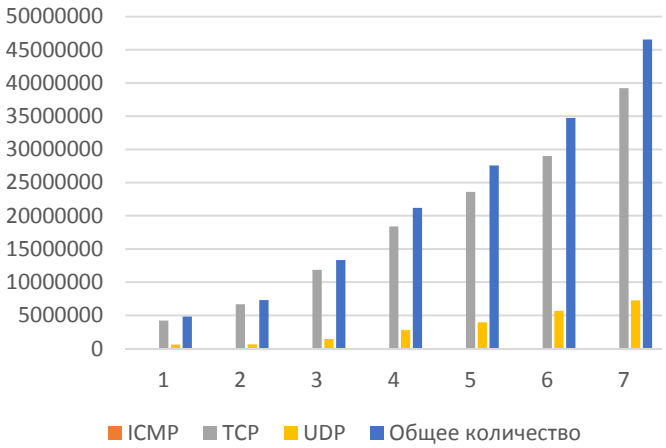


Рис. 1. Зависимость количества записей в базу данных от количества циклов передачи трафика

Полученная зависимость производительности системы от количества узлов в кластере представлена на рис. 2.

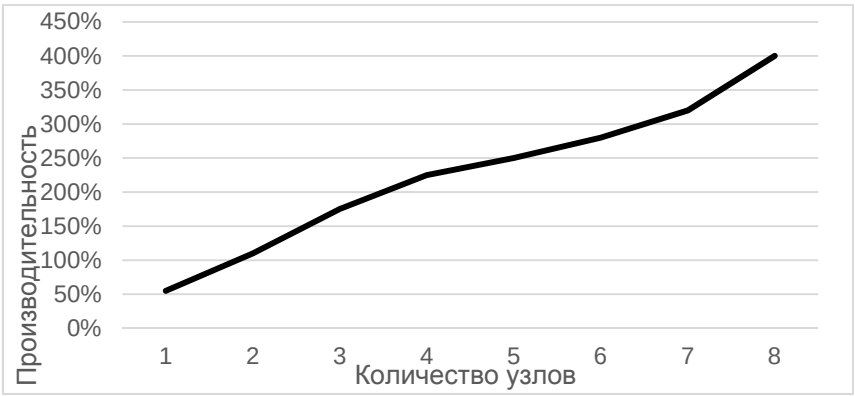


Рис. 2. Зависимость производительности системы от количества узлов в кластере

Производительность системы зависит от количества узлов в кластере Hadoop. Для измерения производительности предлагаемой системы сгенерирован дамп трафика: 29 файлов размером 2,42 Gb.

Анализ производительности для разного числа зависимых узлов осуществлялся на основе обработки данных с использованием 2 Гб файла, содержащего сигнатурные правила. Когда количество узлов в системе 8, производительность системы максимальна, что в 4,2 раза лучше, чем, когда в системе один узел (рис. 2).

Заключение

В работе показана возможность хранения и обработки событий с помощью IDS Snort в среде Hadoop. Результаты показывают, что Hive в среде Hadoop может запрашивать всю информацию, содержащуюся в протоколах. Выявлены зависимости количества записей, произведенных в базу данных сетевого трафика, от количества параллельных рабочих систем, обосновано применение файловой системы HDFS, показана зависимость производительности системы от количества узлов в кластере Hadoop.

В будущих исследованиях планируется развивать решения параллельной обработки трафика с целью выявления компьютерных атак, совершенствованию архитектуры системы обработки и анализа трафика, а также проведению последующих практических экспериментов.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369, 18-07-01488, 18-37-20047, 18-29-22034, 18-37-20047) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Котенко И. В., Степашкин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды Института системного анализа Российской академии наук. 2007. Т. 31. С. 126–207.

2. Котенко Д. И., Котенко И. В., Саенко И. Б. Методы и средства моделирования распределенных атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. № 3 (22). С. 5–30.

3. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

4. Котенко И. В., Саенко И. Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. № 1 (24). С. 21–40.

5. Zuech R., Khoshgoftaar T. M., Wald R. Intrusion detection and Big Heterogeneous Data: a Survey // Journal of Big Data. 2015. Vol. 2, No. 1, PP. 1–41.

6. Ahn S. H., Kim N. U., Chung T. M. Big Data Analysis for detecting unknown attack // IEEE/IFIP Network Operations and Management Symposium Workshops. 2010. PP. 357–361.

УДК 654.926
ГРНТИ 59.39.37

ВИБРО-АКУСТИЧЕСКАЯ СИСТЕМА РАСПРЕДЕЛЕННЫХ ДАТЧИКОВ «ДУНАЙ»

В. С. Кондратенко[1], Э. М. Муратов[2], М. А. Слепцов[3]

[1]МИРЭА – Российский технологический университет
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[3]ООО «Компания Т8»

Система Дунай позволяет в режиме реального времени обнаруживать, классифицировать и идентифицировать потенциально опасные события на линейной части трубопровода с точностью до 10 метров без необходимости развертывания полевых датчиков: в роли чувствительного элемента в данных системах выступает волоконно-оптический кабель. При этом стоит отметить, что система работает автономно в полностью автоматическом режиме, то есть не требует вмешательства оператора (только в случае необходимости подтверждения степени достоверности выявленного события).

волоконно-оптический датчик, волоконно-оптический кабель, оптический рефлектометр, обнаружение воздействий.

Введение

Распределенные волоконно-оптические датчики привлекательны в силу большой распространенности волоконно-оптических линий связи (ВОЛС). Оптическое волокно – идеальная среда для передачи любого вида информации, оптические линии связи широко распространены и часто проходят вдоль важных стратегических объектов. Очень заманчиво использовать оптическое волокно в качестве чувствительного элемента для детектирования акустических сигналов с высоким пространственным разрешением [1].

Распределенные акустические датчики востребованы в различных отраслях промышленности, в системах безопасности нового поколения и в сейсмологии. Области применения таких приборов весьма обширны.

Широкие возможности использования оптического волокна как системы распределённых акустических датчиков появились благодаря созданию когерентного рефлектометра.

Первая статья, посвящённая когерентному рефлектометру, была опубликована ещё в 1992 г., однако первые коммерческие образцы появились несколько лет назад. Для создания когерентного рефлектометра, пригодного

для практического применения, потребовалось решить целый ряд технических задач, связанных с подбором физических характеристик источника излучения, параметров зондирующего импульса, разработкой алгоритмов обработки сигнала и распознавания воздействий [2]. Прототип когерентного рефлектометра «Дунай» российского производства был описан в 2010 г.

Физические принципы работы

Принцип работы аналогичен принципу действия радара или оптического рефлектометра (рис. 1): короткий световой импульс направляется в волокно и на обратном пути происходит регистрация рассеянного и отраженного излучения.

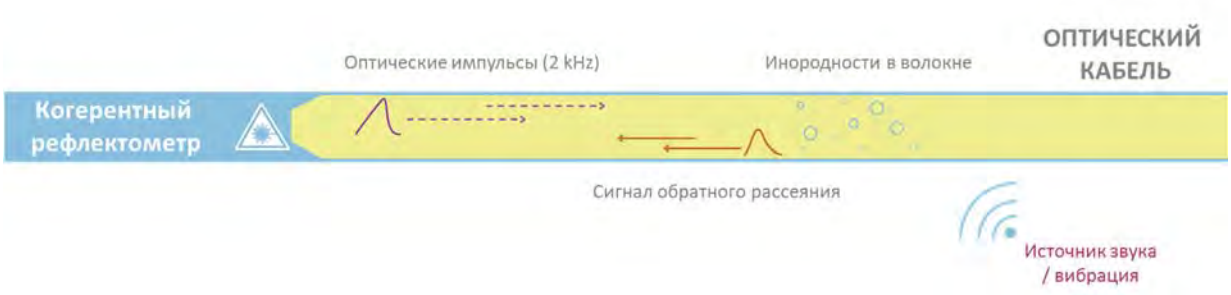


Рис. 1. Принцип работы оптического рефлектометра

При распространении оптического импульса по оптическому волокну часть света отражается обратно. Отражение происходит как от дефектов волокна, так и от неоднородностей показателя преломления (центров рассеяния), равномерно распределенных по волокну. Разветвитель или оптический циркулятор направляет рассеянное излучение на фотоприёмник (использование циркулятора позволяет вдвое сократить потери мощности сигнала, что актуально при ограниченной мощности лазера). Таким образом, можно зарегистрировать отражённое излучение и построить график зависимости мощности отражённого сигнала от времени – рефлектограмму [3].

Вид этой рефлектограммы будет зависеть от того, какой источник излучения используется в рефлектометре – обычный или узкополосный (когерентный). Разницу можно пояснить на простом примере: представим, что в волокне есть всего два близко расположенных центра рассеяния, от которых отражается зондирующий импульс.

В обычном рефлектометре, который применяется для измерения потерь в линии и обнаружения дефектов волокна, используется широкополосный лазер. Отражённые сигналы при этом складываются не когерентно: разность их фаз друг относительно друга меняется во времени, и амплитуда суммарного сигнала получается нерегулярной (случайной). Мощность такого сигнала равна сумме мощностей отдельных сигналов и не зависит от колебаний расстояния между центрами рассеяния.

В когерентном рефлектометре используется существенно более узкополосный и стабильный источник излучения, за счёт чего отражённые сигналы складываются когерентно: разность их фаз друг относительно друга постоянна во времени. Суммарный сигнал при этом может иметь мощность от нуля (если отражённые сигналы сложились в противофазе) до 4P (если фазы двух отражённых сигналов совпали). Разность фаз очень чувствительна к колебаниям расстояния между центрами рассеяния: его изменение всего на 100 нм вызывает заметное изменение мощности суммарного сигнала. На этом эффекте и основано применение когерентного рефлектометра для задач мониторинга [4].

Когерентная рефлектограмма представляет собой сильно изрезанную линию, форма которой очень чувствительна к различным воздействиям на волокно (тепловым, акустическим, электромагнитным) (рис. 2).

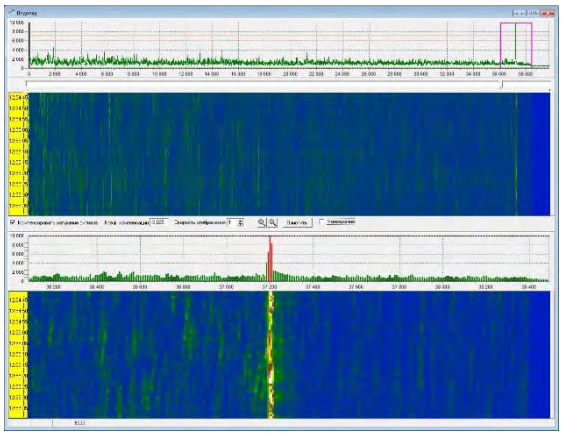


Рис. 2. Пример когерентной рефлектограммы

Такая рефлектограмма практически непригодна для обнаружения дефектов волокна, но зато может эффективно применяться для обнаружения и анализа внешних воздействий.

Компания Т8 единственная отечественная компания в России, которая в своей системе «Дунай» регистрирует изменение оптической фазы в отраженном сигнале.

Работа с фазой дает огромные преимущества:

– вследствие линейности отклика – отсутствие спектральных искажений сигнала;

– однородная чувствительность вдоль всего волокна;

– точная калибровка измеряемых сигналов;

– обработка суб-герцовых сигналов – сейсмика, геопроцессы, температурная деформация.

Обнаружение воздействий

Для обнаружения воздействия на волокно необходимо сделать ряд последовательных рефлектограмм. В системе «Дунай» зондирующий импульс посылается в волокно с частотой 1…2 кГц, таким образом, каждую секунду снимается 1–2 тыс. рефлектограмм. Анализируя происходящие в них изменения, можно локализовать место воздействия, изучить спектр воздейству-

ющего сигнала, оценить частоту и интенсивность воздействия, его продолжительность и характер изменения во времени. На основе этих данных можно сделать предположения о причине воздействия (рис. 3).

Простейший приём обработки полученных данных заключается в вычислении максимальной разности между несколькими последовательными рефлектограммами для каждой точки волокна. Построенный таким образом график называется разностной рефлектограммой. Для тех участков волокна, где осуществляется внешнее воздействие, амплитуда разностной рефлектограммы будет заметно выше уровня шума.

Рис. 3. Определение причины и места воздействия

По набору рефлектограмм можно для любой интересующей точки волокна построить график зависимости амплитуды сигнала от времени (сигналограмму). В лабораторных условиях сигналограмма позволяет оператору буквально прослушать воздействующий сигнал (например, голос человека). Для кабеля, проложенного в грунте, применяется в основном автоматический анализ сигналограмм, т. к. почва не пропускает колебания с частотой выше 200 Гц и прослушивание сигнала не столь информативно.

Применяя к сигналограмме фурье-преобразование, можно получить спектр воздействующего сигнала в интересующей точке волокна (спектрограмму). Экспериментально установлено, что различные воздействия оказывают наибольшее воздействие в разных участках спектра. Поэтому для более эффективного анализа внешних воздействий из спектра можно выделять полосовыми фильтрами различные участки, восстанавливая затем отфильтрованную сигналограмму.

Применение различных методов обработки сигнала и распознавания событий позволяет автоматически выделять и классифицировать происходящие воздействия, записывать происходящие события в базу данных, формировать сигналы тревоги для службы охраны.

Описание устройства

Устройство имеет три горизонтальных слота 1U, в которые устанавливаются три платы: приёмо-передающий модель, усилительный модуль и серверный компьютер для обработки данных (рис. 4).

Рис. 4. Внешний вид и описание блоков оборудования «Дунай»

К устройству, в усилительный модуль, подключается оптическое волокно. Типовая дальность работы (расстояние вдоль оптического волокна, на котором возможно обнаружение события) составляет около 50 км, однако существенно зависит от ряда факторов (тип и состояние грунта, тип и глубина прокладки кабеля, тип события).

Дальность работы системы можно увеличить с помощью дополнительных оптических усилителей, в том числе и с удаленной накачкой [5].

Для объектов большой протяжённости создаётся система устройств, управляемых из единого центра. Канал управления можно организовать по отдельному рабочему волокну с использованием технологии спектрального уплотнения, либо силами сторонней сети передачи данных заказчика.

Система вычисляет расстояние до места события, отображает место события на карте местности. Все события автоматически регистрируются в журнале. Возможно формирование сигналов тревоги по заданным критериям и их передача другим охранным системам.

В состав устройства входит плата промышленного компьютера, где выполняется основная часть обработки данных: первичная обработка и фильтрация, обнаружение и классификация событий. На рабочем месте оператора выполняются только задачи, не требующие большой вычислительной мощности: визуализация данных, поступающих с одного или нескольких рефлектометров, и отображение событий на схеме сети или на карте местности.

Это позволяет организовать различные варианты конфигурации в зависимости от требований заказчика, включая сетевой доступ и удалённые рабочие места. Для интеграции со сторонними приложениями предоставляется API, что позволяет легко интегрировать систему Дунай в существующие системы безопасности.

Практическое применение

В 2012 г. оборудование «Дунай» было сертифицировано в системе ГОСТ Р.

В 2012–2018 г. проведены многочисленные полевые испытания на сетях связи ООО «Газпром» и ОАО «Ростелеком», которые подтвердили эффективность оборудования. «В процессе тестовой эксплуатации продемонстрирована декларируемая чувствительность системы по всей длине

кабеля…», – отмечается в отзыве ОАО «Газпром», подписанном в ноябре 2013 г.

Основное назначение системы «Дунай» – обнаружение несанкционированной активности (перемещение людей и техники, разработка грунта ручным или механизированным способом) (рис. 5), локализация аварий и неисправностей, отслеживание работы подрядчиков. Одно из наиболее перспективных применений системы – контроль охранной зоны магистральных трубопроводов. Система может также применяться для мониторинга обстановки вдоль волоконно-оптических кабелей связи, для охраны государственной границы, контроля периметра охраняемых объектов и др.

Рис. 5. Примеры применения оборудования «Дунай»

Система надёжно распознаёт около 10 типов событий, включая перемещение пешехода, ручную копку, проезд грузового автомобиля, работу тяжёлой техники и др. Протяжённость охранной зоны, контролируемой одним рефлектометром, может составлять несколько десятков километров. Чувствительность системы к внешним воздействиям зависит от типа воздействия, физических характеристик кабеля (конструкции, глубины укладки), состояния грунта. В среднем, перемещение и работа тяжёлой техники надёжно детектируется на расстоянии до 100 м от кабеля, движение грузового автомобиля – до 10 м, движение пешехода – непосредственно над кабелем.

Заключение

Волоконно-оптические системы мониторинга на основе когерентного рефлектометра обладают многими преимуществами, среди которых: экономичность, скрытность установки, высокая чувствительность, всепогодность, простота в обслуживании. Несомненно, они найдут широкое применение в задачах охраны и контроля протяжённых объектов.

Для мониторинга утечек из газо- и нефтепроводов, контроля температуры теплоносителя, мониторинга температуры промышленных конвейеров

могут использоваться системы DTS, также созданные на основе когерентных рефлектометров.

Список используемых источников

1. Кондратенко В. С., Слепцов М. А. Разработка новых метрологических методов для обеспечения качественной эксплуатации волоконно-оптической системы // Материалы МНТК «Информатика и технологии. Инновационные технологии в промышленности и информатике»; Московский технологический университет, ФТИ. Вып. 2 (XXII) / Под редакцией В. С. Кондратенко. М. : 2016. С. 24–28.

2. Shatalin S., Treschikov V., Rogers A. Interferometric optical time-domain reflectometry for distributed opticalfiber sensing // Appl. Opt. 1998. V. 37. PP. 5600.

3. Нестеров Е. Т., Трещиков В. Н., Камынин В. А., Наний О. Е. Когерентный рефлектометр с полупроводниковым источником излучения // Телекоммуникации и транспорт (T-Comm), спец. выпуск «Метрология: измерения и технологии». 2010. С. 36.

4. Нестеров Е. Т., Слепцов М. А., Трещиков В. Н., Наний О. Е., Сусьян А. А. Когерентный оптический рефлектометр. Концепция создания прибора // Телекоммуникации и транспорт. 2010. № 8. С. 51–54.

5. Сусьян А. А., Наний О. Е., Камынин В. А., Нестеров Е. Т., Трещиков В. Н., Озеров А. Ж., Слепцов М. А. Метод увеличения дальности работы когерентного оптического рефлектометра // Письма в ЖТФ. 2011. Т. 37. № 9. С. 55.

УДК 004.75
ГРНТИ 20.23.17

АРХИТЕКТУРА И ПРОГРАММНЫЙ ПРОТОТИП СИСТЕМЫ ОБНАРУЖЕНИЯ ИНСАЙДЕРА КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ

И. В. Котенко, А. Ю. Овраменко, И. А. Ушаков

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

Работа посвящена разработке программного прототипа системы обнаружения инсайдера для своевременного выявления потенциальных нарушителей информационной безопасности. Рассмотрена предложенная архитектура и реализованный программный прототип системы обнаружения инсайдера компьютерной сети.

большие данные, UBA, UEBA, информационная безопасность, NoSQL.

Внутренние угрозы безопасности компьютерной сети представляют одну из наиболее существенных опасностей, а при наметившейся тенденции

стремительного роста корпоративных сетей как вертикально, так и горизонтально, проблема поиска инсайдеров (умышленных и неумышленных) стоит наиболее остро [1, 2].

В работе ставится задача разработки перспективной системы обнаружения инсайдера компьютерной сети, основанной на технологиях больших данных. Для этого на настоящем этапе исследований разработана архитектура системы обнаружения инсайдера и реализован ее программный прототип.

Рассмотрим архитектуру системы обнаружения инсайдера в компьютерной сети. Предлагаемая архитектура системы обнаружения инсайдера представлена на рис. 1.

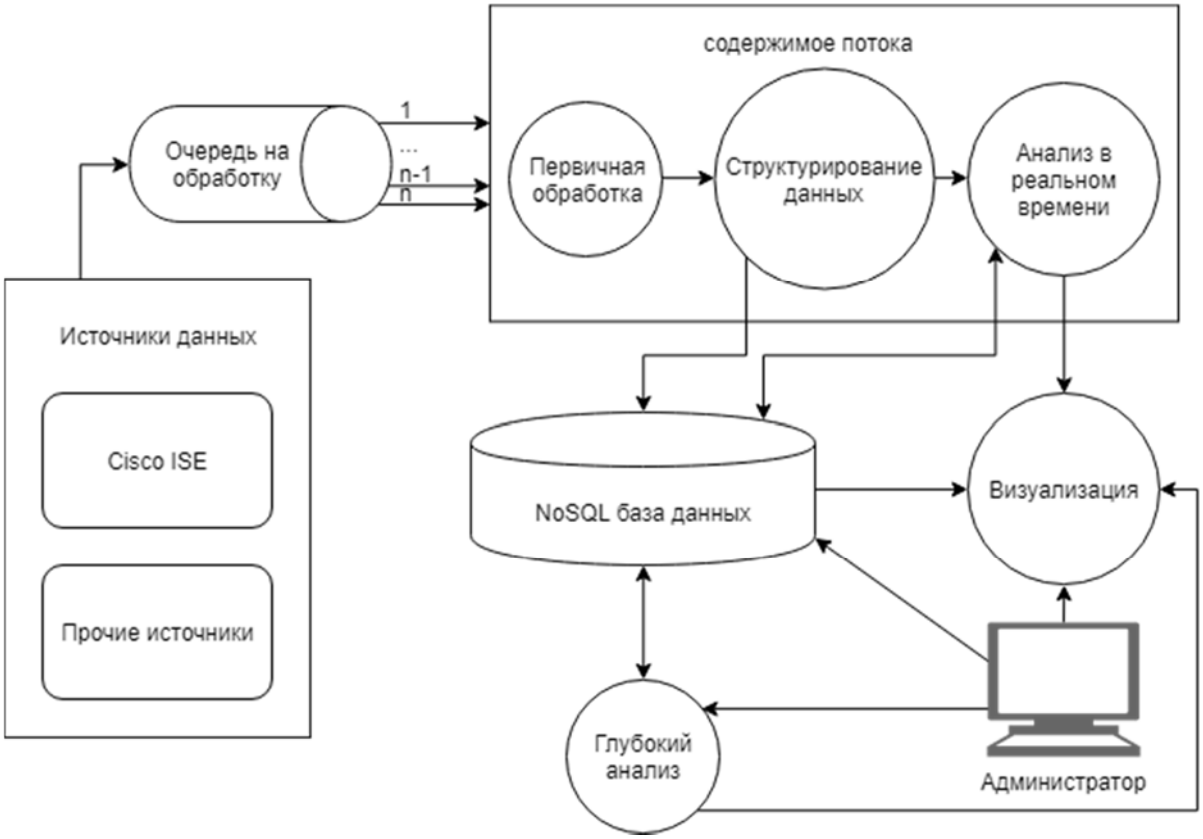


Рис. 1. Архитектура системы обнаружения инсайдера

Основным источником данных является компонент Cisco Identity Services Engine (Cisco ISE), представляющий собой многофункциональное решение, осуществляющее полный контроль доступа к корпоративной сети способное определить, кто подключается к корпоративной сети, откуда и с какого устройства [3].

Помимо сервисов аутентификации, авторизации, профилирования и управления гостевым доступом, Cisco ISE позволяет контролировать

кто находится в компьютерной сети и какими ресурсами он пользуется. Также возможен сбор данных из других источников.

После сбора, данные помещаются в очередь на обработку. Это необходимо для организации корректной работы многопоточных операций. Из очереди данные разделяются на N потоков. Количество потоков зависит от аппаратных возможностей станции, на которой запущена предлагаемая система обнаружения инсайдера.

Полученные из очереди данные обрабатываются блоком первичной обработки. В ходе этого этапа удаляются лишние поля, приходящие от Cisco ISE, а востребованные поля представляются для дальнейшей обработки.

Перед записью в базу данных, пришедшие после «очистки» данные структурируются и подвергаются дальнейшей обработке.

Обработка проводится для полей, значения которых необходимо рассчитывать лишь единожды. Они хранятся в базе данных вместе с остальными данными, что позволяет обратиться к ним как к обычному полю, а не рассчитывать их при каждом обращении.

После всех описанных выше этапов, происходит запись в базу данных NoSQL [4].

В качестве системы управления базами данных (СУБД) возможно использование OrientDB – открытой СУБД, объединяющей в себе возможности документо-ориентированной и графо-ориентированной баз данных. Также данный СУБД поддерживает объектно-ориентированный интерфейс, который работает поверх документо-ориентированного слоя [5].

Пример представления информация об активности пользователей сети в разные моменты времени отображенный средствами OrientDB в виде графов (рис. 2).

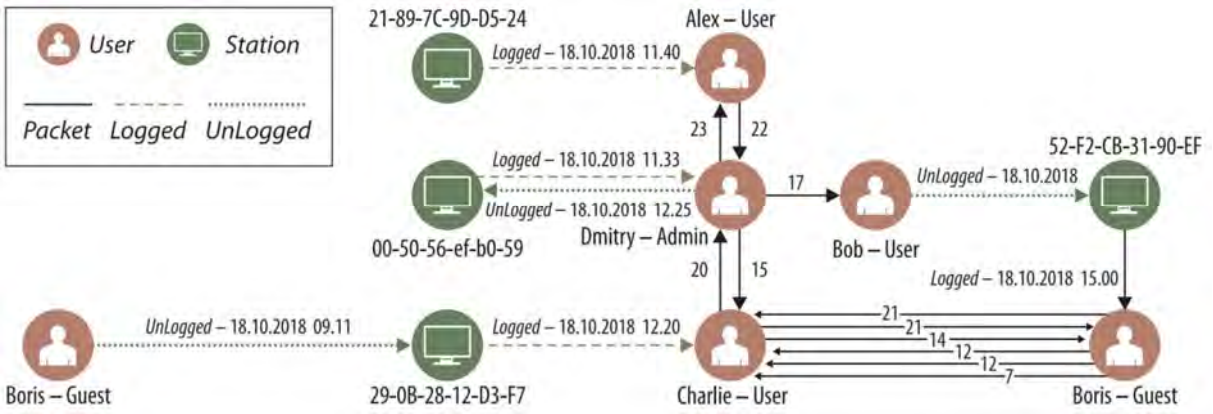


Рис. 2. Представление информации об активности пользователей средствами OrientDB

Модуль анализа в реальном времени необходим для проверки текущего потока данных на наличие угроз безопасности. Помимо данных самого потока модуль способен обращаться к базе данных для анализа предыдущих итераций [6, 7]. Результаты своей работы он записывает в базу данных.

Для большей наглядности используется модуль, отвечающий за визуализацию данных из базы данных. Также он необходим для отображения результатов анализа защищенности в реальном времени по запросу администратора.

В результате описанного выше комплекса мероприятий формируется интегрированная база данных, исследуемых на наличие аномалий в поведении пользователей. Для этого применяется Apache Spark - фреймворк с открытым исходным кодом для реализации распределённой обработки неструктурированных и слабоструктурированных данных [8].

Для управления полученной совокупностью программных решений требуется участие администратора. Также одной из его обязанностей является своевременное принятие решений по выбору контрмер, необходимых для противодействия инсайдеру.

В настоящее время с разработанным программным прототипов выполняется серия экспериментов. Направления дальнейших исследований связаны с развитием программного прототипа и проведением экспериментов.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369, 18-07-01488, 18-37-20047, 18-29-22034, 18-37-20047) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика «РИ-2016» : материалы конференции. 2016. С. 168–169.

2. Красов А. В., Сахаров Д. В., Ушаков И. А., Лосин Е. П. Обеспечение безопасности передачи Multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34–42.

3. Cisco Identity Services Engine [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/products/security/identity-services-engine/index.html (дата обращения 04.04.2019).

4. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Овраменко А. Ю. Гибридная модель базы данных NOSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1 (85). С. 46–54.

5. Первый релиз NoSQL БД OrientDB [Электронный ресурс]. URL: http://www.opennet.ru/opennews/art.shtml?num=33847 (дата обращения 04.04.2019).

6. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5 (54). С. 9–10.

7. Kotenko I., Kuleshov A., Ushakov I. Aggregation of Elastic Stack instruments for storing and processing of security information and events // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017.

8. Карау Х., Конвински Э., Венделл П., Захария М. Изучаем Spark. Молниеносный анализ данных. М. : ДМК Пресс, 2015. 304 с.

УДК 004.75
ГРНТИ 20.23.17

ОБЩАЯ МЕТОДИКА ОБНАРУЖЕНИЯ ИНСАЙДЕРА КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ

И. В. Котенко, Д. В. Пелёвин, И. А. Ушаков

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

В статье рассматривается общая методика анализа поведения пользователей в условиях корпоративной среды для дальнейшего использования совместно с технологиями больших данных для выявления внутренних нарушителей.

большие данные, UBA, UEBA, информационная безопасность, NoSQL.

В настоящее время гораздо больший риск для безопасности данных в корпоративной сети представляют внутренние нарушители по сравнению с внешними угрозами информационной безопасности [1].

В связи с этим необходимо определить общую методику обнаружения внутренних нарушителей информационной безопасности с использованием современных средств детектирования подозрительного поведения пользователей [2, 3].

Под инсайдером определим некоторого авторизованного сотрудника организации, предполагающего совершение злонамеренной активности или нанесение ущерба внутри неё и аутентифицированного в некоторой системе с использованием персональных данных [4].

Ключевой проблемой безопасности в организации является определение скомпрометированных аккаунтов и инсайдеров внутри компании, которые могут принести ущерб своей деятельностью. Ущерб может быть, как экономическим, так и материальным.

Выявление инсайдерской атаки представляет собой трудоёмкую задачу. Необходимо выделить из событий те, которые являются вредоносными.

Определим потенциальные классы атак на внутренние сети организации и представим их в таблице [5].

ТАБЛИЦА. Определение потенциальных атак инсайдера

Профиль	IT-саботаж	Кража интеллектуальной собственности	Фальсификация	Шпионаж
Кто	Технические работники	Инженеры, программисты, персонал	Сотрудники низкого уровня	Любые сотрудники
	Привилегированный персонал		Менеджеры	
Когда	При устройстве на работу	За определенный срок до покидания организации	В течении Длительного времени	В течении длительного времени
				При различных событиях
Зачем	Желание отомстить	Начало своего бизнеса	Жадность	Заказ, жадность
		Смена должности		
		Для другой организации		
Каким образом	Наличие доступа	Копирование документов, пересылка по e-mail	Коррупция	Все остальные методы
			Неадекватная реакция	
Что затрагивает	Рабочие системы сотрудника	Кража информации, с которой работала организация	Персональная информация	Похищение информации

Выделим ниже основные аспекты, важные для определения методики [6].

1. *Опыт предыдущих атак*. Он основывается на анализе поведения раннее определенного внутреннего нарушителя, действия которого были выявлены ранее и, на основании действий которого, можно сделать выводы о поведении следующих нарушителей.

2. *Аномальные попытки входа*. Следует обращать внимание на частоту и количество попыток входа в систему за ограниченный период времени, независимо от того, успешные они или нет.

3. *Всплески активности.* Хорошим способом обнаружения аномалий может являться всплеск активности однотипных действий в сети. Например, большое число попыток входа на конкретный аккаунт или частое изменение файлов может не являться самой угрозой, но служить сигналом для более тщательного исследования поведения пользователя.

4. *Активность в виртуальных частных сетях.* Высокая нагрузка в виртуальной сети и нестандартное географическое положение пользователя может сигнализировать об опасности.

5. *Отслеживание общих аккаунтов.* Слежение за общими аккаунтами организации необходимо для сохранения информационной безопасности. Единовременный вход в систему с разных устройств может быть признаком компрометации аккаунта.

6. *Отделение пользовательских аккаунтов от сервисных.* Хорошей практикой является редкое использование привилегированных аккаунтов и только для тех случаев, когда обычный аккаунт не имеет достаточно прав для выполнения задачи. Такое действие предупредит потенциального инсайдера от доступа к информации.

Все описанные события могут соответствовать заранее установленным правилам, шаблонам, паттернам, что упрощает поимку нарушителя с помощью наблюдательности администратора или специально разработанных систем аналитики сетевой активности через логирование, профилирование и сбор статистики.

Основная идея состоит в том, чтобы на основе мониторинга действий пользователя выявлять аномальную активность, которая может соответствовать инсайдерской деятельности.

Решение задачи сбора всей необходимой информации для подобного мониторинга сети и ее дальнейшей обработки может стать серьезной проблемой для организации ввиду неоднородности поступающей информации и сложности её анализа. Поэтому привычные методы работы с данными не удовлетворяют всех потребностей информационной безопасности.

Хранение больших объемов данных при использовании традиционных технологий может быть экономически нецелесообразно, по этой причине большая часть информации удаляется после фиксированного периода времени [7, 8]. В этом случае необходимо обратиться к новым и перспективным способам хранения и обработки данных, называемым технологиями больших данных.

Информация о сетевой активности, поступающая от различных источников, является достаточно неоднородной и неструктурированной, что является верным признаком того, чтобы использовать для нее базы данных NoSQL. Это должно упростить ее обработку для своевременного обнаружения инсайдеров в компьютерной сети.

Например, при сборе информации о сетевой активности в режиме реального времени мы можем использовать графовую базу данных.

Модель такой базы представляется в виде параметризированного графа (рис.), который состоит из узловых точек и ребер, причем узловые точки выступают в качестве объектов, а ребра выступают в качестве связей между объектами [9].

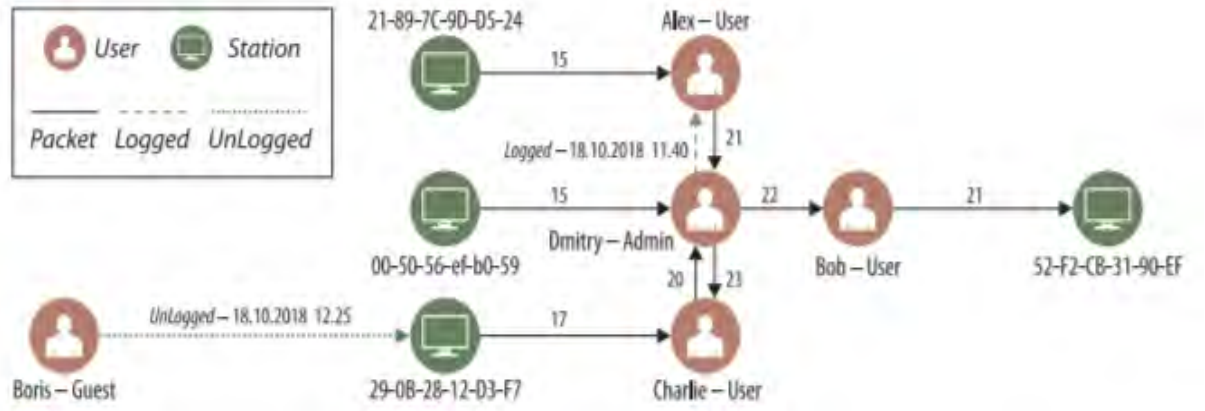


Рисунок. Представление модели графовой базы данных

Граф также состоит из свойств, связанных с узловыми точками. При его построении используется подход, который называется «смежность без индекса», означающий, что каждая узловая точка включает в себя указатель на смежную узловую точку.

Благодаря такому подходу можно работать с большим числом записей. В базе основной упор делается на связь между данными, обеспечивая бессхемное хранение полуструктурированных данных.

Используя подобный подход, можно выделить ручной и автоматизированный способы решения задачи обнаружения инсайдера.

При ручном способе сетевой администратор сможет в режиме реального времени наблюдать за поведением пользователей в сети и делать своевременные выводы о происходящих действиях, обнаруживая аномалии и пресекая нежелательную активность.

В качестве второго способа обнаружения инсайдера может выступать автоматизированная обработка данных с помощью технологий машинного обучения, основанного на наблюдениях за системой, в которой принятие решения о вредоносности конкретных действий будет основываться на поведенческом анализе предшествующих событий. Этот способ является основным для проведения авторами дальнейших исследований задачи обнаружения инсайдеров.

Предлагаемая авторами общая методика обнаружения инсайдера в компьютерной сети основана на представленных выше процедурах и технологиях обработки больших данных для анализа большого объема информации о действиях пользователей за определенный интервал времени (час, сетки, недели, месяцы), а также использовании как ручного, так и автоматизированного способа решения задачи обнаружения инсайдера.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369, 18-07-01488, 18-37-20047, 18-29-22034, 18-37-20047) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Котенко И. В., Степашкин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды ИСА РАН. 2007. Т. 31.

2. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.

3. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

4. Data Breach Investigations Report, Verizon. [Электронный ресурс]. 2017. URL: https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf (дата обращения 01.02.2019)

5. Kont M., Pihelgas M., Wotjtkowia J. Insider Threat Detection Study, 2015. P. 1–59.

6. Brooks R. Insider Threat Detection: 10 Techniques for Top-to-Bottom Defence. [Электронный ресурс]. URL: https://blog.netwrix.com/2017/12/12/insider-threat-detection-10-techniques-for-top-to-bottom-defense/ (дата обращения 03.04.2019).

7. Kotenko I., Kuleshov A., Ushakov I. Aggregation of Elastic Stack instruments for storing and processing of security information and events // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017.

8. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.

9. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Овраменко А. Ю. Гибридная модель базы данных NOSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1 (85). С. 46–54.

УДК 004.056
ГРНТИ 20.23.17

ВАРИАНТ АРХИТЕКТУРЫ СИСТЕМЫ АНАЛИЗА ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В СЕТИ ИНТЕРНЕТ С ПРИМЕНЕНИЕМ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ

И. В. Котенко[1], О. Н. Тушканова[1,2]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский политехнический университет Петра Великого

В работе предложен вариант архитектуры разрабатываемой интеллектуальной системы аналитической обработки цифрового сетевого контента, который обеспечивает реализацию методов и алгоритмов обработки данных, в первую очередь в контексте задачи многоаспектной оценки и категоризации информационных объектов в сети Интернет, например, вебсайтов, по их смысловому содержанию. Информационные объекты обычно содержат большой объем контента, представленного гетерогенными данными, и обладают сложной структурой, поэтому задачу анализа таких объектов следует отнести к области больших данных, соответственно, для ее своевременного решения требуется использование параллельных вычислений.

информационный объект, система аналитической обработки, задача классификации, параллельные вычисления.

Глобальная сеть состоит из огромного количества источников разнородной информации, которая по смысловому наполнению часто может интерпретироваться как нежелательная, сомнительная или вредоносная [1, 2]. Обнаружение таких источников информации является важным, поскольку их распространение и использование может приводить к серьезным негативным последствиям как на локальном уровне, затрагивающем интересы и права отдельных лиц, так и на глобальном уровне, находящем отражение в международных разногласиях и конфликтах.

Целью данной работы является краткое представление варианта архитектуры разрабатываемой в рамках научно-исследовательского проекта интеллектуальной системы аналитической обработки цифрового сетевого контента, направленной на обнаружение и противодействие нежелательной, сомнительной и вредоносной информации в глобальной сети Интернет.

Одной из наиболее важных функциональностей разрабатываемой системы является своевременный многоуровневый и многомодульный анализ сетевых информационных объектов (ИО) с целью обнаружения нежелательной информации.

Под информационным объектом (ИО) будем понимать логически цельный блок информации, представленный в определенной фиксированной форме, который создан и используется в ходе информационной составляющей деятельности человека [3, 4]. Примерами сетевых ИО являются информационные и новостные вебсайты, веб-страницы, форумы, социальные сети, игровые и медиа-порталы и т. д.

Любые ИО в первую очередь характеризуются своим смысловым наполнением, к которому можно отнести тексты на различных естественных языках, медиа-контент, например, изображения, видео, аудио, фрагменты других ИО, встроенные с помощью элемента IFrame, например, карты, исполняемые сценарии, например, скрипты на языке JavaScript. Каждый сетевой ИО обладает доменным именем (URL) и множеством IP-адресов. Кроме того, ИО может характеризоваться набором других разнородных атрибутов (числовыми, булевыми, ординальными, номинальными), содержать данные специальных форматов, (веб–ссылки, адреса электронной почты, номера телефонов, геопозиция и т. п.). Дополнительно, для многих сетевых ИО можно получить информацию о том, какие технологии использованы на серверной стороне соответствующего приложения. Помимо этого, такие объекты могут обладать сложной, многоуровневной, иерархической или нелинейной структурой, храниться в распределенных базах данных или иметь характер потоков во времени и представляться множеством транзакций.

Принимая во внимание вышеупомянутые факторы, задачу анализа ИО очевидно следует относить к области больших данных, соответственно, для ее своевременного решения требуется использование параллельных вычислений.

На рисунке приведена схема архитектуры и взаимодействия компонентов разрабатываемой системы аналитической обработки цифрового сетевого контента с целью обнаружения и противодействия нежелательной, сомнительной и вредоносной информации.

Согласно общей концепции разрабатываемой системы в рамках анализа ИО в первую очередь должны решаться задачи многоаспектной оценки и категоризации смыслового наполнения ИО. Одним из способов решения этой задачи является автоматическая классификация сетевых ИО с использованием данных об ИО, собранных в распределенное хранилище с помощью интеллектуальных сканеров (рис., компонент сбора данных об ИО (1а)). В качестве вектора признаков могут рассматриваться любые комбинации доступных характеристик ИО, важнейшей из которых является текст на естественном языке. В качестве обучающей выборки может выступать набор предварительно категоризированных ИО, например, веб-страниц или веб-сайтов. (рис., компонент предобработки данных (1б)). Для решения задачи автоматической классификация сетевых ИО (рис., компонент

классификации и оценки результатов (2) и компонент адаптации и переобучения (5)) предполагается использовать методы машинного обучения, которые частично описаны работах [5, 6, 7, 8, 9].

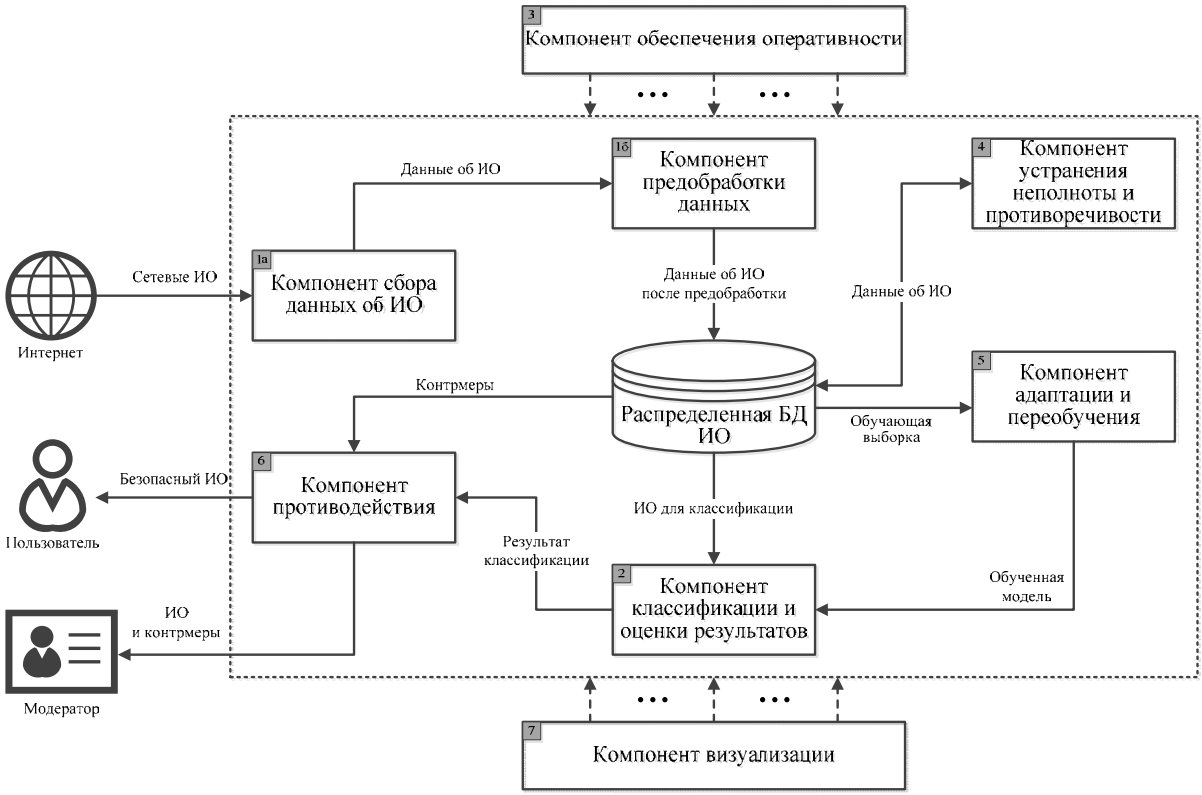


Рисунок. Схема архитектуры и взаимодействия компонентов системы аналитической обработки цифрового сетевого контента с целью обнаружения и противодействия нежелательной, сомнительной и вредоносной информации

Требования к своевременности решения задач разрабатываемой системы аналитической обработки цифрового сетевого контента обуславливают необходимость распределенного хранения гетерогенных данных о сетевых ИО и использования технологий параллельных вычислений, а значит и необходимость взаимодействия с компонентом обеспечения оперативности всеми другими компонентами разрабатываемой системы. Необходимость использования технологий параллельных вычислений и распределенного хранения данных о сетевых ИО обусловлена также требованиями к компоненту сбора и предварительного анализа данных об ИО. Соответствующий компонент обеспечения оперативности реализован с помощью программной платформы параллельной обработки данных Apache Hadoop [10] и системы распределенных вычислений Spark [11]. Для решения задачи многоаспектной оценки и категоризации смыслового наполне-

ния ИО с помощью машинного обучения планируется использовать библиотеку с открытым исходным кодом Spark MLlib [12], так как она поддерживает наиболее эффективные алгоритмы обучения для больших данных.

Более подробно функциональные и архитектурные особенности компонентов будут описаны в других работах научного коллектива, посвященных научно-исследовательскому проекту по разработке интеллектуальной системы аналитической обработки цифрового сетевого контента.

Работа выполнена при финансовой поддержке Гранта РНФ (проект № РНФ 18-11-00302) в СПИИРАН.

Список используемых источников

1. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерства внутренних дел Российской Федерации, Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службы от 18.05.2017 г. № 84/292/351/ММВ-7-2/461.

2. Федеральный список экстремистских материалов. URL: http://minjust.ru/ru/extremist-materials (дата обращения 20.03.2019).

3. Минькович Т. В. Информационные технологии: понятийно-терминологический аспект // ОТО. 2012. № 2. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-ponyatiyno-terminologicheskiy-aspekt (дата обращения 20.03.2019).

4. Виткова Л. А. Обзор степени разработанности темы мониторинга и противодействия угрозам информационно-психологической безопасности в социальных сетях // Информационные технологии и телекоммуникации. 2018. Т. 6, № 3. С. 1–9.

5. Kotenko I., Chechulin A., Komashinsky D.: Categorisation of web pages for protection against in-appropriate content in the internet. International Journal of Internet Protocol Technology, 10 (1), 2017, pp. 61–71.

6. Qi X., Davison B. D. Web Page Classification: Features and algorithms. ACM Computing Surveys (CSUR), 2009, pp. 1–31.

7. Feldman R., Sanger J., Text Mining Handbook: Advanced Approaches in Analyzing Unstructured Data, Cambridge University Press, New York, NY, 2006.

8. Mikolov T., Chen K., Corrado G., and Dean J. Efficient Estimation of Word Representations in Vector Space. In Proceedings of Workshop at ICLR, 2013.

9. Ma J., Saul L. K., Savage S., Voelker G. M. Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs. In: Proceedings of Conference on Knowledge Discovery and Data Mining, pp. 1245-1254. ACM, 2009.

10. The Apache Hadoop. URL: https://hadoop.apache.org. (дата обращения 20.03.2019).

11. The Apache Spark. URL: http://spark.apache.org (дата обращения 20.03.2019).

12. Spark MLlib. URL: https://spark.apache.org/mllib (дата обращения 20.03.2019).

УДК 004.056
ГРНТИ 81.93.29

АРХИТЕКТУРА ПЕРСПЕКТИВНОЙ СИСТЕМЫ UEBA ДЛЯ ПРОВАЙДЕРОВ ОБЛАЧНЫХ УСЛУГ

И. В. Котенко, Б. А. Тынымбаев

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Анализируются преимущества применения систем класса поведенческого анализа пользователей и сущностей для провайдеров облачных услуг. Дано описание класса систем, называемых брокерами безопасности облачного доступа и показана их связь с аналитическими системами класса UEBA. Описана схема взаимодействия с источниками событий информационной безопасности, приведены примеры математических моделей анализа поведения пользователей и возможные области применения потенциальной системы UEBA в сфере облачных технологий.

защита информации, аналитика безопасности, модели поведения пользователей, информационная безопасность.

Область аналитических инструментов в сфере кибербезопасности стремительно разрастается, помимо систем класса SIEM (*Security information and event management*) всё чаще начинают использоваться системы UEBA (*User and Entity Behavior Analytics*), которые на основе поведенческого анализа пользователей и сущностей позволяют обнаруживать внешние и внутренние угрозы. Очевидна тенденция повышения уровня зрелости программных решений в сфере информационной безопасности с помощью добавления аналитики, в том числе методов машинного обучения.

Наиболее полезное и уместное использование системы UEBA видится в инфраструктурах облачных сервис-провайдеров. Согласно [1] к 2021 году 94 % задач и виртуальных вычислений будут выполняться в облачных центрах обработки данных (ЦОД), а в традиционных ЦОД – только 6 %. Таким образом, задача безопасности облачных данных становится все более актуальной. Для обеспечения информационной безопасности в облаках и соблюдения требований внутренних служб информационной безопасности и внешних регулирующих органов в части работы с облачными данными на рынке предлагаются решения класса Cloud Access Security Brokers (CASB) – брокеры безопасности облачного доступа.

Решения CASB позволяют отслеживать события информационной безопасности, внедрять политики предоставления доступов, защиты данных и соответствия требованиям регуляторов для провайдеров облачных услуг.

CASB становится неким аналогом прокси-сервера, применительно к функциям безопасности, для пользователей облачных услуг.

В [2] приведён пример использования аналитики по поведению пользователей в решениях CASB. Решая задачу о разработке архитектуры системы UEBA для CASB, следует взять за основу необходимые данные, методы, а также сценарии реализации и обнаружения угроз (табл.) [3].

ТАБЛИЦА. Данные, методы и сценарии для UEBA

Данные и средства	Описание	Пример
Данные	Логи, предупреждения системы предотвращения утечки данных, SIEM, сетевые потоки, данные систем идентификации пользователей, HR-данные и др.	Логи системной аутентификации и информация о пользователях
Методы	Машинное обучение с «учителем», обучение без «учителя», статическое моделирование и др.	Сравнение каждого с каждым, сравнение внутри групп и модель активности с учетом времени
Сценарии обнаружения угроз	Обнаружение скомпрометированных аккаунтов, кражи данных перед отправкой, саботажа работников, искажения общих аккаунтов и др.	Обнаружение отзыва аккаунта внешним атакующим

Помимо стандартных входных данных о пользователях, для облачных сервис-провайдеров важна геолокация пользователей, часовой пояс, тип рабочей станции, браузера и т. д. Также для составления коллекции входных данных важно заполнение первичной анкеты пользователя, наподобие профайла в информационных системах обработки данных о людских ресурсах (HR-данных).

Один из методов поведенческого анализа пользователей может основываться на использовании модели подсчета уровня доверия к пользователям. Понятно, что поведение пользователя не может быть определено только по историческим данным.

Например, в [4] предложена методика расчета уровня доверия к пользователям. Выделено 4 типа уровней доверия:

(1) прямой уровень доверия T_d (статистика в реальном времени взаимодействия пользователя с облачной платформой);

(2) рекомендательный уровень доверия T_r (уровень, полученный при взаимодействии пользователя с другими пользователями);

(3) исторический уровень доверия T_h (результат подсчёта последнего уровня доверия в соотношении нормального и аномального поведения);

(4) интегрированный уровень доверия T_c, который является синтезом предыдущих уровней.

В итоге, формула подсчёта интегрированного уровня доверия выглядит следующим образом:

$$T_c = [\alpha * T_d + \beta * T_r + \gamma * T_h],$$

где α, β, γ – весовые коэффициенты, и $0 < \alpha, \beta, \gamma < 1$, $\alpha + \beta + \gamma = 1$.

Для вычисления уровней доверия используется параметр количества запросов пользователей (внутренних и внешних). Например, рекомендуемый уровень доверия вычисляется по формуле

$$T_r = [\left(\sum_{i=1}^{w}(\frac{T_{ci}}{w}) * (\frac{Inter_{success}^{inner}}{Inter^{inner}})\right) + (\frac{Inter_{success}^{outer}}{Inter^{outer}})],$$

где w, $Inter^{inner}$, $Inter_{success}^{inner}$ – количество пользователей, запросов пользователей и успешных запросов пользователей внутри облака, $Inter^{outer}$, $Inter_{success}^{outer}$ – количество внешних запросов и внешних успешных запросов пользователей, T_{ci} – интегрированный уровень доверия i-го пользователя. При этом важно выбрать временной интервал, на котором рассчитывается уровень доверия.

В [5] поведение пользователей определяется на основе следующих правил:

поведение пользователя с устаревшими данными/логами, истекшим сроком действия учётной записи и т. п. расценивается как подозрительное;

поведение оценивается в пропорции времени поведения и уровня ненормальности поведения;

доверие к пользователю определяется в пропорции количества успешных попыток доступа к ресурсам к общему количеству попыток доступа;

для предотвращения риска мошенничества оценка доверия повышается медленно;

для наказания вследствие обмана используется быстрое снижение оценки доверия.

Данная система является привлекательной для использования в системе UEBA, рассматривающих риски мошенничества, как критичные риски компании.

Основу системы UEBA составляют сценарии обнаружения угроз, наиболее критичные и значимые для любой организации.

Для определения угроз, необходимо использовать, в первую очередь, стандартные сценарии:

обнаружение компрометации учётных записей пользователей,

обнаружение скомпрометированного конечного устройства,

обнаружение утечки данных,

использование несанкционированного внутреннего доступа, включая привилегированные доступы,

предоставление дополнительной информации и контекста для исследования.

Кроме того, должны использоваться специфичные сценарии угроз, свойственные конкретному облачному провайдеру.

Типичная архитектура системы UEBA может включать компонент анализа поведения пользователя, компонент аналитических вычислений, выполняемых в реальном времени, компонент машинного обучения и компонент реализации «приманок». Схематично архитектура системы UEBA для провайдера облачных услуг представлена на рисунке.

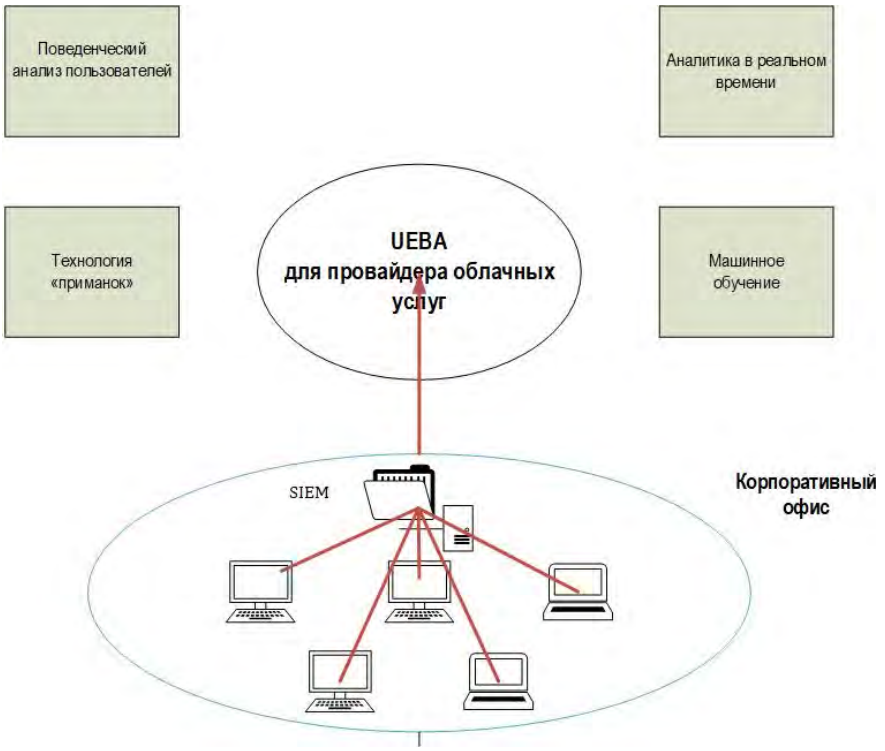


Рисунок. Архитектура системы UEBA для провайдера облачных услуг

Для спецификации атак в общем виде можно применять различные виды сценариев [6, 7]. Сценарный уровень модели компьютерных атак учитывает первичные знания злоумышленника об атакуемой компьютерной сети, его общий уровень знаний и умений, определяет конкретный атакуемый объект (один хост) и цель атаки (например, «определение ОС хоста», «реализация атаки отказа в обслуживании» и т. п.). Сценарный уровень содержит этапы сценария, множество которых состоит из следующих элементов: разведка, внедрение (первоначальный доступ к хосту), повышение привилегий; реализация угрозы; сокрытие следов; создание потайных ходов.

Одним из решений по настройке системы является использование «приманок» [8]. В [9] предложен подход к использованию технологий об-

мана и серверов «приманок» для анализа поведения пользователей. При попытке доступа, атакующего к файлу, автоматически генерируется «обманный файл» с тем же названием, так что злоумышленнику кажется, что это и есть цель его атаки.

Профайлы пользователей составляются для моделирования ситуации получения доступа пользователя к данным в облаке. Например, в полиции отдельных стран уже используют модель, основанная на профайлах поведения граждан, для обнаружения мошенничества. Технология «приманок» используется в случае успешной авторизации при обнаружении подозрительного поведения.

В работе представлен класс систем, называемых брокерами безопасности облачного доступа, и показана их взаимосвязь с аналитическими системами поведенческого анализа пользователей и сущностей.

В дальнейших исследованиях планируется построить прототип данной системы с использованием технологий больших данных и машинного обучения и провести его экспериментальную оценку.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369, 18-07-01488, 18-37-20047, 18-29-22034, 18-37-20047) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021.
2. Friedman J., Bouchard M. Definitive guide to Cloud Access Security Brokers, 2015.
3. Barros A., Chuvakin A. Demystifying Security Analytics: Sources, Methods and Use Cases, Gartner. 27.03.2017.
4. Chen Z., Tian L., Lin Ch. Trust evaluation model of cloud user based on behavior data // International Journal of Distributed Sensor Networks, 2018, Vol. 14 (5).
5. Ch. Naveen Kumar Reddy. Evaluation of Behavioral Security in Cloud Computing // IJCSIT 2012. P. 3328–3333.
6. Котенко И. В., Степашкин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды ИСА РАН. 2007. Т. 31.
7. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.
8. Котенко И. В., Степашкин М. В. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН. 2004. Т. 1, № 2. С. 211–230.
9. Котенко И. В., Степашкин М. В. Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Известия высших учебных заведений. Приборостроение. 2006. Т. 49, № 3. С. 3–9.
10. Kulkarni T. R., Waghmare V., Chaudhary D., Kulkarni P. Security Implementation in cloud computing using User Behavior Profiling and Decoy Technology // World Journal of Technology, Engineering and Research, Vol. 3, Issue 1, 2018. P. 108–113.

УДК 004.056
ГРНТИ 81.93.29

ОБЗОР РЕШЕНИЙ КЛАССА UEBA

И. В. Котенко, Б. А. Тынымбаев

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Проводится анализ текущих решений в области анализа поведения пользователей и систем класса UEBA. Рассматриваются как коммерческие решения, так и научные исследования в области аналитики поведения пользователей, в том числе отражающие сценарии обнаружения угроз, модели и алгоритмы подсчёта рейтинга профилей пользователей. На основе проведённых исследований предлагается модель перспективной система класса UEBA.

защита информации, аналитика поведения пользователей, UEBA-системы, информационная безопасность.

Решения класса UEBA (*user and entity behavior analytics*), согласно определению исследовательской компании Gartner, направлены на анализ поведения пользователей и сущностей, который рассматривается как процесс кибербезопасности, имеющий целью обнаружение внутренних угроз, целенаправленных атак и финансового мошенничества [1, 2].

Инструменты UEBA должны обеспечить анализ данных, учитывая особенности каждого типа данных безопасности, реализуя отображение идентификаторов пользователей и других сущностей на признаки подозрительного поведения. Решения UEBA, кроме данных о пользователях и их деятельности, а также данных о сущностях и сценариях их функционирования, могут использовать внешние данные и сведения об угрозах безопасности, которые собираются с помощью мониторинга социальных сетей или углубленного изучения веб-активности.

Системы UEBA реализуют следующие функции:

1) распознавание идентификаторов пользователей (и других сущностей), с учетом взаимосвязи между ними и с использованием различных методик анализа данных;

2) анализ характеристик и действий пользователей и групп пользователей для определения их подозрительного поведения, это делается с помощью построения базовых паттернов нормального поведения пользователей;

3) предоставление различных аналитических инструментов анализа поведения, таких как статические и предиктивные модели, правила обнаружения, анализ связей сущностей, геопространственный анализ и анализ социальных сетей.

В настоящее время наблюдается значительный рост использования UEBA-систем для обнаружения внутренних угроз и попыток кражи данных. На сегодняшний день наиболее известны следующие вендоры UEBA: Exabeam Security Intelligence Platform, Gurucul Risk Analytics (GRA), Interset, Niara Analyzer (недавно приобретен компанией *Hewlett Packard Enterprise, Aruba division*), Securonix UEBA, Splunk UBA (в результате приобретения компанией *Splunk* решения *Caspida*).

Системы UEBA базируются на таких компонентах, как данные, методы и сценарии обнаружения угроз.

Данные система UEBA может собирать из множества источников, в том числе логов информационных систем IDS, IPS (*intrusion detection, prevention system*), файерволов, доступа к веб-приложениям, прокси-сервера, службы каталогов, социальных сетей, систем учета кадровых ресурсов и др.

Согласно [2], выделено большое количество сценариев определения угроз UEBA. В таблице представлены типичные сценарии обнаружения угроз [3].

Различия среди систем UEBA – в методах обнаружения угроз и последующего реагирования. Практически все решения UEBA используют машинное обучение. Система машинного обучения использует данные из множества источников для построения собственной логики поведенческого анализа пользователей и сущностей.

В [4] описаны различные классы систем машинного обучения, используемые в решениях класса UEBA:

1) обучение с учителем, которое используется в задачах классификации, содержит в себе алгоритмы линейной регрессии, многоклассовой классификации и поддержку векторных машин;

2) обучение «без учителя», которое используется в задачах кластеризации.

Алгоритмы классификации в решениях UEBA позволяют, например, пользователю автоматически определять категории, такие как «спам» или «не спам», или «зловредный» и «незловредный» файл, или посредством метода классификации определять тип хоста (клиент, сервер, или база данных).

Интересны исследования в области аналитики поведения пользователей. В [5] представлена вероятностная модель определения аномалий ChainSpot. Для построения данной вероятностной модели используются Марковские цепи.

ТАБЛИЦА. Сценарии обнаружения угроз

Обнаружение компрометации учётной записи	Определяются ситуации неавторизованного использования учётных записей. Компрометация учётной записи – один из примеров данного сценария.
Обнаружение скомпрометированной рабочей станции	Обнаруживаются скомпрометированные сетевые устройства, зараженные вредоносным ПО и демонстрирующие подозрительное поведение. Данный сценарий отличен от сценария, при котором обнаруживается вредоносная деятельность на конечном устройстве, так как не привязан к специфичной учётной записи.
Обнаружение утечки данных	Используется для выявления утечки данных. Неавторизованная или целенаправленная утечка данных может произойти и у авторизованного пользователя. Данный сценарий направлен на определение такого типа активности, которая необходима для выявления скомпрометированных учётных записей и конечных устройств. Данный сценарий часто фокусируется на предупреждениях от системы предотвращения утечки данных, логах решений класса CASB (*cloud access security broker*) и/или данных сетевого трафика, более подробно в [4].
Использование несанкционированного доступа, включая привилегированный доступ	Используется для выявления пользователей (включая и работников, и доверенных третьих лиц), злоупотребляющих своими привилегиями. Примеры типов активности с превышением привилегий или неавторизованного доступа к данным: получение доступа к базе данных с персональной информацией; или в случае злоупотребления системными привилегиями - создание новой пользовательской учётной записи или присваивание дополнительных привилегий в разрез политики безопасности.
Предоставление дополнительной информации и контекста для исследования	Технологии UEBA позволяют исследовать большие объёмы информации касательно пользователей и сущностей в организации для определения аномалий, связанных с угрозами. Эта информация используется аналитиками, которые выполняют сортировку предупреждений и расследование инцидентов. Если аналитик подозревает, что конечная станция была скомпрометирована, то он может использовать решение UEBA для получения информации о пользователях данной рабочей станции, анализируя их регулярное поведение и роль рабочей станции в сети.
Разработка отдельных сценариев	Вендоры UEBA часто упоминают о применении новых сценариев, отличающихся от предустановленного набора: начиная с обнаружения мошенничества до трекинга наркотиков в организациях здравоохранения. Свойство собирать отдельные данные и создавать типичные модели машинного обучения - достаточно важное для решений UEBA.

В [6] отношения пользователей внутри облачного ресурса представлены в виде графа, на основе которого вычисляется уровень доверия к пользователю.

Исходя из последних тенденций перехода информационных систем в облачные сервисы, интерес представляет исследование существующих алгоритмов безопасности анализа поведения пользователей в облачном окружении.

В [7] представлено описание следующих алгоритмов, которые могут быть использованы для анализа поведения пользователей в облачном окружении: алгоритм определения ранга облаков, алгоритм энтропий, алгоритм обнаружения аномального поведения, алгоритм случайных сетей Петри, алгоритм динамики нажатия клавиш, алгоритм обучения на правилах. Недостатком всех перечисленных алгоритмов является отсутствие распознавания или раннего обнаружения внешних уязвимостей, которые являются одной из критичных угроз для облачных ресурсов.

Также стоит отметить тенденции использования аналитики поведения пользователей и в более доступных решениях – в программных продуктах рабочих станций: к примеру, недавно «Лаборатория Касперского» анонсировала новую функцию адаптивного контроля аномалий (*Adaptive Anomaly Control*) для анализа поведения пользователей в своем продукте Kaspersky Security для бизнеса.

Резюмируя, следует отметить, что, при использовании передовых инструментов аналитики, решения класса UEBA становятся все более востребованными. Главный тренд, согласно исследовательской компании Gartner, состоит в следующем: поскольку решения класса UEBA все чаще связываются с решениями класса SIEM и развиваются до более широких платформ, большинство организаций будут искать решения SIEM нового поколения или гибриды UEBA-SIEM, например, в форме их аналитических хабов. В будущих исследованиях предусматривается анализ, разработка и экспериментальная оценка моделей, алгоритмов и методик поведенческого анализа пользователей и сущностей для провайдеров облачных услуг.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369, 18-07-01488, 18-37-20047, 18-29-22034, 18-37-20047) и бюджетной темы 0073-2019-0002.

Список используемых источников

1. Котенко И. В. Аналитика кибербезопасности: анализ современного состояния и перспективные направления исследований // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей в 4-х т. 2018. Т. 1. С. 10–19.

2. Chuvakin A., Barros A. A comparison of UEBA technologies and solutions // Gartner, 29.03.2017.
3. Barros A., Chuvakin A. Demystifying Security Analytics: Sources, Methods and Use Cases // Gartner, 27.03.2017.
4. Friedman J., Bouchard M. Definitive guide to Cloud Access Security Brokers.: Visibility, Security and Compliance for Applications and Data in the Cloud, 2015. 52 p.
5. Chin-Hao E. M. User Entity Behavior Analysis for Cyber Security // (ISC)2 APAC Congress, Orlando, 12–15 Sept. 2016.
6. Chen S., Wang G.,Jia W. A Trust Model Using Implicit Call Behavioral Graph for Mobile Cloud Computing // Cyberspace Safety and Security. Lecture Notes in Computer Science, vol. 8300. Springer, Cham.
7. Arasu1 T., Raj E. G. D. P., Prashanth B. Algorithms for user behavior analysis in cloud environment // IJRASET. Vol. 5. Issue XII. 2017.

УДК 004.056
ГРНТИ 81.93.29

СОЗДАНИЕ И УПРАВЛЕНИЕ SECURITY OPERATIONS CENTER ДЛЯ ЭФФЕКТИВНОГО ПРИМЕНЕНИЯ В РЕАЛЬНЫХ УСЛОВИЯХ

А. А. Казанцев, А. В. Красов, А. И. Катасонов, А. М. Гельфанд

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

С развитием технологий возможных угроз безопасности организаций, все больше растут требования к системам, обеспечивающим информационную безопасность компании, в связи с этим вопрос создания эффективного SecurityOperationsCenter встает особенно остро. В открытых источниках недостаточно описаны методики создания SOC для использования в реальных условиях.

SecurityOperationsCenter, SOC.

По мере того, как угрозы безопасности продолжают развиваться в возможностях, для организаций вырастает спрос на создания Security Operations Center (SOC). Согласно отчету о расследовании нарушений VerizonDataBreast 2015 года: «В 60 % случаев злоумышленники могут скомпрометировать организацию в течение нескольких минут», и «75 % атак, распространяемых от жертвы 0 до жертвы 1 в течение одного дня (24 часа)». Ожидание реагирования на нарушение до тех пор, пока ущерб не будет

нанесен, скорее всего, приведет к чрезвычайно дорогостоящему восстановлению [1, 2, 3, 4].

Пять основных шагов связаны с разработкой SOC:

1 – Планирование SOC,

2 – Проектирование SOC,

3 – Строительство SOC,

4 – Управление SOC,

5 – Обзор SOC.

В следующих разделах рассматриваются действия, требуемые на каждом этапе разработки SOC.

Оценка возможностей безопасности при планировании Security Operations Center

Планирование начинается с оценки ваших существующих возможностей безопасности для людей, процессов и технологий. Этот подход позволяет вам установить базовый уровень, который можно сравнить с целями будущего SOC.

Методология оценки должна придерживаться следующих шагов:

– Определите цели бизнеса SOC и IT.

– Определите возможности для оценки, основанные на целях SOC.

– Собирайте информацию, связанную с людьми, процессами и технологическими возможностями.

– Проанализируйте собранную информацию и назначьте уровни готовности для оцениваемых возможностей.

– Представлять, обсуждать и формализовать выводы.

Демонстрация процесса представлена на рис. 1.

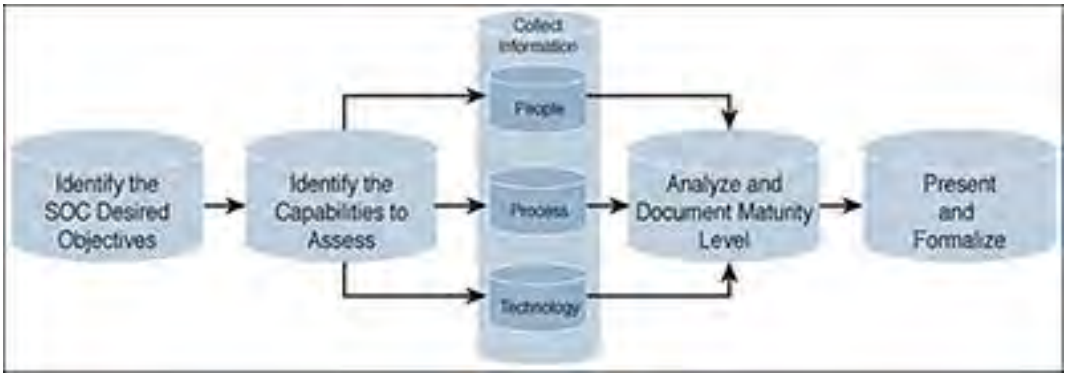


Рис. 1. Методология оценки возможностей операций по обеспечению безопасности

Идея состоит в том, чтобы сначала установить бизнес-цели организации. Следующим шагом будет список возможностей, которые вернутся к бизнес-целям, которые были определены на первом этапе. Возможности

включают существующих людей, процессы и технологии. Уровни готовности устанавливаются для каждой возможности, чтобы можно было определить приоритеты для разработки плана построения будущего SOC.

Вторая часть этапа планирования – это разработка стратегии SOC, которая состоит из следующих пунктов:

Миссия SOC,
Стратегические цели SOC,
Область СС,
Модель работы SOC,
Услуги SOC,
Возможности развития SOC,
Основные показатели эффективности (KPI) SOC.

Недостаточная или неточная оценка возможностей SOC приведет к слабой стратегии SOC, которая не соответствует целям организации.

Фаза планирования должна определить модель работы: физическая, виртуальная или гибридная? На этапе планирования будет также определен тип услуг, предоставляемых SOC, укажите, отвечает ли SOC за всю сеть или подмножество сетей, и укажите детали этих служб.

Проектирование и строительство SOC

Как только этап планирования будет завершен, следующим шагом будет разработка SOC. Шаги проектирования и строительства практически неразрывно связаны, и выбор технологий является важной частью обеих фаз для будущего SOC. Важным направлением является то, как SOC собирает данные. Обычно эта задача выполняется с использованием централизованного инструмента сбора данных, такого решение как Security Information and Event Management (SIEM). Другие инструменты безопасности, такие как брандмауэры, фильтры содержимого, системы обнаружения/предотвращения вторжений и т. д., будут экспортировать события в SIEM, позволяя аналитикам SOC оценивать все события, чтобы получить более полную картину текущего состояния безопасности организации. На рис. 2 (см. ниже) показан пример зрелого SOC с многоуровневой безопасностью, сегментацией сети и технологиями мониторинга.

Лучшим подходом будет использование многоуровневых возможностей защиты / обнаружения, таких как: Фильтр содержимого, который знает о вредоносных веб-источниках; IPS для обнаружения атак; Технология обнаружения нарушений, в поисках неизвестных угроз, упущенных IPS; Инструмент (например, NetFlow), который основывает сеть, а затем контролирует ее для необычных тенденций данных

Защита должна расширяться во всех областях сети. Если вы не обеспечиваете одинаковый уровень безопасности для различных частей вашей

сети, наименее защищенная область, скорее всего, будет выбрана для сторонней атаки.

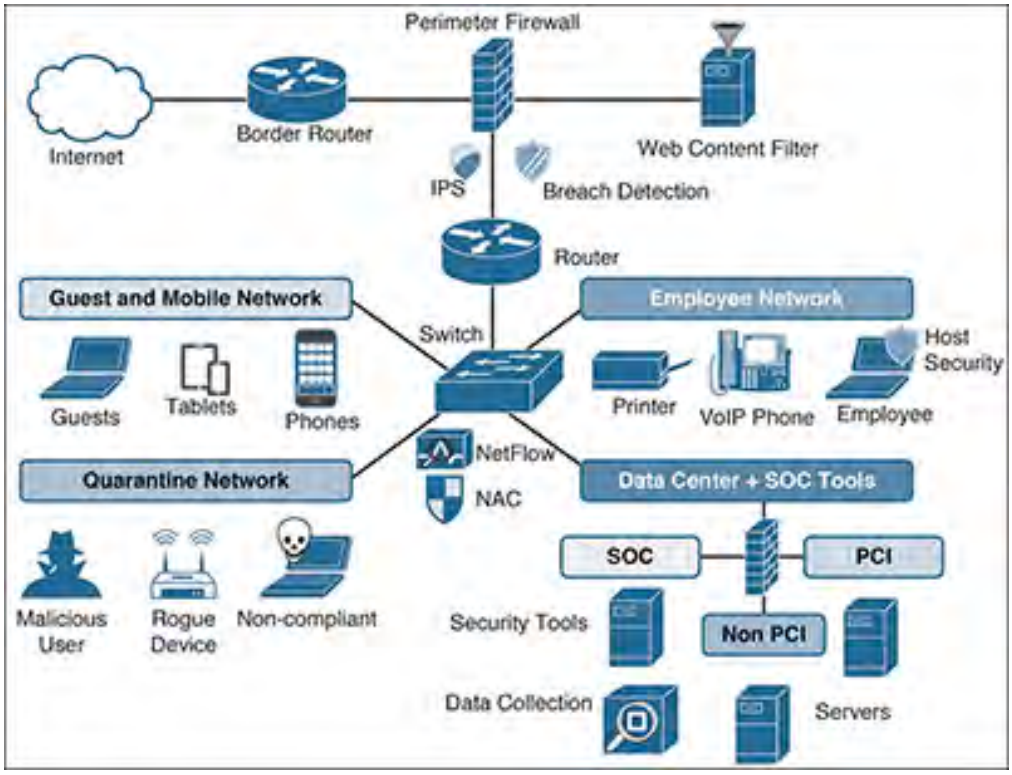


Рис. 2. Пример развитой архитектуры SOC

Для того чтобы выявить самую слабую связь в организации, SOC должна включать в себя возможности управления уязвимостями.

Технологии, необходимые для жизненного цикла управления уязвимостями, могут включать инструменты оценки, которые идентифицируют и квалифицируют уязвимости (такие как *Nessus*, *OpenVAS* или *Metasploit*), а также различные подходы к вычислению того, насколько риск связан с угрозой, чтобы определить, как смягчать, передавать, принимать или избегать уязвимостей.

Как только проект будет закончен, последняя область, которую следует рассмотреть перед переходом на этап операции, – это оценка квалификации людей.

Управление SOC

Как только SOC построен, настало время перейти в фазу работы, также известную как фаза «golive». Крайне важно, чтобы новый SOC преодолел некоторые ключевые проблемы перед текущей датой:

– Важно подтвердить, что у SOC еще есть исполнительное спонсорство. Во многих случаях большой промежуток времени проходит между

первоначальным сигналом от руководства до того момента, когда SOC фактически готова к работе.

– Процессы будут сложными, поскольку некоторые из них будут новыми и нуждаются в проверке.

– Необходимо проверить технологию, чтобы все функционировало должным образом.

– Может потребоваться обучение для членов команды, которые несут ответственность за использование и поддержание решений.

Переход от каждого шага от строительства до эксплуатации SOC требует хорошо управляемого плана перехода. Успешные планы перехода, как правило, разделяют некоторые общие факторы успеха:

– Критерии успеха ясны и понятны. Простой контрольный список критериев успеха, согласованный со спонсорами в рамках проекта, который будет основой для управления ожиданиями и исполнением.

– Ресурсы детализированы и хорошо структурированы. Ресурсы могут относиться к людям, времени или деньгам. Должно быть понятно, как и когда каждый ресурс ожидается на протяжении всего проекта.

– Требования к навыкам, технологиям, результатам и контенту ясны и достижимы. Для выполнения этой работы ваша команда должна быть достаточно квалифицированной для перехода к работе.

– Простые проверки могут быть выполнены, чтобы убедиться, что цель была успешно завершена. Должен быть разработан простой контрольный список, в котором четко указывается, как будут оцениваться результаты каждого вида деятельности, задачи или этапы.

Обзор построенной SOC

После того, как SOC будет запущен, на заключительном этапе рассматривается, насколько успешно функционирует SOC, а также выявляются области для улучшения. Анализ SOC не очень отличается от анализа любой другой важной и дорогостоящей бизнес-функции. Следующий пятиступенчатый метод хорошо подходит для разработки отчета для обновления руководства по текущему состоянию SOC:

– Определите область обзора. Это может включать в себя все аспекты SOC как часть всеобъемлющего обзора, но зачастую более полезно ограничить сферу охвата конкретными областями.

– Определите участников. Вам нужно понять, кто будет выступать и участвовать в обзоре. Конкретные участники могут зависеть от сферы.

– Создать четкую методологию. Вам нужна четкая методология для руководства любым обзором, а также ожидаемые результаты и результаты на основе заранее определенного шаблона.

– Определите частоту. Решите, как часто выполнять такие обзоры. Некоторые типы обзоров могут или должны происходить чаще. Например, рекомендуется проводить частые обзоры после инцидента в течение первых 72 часов.

– Приоритет результатов и действий. Любые области для улучшения и связанные с ними элементы действий должны быть приоритетными, выполняться и развиваться для обеспечения того, чтобы необходимые изменения были завершены.

SOC должна продолжать работать над улучшением ключевых показателей эффективности (KPI) для возможностей, которые соответствуют бизнес-целям, чтобы судить о том, работают ли службы на ожидаемых уровнях. SOC должны ориентироваться на цели KPI для каждой категории возможностей, созданной на этапе проектирования, связанной с определенными временными рамками, такими как ежеквартальные обзоры. Неспособность достичь целей может указывать на необходимость большего количества людей, процессов или технологий.

Заключение

Со всеми этими требованиями легко понять, почему SOC могут не выполнить свои первоначальные обещания. Никакая SOC не идеальна, но здоровый SOC может развиваться к лучшему. Усилия по поддержанию, пересмотру и улучшению вашего SOC являются основополагающими для его долгосрочной жизнеспособности.

Список используемых источников

1. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

2. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передачи данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141–146

3. 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: сборник научных статей в 2 т. 2015. С. 310–313.

4. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств elastic stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.

УДК 004.056.53
ГРНТИ 81.93.29

KERBEROS, ЗАЩИТА ДАННЫХ В BIG DATA

А. В. Красов, В. Е. Радынская, А. А. Тасюк

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

Работа с большими данными накладывает большую ответственность. В условиях роста объема данных и соответственно увеличения количества приложений и платформ, обращающихся к этим данным, появляются новые уязвимости, с которыми необходимо бороться.

Многие протоколы, используемые в Интернете, не обеспечивают никакой безопасности. Инструменты для кражи паролей из сети часто используются злоумышленниками. Таким образом, приложения, которые отправляют незашифрованный пароль по сети, чрезвычайно уязвимы. Хуже того, другие клиент-серверные приложения полагаются на клиентскую программу, чтобы быть «честными» о личности пользователя, который ее использует. Другие приложения полагаются на клиента, чтобы ограничить его действия теми, которые ему разрешено делать, без каких-либо других принудительных действий со стороны сервера. Статья посвящена методам защиты больших данных при помощи протокола Kerberos.

Kerberos, big data, защита данных, криптография, аутентификация.

Большие данные – это совокупность технологий, которые призваны совершать три операции. Во-первых, обрабатывать большие по сравнению со «стандартными» сценариями объемы данных. Во-вторых, уметь работать с быстро поступающими данными в очень больших объемах. То есть данных не просто много, но их постоянно становится все больше и больше. В-третьих, они должны уметь работать со структурированными и плохо структурированными данными параллельно в разных аспектах [1].

Появление больших данных в публичном пространстве было связано с тем, что эти данные затронули практически всех людей, а не только научное сообщество, где подобные задачи решаются давно. В публичную сферу технологии Big Data вышли, когда речь стала идти о вполне конкретном числе – числе жителей планете. 7 миллиардов, которые собираются в социальных сетях и других проектах, которые агрегируют людей. YouTube, Facebook, ВКонтакте, где количество людей измеряется миллиардами, а количество операций, которые они совершают одновременно, – огромно. Поток данных в этом случае – это пользовательские действия. Например, данные того же хостинга YouTube, которые переливаются по сети в обе сто-

роны. Под обработкой понимается не только интерпретация, но и возможность правильно обработать каждое из этих действий, то есть поместить его в нужное место и сделать так, чтобы эти данные каждому пользователю были доступны быстро, поскольку социальные сети не терпят ожидания.

Работа с большими данными накладывает большую ответственность. В условиях роста объема данных и соответственно увеличения количества приложений и платформ, обращающихся к этим данным, появляются новые уязвимости, с которыми необходимо бороться.

Для работы с Большими данными необходим соответствующий инструмент, такой как Cloudera. Ключевой продукт – CDH (*Cloudera Distribution including Apache Hadoop*) – связка наиболее популярных инструментов из инфраструктуры Hadoop под управлением Cloudera Manager. Менеджер берёт на себя ответственность за развёртывание кластера, установку всех компонентов и их дальнейший мониторинг. Кроме CDH компания развивает и другие свои продукты, например, Impala. Отличительной чертой Cloudera также является стремление первыми предоставлять на рынке новые технологии, пусть даже и в ущерб стабильности.

На сегодняшний день платформа Hadoop обеспечивает надежную защиту на уровне файловой системы. Хочу напомнить, что файловая система HDFS (*Hadoop Distributed File System*) реализуется поверх другой нативной файловой системы (например, ext3). Средства контроля доступа для Hadoop реализуются с использованием разрешений на основе файлов, соответствующих модели разрешений UNIX®. Хотя эта модель предоставляет разрешения на уровне файлов в рамках HDFS, ей не хватает более детализированных средств управления доступом [2].

Решение было найдено в протоколе Kerberos. Kerberos – это протокол проверки подлинности сети, который был разработан для обеспечения надежной аутентификации для клиент-серверных приложений с помощью использования симметричного шифрования [3].

Протокол Kerberos предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы. Другими словами, протокол идеально подходит для применения в Интернет и аналогичных сетях.

Основная концепция протокола Kerberos очень проста – если есть секрет, известный только двоим, то любой из его хранителей может с лёгкостью удостовериться, что имеет дело со своим напарником. Для этого ему достаточно проверить, знает ли его собеседник общий секрет [4].

Протокол Kerberos решает эту проблему средствами криптографии с секретным ключом. Вместо того, чтобы сообщать друг другу пароль, участники сеанса связи обмениваются криптографическим ключом, знание

которого подтверждает личность собеседника. Но чтобы такая технология оказалась работоспособной, необходимо, чтобы общий ключ был симметричным, т. е., он должен обеспечивать как шифрование, так и дешифрование информации. Тогда один из участников использует его для шифрования данных, а другой с помощью этого ключа извлекает их.

Перейдем непосредственно к описанию протокола, показано на рис. 1.

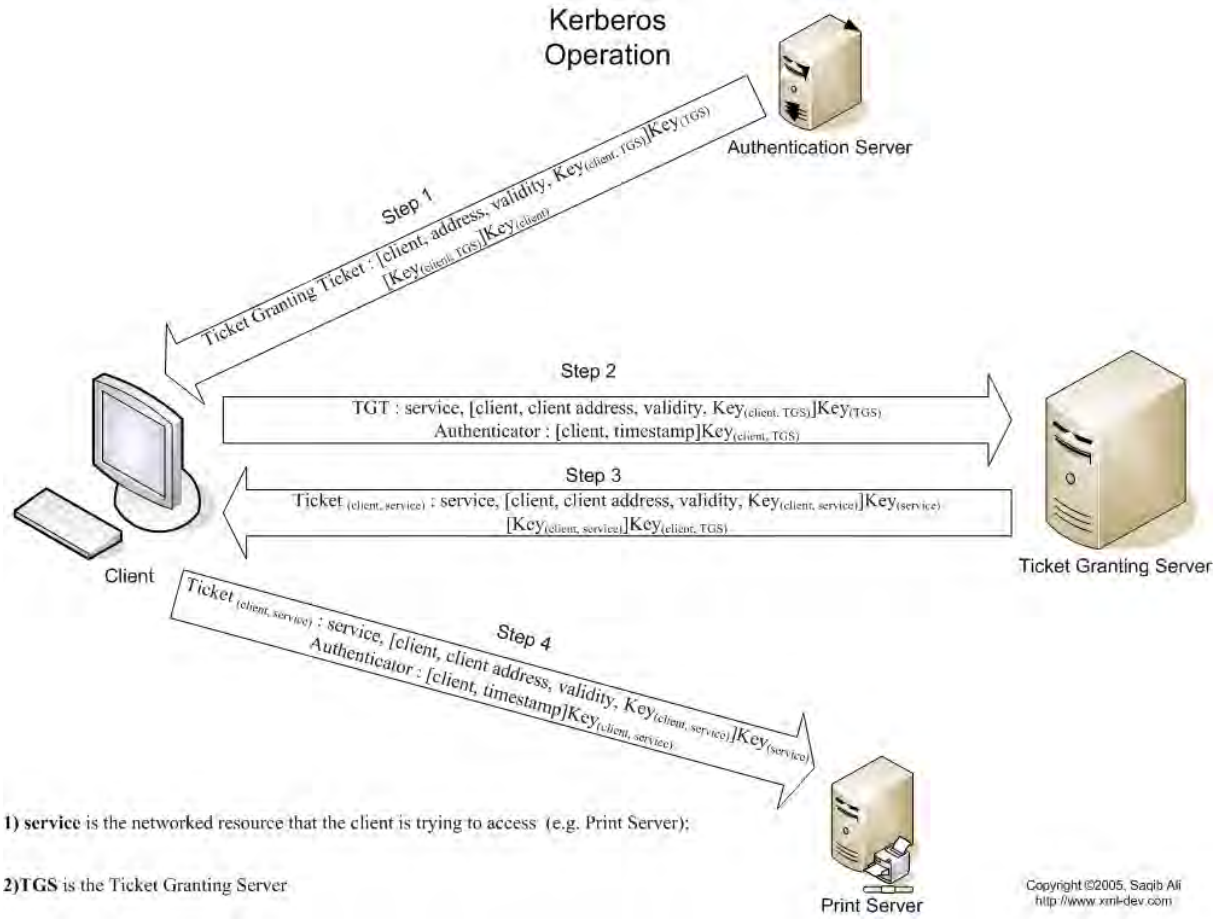


Рис. 1. Протокол Kerberos

Вход пользователя в систему

1. Пользователь вводит имя пользователя и пароль на клиентской машине. Также разрешается использовать другие механизмы, такие как PKINIT (RFC 4556), позволяющий использовать открытые ключи вместо паролей.

2. Клиент преобразует пароль в ключ симметричного шифра. Для этого используется либо встроенный генератор ключей, либо односторонний хэш в зависимости от используемого криптографического набора.

Аутентификация клиента

1. Клиент посылает сообщение с идентификатором пользователя на сервер аутентификации **AS** с запросом услуги от имени пользователя. **AS** генерирует секретный ключ путем хэширования пароля пользователя, найденного в базе данных.

2. **AS** проверяет, существует ли клиент в базе данных. Если да, то **AS** посылает обратно следующие два сообщения клиенту:

– Сообщение A: Сессионный ключ Клиент/**TGS**, зашифрованный с использованием секретного ключа клиента / пользователя.

– Сообщение B: Мандат для получения мандата (**TGT**, который включает в себя идентификатор клиента, сетевой адрес клиента, срок действия мандата, и сессионный ключ Клиент/**TGS**), зашифрованный с использованием секретного ключа **TGT**

3. После того, как клиент принимает сообщения A и B, он пытается расшифровать сообщение A с помощью секретного ключа, сгенерированного из пароля, введенного пользователем. Если пользователь ввел пароль, который не совпадает с паролем в базе данных **AS**, секретный ключ клиента будет отличаться и, следовательно, клиент не сможет расшифровать сообщение A. С действительным паролем и секретным ключом клиент расшифровывает сообщение A, чтобы получить сессионный ключ Клиент/**TGS**. Этот сессионный ключ используется для дальнейших коммуникаций с TGS. В этот момент у пользователя достаточно данных, чтобы авторизоваться на **TGS**.

Авторизация клиента

1. При запросе сервиса клиент отправляет следующие сообщения серверу **TGS**:

– Сообщение C: **TGT** из сообщения B и идентификатор запрошенной службы.

– Сообщение D: аутентификатор (который состоит из идентификатора клиента и метки времени), зашифрованный сессионным ключом Клиент/**TGS**.

2. После получения сообщений C и D, TGS извлекает сообщение B из сообщения C. Затем расшифровывает сообщение B используя свой закрытый ключ. Это дает ему «сессионный ключ Клиент/**TGS**». Используя этот ключ, **TGS** расшифровывает сообщение D (аутетификатор) и посылает два следующих сообщения клиенту:

– Сообщение E: мандат сервиса (который включает в себя идентификатор клиента, сетевой адрес клиента, срок действия и сессионный ключ клиент/сервис), зашифрованный закрытым ключом сервиса.

– Сообщение F: сессионный ключ клиент/сервис, зашифрованный с помощью сессионного ключа Клиент/**TGS**.

Запрос сервиса клиентом

1. Получив сообщения E и F от **TGS**, клиент обладает достаточной информацией, чтобы идентифицировать себя в **SS**. Клиент подключается к **SS** и посылает два следующих сообщения:

– Сообщение E из предыдущего шага (мандат сервиса, зашифрованный закрытым ключом сервиса).

– Сообщение G: новый аутетификатор, который включает в себя идентификатор клиента, метку времени, и зашифрован с помощью сессионного ключа клиент/сервис.

2. **SS** расшифровывает мандат, используя свой собственный секретный ключ, чтобы получить сессионный ключ клиент/сервис. Используя сессионный ключ, **SS** расшифровывает аутентификатор и посылает следующее сообщение для подтверждения готовности обслужить клиента и показать, что сервер действительно является тем, за кого себя выдает:

– Сообщение H: метка времени найдено в аутентификаторе клиента, зашифрованное с помощью сессионного ключа клиент/сервис.

3. Клиент расшифровывает подтверждение с помощью сессионного ключа клиент/сервиса и проверяет, корректна ли метка времени. Если это так, то клиент может доверять серверу и может начать посылать запросы на сервер.

4. Сервер предоставляет запрашиваемые услуги клиенту.

Недостатки и ограничения протокола

1. Единая точка отказа: требуется постоянное наличие центрального сервера. Когда сервер Kerberos падает, новые пользователи не могут войти. Это может быть устранено с помощью нескольких серверов Kerberos и резервных механизмов аутентификации [5].

2. Kerberos имеет строгие требования к времени, что означает, что часы участников должны быть синхронизированы в заданных пределах. Мандаты имеют время жизни и, если часы клиента не синхронизированы с часами сервера Kerberos, аутентификация не будет выполнена. Конфигурация по умолчанию требует, чтобы часы расходились не боле чем на пять минут друг от друга. На практике, как правило, используются демоны Network Time Protocol для синхронизации часов у клиентов.

3. Протокол администрирования не стандартизирован и зависит от конкретной реализации сервера. Смена пароля описана в RFC 3244.

4. В случае использования симметричной криптографии (Kerberos может работать с использованием как симметричной, так и асимметричной (с открытым ключом) криптографии), так как все способы аутентификации управляются централизованно центром распределения ключей (KDC), эта особенность инфраструктуры аутентификации позволит злоумышленнику выдавать себя за пользователя.

5. Каждый сетевой сервис, требующий смены имени хоста, должен будет обновить собственный набор ключей Kerberos. Это усложняет использование виртуального хостинга и кластеров.

6. Kerberos требует, чтобы учетные записи пользователей, клиенты и пользователи услуг на сервере, все доверяли серверу Kerberos (все должны быть в одном и том же домене с Kerberos или в доменах, имеющих доверительные отношения друг с другом). Kerberos не может использоваться в случаях, когда пользователи хотят подключаться к службам от неизвестных / ненадежных клиентов, как в обычном интернете.

Уязвимости протокола

Шифр DES может быть использован с Kerberos, однако он больше не является Интернет-стандартом, так как он является уязвимым. Уязвимости, однако, существуют во многих продуктах, использующих Kerberos, которые не были обновлены для замены DES на более новые шифры, такие как AES, например.

В ноябре 2014 года Microsoft выпустила патч (MS14-068), чтобы исправить уязвимость в реализации Windows сервера KDC. Уязвимость, согласно заявлению, позволяла пользователям "поднять" их привилегии до уровня домена.

Список используемых источников

1. Сахаров Д. В., Мельников С. Е., Штеренберг С. И. Инфраструктура связи на крайнем севере как база для формирования единой инфосреды // Электросвязь. 2016. № 5. С. 18–20.

2. Безопасность данных Hadoop и решение Sentry. Режим доступа: https://www.ibm.com/developerworks/ru/library/sehadoop/index.html

3. Сахаров Д. В., Штеренберг С. И., Левин М. В., Колесникова Ю. А. Разработка модели обеспечения отказоустойчивости сети передачи данных // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 4. С. 14–20.

4. Штеренберг С. И., Полтавцева М. А. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 59–68.

5. Калинин М. О., Штеренберг С. И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. 2018. № 3 (15). С. 47–54.

УДК 004.72
ГРНТИ 81.93.29

АНАЛИЗ ОБХОДА ПОЛИТИК БЕЗОПАСНОСТИ SDN

А. В. Красов, Н. В. Савинов, К. А. Токарева, И. А. Ушаков

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

В данной статье приведено рассмотрение угроз безопасности, таких как обход предопределенных обязательных политик путем перезаписи записей потока и подслушивания данных путем вставки мошеннических записей потока. В этой статье разработаны решения безопасности для вышеуказанных проблем безопасности.

безопасность, программно-конфигурируемая сеть SDN, контроллер, приложение, коммутатор, OpenFlow, политики, профиль приложения.

В общем, угрозы безопасности SDN являются общими для традиционных сетей, но профиль этих угроз (включая их вероятность и влияние и, следовательно, их общий уровень риска) изменяется с новой архитектурой SDN. С централизованным контроллером SDN влияние DoS / DDoS-атак с южных интерфейсов может быть хуже, чем у одного маршрутизатора. Поддельный контроллер SDN может потенциально управлять всей сетью, в которой коммутаторы управляются этим поддельным контроллером, в то время как поддельный маршрутизатор может атаковать только трафик, проходящий через него [1].

С SDN возникают некоторые проблемы с безопасностью. Приложения – это программы, которые явно, напрямую и программно сообщают о своих сетевых требованиях и желаемом сетевом поведении (т. е. сетевые политики) контроллеру через северные интерфейсы. Контроллер преобразует эти сетевые политики в потоковые записи и вставляет их в таблицу потоков. Однако в настоящее время запись потока в таблице потоков OpenFlow не отличает приложение, генерирующее новую запись потока от другого приложения, генерирующего старую запись потока. Таким образом, возможно, что новая сетевая политика, сгенерированная общим приложением, может заменить политику безопасности без обхода, переопределенную администратором безопасности. На рис. 1 администратор безопасности проактивно настраивает политику безопасности без обхода следующим образом: пакеты должны быть отправлены на брандмауэр для обнаружения, если эти пакеты доставляются из хоста A (172.0.0.1) в Host B (172.0.0.2), поскольку путь передачи данных path_1 в зеленый цвет (путь_1: Host A -> SDN_Switch_1 -> SDN_Switch_2 -> Брандмауэр ->

SDN_Switch_3 -> Host B). Спустя некоторое время приложение App_X нуждается в кратчайшем пути для транспортировки данных с низкой задержкой и генерирует политику следующим образом: будет выбран самый короткий путь транспортировки, если эти пакеты будут доставлены из хоста A (172.0.0.1) в узел B (172.0.0.2), т. к. путь передачи данных_2 в коричневом (путь_2: хост A -> SDN_Switch_1 -> SDN_Switch_3 -> хост B). В соответствии с форматом записи потока в таблице потоков OpenFlow контроллер заменит прежнюю политику безопасности без обхода более поздней политикой пути. Это нарушает намерение администратора безопасности, и обязательная политика безопасности будет принята [2].

Рис. 1. Обход предопределенной обязательной политики

Другая проблема безопасности заключается в том, что злоумышленник может захватить сервер приложений и вставить мошеннические записи потока, чтобы совершать атаки подслушивания данных [3]. На рис. 2 злоумышленник захватывает сервер приложений для генерации политики следующим образом: пакеты копируются и пересылаются злоумышленнику с IP-адресом 192.0.0.10, если эти пакеты доставляются из хоста A (172.0.0.1) в Host B (172.0.0.2) эта политика преобразуется в запись потока, а затем вставляется в таблицы потоков SDN_Switch_1 через сообщение OFPT_Flow_MOD с контроллера. Таким образом, злоумышленник может легко перехватить пакеты от хоста A до хоста B.

SDN-ориентированная сеть управляется самостоятельно. Важно, чтобы контроллер обнаруживал атаки и автоматически уменьшал их.

Рис. 2. Атаки подслушивания данных путем вставки мошеннических записей потока

В настоящее время протокол OpenFlow как одна из реализаций южного интерфейса SDN поддерживает только обнаружение сканирования заголовка пакета. В коммутаторах потоки пересылаются или удаляются путем сопоставления заголовка пакета с полями соответствия в таблицах потоков OpenFlowTM. Чтобы обнаружить некоторые атаки, такие как информация о червях или троянах, или спаме, и уменьшить их, необходимо выполнить проверку сканирования пакетных данных. Однако текущий протокол OpenFlowTM не поддерживает обнаружение сканирования пакетных данных.

Настоящая статья рассматривает решений безопасности и предлагает комплексную архитектуру безопасности для предоставления специальных служб безопасности (например, правильное соблюдение обязательной сетевой политики, поддержка обнаружения сканирования пакетных данных, надежное получение сетевой политики, точное преобразование сетевой политики в потоковые записи и т. д.) и общие службы безопасности (например, аутентификация, авторизация, конфиденциальность, целостность, программные патчи, доверенные вычисления) [2] для SDN, чтобы можно было решить как общие проблемы безопасности, так и новые проблемы безопасности, как описано выше.

Для обеспечения безопасности предлагаются следующие решения:

1. Схема детализированного именования потока (*Fine-grained naming scheme for the flow entry*): в настоящее время компоненты «поля соответствия» и «приоритет» объединяются для идентификации уникальной записи потока в таблице потоков OpenFlowTM. Таким образом, запись потока в таблице потоков не отличает приложение, генерирующее новую запись потока от другого приложения, генерирующего старую запись потока. Таким образом, сервер приложений может создать новую запись потока, чтобы заменить запись потока, которая отражает обязательную политику, предопределенную администратором безопасности.

Чтобы разработать детализированную схему именования потока, добавятся две новые функции. Одна из них – роль другой создатель политики, другой – уровень привилегий безопасности.

2. Обнаружение сканирования пакетных данных: необходимо обеспечить обнаружение сканирования пакетных данных, чтобы обнаруживать и смягчать некоторые атаки, такие как информация о червях и троянах и спаме. Администратор настраивает политики для случайного обнаружения некоторых пакетов потока, а не всех пакетов потока для повышения производительности. Существует одна возможная схема обнаружения сканирования пакетных данных: выбор первых m последовательных пакетов из каждого потока для обнаружения сканирования пакетных данных. Эта схема может быть сконструирована для всех потоков или только для потоков, удовлетворяющих некоторым условиям, таким как пакеты с определенного IP-адреса источника и / или для определенного адресата.

3. Разрешение сетевого API: чтобы защитить сервер приложений от захвата злоумышленником для вставки мошеннических записей потока для совершения атак, необходимо поддерживать авторизацию сетевого API. Структура авторизации для сетевого API может относиться к IETF OAuth2.0, и ее реализация на основе RESTful API может относиться к OMA Autho4APIv1.0. При реализации авторизации для северных интерфейсов контроллера SDN можно смягчить некоторые атаки, такие как вставка мошеннической записи потока с захваченных серверов приложений и спуфинг контроллера SDN.

В заключение, необходимо отметить, что данные меры предполагают комплексную архитектуру безопасности для SDN. Это также может помочь разработчику реализовать функции безопасности при разработке SDN-контроллеров. Однако, как интегрировать эту архитектуру безопасности в существующие коммерческие сети, такие как сети операторов связи и мобильные сети, не обсуждается. Этот вопрос нуждается в дальнейших исследованиях.

Список используемых источников

1. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности. СПб. : Изд-во СПбГУТ, 2012. 396 с.

2. Дубровин Н. Д., Ушаков И. А., Чечулин А. А. Применение технологии больших данных в системах управления информацией и событиями безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V международной научно-технической и научно методической конференции : сб. науч. ст. 2016. С. 348.

3. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–63.

УДК 004.72
ГРНТИ 49.37.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ МОНИТОРИНГА SDN-СЕТЕЙ

А. В. Красов, И. А. Ушаков, В. А. Федоров

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

В данной статье рассматриваются вопросы мониторинга сетей SDN в целях обеспечения безопасности и повышения отказоустойчивости этих сетей, также дается общее представление о работе SDN. Рассматриваются основные характеристики, принципы работы и некоторые отличительные черты существующих решений для мониторинга SDN, а также приводится сравнительный анализ рассмотренных технологий.

SDN, сети, мониторинг, анализ, безопасность.

Современный бизнес в сфере информационных технологий не стоит на месте. Компьютерные сети в компаниях должны соответствовать многим критериям, таким, как масштабируемость, отказоустойчивость и т. д. В связи с этим на смену классическим сетям приходят так называемые программно-конфигурируемые сети (*Software-Defined Networking*). Программно-конфигурируемые сети (SDN), предусматривают разделение плоскости данных и плоскости управления, делая сетевые коммутаторы в плоскости данных простыми устройствами пересылки пакетов и оставляя логически централизованное программное обеспечение для управления поведением всей сети. SDN предоставляет новые возможности для управления сетью [1].

Технология SDN является достаточно новой, следовательно, в ней еще присутствует ряд существенных недостатков. Важнейшим из них можно назвать высокую уязвимость SDN контроллера. Помимо контроллера подвергнуться атаке могут и остальные узлы сети. Решить проблему безопасности можно с помощью мониторинга каждого узла этой сети. Под мониторингом подразумевается сбор информации со всех узлов сети, а также последующая обработка этой информации с целью анализа состояния устройств в конкретный момент времени. Все это реализуется с помощью технологий «больших данных» (*big data*) – технологии обработки и анализа структурированных и неструктурированных данных больших объемов [2, 3]. Основной целью технологии больших данных в контексте мониторинга

компьютерных сетей является возможность консолидировать и анализировать информацию об инцидентах, собираемую с множества устройств сети. Исходя из этого, в статье будут рассмотрены решения, предназначенные для мониторинга SDN.

Одним из таких методов является использование архитектуры Orchsec. Данная архитектура (рис. 1) направленна на улучшение безопасности сети посредством использования мониторинга и функций управления SDN.

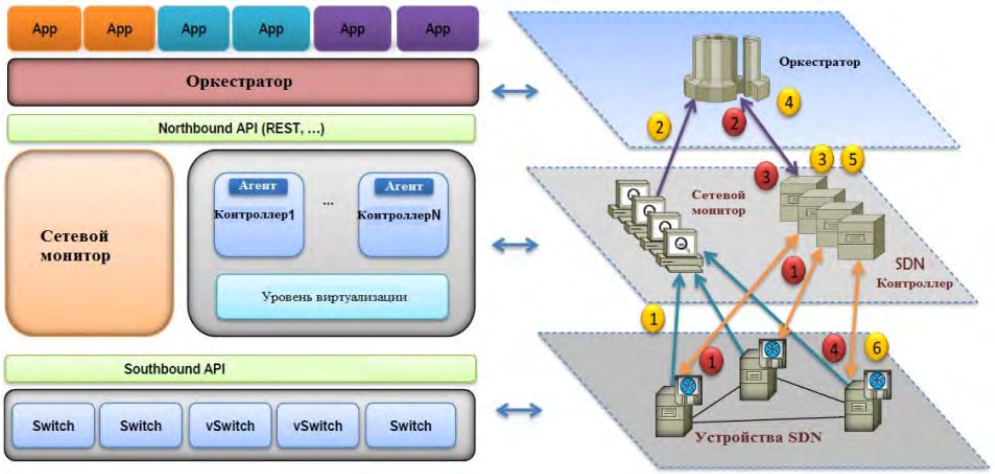


Рис. 1. Архитектура OrchSec

Для понимания принципа работы данной архитектуры следует рассмотреть предназначение каждого элемента, представленного на схеме:

– *Виртуальные / физические коммутаторы*: устройства, которые взаимодействуют с контроллером SDN с помощью протокола OpenFlow.

– *Сетевой монитор*: компонент, который отслеживает сетевой трафик, применяет фильтры трафика, а также инициирует события, соответствующие возникновению заранее определенных ситуаций в сети.

– *Контроллеры*: Компоненты, которые могут общаться с коммутаторами посредством протокола OpenFlow.

– *Оркестратор*: Наиболее важный компонент архитектуры, содержащий в себе приложения, разработанные для безопасности сети. Оркестратор связывается с сетевым монитором для получения информации о важных событиях, произошедших в сети, и ее состоянии на данный момент времени. Проанализировав полученную информацию, оркестратор принимает решение, которое в последующем пересылает контроллеру для настройки работы сети по определенному шаблону. После перенастройки работы сети информация о ее состоянии перенаправляется обратно в оркестратор для дальнейшей проверки. Связь между контроллерами и оркестратором обеспечивается посредством приложений, установленных на каждом контроллере, называемых Orchestrator Agent [4].

Далее рассмотрим инструмент под названием SOFTmon. Данный инструмент представляет собой способ мониторинга потока с использованием Northbound интерфейса NOS (*Network Operation System*). Ключевой идеей SOFTmon является внедрение независимого инструмента мониторинга трафика, который добавляет дополнительные возможности мониторинга, а также визуализирует полученные данные.

Концептуальная архитектура самого SOFTmon (рис. 2) основана на шаблоне многоуровневой программной архитектуры. Нижний слой является уровнем доступа к данным и включает базу данных, файловый ввод-вывод и поддерживает передачу состояния (REST). Этот слой обеспечивает основную функциональность, требуемую для связи с NOS (программным обеспечением контроллера). Далее следует слой, включающий в себя модель данных. Модель данных вычисляет метрики производительности при помощи статистических данных, собираемых с NOS. Сама модель данных состоит из трех основных элементов. В первую очередь, это – топология, включающая в себя все сетевые устройства, а также соединения между ними. Следующим элементом являются так называемые счетчики, содержащие в себе собираемые статистические данные. Последний элемент – метрики [5]. Они необходимы для визуализации производительности сети. Именно визуализации является отличительной особенностью представленного решения. Верхний слой содержит графический интерфейс, предназначенный для взаимодействия с пользователем. Он включает в себя вкладки с различными опциями измерений и диаграммами для графического представления показателей производительности в режиме реального времени.

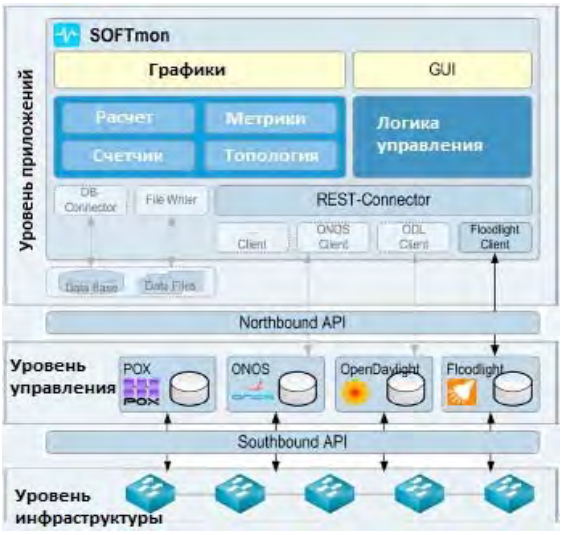


Рис. 2. Архитектура SOFTMon

Следующим рассматриваемым решением будет комбинирование sFlow и OpenFlow протоколов. В данном случае протокол sFlow расширяет возможности OpenFlow [6], а также дает некоторые преимущества:

– улучшение масштабируемости сети;

– снижение требуемой связи между коммутаторами и контроллером, тем самым предотвращение перегрузки в плоскости управления.

Архитектура предлагаемого решения (рис. 3).

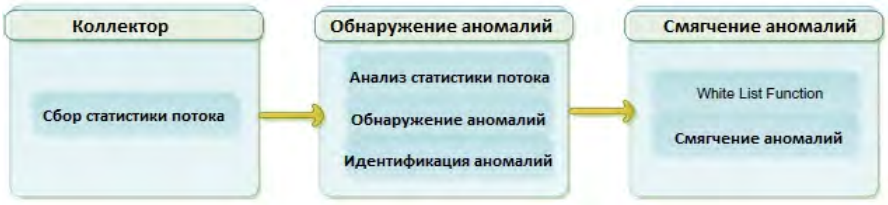


Рис. 3. Архитектура рассматриваемой системы

Принципы проектирования данной архитектуры основаны на следующих ключевых свойствах:

– Модульная конструкция:

Первый модуль отвечает за мониторинг сети на основе сбора информации с потока данных. Собранные данные обрабатываются во втором модуле, который отвечает за обнаружение и идентификацию различных атак. Третий модуль отвечает за принятие решений по предотвращению атак (минимизации их последствий).

– Совместимость с любыми OpenFlow-устройствами.

– Использование плоскости данных и плоскости управления для быстрого обнаружения атак в режиме реального времени.

– Использование методов выборочного контроля пакетов.

Принципы проектирования данной архитектуры основаны на следующих ключевых свойствах:

– Модульная конструкция:

Первый модуль отвечает за мониторинг сети на основе сбора информации с потока данных. Собранные данные обрабатываются во втором модуле, который отвечает за обнаружение и идентификацию различных атак. Третий модуль отвечает за принятие решений по предотвращению атак (минимизации их последствий).

– Совместимость с любыми OpenFlow-устройствами.

– Использование плоскости данных и плоскости управления для быстрого обнаружения атак в режиме реального времени.

– Использование методов выборочного контроля пакетов.

Архитектура SDN существенно изменяет структуру сети, следовательно, появляются новые угрозы безопасности, вызванные уязвимостями отдельных компонентов инфраструктуры. В связи с этим, были рассмотрены решения, обеспечивающие безопасность SDN. Выбор конкретного метода зависит от его характеристик (табл., см. ниже), а также от возможностей компании. Например, для обеспечения максимальной продуктивности при работе SOFTmon требуется наличие квалифицированного сотрудника, который будет принимать решение на основе полученной информации. Также данный метод подходит для небольших сетей, в то время как работу с масштабными сетями следует доверить специализированным приложениям, входящим в состав Orchsec. Для сетей с большим количеством

устройств также важно не допустить управляющему трафику перегружать сеть. [7, 8] Эту задачу решает метод комбинирования SFlow и OpenFlow протоколов.

ТАБЛИЦА. Сравнительные характеристики рассмотренных решений

Рассматриваемое решение	Основные особенности	Обеспечение безопасности сети	Способ интеграции в сеть SDN
Orchsec	Управление сетью осуществляется контроллером, в то время как самим контроллером управляет Orchestrator	Приложения для обеспечения безопасности сети, входят в отдельный компонент – Orchestrator	Осуществляется посредством приложений Orchestrator Agent, установленных на каждом контроллере
SOFTmon	Возможность визуализации статистики для последующего анализа	Является дополнительной утилитой, предоставляющей информацию для анализа сети. Предотвращение атак производится пользователем	Является отдельной утилитой, производящей сбор информации посредством связи с NOS (программным обеспечением контроллера)
Комбинирование SFlow и OpenFlow протоколов	Разгрузка плоскости управления, посредством сокращения кол-ва сообщений, передаваемых между устройствами	Для предотвращения атак (минимизации их последствий) служат специализированные приложения	Связь с сетью осуществляется посредством протокола OpenFlow

Список используемых источников

1. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. Т. 4. № 2. С. 53–56.

2. Котенко И. В., Ушаков И. А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23–33.

3. Котенко И. В., Кулешов А. А., Ушаков И. А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack // Труды СПИИРАН. 2017. № 5 (54). С. 5–34.

4. Adel Zaalouk, Rahamatullah Khondoker, Ronald Marx, Kpatcha Bayarou OrchSec Demo: Demonstrating the Capability of an Orchtestrator-based Architecture for Network Security [Электронный ресурс] // Open Networking Summit ONS: materials of scientific conference, At Santa Clara, March 2014. URL: https://www.researchgate.net/profile/Rahamatullah_Khondoker/publication/293174620_OrchSec_Demo_Demonstrating_the_Capability_of_an_Orchtestrator-based_Architecture_for_Network_Security.pdf (дата обращения 19.12.2018).

5. Marc Hartung, Marc Körner. SOFTmon – Traffic Monitoring for SDN // Procedia Computer Science. 2017. № 110. PP. 516–523.

6. Альшаев И. А., Красов А. В., Ушаков И. А. Исследование принципов работы протокола OpenFlow в программно-конфигурируемых сетях // Труды учебных заведений. 2017. Т. 3. № 2. С. 16–27.

7. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передач данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141–146.

8. Исаченков П. А., Красов А. В., Левин М. В. Исследование эффективности метода управления потоками трафика на основе информации о нагрузке в программно-определяемой сети с неравными метриками маршрутов // Современная наука и инновации. 2017. № 2 (18). С. 32–38.

УДК 004.72
ГРНТИ 49.37.29

АНАЛИЗ УЯЗВИМОСТЕЙ И РЕЛЕВАНТНЫХ РЕШЕНИЙ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ SDN-СЕТЕЙ

А. В. Красов, И. А. Ушаков, Д. И. Щипцов

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

Программно-определяемая сеть или программно-конфигурируемая сеть – это новый подход к построению сетей передачи данных в которой уровень управления сетью отделён от устройств передачи данных и реализуется программно. В статье приведен небольшой обзор проблем безопасности SDN и их решений.

защита информации, SDN, протокол OpenFlow, программно-конфигурируемые сети, информационная безопасность.

Введение

В SDN (*software-defined networking*) логически централизованная плоскость управления контролирует всю сеть и принимает решения о переадресации пакетов для коммутаторов, то есть плоскости передачи данных, внутри сети. Эти особенности повышают эффективность сетевого оборудования и снижают затраты на эксплуатацию сетей.

Архитектура SDN

Функционирование SDN представляется в виде трехуровневой модели, предоставленной Open Networking Foundation – некоммерческой организации развития SDN, в которую входят Cisco, Huawei, Juniper, Google, Microsoft, Oracle, Dell и многие другие компании.

Архитектура SDN имеют следующую структуру (рис.):

– уровень передачи (уровень инфраструктуры);
– уровень управления (уровень контроля);
– уровень приложений.

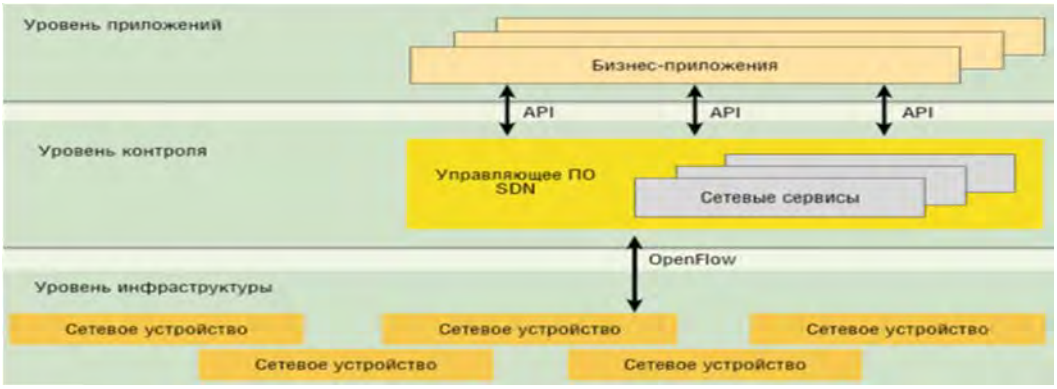


Рисунок. Архитектура SDN

Работа между сетевым контроллером и передающими устройствами осуществляется с помощью специального программного интерфейса, который используется для прямого управления устройствами. Самым распространенным интерфейсом в наше время является протокол OpenFlow [1].

Уязвимости в SDN

В этом разделе анализируются уязвимости SDN на основе его архитектуры и конкретных особенностей.

Есть две наиболее очевидные особенности SDN. Первая – это централизация контроля сети. Вторая – это программируемые контроллеры. Эти две функции существенно упрощают управление сетью по сравнению с традиционными сетями. Однако из-за этих особенностей эта новая сетевая парадигма становится праздником для злоумышленников. Для проведения анализа безопасности разделим уязвимости на 7 основных категорий [2].

1. *Несанкционированный доступ*. Одна из оригинальных особенностей SDN описана как логически централизованное управление. Поэтому в функциональной архитектуре SDN несколько контроллеров могут осуществлять доступ к плоскости данных сети. Также, приложения из нескольких источников (сторонние приложения) могут связываться с пулом контроллеров. Контроллер обеспечивает абстракцию для приложений, так что приложения

могут читать или записывать состояние сети, что фактически является уровнем управления сетью. Если злоумышленник выдал себя за контроллер или приложение, он может получить доступ к сетевым ресурсам и манипулировать работой сети.

2. *Утечка данных*. Существует множество потенциальных действий, описанных в спецификации коммутатора OpenFlow для обработки пакетов [3]. Злоумышленник может определить действие, примененное к конкретным типам пакетов, с помощью анализа времени обработки пакетов. Обнаружив тип пакета, который перенаправляется на контроллер, злоумышленник может генерировать поток поддельных запросов, ведущих к атаке типа «отказ в обслуживании» (DoS). Связь между этим типом утечки данных и DoS-атакой иллюстрируется в [4].

3. *Изменение данных*. Контроллер имеет возможность программировать сетевые устройства для управления потоком трафика в SDN [5]. Если злоумышленник сможет захватить контроллер, он будет фактически контролировать всю систему. Из этой привилегированной позиции злоумышленник может вставлять или изменять правила потока в сетевых устройствах, что позволит управлять пакетами внутри сети в интересах злоумышленника.

4. *Вредоносные/скомпрометированные приложения.* Учитывая, что контроллер выступает в качестве абстракции от плоскости данных для приложений, и что SDN позволяет интегрировать сторонние приложения в архитектуру, вредоносное или неправильно спроектированное приложение может оказать столь же пагубный эффект в сети, как скомпрометированный контроллер.

5. *Отказ в обслуживании (DoS) и распределённая атака типа «отказ в обслуживании» (DDoS).* Одним из самых больших недостатков безопасности в SDN являются атаки DoS/DDoS. По сравнению с традиционными сетями этот вид атак в SDN еще хуже из-за логически централизованного управления. Механизм реактивного кэширования делает коммутаторы и контроллеры уязвимыми для атаки DoS. Злоумышленник может загрузить коммутатор большим числом пакетов. Все это может значительно увеличить вычислительную нагрузку на контроллер или даже прервать его работу [6].

6. *Проблемы с конфигурацией.* Политики и протоколы безопасности сети постоянно совершенствуются и разрабатываются по мере обнаружения уязвимостей сети. Многие из них будут применяться к уровням и интерфейсам инфраструктуры SDN. Тем не менее, от таких политик будет мало пользы, если они реализованы или отключены без понимания последствий для безопасности развертывания сети. Также открытие интерфейсов между сетевыми компонентами может привести к значительным уязвимостям.

7. *Безопасность системного уровня SDN.* На системном уровне в SDN также существует ряд проблем безопасности. Основной проблемой является удовлетворение процесса контроля. С точки зрения работы сети крайне важно иметь возможность обеспечить контролируемый перечень сетевых устройств. Это включает знание того, какие устройства работают, как они связаны с сетью и т. д.

Решения для уязвимостей

Были определены семь категорий проблем безопасности. В процессе категоризации решений, представленных в литературе, установлено, что решения предлагаются только в 5 из 7 категорий. На сегодняшний день не предложены решения проблем утечки данных и изменения данных. В таблице представлена классификация уязвимостей SDN, исследовательские работы и предложенные решения в этих областях.

ТАБЛИЦА. Анализ релевантных решений в области безопасности SDN-сетей

Проблема безопасности	Исследование	Предложенное решение
Несанкционированный доступ	Authentication for Resilience [7]	Иерархическая система контроллеров/ коммутаторов для уменьшения точек отказа
	AuthFlow [8]	Механизм аутентификации и контроля доступа на основе учетных данных хоста
Вредоносные приложения	FortNOX [9]	Ядро обеспечения безопасности для определения приоритетов правил потока с авторизацией на основе ролей
	ROSEMARY [10]	Контроллер, реализующий стратегию сдерживания и устойчивости сетевого приложения
Отказ в обслуживании (DoS)	CPRecovery [11]	Компонент CPRecovery обеспечивает целостное резервное копирование основного контроллера
	VAVE [12]	Контроллер NOX позволяет глобально определить правила проверки адресов
Проблемы с конфигурацией	NetPlumber [13]	Инкрементные вычисления для проверки обновлений политики в режиме реального времени
	LPM [14]	Многоуровневая структура управления политиками (разрешить зависимости между модулями, приложениями и внутри таблиц)
Безопасность системного уровня SDN	FRESCO [15]	Структура разработки приложений для служб безопасности
	Debugger for SDN [16]	Прототип сетевого отладчика для SDN

Список используемых источников

1. Красов А. В., Левин М. В., Цветков А. Ю. Метод управления трафиком в гибридной программно-определяемой сети // Информационные технологии и телекоммуникации. 2016. № 2. С. 53–56.

2. Scott-Hayward, S., Natarajan, S., & Sezer, S. A Survey of Security in Software Defined Networks. IEEE Communications Surveys and Tutorials, 2016. 18 (1), pp. 623–654.

3. Красов А. В., Левин М. В., Цветков А. Ю. Управление сетями передач данных с изменяющейся нагрузкой // Всероссийская научная конференция по проблемам управления в технических системах. 2015. № 1. С. 141–146.

4. S. Shin and G. Gu, “Attacking Software-Defined Networks: The First Feasibility Study” // In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 165–166.

5. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Методология управления потоками трафика в программно-определяемой адаптивной сети // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 4. С. 3–8.

6. Zhen Yao and Zheng Yan. “Security in Software-Defined-Networking: A Survey” // Security, Privacy, and Anonymity in Computation, Communication, and Storage 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16–18, Proceedings, pp. 319–332.

7. D. Yu, A. W. Moore, C. Hall, and R. Anderson, Authentication for Resilience: The Case of SDN // Ser. Security Protocols XXI. Springer, 2013, pp. 39–44.

8. D. M. F. Mattos, L. H. G. Ferraz, and O. C. M. B. Duarte, “AuthFlow: Authentication and Access Control Mechanism for Software Defined Networking” // Annals of Telecommunications 2016, Volume 71, Issue 11–12, pp 607–615.

9. P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu. A security enforcement kernel for OpenFlow networks // in Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, pp. 121–126.

10. S. Shin, Y. Song, T. Lee, S. Lee, J. Chung, P. Porras, V. Yegneswaran, J. Noh, and B. B. Kang, “Rosemary: A Robust, Secure, and HighPerformance Network Operating System // in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2014, pp. 78–89.

11. P. Fonseca, R. Bennesby, E. Mota, and A. Passito. A replication component for resilient OpenFlow-based networking // in Network Operations and Management Symposium (NOMS), 2012 IEEE. IEEE, 2012, pp. 933–939.

12. G. Yao, J. Bi, and P. Xiao. Source address validation solution with OpenFlow/NOX architecture // in 19th IEEE International Conference on Network Protocols (ICNP). IEEE, 2011, pp. 7–12.

13. P. Kazemian, M. Chang, H. Zeng, G. Varghese, N. McKeown, and S. Whyte. Real time network policy checking using header space analysis // in USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2013, pp. 99–111.

14. W. Han, H. Hu, and G.-J. Ahn. LPM: Layered Policy Management for Software-Defined Networks // Ser. Data and Applications Security and Privacy XXVIII. Springer, 2014, pp. 356–363.

15. S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyso. FRESCO: Modular composable security services for software-defined networks // in Proceedings of Network and Distributed Security Symposium, 2013.

16. N. Handigol, B. Heller, V. Jeyakumar, D. Mazieres, and N. McKeown. Where is the debugger for my software-defined network? // in Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, pp. 55–60.

УДК 519.852.33
ГРНТИ 27.41.77

ТИПЫ КРОССОВЕРОВ ДЛЯ ПОИСКА ОПТИМАЛЬНЫХ МАРШРУТОВ ДОСТАВКИ СООБЩЕНИЙ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ С ПОМОЩЬЮ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ПО МОДЕЛИ УИТЛИ

А. К. Краубнер, В. А. Мешалкин

Военная Академия Связи имени Маршала Советского Союза С. М. Буденного

Рассматривается проблема выполнения требований по своевременности доставки сообщений документальной электросвязи. Сложность построения маршрута определяется количеством получателей (источников) и их пространственным распределением. Из множества задач дискретной оптимизации, наиболее подходящей является задача коммивояжера. Для решения было предложено использовать модель Уитли генетического алгоритма. Целью работы является исследование и подбор наиболее подходящих типов кроссоверов для решения задачи коммивояжера по модели Уитли генетического алгоритма. В статье описаны наиболее подходящие типы кроссоверов для решения задачи коммивояжера с помощью генетических алгоритмов по модели Уитли. Приведены результаты испытаний и сравнительный анализ эффективности предложенных кроссоверов.

генетические алгоритмы, модель Уитли, кроссовер, генетический оператор, документальная электросвязь, задача коммивояжера, беспилотные летательные аппараты, тактическое звено управления.

Задача коммивояжера – одна из самых известных оптимизационных задач, заключающаяся в поиске кратчайшего маршрута, проходящего через конечное количество городов по одному разу. Поиск решения данной задачи необходим во многих областях промышленности и народного хозяйства, таких как комплексы многооперационной обработки, конвейерное производство, железнодорожные и судовые погрузочные системы, а так – же при формировании маршрутов доставки сообщений документальной электросвязи с применением беспилотных летательных аппаратов. Проще

всего представить задачу коммивояжера в виде модели на графе. Маршрут должен включать посещение каждой вершины, только один раз. Иначе говоря, цель задачи коммивояжера заключается в отыскании во взвешенном графе гамильтонова цикла с минимальным весом [1, 2, 3]. Задача относится к классу сложных NP-полных задач.

Целью данной работы является исследование и подбор наиболее подходящих типов кроссоверов для решения решения задачи коммивояжера по модели Уитли генетического алгоритма.

Модель Уитли не имеет строгих требований к типу используемых генетических операторов, таких как кроссоверы и мутации, однако задача коммивояжера накладывает определенные ограничения, ввиду того что каждая вершина должна быть посещена, при этом только один раз.

$$\sum_{i=1}^{N} X_{i,j} \ = 1, i = 1..N.$$

где: $X_{i,j}$ – матрица переходов с компонентами, N – число городов.

Следующие виды кроссоверов были выбраны как наиболее подходящие: циклический кроссовер, одноточечный кроссовер, двухточечный кроссовер.

Циклический кроссовер. В этом виде кроссовера города попадают к потомку поочередно, циклически, от каждого родителя. Первый город от первого родителя, второй от второго, и так далее. Если очередная родительская вершина уже заняла позицию в новой особи, то вместо него отправляется следующая неиспользованная вершина.

Нужно отметить, что гены у родителей должны браться у одной из родительских особей в нормальном порядке, а в другой в обратном, так как показано на рис. 1. Это решение помогает сохранить большее количество родительских связей между вершинами.

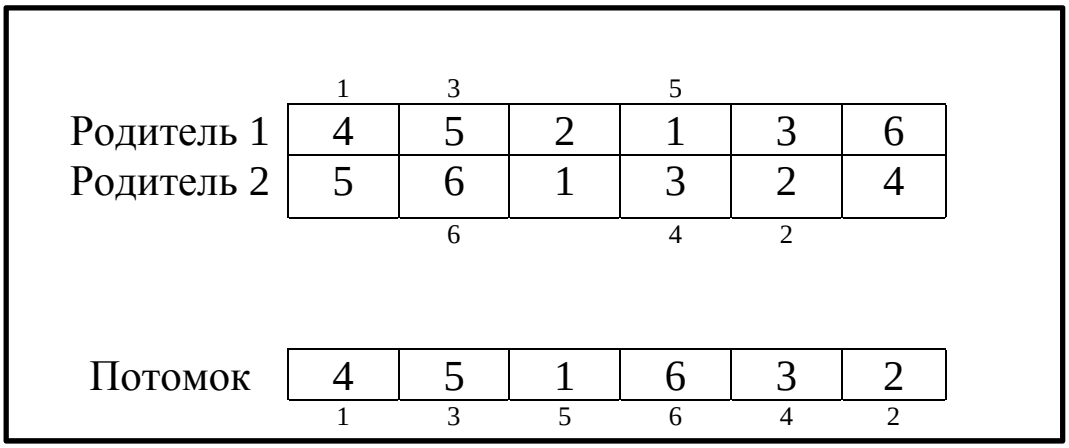


Рис. 1. Циклический кроссовер

Одноточечный кроссовер. Одноточечный кроссовер считается классическим для многих моделей ГА. В начале необходимо выбрать так называемую точку сдвига. Она выбирается случайно, и располагается между двумя соседними генами. Из первого родителя в наследующую без изменений особь попадают все города от начала до точки сдвига. Из второй особи от точки сдвига и до последнего гена попадают все города, которые еще не были задействованы в формировании потомка. Если после этих операций в дочерней особе остаются пустые гены, то их необходимо заполнить оставшимися городами из второго родителя.

Пример одноточечного кроссовера на рис. 2. Так как от второго родителя из нужной половины хромосомы «новым», оказался всего один город, то остальные берутся первой половины хромосомы.

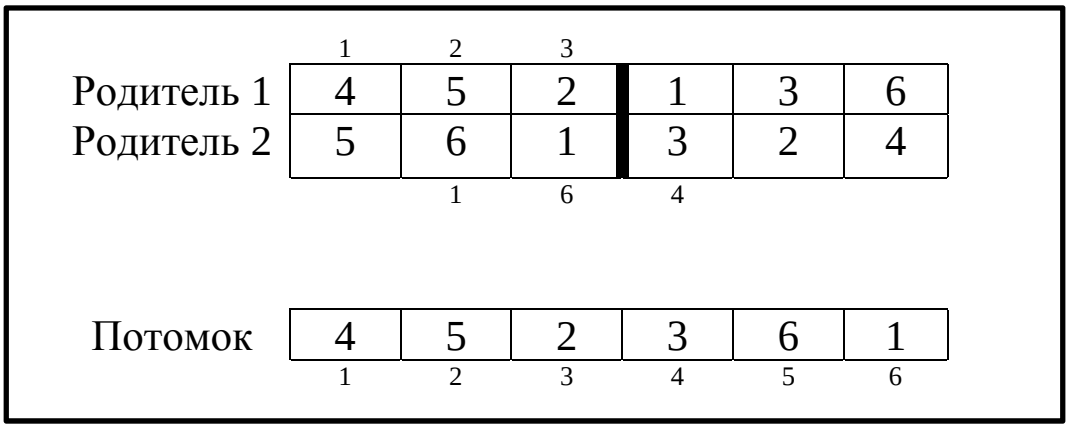


Рис. 2. Одноточечный кроссовер

Двухточечный кроссовер. Основным отличием двухточечного кроссовера от одноточечного является наличие второй точки сдвига. Города, которые находятся между точками из первой особи, без изменений переходят в дочернюю особь. Аналогично, из противоположных частей второй особи гены переписываются в потомка, приоритет при переносе получают города, которые сохранят свой локус при переносе, как представлено на рис. 3 (см. ниже).

В рамках исследования выбранных кроссоверов были произведены тестовые запуски генетического алгоритма по модели Уитли для решения задачи коммивояжера с использованием только кроссоверов без мутаций. Поиск кратчайшего маршрута осуществлялся на графе с 11 вершинами. Решение, полученное точным методом полного, составляет 191. Средние результаты качества финального поколения за 100 запусков алгоритма с идентичными параметрами представлены на рис. 4, время работы показано на рис. 5.

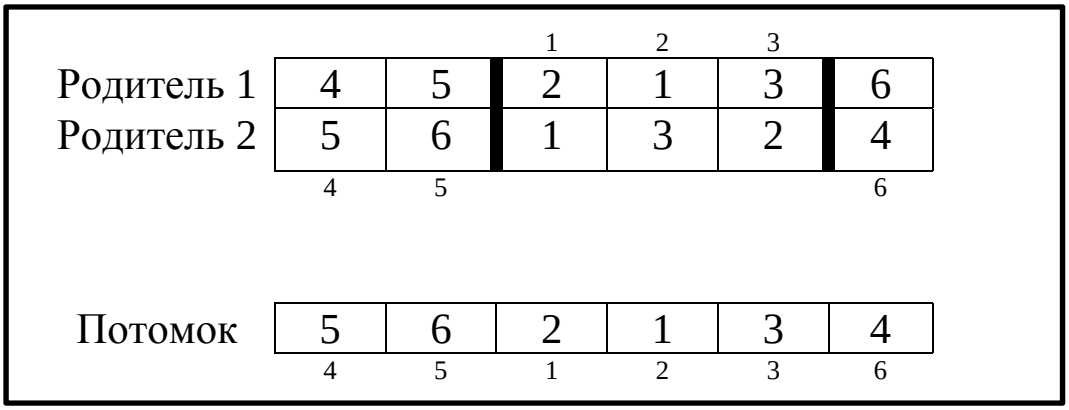


Рис. 3. Двухточечный кроссовер

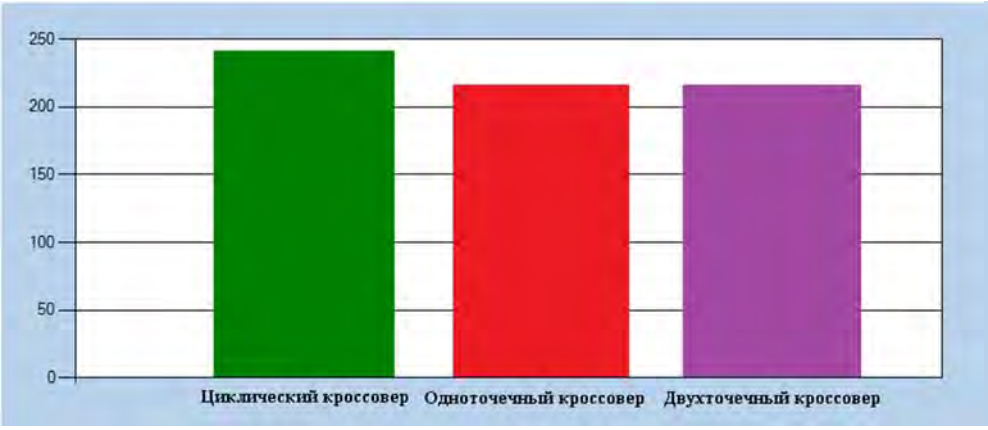


Рис. 4. Качество полученных решений

Рис. 5. Время работы

На основе проведенных испытаний можно сделать вывод о том, что все отобранные кроссоверы пригодны для использования в генетическом алгоритме по модели Уитли для решения задачи коммивояжера. Наиболее эффективным кроссовером без применения мутаций является циклический кроссовер, он же демонстрирует наилучшее время ввиду алгоритмической простоты в сравнении с остальными представленными типами кроссоверов.

Список используемых источников

1. Дасгупта С., Пападимитриу Х., Вазарани У. Алгоритмы, пер. с англ. / Под ред. А. Шеня. М. : МЦНМО, 2014. 320 с.
2. Ерзин, А. И., Кочетов Ю. А. Задачи маршрутизации. Новосиб. гос. ун-т. Новосибирск : РИЦ НГУ, 2014. 95 с.
3. Емельянов В. В., Курейчик В. В., Курейчик В. М. Теория и практика эволюционного моделирования. М. : ФИЗМАЛИТ, 2003. 432 с.

УДК 621.39
ГРНТИ 49.13

ОПТИЧЕСКИЙ УСИЛИТЕЛЬ EDFA КАК ШИРОКОПОЛОСНЫЙ ИСТОЧНИК ИЗЛУЧЕНИЯ. ЧАСТЬ 1

В. С. Кузнецов, М. В. Маляров

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

В данной работе рассматривается возможность получения широкого и равномерного спектра, обладающим высоким уровнем мощности, на основе усилителя на оптическом волокне, легированном ионами эрбия. Источники усиленной спонтанной эмиссии обладают рядом преимуществ и могут быть использованы во многих областях науки и техники. В моделирующей программе проведено исследование зависимости ширины, равномерности и мощности спектра излучения от таких параметров оптического усилителя, как тип и длина активного волокна, параметр насыщенности, уровень мощности и количество источников излучения накачки.

EDFA, спектральный диапазон, усиленная спонтанная эмиссия.

Источники излучения, обладающие довольно высокой и стабильной выходной мощностью, в качестве которой используется усиленное спонтанное излучение (ASE), могут быть актуальны для различных лабораторных работ, в качестве измерений пассивных компонентов систем плотного спектрального мультиплексирования.

Данная работа подразумевает моделирование в программной среде GainMaster [1] с использованием эрбиевых оптических волокон (ЭОВ) серии IsoGain I-4, I-6, I-25. Изменяя такие параметры оптического усилителя, как способ подключения сигнала накачки, уровень ее мощности и длина эрбиевого волокна, были смоделированы различные варианты широкополосных источников.

Прежде всего необходимо определить способ подключения и количество источников накачки. Для этого были смоделированы схемы (рис. 1) оптического усилителя с попутным, встречным и двунаправленным подключениями.

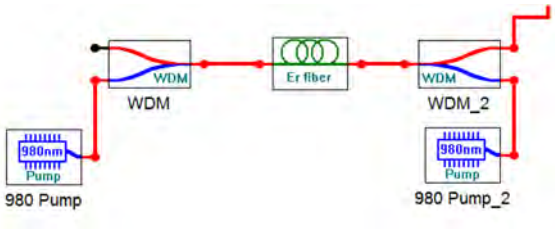


Рис. 1. Общая структурная схема EDFA

Исследование проводилось для различных конфигураций оптического усилителя. Изменение уровня мощности сигнала накачки происходило от 12 до 21 дБм, изменение длины волокна от 3 до 21 метра. Задачей моделирования являлось определение оптимальных параметров усилителя, при которых достигается широкополосный источник с высоким уровнем выходной мощности.

В таблице 1 представлены выборочные результаты моделирования для попутной схемы подключения источника накачки для волокна I-4.

ТАБЛИЦА 1. Моделирование ЭОВ с I-4 с попутным включением

p_p, дБм	$l_{ЭОВ}$, м	λ_{max}, нм	p_Σ, дБм	p_{1550}, дБм/нм	$S \leq 1$ дБ, нм	$S \leq 5$ дБ, нм
12	3	1530,20	−15,98	−34,51	39,39	57,57
	12	1530,20	2,44	−16,14	35,35	43,43
	18	1531,21	−1,03	−17,04	20,20	41,41
	21	1558,48	−4,01	−19,69	20,20	41,41
15	3	1530,20	−15,4	−34,02	39,39	56,56
	12	1530,20	6,77	−12,99	34,34	42,42
	18	1531,21	5,02	−11,83	35,35	42,42
	21	1531,21	3,63	−12,25	19,19	41,41
18	3	1530,20	−15,11	−33,77	38,38	55,55
	12	1530,20	10,16	−10,61	35,35	41,41
	18	1531,21	9,18	−8,55	35,35	40,40
	21	1531,21	8,2	−8,3	34,34	40,40
21	3	1530,20	−14,96	−33,65	38,38	55,55
	12	1530,20	13,08	−8,63	34,34	42,42
	18	1531,21	12,69	−5,94	34,34	40,40
	21	1531,21	11,89	−5,33	20,20	40,40

Из таблицы 1 видно, что с увеличением длины волокна ($l_{ЭОВ}$) увеличивается суммарный выходной уровень мощности (p_{Σ}), но уменьшается ширина полосы источника (S). Ширина полосы рассчитывалась относительно уровня мощности на длине волны 1550 нм с отклонением от этого уровня не более 1 и не более 5 дБ.

При одинаковой длине волокна чем выше уровень мощности накачки (p_p), тем выше выходной уровень мощности. Поэтому в зависимости от изначальных требований к устройству необходимо подбирать оптимальные параметры.

На рис. 2 приведен пример спектрограммы усиленной спонтанной эмиссии, полученной при попутном включении накачки с уровнем мощности 12 дБм; длина эрбиевого волокна 21 метров. В этом случае стоит отметить, что с увеличением длины эрбиевого волокна спектр эмиссии смещается в длинноволновую область [2]. Для получения более ровного спектра необходимо использовать оптимизирующие фильтры.

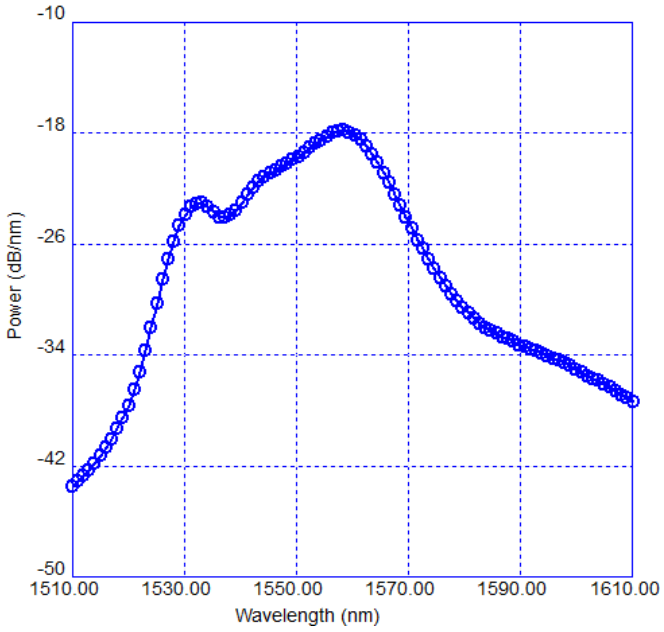


Рис. 2. Пример спектрограммы ASE с ЭОВ I-4

При исследовании со встречным подключением источника накачки (табл. 2) необходимо отметить, что с увеличением длины активного волокна максимальный спектр эмиссии остается на длине волны 1530 нм. Спектр на выходе остается стабильным при изменении параметров усилителя, а выходная мощность по сравнению с попутным включением возрастает.

ТАБЛИЦА 2. Моделирование ЭОВ с I-4 со встречным включением

p_p, дБм	$l_{ЭОВ}$, м	λ_{max}, нм	p_Σ, дБм	p_{1550}, дБм/нм	$S \leq 1$ дБ, нм	$S \leq 5$ дБ, нм
12	3	1530,20	−15,97	−34,5	39,39	57,57
	12	1530,20	4,73	−14,62	35,35	42,42
	18	1531,21	5,85	−12,05	35,35	42,42
	21	1531,21	5,95	−11,63	36,36	43,43
15	3	1530,20	−15,4	−34,02	39,39	56,56
	12	1530,20	8,43	−11,94	35,35	43,43
	18	1531,21	9,96	−8,56	35,35	41,41
	21	1531,21	10,19	−7,62	35,35	42,42
18	3	1530,20	−15,11	−33,77	38,38	55,55
	12	1530,20	11,45	−9,83	34,34	42,42
	18	1531,21	13,32	−5,96	35,35	41,41
	21	1531,21	13,65	−4,74	35,35	41,41
21	3	1530,20	−14,96	−33,7	39,39	55,55
	12	1530,20	14,07	−8,04	34,34	40,40
	18	1530,20	16,28	−3,8	35,35	40,40
	21	1531,21	16,7	−2,37	34,34	41,41

Для наглядности сравним полученные результаты на примере (рис. 3). Видно, что при одних и тех же параметрах выходной уровень мощности при встречном включении накачки выше.

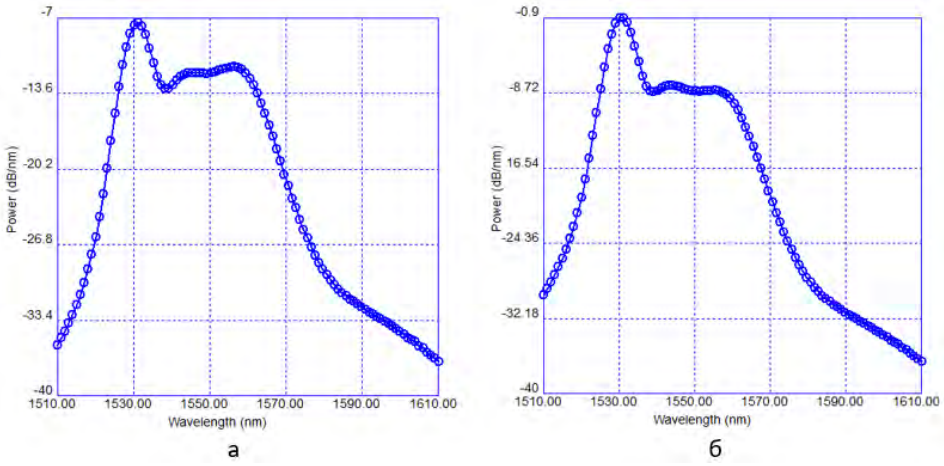


Рис. 3. Пример спектрограмм ASE с ЭОВ I-4 с попутным (а) и встречным (б) включением накачки. Уровень мощности накачки 15 дБм, длина эрбиевого волокна 18м

Включение двух источников накачки позволяет добиться увеличения выходной мощности, однако сильного влияния на ширину спектра это не оказывает. Поэтому было принято решение оставить схему со встречным источником как наиболее эффективную.

Эрбиевое волокно I-6 имеет несколько больший параметр насыщенности ($3{,}881 \cdot 10^{15}$ 1/м·с) по сравнению с волокном I-4 ($3{,}091 \cdot 10^{15}$ 1/м·с), поэтому снижение темпа увеличения выходной мощности достигается уже при 12–15 метрах (табл. 3).

ТАБЛИЦА 3. Моделирование ЭОВ с I-6 со встречным включением

p_p, дБм	$l_{ЭОВ}$, м	λ_{max}, нм	p_Σ, дБм	p_{1550}, дБм/нм	$S \leq 1$ дБ, нм	$S \leq 5$ дБ, нм
12	3	1530,20	−12,3	−30,88	37,37	51,51
	12	1531,21	5,66	−12,22	35,35	42,42
	15	1531,21	5,98	−11,25	36,36	43,43
	21	1531,21	6,07	−10,95	36,36	42,42
15	3	1530,20	−11,48	−30,21	37,37	51,51
	12	1531,21	9,59	−9,06	36,36	41,41
	15	1531,21	10,1	−7,5	21,21	41,41
	21	1531,21	10,41	−6,25	20,20	42,42
18	3	1530,20	−11,06	−29,87	37,37	51,71
	12	1531,21	12,84	−6,61	35,35	41,41
	15	1531,21	13,49	−4,7	35,35	41,41
	21	1531,21	13,97	−2,72	20,20	40,40
21	3	1530,20	−10,85	−29,7	37,37	50,50
	12	1531,21	15,7	−4,54	34,34	41,41
	15	1531,21	16,5	−2,36	34,34	41,41
	21	1531,21	17,15	0,2	19,19	40,40

Активное волокно I-25 обладает еще большим параметром насыщенности ($1{,}605 \cdot 10^{16}$ 1/м·с), поэтому оптимальные длины активного волокна составляют 3–4 метра (табл. 4).

ТАБЛИЦА 4. Моделирование ЭОВ с I-25 со встречным включением

p_p, дБм	$l_{ЭОВ}$, м	λ_{max}, нм	p_Σ, дБм	p_{1550}, дБм/нм	$S \leq 1$ дБ, нм	$S \leq 5$ дБ, нм
12	1	1530,20	−5,5	−24,15	36,36	46,46
	3	1530,20	5,62	−11,4	36,36	42.42
	4	1530,20	5,92	−10,7	21,21	43,43
15	1	1530,20	−3,93	−22,89	36,36	46,46
	3	1530,20	9,51	−7,95	21,21	41,41
	4	1530,20	10,05	−6,51	20,20	41,41
18	1	1530,20	−3,04	−22,18	37,37	45,45
	3	1530,20	12,77	−5,22	33,33	42,42
	4	1530,20	13,49	−3,29	20,20	42,42
21	1	1530,20	−2,55	−21,79	37,37	45,45
	3	1530,20	15,76	−2,84	35,35	41,41
	4	1530,20	16,53	−0,59	20,20	41,41

Сравним результаты моделирования при наибольших уровнях мощности источников накачки (табл. 5). При мощности 18 дБм волокно I-6 позволяет получить более высокие мощности на длинах волн вблизи 1550 нм. Волокно I-25 в данном случае наименее эффективно, так как ширина спектра источника наименьшая.

При этом, если еще больше увеличить мощность накачки и уменьшить длину волокна I-25, оно становится наиболее эффективным по ширине, но выходной уровень наибольший при использовании волокна I-6.

ТАБЛИЦА 5. Сравнение результатов моделирования

Тип ЭОВ	$l_{ЭОВ}$, м	p_p, дБм	p_Σ, дБм	p_{1550}, дБм/нм	$S \leq 1$ дБ, нм
I-4	18	18	13,31	−5,96	35,35
I-6	15	18	13,48	−4,69	35,35
I-25	4	18	13,49	−3,29	20,20
I-4	21	21	16,7	−2,37	34,34
I-6	21	21	17,14	0,19	19,19
I-25	3	21	15,76	−2,83	35,35

Таким образом, было проведено моделирование оптических усилителей EDFA, усиленную спонтанную эмиссию которых можно использовать в качестве широкополосного источника.

Список используемых источников

1. GAINMASTER^{TM} Amplifier Designed Software Manual Revision1. – Fibercore Limited, 2016. 16 с.

2. Курков А. С., Наний О. Е. Эрбиевые волоконно-оптические усилители // Ligtwave – russian edition. № 1, 2003. – 21 p.

Статья предоставлена заведующим кафедрой СПбГУТ, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 004.056.5
ГРНТИ 81.93.29

ОБЗОР СОСТОЯНИЯ ИССЛЕДОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИМЕНЕНИЕ SIEM-СИСТЕМ

А. Д. Кузнецова, Д. В. Сахаров

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

В статье рассматривается вопрос обеспечения информационной безопасности на предприятии с применением SIEM, позволяющим анализировать и регистрировать угрозы безопасности информации в режиме реального времени. Применение данной технологии является актуальной и перспективной технологией для критически важных инфраструктур, так как позволяет добиться практически полной автоматизации процесса выявления угроз, тем самым сделав акцент на своевременном выявлении инцидентов безопасности инфраструктуры и существенного сокращения возможных потерь. В статье приводится описание и основные характеристики SIEM системы, анализ обеспеченности информационной безопасностью предприятий, актуальность внедрения данных систем и их недостатки.

информационная безопасность, защита информации, SIEM системы.

Введение

Проблема выполнения мероприятий по обеспечению информационной безопасности (ИБ) является достаточно актуальной, поскольку следует приводить в исполнение ряд задач, таких как осуществление мониторинга,

сбора, анализа и реагирования инцидентов ИБ [1, 2, 3]. Однако в данный момент, решение поставленной задачи осуществляется не в полной мере. Количество средств защиты информации в настоящее время неуклонно растет, а это усложняет инфраструктуру и процесс обработки информации в целом. В таких условиях решение поставленных задач становится все более трудоемким. Наиболее эффективным подходом считается применение систем класса SIEM (*Security Information and Event Management*).

Описание

Сегодня на рынке средств защиты информации представлено множество решений класса SIEM, отличающиеся архитектурой и функциональными возможностями. Производительностью обработки регистрируемых событий безопасности, применяемыми технологиями выявления зависимостей между отдельными событиями, используемыми показателями состояния защищаемой инфраструктуры. Особенностями построения интерфейса и др. Многообразие и вариативность характеристик современных SIEM систем обусловливает актуальность задачи их классификации.

Решения SIEM обеспечивают управление информацией и событиями безопасности, реализуя функции сбора и хранения, обработки и анализа зарегистрированных событий безопасности, с целью выявления и разбора инцидентов, а также проверки соответствия системы управления ИБ существующим требованиям и нормам. Данные системы позволяют повысить эффективность управления сетевой инфраструктурой в целом.

Основными задачами по обеспечению информационной безопасности, которые должна выполнять SIEM-система, считаются[4]:

– объединение и хранение журналов событий;
– обработка и корреляция событий;
– уведомление о совершившихся инцидентах;
– выявление конфликтов;
– управление происшествиями;
– наглядная визуализация.

Основными исходными данными, которые используются SIEM системой для решения указанных задач, являются журналы событий с ОС, сетевых устройств, приложений и СЗИ. Сбор и анализ подобных событий отражает действия пользователей и программ, оказавших влияние на безопасность инфраструктуры.

Кроме того, типовая SIEM-система имеет способность выявлять[5]:

– обнаружения в режиме реального времени атак и нарушений критериев и политик безопасности, как во внутреннем, так и внешнем периметрах сети;

– ошибки конфигураций в средствах защиты и информационных системах;

– попытки несанкционированного доступа к конфиденциальной информации.

Как правило, основную работу для решения поставленных перед системой задач выполняют следующие компоненты:

1. Агенты, собирающие журналы событий и отправляющие их на сервер.

2. Хранилища, отвечающие за сохранность и целостность журналов событий.

3. Сервер приложений, реализующий функции защиты, для выработки предупреждений или управленческих решений по защите информации.

Анализ предметной области

Говоря о роли ИБ на предприятии, важно понимать ее сферу не только в рамках корпоративной отрасли, а также на уровнях страны и мира. Итоговое соотношение атак и угроз на информационную систему указывает, что Россия располагается на втором месте по количеству кибертеррористических актов и хакерских атак.

Сложившаяся обстановка дает возможность пользоваться условно комфортным режимом и направить силы на повышение уровня защиты от предполагаемых угроз. Стоит заметить, что и государственные защитные меры неидеальны, о чем говорят прогрессирующие взломы правительственных серверов в разных странах мира. К примеру, во время президентских выборов РФ в 2012 г. на участках для голосования была использована система веб-трансляции, для фиксации нарушений избирательного законодательства. Тогда на систему в течение суток было совершено до 1,2 миллиона атак. В этом же году злоумышленники атаковали государственные информационные сети Израиля 44 миллиона раз, Ирана – 28, США – 12. Для сравнения: в течение 2016 года в России на государственные и частные ресурсы было совершено уже 70 миллионов кибернападений, что говорит о скорости возрастания и серьезности угрозы [6].

Вне зависимости от уровня обеспечения ИБ, будь это у частной компании, федеральной службы, либо на уровне государственного аппарата, основной проблемой является утечка информации. По исследовательским данным за 2017 г. специалистами компании «СёрчИнформ», выявлено, что:

– 21 % опрошенных компаний пострадали от утечки информации, 15 % удалось предотвратить кражу данных, 46 % организаций не сталкивались с подобными инцидентами, 18 % не владеют подобной информацией.

Причинами ИБ-инцидентов отмечается:

– 43 % вирусных заражений ПК, 37 % технические проблемы, 21 % случайное разглашение информации, 21 % атаки извне, 10 % действия инсайдеров, 7% кража или потеря периферийных устройств.

Используемыми средствами защиты информации чаще всего отмечались:

– 82 % антивирусные программы, 66 % Средства администрирования Windows, 62 % Firewall, 48 % Proxy, 25 % DLP-система, 14 % IDS/IPS, 7 % SIEM-система, 2 % никакие.

Системы обеспечения ИБ должны обеспечивать защиту информации, как на сетевом, так и на прикладном уровнях, для защиты от внутренних и внешних угроз. Большинство систем безопасности работают отдельно друг от друга, без возможности обмениваться событиями ИБ. При этом все средства информационной безопасности могут работать гораздо более эффективно, если информация об обнаруженных ими инцидентах будет централизованно собираться и обрабатываться.

Именно для решения поставленной цели необходимо применять SIEM системы. При этом, SEIM – это инструмент не только ИБ, но и инфраструктуры предприятия в целом.

На основе мощных корреляционных механизмов можно эффективно обеспечивать непрерывность работы IT-сервисов, выявлять сбои в аппаратном обеспечении, а также информационных и операционных системах. Простейший пример – «login failed»: по одному случаю сложно судить о непреднамеренных действиях, но при выявлении трех и более таких события с одной учетной записи свидетельствует о попытках подбора. В случае правильного внедрения SIEM системы и корректного интегрирования со всеми системами безопасности, предприятие получает централизованную базу событий ИБ [7].

Недостатки

Выявив актуальность применения SIEM систем и реализации с помощью них основных задач обеспечения ИБ, также стоит отметить их недостатки, а это:

1. *Импортозамещение*. Если рассматривать вопрос внедрения SIEM на предприятии государственного уровня, то стоит отметить, что производителями хороших SIEM являются иностранные копании. А согласно Постановлению Правительства РФ от 26 сентября 2016 г. № 968 «Об ограничениях и условиях допуска отдельных видов радиоэлектронной продукции, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд», закупка и внедрение таких устройств запрещена. Это предполагает для заказчика ориентир только на русский рынок [8].

2. *Цена владения SIEM*. Информация о стоимости владения такой системой считается доступной. Так, к примеру, стоимость SIEM решений от IBM, Hewlett-Packard и Positive Technologies составляет от 3 миллионов рублей, что не всегда удовлетворяет малый и средний бизнес.

3. *Неоднородность*. Инновационная SIEM-система должна быть гибкой в интеграции с имеющейся инфраструктурой, собирать и анализировать данные от огромного количества разнообразных устройств и программных обеспечений. В связи с этим обстоятельством далеко не каждая SIEM-система сможет справиться.

4. *Защищенность SIEM-системы*. Проанализировав единство SIEM системы, их защищенность вызывает большой вопрос. Подмена злоумышленником доверенного объекта, взлом базы данных SIEM-системы, вот лишь малая часть проблем. На данный момент общеизвестен целый ряд критичных уязвимостей для таких SIEM, как IBM qRadar и HP ArcSight и этот список далеко не окончательный.

Выводы

В результате рассмотрения представленного вопроса о применении SIEM систем, хочется отметить, что в настоящее время, нет необходимости создания модернизированных инфраструктур, отвечающих лишь за определённые области обеспечения информационной безопасности. Гораздо актуальным и целесообразным является переход на качественно новый уровень – использование SIEM-систем, обрабатывающих сведения от систем мониторинга и защитных систем, действий пользователей и решения объедения сбора событий в единую структуру. Активно возрастающее внимание к SIEM-системам сформировано в первую очередь рвением компаний обеспечить высокий уровень защиты их инфраструктуры. Вышеуказанные недостатки, при детальном рассмотрении, являются скорее возможностями, для дополнительного исследования. В ходе дальнейшего изучения исследований информационной безопасности и применения SIEM систем, планируется провести ряд экспериментов по внедрению SIEM системы на предприятии и аналитике поведения системы при возникновении угроз ИБ.

Список используемых источников

1. Виткова Л. А., Дудникова М. Н., Петрова А. Н. Вопросы управления информационной безопасностью // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 143–146.

2. Булатов Н. А., Виткова Л. А., Шашкин В. С. Теоретические аспекты управления информационной безопасности на предприятии // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 117–122.

3. Аникевич Е. А., Виткова Л. А., Сацук Е. Н., Сергеева И. Ю. Предотвращение утечек конфиденциальной информации в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 46–51.

4. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. № 20. С. 27–56.

5. Шабуров А. С., Борисов В. И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы. // Вестник ПНПИПУ, Электротехника, информационные технологии, системы управления. 2016. № 19. С. 111–124.

6. Overcoming Common Causes for SIEM Solution Deployment Failures. URL: https://www.gartner.com/doc/2828417/overcoming-common-causes-siem-deployment (дата обращения 02.02.2019).

7. Андреянов Я. В., Андрианов В. И., Виткова Л. А., Потехин И. Ю. / Информационная безопасность в деятельности органов государственной власти // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2017. С. 37–41.

8. Постановление Правительства РФ от 26 сентября 2016 г. № 968 «Об ограничениях и условиях допуска отдельных видов радиоэлектронной продукции, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

УДК 621.3:535.8
ГРНТИ 20.53.19:29.33

ЛАБОРАТОРНАЯ УСТАНОВКА ДЛЯ ИЗУЧЕНИЯ И РАЗРАБОТКИ ОПТОЭЛЕКТРОННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

М. С. Кузьмин, С. А. Рогов

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

Приводится описание оптико-цифровой установки для проведения лабораторных работ по основам фурье-оптики и оптической обработки информации. Наряду с учебным применением, установка позволяет осуществлять научные разработки и физическое моделирование новых устройств для задач обработки сигналов и изображений в системах различного назначения.

лабораторные работы, оптическая обработка изображений и сигналов, пространственный модулятор света, жидкокристаллическая матрица, оптический фурье-процессор, коррелятор совместного преобразования.

Одной из задач, решаемой методами информационной оптики является оптическая обработка сигналов [1]. Оптические и оптоэлектронные устройства обработки имеют ряд преимуществ перед электронными цифровыми системами и, прежде всего, – высокое быстродействие. Наибольшее развитие к настоящему времени получили аналоговые оптические методы обработки на основе фурье-оптики, в которых просто осуществляется ряд интегральных преобразований, широко используемых при обработке сигналов и изображений (преобразование Фурье, вычисление корреляционных функций и др.).

Хотя основные принципы фурье-оптики достаточно хорошо изучены, исследования, направленные на создание устройств, пригодных для практического применения продолжаются. Параметры реальных устройств в значительной мере определяются возможностями используемой элементной базы, в частности устройств ввода информации в оптическую систему. Применение новых пространственных модуляторов света (ПМС) позволяет не только улучшить параметры известных устройств, но и предложить новые схемы обработки информации.

Разработанная экспериментальная установка предназначена как для проведения лабораторных работ по основам фурье-оптики, так и экспериментального исследования новых применений оптической обработки сигналов и изображений. В качестве устройства ввода в ней использована жидкокристаллическая (ЖК) матрица от видеопроектора.

Оптическая схема установки представлена на рис. 1. Она состоит из последовательно расположенных на оптической оси полупроводникового лазера, нейтрального светофильтра, поляризатора, телескопической системы линз (для расширения лазерного луча до размеров устройства ввода), ЖК ПМС, объектива фурье-преобразования, поляроида-анализатора и матричного фотоприемника (WEB-камеры). Пленочные поляроиды обеспечивают блокировку света, проходящего через ЖК ПМС при нулевом управляющем напряжении на его элементах [2]. ЖК матрица размером 10,5×9 мм^2 имела число элементов 1024×768. Ввод сигналов в матрицу осуществляется из памяти компьютера через устройство ввода изображений от видеопроектора, доработанное с целью устранения лишних каналов, цепей контроля и блокировок.

Экспериментальная установка может работать в двух основных режимах:

– как анализатор спектра пространственных частот входных сигналов (оптический фурье-процессор);

– как однокаскадный коррелятор совместного преобразования [3].

В первом случае входные изображения или сигналы из памяти компьютера с помощью ЖК ПМС подаются на вход оптической системы, а вы-

ходные сигналы, регистрируемые фотоприемником, передаются в компьютер для представления на мониторах в удобном для анализа виде (общий вид, сечения и др.). На рис.2 в качестве примера показаны полученные в системе двумерный спектр и его сечение по горизонтальной оси при подаче на вход изображения в виде прямоугольной апертуры.

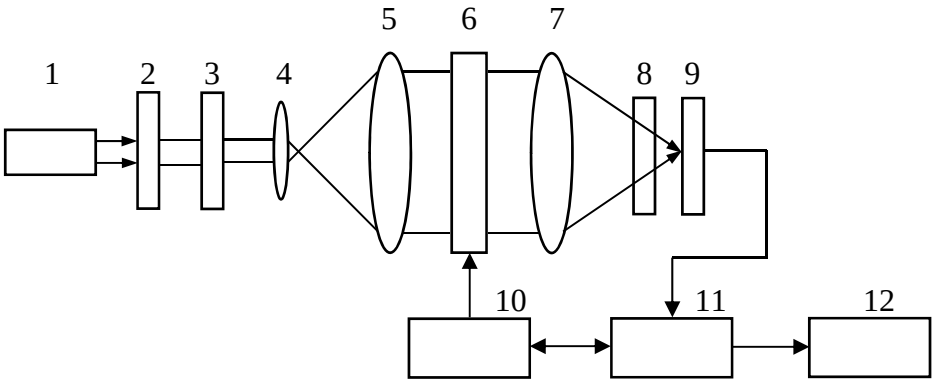
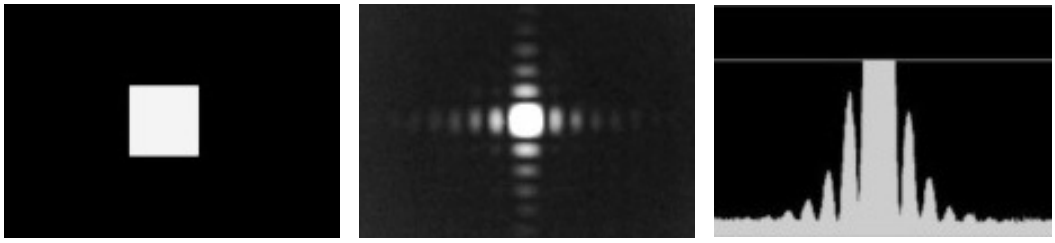


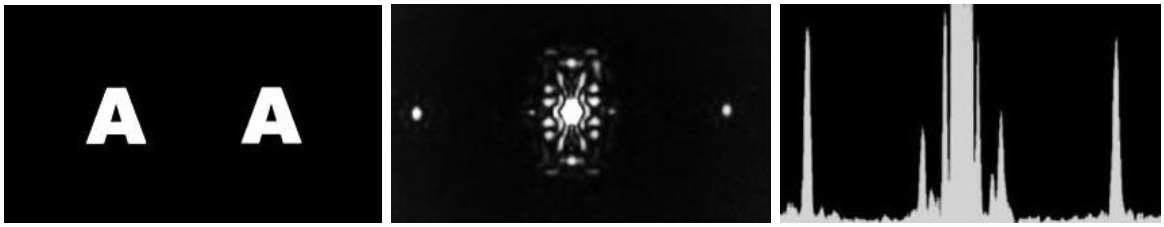
Рис. 1. Схема фурье-процессора с жидкокристаллическим вводом:
1 – лазер, 2 – нейтральный фильтр, 3, 8 – поляризаторы, 4, 5 – линзы расширителя светового пучка, 6 – ЖК ПМС, 7 – фурье-объектив, 9 – WEB-камера, 10 – блок управления ЖК ПМС, 11 – компьютер, 12 – мониторы



а) б) в)

Рис. 2. Сигналы фурье-процессора: а) входное изображение, б) его спектр, в) горизонтальное сечение спектра

Во втором режиме обработка осуществляется в два этапа. Сначала на выходе процессора формируется совместный спектр входного и опорного изображений (или одномерных сигналов). Затем полученный совместный спектр с помощью компьютера подаётся на вход вместо входного и опорного сигналов, при этом на выходе процессора регистрируется корреляционная функция. Перед подачей совместного спектра на вход компьютер может осуществлять его обработку с целью улучшения параметров корреляторa (локализации корреляционных пиков, увеличения отношения сигнал-шум, и др.) [4]. На рис. 3 показаны сигналы при распознавании буквы «А», которые формируются в системе, работающей в режиме коррелятора совместного преобразования.



а) б) в)

Рис. 3. Входной (а) и выходной (б) сигналы и центральное сечение выходного сигнала (в) при работе установки в режиме коррелятора совместного преобразования

На основе созданной установки могут быть реализованы такие алгоритмы обработки информации, как анализ пространственных спектров изображений, спектральный анализ и корреляционная обработка сигналов, корреляционный алгоритм сравнения изображений. Эти алгоритмы находят применение в задачах распознавания изображений и сигналов, в радиоразведке, в многоканальных системах связи, в радиолокации, в системах обработки сигналов антенных решеток и других. Если изготовить разработанную установку в малогабаритном варианте, она будет обладать всеми основными преимуществами оптических устройств обработки информации – высоким быстродействием, малыми габаритами и энергопотреблением – и при соответствующей адаптации может быть использована для решения конкретных практических задач.

В других случаях, когда на входе оптического процессора целесообразно использовать не ЖК ПМС, а иное устройство ввода, например, акустооптический модулятор, разработанная установка может быть применена для физического моделирования работы оптической системы с имитацией ее входных сигналов с помощью ЖК матрицы. В качестве примера, на рис. 4 показан выходной сигнал системы оптической обработки сигналов линейной антенной решетки. В соответствии с теорией [5], на выходе фурье-процессора в зоне обзора антенной решетки (обозначена штриховой линией) наблюдается смещение пятен дифракции первого порядка на величину, пропорциональную частоте сигнала – по вертикальной координате – и на величину, пропорциональную линейному сдвигу фаз, связанному с углом прихода радиоволны на антенную решетку – по горизонтальной.

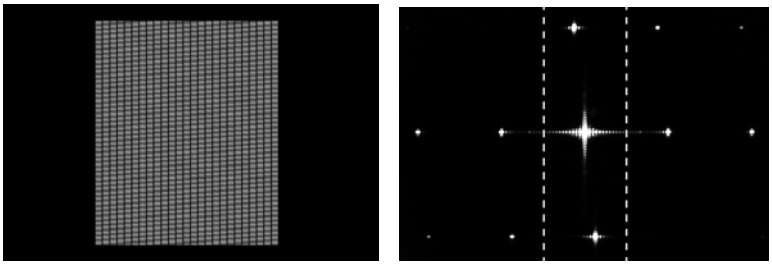


Рис. 5. Входной (а) и выходной (б) сигналы оптической системы обработки сигналов 25-элементной антенной решетки

К настоящему времени разработанная установка уже применялась для исследования ряда новых методов оптической обработки сигналов, а также известных методов и устройств, ранее исследованных методами математического моделирования или в экспериментах с использованием устройств ввода, не пригодных для практического применения. В частности, были исследованы система спектрального анализа длинных сигналов со свернутым спектром [6], корреляторы совместного преобразования с фазовым вводом и с нелинейной обработкой совместного спектра [7], коррелятор длинных сигналов с растровым вводом [8], гибридная оптико-цифровая система распознавания по признакам, выделяемым из фурье-спектров [9], продемонстрирована также возможность реализации на ЖК ПМС плоских амплитудных и фазовых оптических элементов, с оперативно управляемыми параметрами [10], проведено исследование влияния нелинейности регистрации совместного спектра на динамический диапазон коррелятора совместного преобразования [11] и взаимного влияния сигналов в соседних строках ЖК матрицы [12]. Некоторые из этих исследований и устройств могут быть положены в основу лабораторных работ, проводимых на разработанной установке без изменений ее конструкции. Достаточно внести дополнения в программу, установленную на управляющий компьютер.

Список используемых источников

1. Евтихиев Н. Н., Евтихиева О. А., Компанец И. Н. и др. Информационная оптика: учебное пособие / Под ред. Н. Н. Евтихиева. М. : МЭИ, 2000. 612 с.

2. Жидкокристаллический дисплей // ru.wikipedia.org. Википедия – свободная энциклопедия.

3. Javidi B., Gregory A., Horner J.L. Single modulator joint transform correlator architectures // Applied optics. 1989. V.28. N 3. P. 411–413.

4. Javidi B. Nonlinear joint power spectrum based optical correlation // Appl. Opt. 1989. V. 28. P. 2358–2367.

5. Ламберт, Арм, Аймет. Электронно-оптическая обработка сигналов в фазированных антенных решетках // Зарубежная радиоэлектроника. 1968. N 8. С. 3–34.

6. Кузьмин М. С., Рогов С. А. Анализатор свернутого спектра с жидкокристаллическим устройством ввода сигналов // Письма в ЖТФ. 2014. Т. 40. № 15. С. 1–5.

7. Кузьмин М. С., Давыдов В. В., Рогов С. А. Экспериментальное исследование коррелятора совместного преобразования // Квантовая электроника. 2018. № 11. С. 1048–1054.

8. Кузьмин М. С., Рогов С. А. Обработка одномерных сигналов с растровым вводом в двумерных оптических корреляторах // ЖТФ. 2015. Т. 85. № 4. С. 156–158.

9. Kuzmin M. S., Rogov S. A. Hybrid Optical-Digital System of Texture Recognition with Liquid Crystal Input Device // Optical Memory & Neural Networks (Information Optics). 2017.V 26. N. 4. P. 298–299.

10. Кузьмин М. С., Рогов С. А. Бинарные фазовые транспаранты на основе жидкокристаллической матрицы видеопроектора // Журнал технической физики. 2018. Т. 88. № 1. С. 85–88.

11. Кузьмин М. С., Рогов С. А. Влияние нелинейности регистрации спектра в корреляторе совместного преобразования при распознавании одинаковых образов // Оптический журнал. 2017. Т. 84. № 8. С. 64–69.

12. Кузьмин М. С., Давыдов В. В., Рогов С. А. Об использовании многорастрового ввода одномерных сигналов в двумерных оптических корреляторах // Компьютерная оптика. 2019. Т. 43. № 3. С. 391–396.

УДК 621.3:535.8
ГРНТИ 20.53.19:29.33

ОПТИЧЕСКИЕ ПРОЦЕССОРЫ С ПАРАЛЛЕЛЬНЫМ ВВОДОМ СИГНАЛОВ В ЖИДКОКРИСТАЛЛИЧЕСКУЮ МАТРИЦУ

М. С. Кузьмин, С. А. Рогов

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

Проведена оценка быстродействия систем оптической обработки информации при параллельном (построчном) вводе сигналов в жидкокристаллический пространственный модулятор света с электронным управлением. Показано, что применение параллельного ввода позволяет в ряде случаев увеличить производительность известных оптических систем до уровня, на порядки превосходящего быстродействие цифровых устройств аналогичного назначения.

жидкокристаллический пространственный модулятор света, параллельная обработка информации, быстродействие оптических процессоров, многоканальные системы, спектральный анализ сигналов, оптические корреляторы.

Основным достоинством аналоговых оптических систем обработки информации по сравнению с цифровыми является высокая скорость выполнения вычислений при небольших габаритах и энергопотреблении процессора [1]. Преобразования в оптических системе осуществляются быстро – за время прохождения света от входа до выхода, однако общее время обработки должно определяться с учетом времени ввода информации в оптическую систему и времени вывода выходных сигналов из неё. Поэтому быстродействие оптических систем в значительной мере зависит от параметров устройства ввода сигналов в оптический процессор.

Высоким быстродействием обладают акустооптические модуляторы. Они позволяют осуществлять ввод электрических сигналов с частотой

до нескольких гигагерц, что соответствует скорости ввода в несколько тысяч отсчетов в микросекунду для одноканального модулятора и в *M* раз больше для модулятора с *M* параллельно работающими каналами. Однако число каналов многоканальных акустооптических модуляторов не превышает нескольких десятков, при этом серийно выпускаются только одноканальные устройства. Создание оптических систем обработки двумерных сигналов (изображений) на основе одноканальных акустооптических модуляторов возможно [2], но такие оптические устройства являются сложными, для ввода информации в системы обработки двумерных сигналов больше подходят двумерные пространственные модуляторы света (ПМС).

Одними из наиболее перспективных ПМС в настоящее время являются жидкокристаллические (ЖК) модуляторы с электронным управлением. Модуляторы такого типа выпускаются промышленностью для видеоаппаратуры, выпускаются также специальные ЖК ПМС для когерентных оптических систем обработки информации [3]. Число разрешимых элементов в ЖК ПМС может достигать нескольких тысяч по каждой из координат, что позволяет одновременно вводить большой объем информации в оптический процессор. Однако ввод сигналов в сам ПМС осуществляется последовательно, за время не менее 1–10 мс.

В работе [4] была предложена структура устройства управления ЖК матрицей, позволяющая осуществлять построчный ввод входных сигналов в ЖК ПМС. При максимальной скорости драйвера строк ЖК матрицы около 100 МГц, время, затрачиваемое на ввод строки, может быть уменьшено до 10 нс, а ввод двумерного сигнала с 1000×1000 элементами потребует около 10 мкс. Исследования показывают [5], что время реакции некоторых жидких кристаллов на изменения управляющего напряжения позволяют достичь такого быстродействия. Рассматриваемый ПМС по скорости ввода информации в оптическую систему эквивалентен акустооптическому модулятору с полосой пропускания 100 МГц, имеющему 1000 параллельных каналов.

Для реализации параллельного ввода сигналов в ПМС из памяти компьютера или от других источников потребуется создание соответствующего устройства управления. Возможность создания такого устройства косвенно подтверждается реализацией параллельного ввода сигналов в 256 каналов оптического процессора в коммерческом компьютере Enlight-256 [6].

Рассмотрим, насколько возрастает быстродействие ряда схем оптической обработки информации при параллельном вводе сигналов в ЖК ПМС.

Двумерное преобразование Фурье

При обычном (последовательном) вводе сигналов в ПМС с числом элементов ~1000×1000 за время 1 мс, получаем (пренебрегая временем оптического преобразования Фурье), что время выполнения двумерного преобразования Фурье оптической системой с учетом времени ввода информации составляет 1 мс. Для выполнения такого же преобразования цифровым процессором, работающим по алгоритму быстрого преобразования Фурье (БПФ), число операций умножения составляет $(1/2)N\lg N = 10^7$оп, где N – число отсчетов во входном сигнале. Таким образом, эквивалентная производительность оптического процессора составляет 10^7оп/1мс = 10^{10}оп/с, что лишь в несколько раз превосходит быстродействие обычных цифровых устройств. При параллельном вводе информации в ПМС время ввода сигналов в оптическую систему составит только 10 мкс (см. выше), производительность при этом будет равна 10^{12}оп/с, что недостижимо для цифровых устройств с небольшими габаритами и энергопотреблением.

Двумерное преобразование Фурье может быть использовано как для обработки изображений, так и быстроизменяющихся сигналов, например, сигналов антенных решеток [7]. В последнем случае быстрый ввод позволит увеличить разрешение устройства по времени при определении параметров принимаемых антенной решеткой сигналов.

Необходимо отметить, что для увеличения быстродействия всей оптической системы при уменьшении времени ввода, требуется уменьшать и время вывода информации из оптического процессора. Это достигается при использовании фотоприемника с небольшим числом параллельно работающих элементов, как например, в гибридной оптико-цифровой системе распознавания изображений по признакам, выделяемым из фурье-спектров [8, 9]. Труднее получить высокую скорость вывода в системах, где требуется регистрация большого числа разрешимых элементов в выходной плоскости и использовании фотоприемников с последовательным выводом. В этом случае в устройствах съёма могут быть использованы разные методы увеличения скорости регистрации - секционированные матричные фотоприемники, системы грубого и точного отсчета и т. п.

Распознавание изображений с использованием корреляционного алгоритма

Корреляционное сравнение двух двумерных сигналов подразумевает вычисление интеграла от произведения этих функций. При числе разрешимых элементов в сигналах 1000×1000 для получения корреляции требуется осуществить 10^6 произведений и просуммировать их. Это легко может быть реализовано в простой некогерентной оптической системе, в которой свет последовательно проходит через два ПМС (один из которых может быть

опорной маской) и затем суммируется на фотоприемнике. В оптическом устройстве все произведения вычисляются одновременно. При времени параллельного ввода изображения в ПМС 10 мкс, производительность такого оптического коррелятора составит 10^6оп/10мкс = 10^{11}оп/с, что более чем на 1–2 порядка превышает производительность обычных цифровых процессоров. Устройство съёма в данном случае (одиночный фотоприемник) не ограничивает быстродействие системы.

Распознавание объекта на большом изображении

Когерентные оптические корреляторы имеют высокую производительность благодаря инвариантности к сдвигу входного сигнала и параллельности обработки всей входной сцены [10]. Так поиск и корреляционное распознавание объекта с числом элементов 100×100 в изображении 1000×1000 требует выполнения $10^4 \times 10^6$ операций умножения (10^4 операций умножения для получения корреляции объекта с участками изображения, при 10^6 возможных смещениях объекта) при этом все корреляции вычисляются в оптической системе одновременно. Даже если использовать последовательный ввод изображения за 1 мс, реализуемый на существующей элементной базе, производительность коррелятора составит 10^{13} оп/с. Устройство регистрации оптических сигналов этом случае осуществляет вывод информации также за время ~1 мс, что технически достижимо, и не тормозит работу всего процессора.

Если использовать параллельный ввод в ПМС и специальные методы увеличения скорости вывода оптической информации для поддержания повышенного быстродействия устройства ввода, производительность коррелятора может быть еще повышена (по возможностям устройства ввода до двух порядков).

Системы корреляционного распознавания сигналов

Как и при распознавании изображений в некогерентных и когерентных корреляторах можно распознавать и одномерные сигналы. Если сигнал не умещается на одной строке ПМС, он может вводиться в ПМС в виде растровой записи [11]. Эквивалентная производительность оптической системы, как и в случае обработки изображений, составит при параллельном вводе сигналов 1011 оп/с для некогерентного коррелятора (без поиска сигнала) и до 10^{15} оп/с – для когерентного.

Системы спектрального анализа сигналов

При обработке коротких сигналов многоканальность ПМС позволяет расширить функциональные возможности процессора, например, можно осуществлять спектральный анализ сигналов в широкой полосе частот

с применением набора гетеродинов [12]. При этом возможен аналоговый параллельный ввод сигналов в столбцы ПМС, как в многоканальном акустооптическом модуляторе. Производительность такой многоканальной системы ненамного меньше, чем у фурье-процессора двумерных сигналов с параллельным вводом.

Заключение

Проведенное рассмотрение показывает, что применение параллельного (построчного) ввода сигналов в ЖК ПМС позволяет в ряде оптических систем обработки информации увеличить производительность до уровня, на порядки превосходящего быстродействие цифровых устройств аналогичного назначения. Для проверки возможности реализации рассмотренных выше процессоров с параллельным вводом требуется проведение их экспериментального исследования.

Список используемых источников

1. Евтихиев Н. Н., Евтихиева О. А., Компанец И. Н. и др. Информационная оптика: учебное пособие / Под ред. Н. Н. Евтихиева. М. : МЭИ, 2000. 612 с.

2. Псалтис Д. Двумерная оптическая обработка сигналов с использованием одномерных входных устройств // ТИИЭР. 1984. Т. 72. № 7. С. 240–255.

3. www.holoeye.com

4. Kuzmin M. S., Rogov S. A. Signal parallel input liquid-crystal devices for multichannel optical processing systems // Optical Memory & Neural Networks (Information Optics). 2016. V. 25. N. 2. P. 102–105.

5. M. W. Geis, R. J. Molnar, G. W. Turner, T. M. Lyszczarz, R. M. Osgood, and B. R. Kimball. 30 to 50 ns liquid-crystal optical switches. //Proc. SPIE 7618: 76180J/1-5. 2010.

6. Белов П. А. и др. Оптические процессоры: достижения и новые идеи. URL: http://ysa.ifmo.ru/data/publication/BOOK008/paper1-001.doc.

7. Ламберт, Арм, Аймет. Электронно-оптическая обработка сигналов в фазированных антенных решетках // Зарубежная радиоэлектроника. 1968. № 8. С. 3–34.

8. Старк Г., О'Тул Р. Статические методы распознавания образов с использованием признаков, выделенных из оптических фурье-спектров // Применение методов фурье-оптики / Под ред. Г. Старка. М. : Радио и связь, 1988. 536 с.

9. Kuzmin M. S., Rogov S. A. Hybrid Optical-Digital System of Texture Recognition with Liquid Crystal Input Device // Optical Memory & Neural Networks (Information Optics). 2017. V 26. N. 4. P. 298–299.

10. Оптическая обработка информации. Применения / Под ред. Д. М. Кейсесента. М. : Мир, 1980. 349 с.

11. Кузьмин М. С., Рогов С. А. Обработка одномерных сигналов с растровым вводом в двумерных оптических корреляторах // ЖТФ. 2015. Т. 85. № 4. С. 156–158.

12. Белошицкий А. П., Комаров В. М., Крекотень Б. П. Акустооптические анализаторы спектра радиосигналов //Зарубежная радиоэлектроника. 1981. № 3. С. 51–70.

УДК 004.5
ГРНТИ 49.40.39

РАЗРАБОТКА И ИССЛЕДОВАНИЕ МОДЕЛЕЙ СЕМАНТИЧЕСКОЙ СОВМЕСТИМОСТИ РАЗЛИЧНЫХ ПЛАТФОРМ И УСЛУГ ИНТЕРНЕТА ВЕЩЕЙ

В. А. Кулик, Н. П. Слепцова

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

В данной статье исследуются вопросы совместимости форматов данных различных платформ и услуг Интернета Вещей. Авторами были рассмотрены различные методы для обеспечения семантической совместимости платформ и услуг ИВ. Также затрагивается вопрос о создании программно-аппаратного комплекса, на базе которого была разработана архитектура модельной сети. На основе разработанной модельной сети была проведена серия экспериментов по анализу различных типов мультимедийного трафика. На основе полученных данных были сделаны выводы о общем характере трафика мультимедийных приложений.

видеонаблюдение, Умный город, IP, RTP, RTCP, RTSP, видео трафик.

На данный момент в IP-сетях распространено множество технологий мультимедийного характера: IP-телефония, IPTV, IP-домофония и т. д. Каждая система имеет свой алгоритм, определенные протоколы передачи данных и предоставления различных услуг для клиентов. Одним из важнейших аспектов работы устройств этого направления является гарантированная доставка данных, с минимальными задержками, высокой скоростью и без потери пакетов. Для контроля качества доставки сообщений в IP-сетях используются параметры качества обслуживания (quality of service, QoS): сетевые задержки, пропускная способность, джиттер, потери пакетов [1]. Мультимедийные приложения активно применяются в таких направлениях как «Умный дом» и «Умный город». Важной задачей в рамках решений «Умный дом» и «Умный город» является обеспечение безопасности жизнедеятельности человека. На базе видеокамер, размещенных по территории города, проводится мониторинг большого количества видеоданных, для решения таких задач как: регулирование дорожного трафика, контроль криминогенной обстановки, отслеживания экстренных ситуаций и др. В настоящее время существует множество различных протоколов передачи и контроля доставки мультимедийной информации. В качестве примера можно привести такие протоколы реального времени как RTP, RTCP, RTSP, RTMP и др.

Проблема взаимодействия различных приложений и протоколов между собой является особенно острой и поэтому важно обеспечить семантическую совместимость для данных услуг в рамках проекта «Умный город». Основным транспортным протоколом в приложениях передачи видеоданных является протокол RTP. Данный протокол определяет тип поля данных, производит нумерация сообщений, присваивает временные метки и контролирует доставку данных. RTP-пакеты переносятся в пакетах протокола UDP для гарантированной доставки мультимедийных данных. RTP поддерживает передачу информации на несколько адресатов через Multicast.

Протокол RTP на практике не отделим от протокола RTCP (*Real-time Transport Control Protocol*) – протокол управления передачей в реальном времени, который позволяет мониторить качество обслуживания и синхронизации между медиа-потоками. RTSP (*real time streaming protocol*)-потоковый протокол реального времени, который позволяет управлять видеопотоком («старт», «пауза», «промотка» и т. д.). Работает на основе протоколов RTP, UDP/TCP [2].

Проект «Умный город» включает в себя систему «Умного видеонаблюдения», которое представляет из себя совокупность IP-камер и сенсоров, объединенных на базе технологий Интернета вещей (*Internet of Things*, IoT). В режиме реального времени потоки видео поступают на сервер, где они обрабатываются и хранятся на протяжении долгого времени. Система позволяет получать информацию ежедневно в любую точку мира, если есть Интернет-соединение. Поддерживается различными платформами и операционными системами, например: Linux, Windows, Android, iOS. Видеонаблюдение обеспечивает контроль и безопасность для города и его жителей. В данной статье цель провести анализ качества обслуживания услуг связи предоставляемых, в рамках решения «Умный город» и «Умный дом». Задачами являются: исследовать существующие решения по реализации пользовательских услуг в рамках систем «Умный город» и «Умный дом» на базе инфраструктуры компании «Ростелеком», разработать модельную сеть для тестирования качества обслуживания услуг связи для исследуемых решений, провести перехват и анализ трафика на базе разработанной модельной сети.

Для того, чтобы начать исследования нужно построить модельную сеть (рис. 1).

Модельная сеть была построена на базе компании «ПАО Ростелеком». Для исследования видеотрафика используется IP-камера, встроенная в IP-домофон, которая обеспечивает

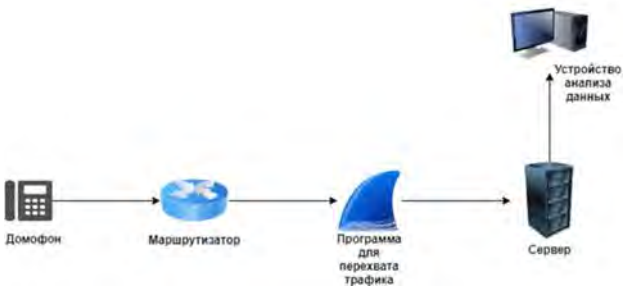


Рис. 1. Структура модельной сети для перехвата видео трафика

передачу потокового детализированного видео. IP-домофоны позволяют просматривать видео в реальном времени из любого места нахождения клиента, с мобильных устройств, которые имеют различных операторов, подключенных к сети Интернет через GSM (*Global System for Mobile communications*). Система позволяет подключаться так же к стационарным телефонам через оптический кабель и технологию PON (*Passive optical network*) и передавать вызовы.

На рис. 2 представлена схема взаимодействия серверов от CPE (*Customer Premises Equipment*), то есть абонентского телекоммуникационного оборудования, до серверов DHCP и DNS, где аппаратура получает свой IP-адрес и URI (*Uniform Resource Identifier*) – имя для web-трансляции через браузер соответственно. Пакеты с информацией проходят через основной сервер, но есть небольшая вероятность, что может прерваться сеанс из-за неполадки, и для таких случаев есть резервное направление.

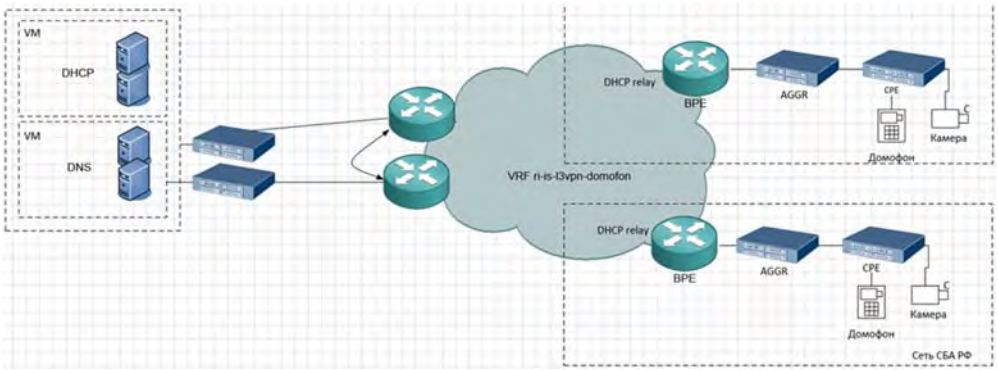


Рис. 2. Организация взаимодействия серверов для предоставления сервисов Домофония и Видеонаблюдение

Видео трафик проходит агрегацию, то есть несколько физических каналов объединяются в один логический, что позволяет увеличить пропускную способность и надежность канала. В таблицах VRF (*Virtual Routing and Forwarding instance*) хранятся маршруты заказчиков, по которым передается мультимедийная информация.

Видеофайл имеет большие размеры, для этого используется стандарт сжатия H.264 без потери качества, что позволяет сохранять объем архивного пространства.

Передача видео трафика происходит по протоколу RTSP, RTCP и H.264 [3].

Видео транслируется в реальном времени на видео панель, установленную в доме у абонента. Соединение происходит через протокол SIP Peer-to-Peer для обеспечения независимости от серверной части PBX.

На рис. 3 показано как с вызывной панели видео поток может проходить от одного оборудования до различной оконечной аппаратуры, таких как, к примеру, сервер Asterisk. Или на SSW (*softswitch*), где трафик направляется на мобильные устройства и стационарные телефонные аппараты.

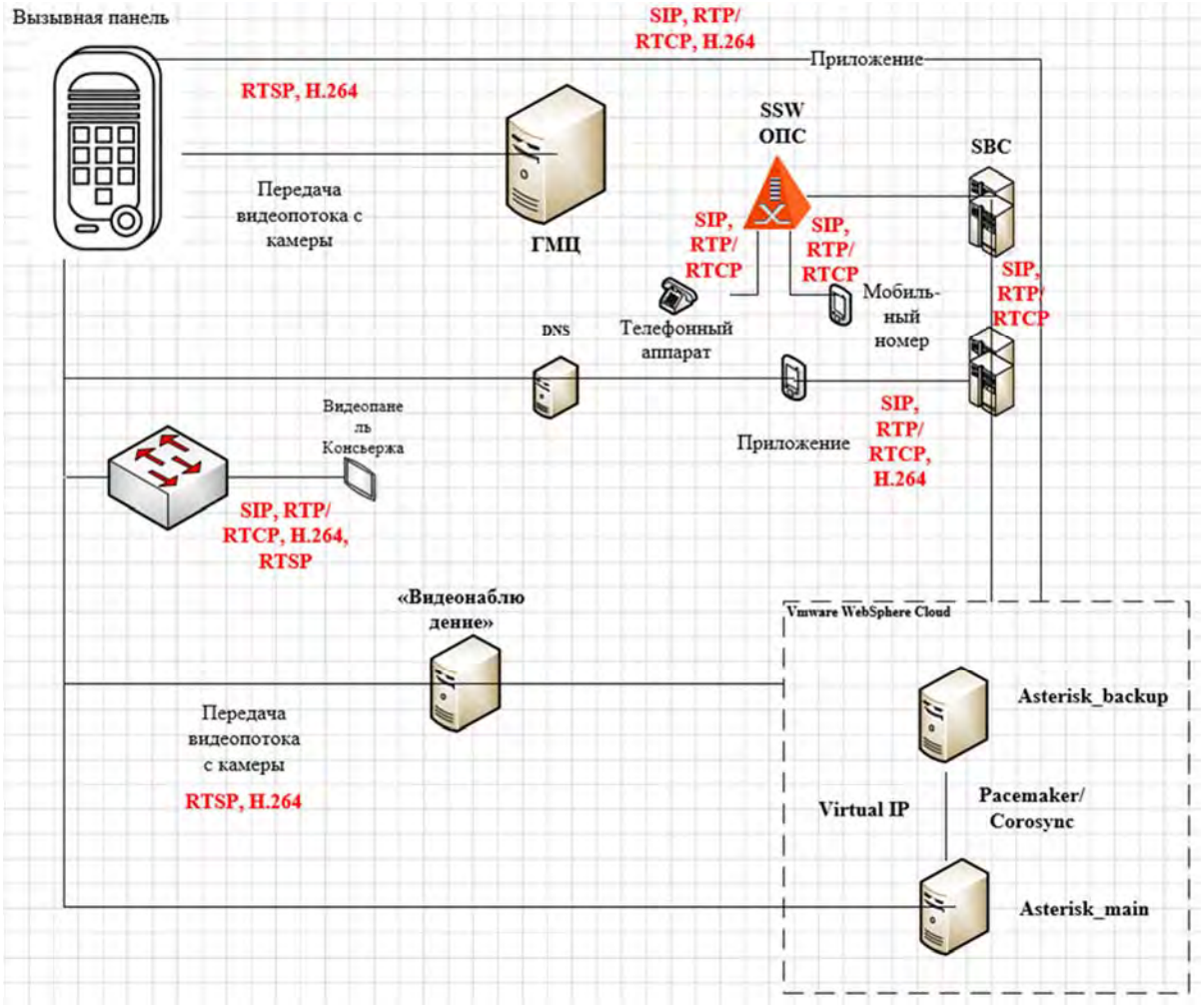


Рис. 3. Архитектура взаимодействия компонентов. Передача видеопотока

По данным исследования перехваченного видео трафика с камеры домофона было выявлены следующие результаты (табл., рис. 4).

ТАБЛИЦА. Результаты исследования

Устройство	Среднее значение интервалов между пакетами, мс	Пропускная способность, байт/с	Джиттер, мс
IP-камера	0,0286	82896,044	0,023

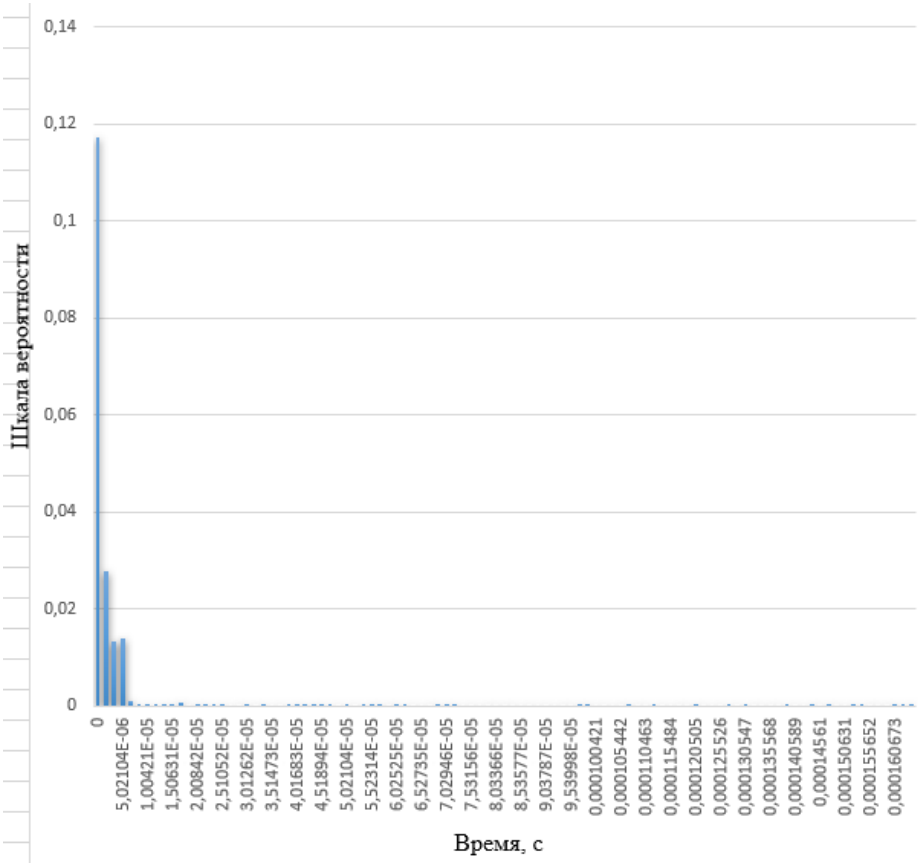


Рис. 4. График вероятностного распределения для видео трафика

По данным проведенного исследования были получены параметры такие как: задержки, джиттер, пропускная способность. Джиттер не превышает требуемого значения в 30 мс (по данным Cisco), значит видео имеет малые задержки и комфортно для просмотра.

Список используемых источников

1. Маколкина М. А. Разработка и исследование моделей оценки качества передачи видео в IP-сетях : автореф. дис. ... канд. техн. наук : 05.12.13 / Маколкина Мария Александровн. СПб., 2014, 18 с.

2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.: ил. ISBN 978-5-496-01967-5.

3. Маколкина М. А. Анализ модели объективной оценки качества передачи видео в IP-сетях // Электросвязь. 2011. № 12. С. 20–23.

Статья представлена доцентом кафедры сетей связи и передачи данных СПбГУТ, доктором технических наук Р.В. Киричком.

УДК 004.654
ГРНТИ 20.53.17

ВЫБОР ДОКУМЕНТНО-ОРИЕНТИРОВАННОЙ СУБД ДЛЯ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

А. С. Куликова, И. Б. Саенко

Военная академия связи имени Маршала Советского Союза С. М. Буденного

Рассматривается проблема организации хранения персональных документно-ориентированных данных в электронном виде. Проводится сравнительный анализ программно-инструментальных средств для решения данной проблемы. Обосновывается выбор СУБД MongoDB в качестве наиболее приемлемого нереляционного средства создания персональной базы документно-ориентированных данных. Детально рассматриваются основные возможности СУБД MongoDB и приводятся примеры реализации баз документальных данных на ее основе.

документ, система управления базами данных, коллекция, репликация.

Системы электронного документооборота на сегодняшний день стремительно внедряются в различных предметных областях. Они имеют неоспоримый ряд преимуществ, таких, например, как высокая скорость и удобство в работе с документацией в электронной форме, организация обмена документацией между отделами и филиалами компании, повышенная степень защиты от несанкционированного доступа. Стоит также отметить экономию места и пространства. В связи с этим системы электронного документооборота находят широкое применение в крупных компаниях и государственных структурах, в любой организации, имеющей необходимость в управлении документацией, в том числе документацией персонального назначения. Однако актуальность хранения персональных данных в электронном виде налагает определенные обязанности по их защите и сохранности, несоблюдение которых, как следствие, может повлечь за собой много проблем. Ведущую роль среди разновидностей прикладного программного обеспечения, применяемого в содержании данных такого рода, играют системы управления базами данных (СУБД). Выбор СУБД имеет большое значение для создания баз данных (БД) и работы с ними.

В качестве СУБД для хранения персональных документальных данных предлагается использовать документно-ориентированную систему MongoDB. В настоящее время она занимает пятое место среди наиболее популярных СУБД по рейтингу издания DB-Engines (рис. 1) (https://db-

engines.com/en/ranking). Первый выпуск версии датируется 2009 годом американской компанией 10gen. Название MongoDB происходит от английского слова «humongous», что означает «огромный», подразумевая при этом способность системы к хранению больших объемов данных [1].

DB-Engines Ranking

The DB-Engines Ranking ranks database management systems according to their popularity. The ranking is updated monthly.

Read more about the method of calculating the scores.

trend chart

343 systems in ranking, February 2019

Rank			DBMS	Database Model	Score		
Feb 2019	Jan 2019	Feb 2018			Feb 2019	Jan 2019	Feb 2018
1.	1.	1.	Oracle	Relational, Multi-model	1264.02	-4.82	-39.26
2.	2.	2.	MySQL	Relational, Multi-model	1167.29	+13.02	-85.18
3.	3.	3.	Microsoft SQL Server	Relational, Multi-model	1040.05	-0.21	-81.98
4.	4.	4.	PostgreSQL	Relational, Multi-model	473.56	+7.45	+85.18
5.	5.	5.	MongoDB	Document	395.09	+7.91	+58.67

Рис. 1. Рейтинг СУБД в издании DB-Engines

Для обоснования выбора MongDB следует подробнее рассмотреть её технологические возможности. Как следует из названия «документно-ориентированная», эта СУБД предназначена для обработки информации, представленной в виде самодостаточной структуры – документа. Если проводить аналогии с реляционными СУБД, то документом в данном случае является строка таблицы, а коллекцией документов – сама таблица. Но поскольку в NoSQL СУБД отсутствуют связи между документами, то информация должна быть представлена в ненормализованной форме. MongoDB допускает также вложенность данных и поддерживает такую структуру, как «документ, вложенный в документ». В отличие от таблиц, структуры в MongoDB не требуют заранее строго определенной схемы. Эта особенность полезна, когда часто меняется схема и набор свойств данных. Необходимые атрибуты могут добавляться динамически по мере необходимости [2].

Следующей особенностью MongoDB является ее хорошая масштабируемость. MongoDB поддерживает горизонтальное масштабирование, заключающееся в способности фрагментации данных. При таком способе масштабирования все данные хранятся не централизованно, а делятся на части и размещаются на разных серверах. Фрагментация является особенно ценной с точки зрения производительности, так как она позволяет повысить скорость чтения и записи данных.

Если оценивать производительность системы, то считается, что MongoDB является довольно медленной на запись, но достаточно быстрой

на чтение. В целом MongoDB обеспечивает достаточно приемлемую производительность для обращения к персональным данным по сравнению, например, с такой известной реляционной СУБД, как PostgreSQL (занимает четвертое место в рейтинге на рис. 1). При этом, как показано на рис. 2, она значительно превосходит PostgreSQL по скорости вставки (*Insert*) данных [3].

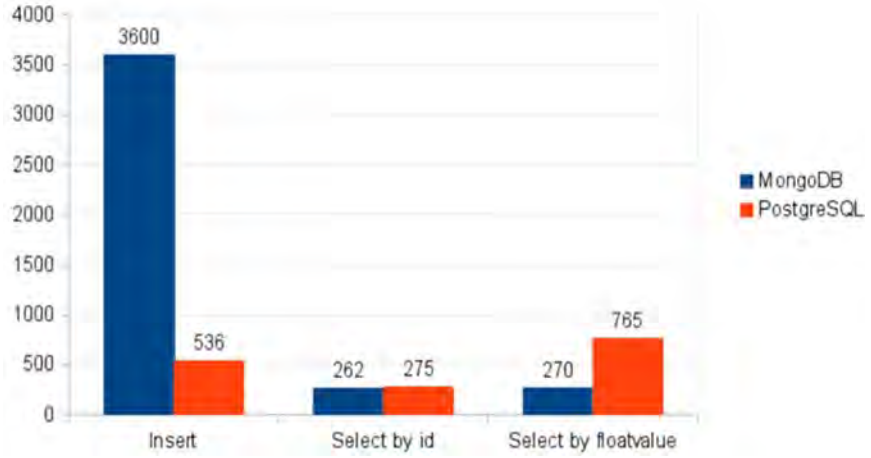


Рис. 2. Сравнительная оценка СУБД по скорости обработки данных

Одним из важных требований к СУБД является доступность данных во внешней памяти. Она определяется сохранностью информации, независящей от сбоев, и безотказностью работы системы в любых условиях. Основным средством обеспечения доступности баз данных MongoDB служит репликация. Высокий уровень доступности обеспечивается с помощью наборов реплик. Это набор состоит из двух или более узлов, участвующих в асинхронной горизонтальной репликации (*master-slave replication*). Узлы, входящий в набор реплик, выбирают ведущего, или главного, среди них. Несмотря на то, что все узлы имеют одинаковые права голоса, некоторые узлы могут оказаться предпочтительнее за счет близости к остальным серверам, большей оперативной памяти и других преимуществ [4].

MongoDB относится к классу NoSQL СУБД с открытым исходным кодом. В отличие от коммерческих в них используется схема лицензирования, дающая возможность бесплатно загружать продукт и открывающая доступ к его исходному коду. Так, установка MongoDB возможна с официального сайта, который предоставляет пакеты дистрибутивов для различных платформ. Каждой платформе доступно несколько дистрибутивов. Для работы с MongoDB имеется хороший выбор графических оболочек (например, графический клиент Robo 3T).

Наконец, очень важным вопросом является безопасность хранения данных. Безопасность БД считается ключевым фактором для любого приложе-

ния, которое включает в себя конфиденциальные данные. MongoDB предоставляет встроенное шифрование, которое не требует дополнительной оплаты за защиту персональных данных. Передача данных между MongoDB и серверным приложением осуществляется двумя способами: через безопасный протокол TLS транспортного уровня или через протокол защищенных сокетов SSL. Эти два протокола шифрования используются для защиты отправленных и полученных данных между двумя системами [5].

СУБД MongoDB подходит для решения многих задач, например, для области электронной коммерции. Приложения для электронной коммерции часто должны иметь гибкую схему товаров и заказов, а также возможность изменять свои модели данных без дорогостоящего рефакторинга базы данных или миграции данных.

Для сравнительной оценки СУБД MongoDB с реляционными системами по реализованным в них возможностям по представлению данных следует сравнить, каким образом создаются с помощью этих СУБД одни и те же базы данных. На рис. 3 показано, каким образом реализуется представление персональных данных в виде самодостаточной сущности в документально-ориентированной базе данных MongoDB, предназначенной для руководителя кадрового отдела. При этом используется формат JSON.

```
{
    "id": "1",
    "firstName": "Thomas",
    "lastName": "Andersen",
    "addresses": [
        {
            "line1": "100 Some Street",
            "line2": "Unit 1",
            "city": "Seattle",
            "state": "WA",
            "zip": 98012
        }
    ],
    "contactDetails": [
        {"email": "thomas@andersen.com"},
        {"phone": "+1 555 555-5555", "extension": 5555}
    ]
}
```

Рис. 3. Персональные данные в формате JSON для документной базы

Для сравнения на рис. 4 (см. ниже) показано, как эти данные, описывающие кадровый состав, представляются в схеме реляционной БД.

Получение всей записи человека из базы данных MongoDB обеспечивается одной операцией чтения, выполняемой для одной коллекции и отдельного документа. Обновление сведений о контактах и адресов в записи человека также обеспечивается одной операцией записи, выполняемой для одного документа. Благодаря денормализации данных приложение может использовать меньше запросов и обновлений для выполнения распространенных операций.

Таким образом, документно-ориентированная СУБД MongoDB хорошо поддается горизонтальному масштабированию, обеспечивает высокую эффективность хранения разносортных данных, не требует разработки схемы базы данных и обеспечивает более простой подход в разработке программного обеспечения. Эти достоинства СУБД MongoDB предоставляют для разработчиков и пользователей новые возможности для хранения и обработки персональных данных.

Рис. 4. Схема реляционной базы данных

Дальнейшие исследования планируется проводить в области практической реализации и экспериментальной оценки различных фрагментов персональных документно-ориентированных баз данных, выполненных в среде этой СУБД.

Список используемых источников

1.Онлайн-руководство по MongoDB [Электронный ресурс]. URL: https://metanit.com/nosql/mongodb (дата обращения 21.03.2019).

2. Садаладж П. Дж., Фаулер М. Новая методология разработки нереляционных баз данных : пер. с англ. М. : ООО «И. Д. Вильямс», 2013. 109 с.

3. Кузнецов С. Д., Посконин А. В. Системы управления данными категории NoSQL [Электронный ресурс]. URL: https://docviewer.yandex.ru/view/611794456 (дата обращения 21.03.2019).

4. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2 (25). С. 113–134.

5. Козлов А. NoSQL базы данных – преимущества и недостатки [Электронный ресурс]. URL: https://andy-blog.ru/nosql-bazy-dannyh-preimushhestva-i-nedostatki (дата обращения 21.03.2019).

УДК 654.021
ГРНТИ 49.33.29

ПРЕДЛОЖЕНИЯ ПО УПРАВЛЕНИЮ ПОТОКАМИ ДАННЫХ В ИНФОКОММУНИКАЦИОННОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ПОСРЕДСТВОМ ИНЖИНИРИНГА ТРАФИКА

Н. Н. Лебедева, С. М. Одоевский, В. П. Хоборова

Военная академия связи имени Маршала Советского Союза С. М. Буденного

Рассмотрены предложения по управлению потоками данных в инфокоммуникационной сети связи специального назначения с применением технологий инжиниринга трафика. Приведен пример моделирования сети связи, и показан эффект от перераспределения нагрузки на сеть с использованием программного комплекса ONEPLAN RPLS-DB TE

инжиниринг трафика, программный комплекс, потоки данных, канальный ресурс.

Современные инфокоммуникационные сети связи специального назначения отличаются необходимостью уметь обеспечивать требуемое качество связи при значительных текущих изменениях состояния сети и информационных потребностей абонентов. В настоящее время такую необходимость стремятся обеспечить новые технологии и протоколы, совместимые с популярными пакетными IP-сетями, которые предоставляют удобные механизмы динамического управления потоками данных (ПД) и которые принято называть инжинирингом трафика (*Traffic Engineering*, ТЕ). В узком смысле под инжинирингом трафика понимаются технологии, которые позволяют достичь сбалансированной загрузки всех ресурсов сети путем рационального выбора путей (маршрутов) прохождения потоков данных через сеть [1, 2].

Решением задач моделирования, анализа и оптимизации инфокоммуникационных сетей в наши дни занимаются многие компании разработчики программного обеспечения. Одной из таких отечественных компаний является компания «ИнфоТел» занимающаяся разработкой программного обеспечения по планированию и оптимизации для транспортных сетей, сетей связи операторов радиосвязи, широкополосного радиодоступа, эфирного телевизионного и радиовещания.

Программный комплекс ONEPLAN RPLS-DB позволяет выполнять распределенные расчеты и конфигурируется под потребности системы

управления с оптимальным использованием сетевых и аппаратных ресурсов.

Одним из автономных модулей ПК ONEPLAN RPLS-DB является модуль ONEPLAN RPLS-DB TE (*Traffic Engineering*) предназначенный для ведения базы данных учета потоков E1/IP, а также для анализа «слабых мест» (перегруженных участков) и поиска оптимальных маршрутов на транспортных сетях, формирования отчетов и служебных записок.

В статье рассматривается пример моделирования сети связи специального назначения с использованием данного модуля. Сеть с отмеченными значениями нагрузки (в процентах) на каждую линию при использовании кратчайших маршрутов (для передачи данных между всеми корреспондирующими парами узлов (КПУ), рассчитанных в программе NetSw [3] в соответствии с типовым протоколом маршрутизации RIP, показана на рис. 1.

При моделировании предполагалось, что рассматриваемая сеть построена на оборудовании SDH (NGSDH) с пропускной способностью линий c_r = 155 Мбит/с (STM-1/63E1/Eth100), $r \in [1, R]$, $R = 20$ (количество линий/ребер), $n \in [1, N]$, $N = 20$ (количество узлов/вершин) и $k = [1, K]$, $K = 34$ (количество КПУ), размер пакета 1,5 кбайт (12000 бит).

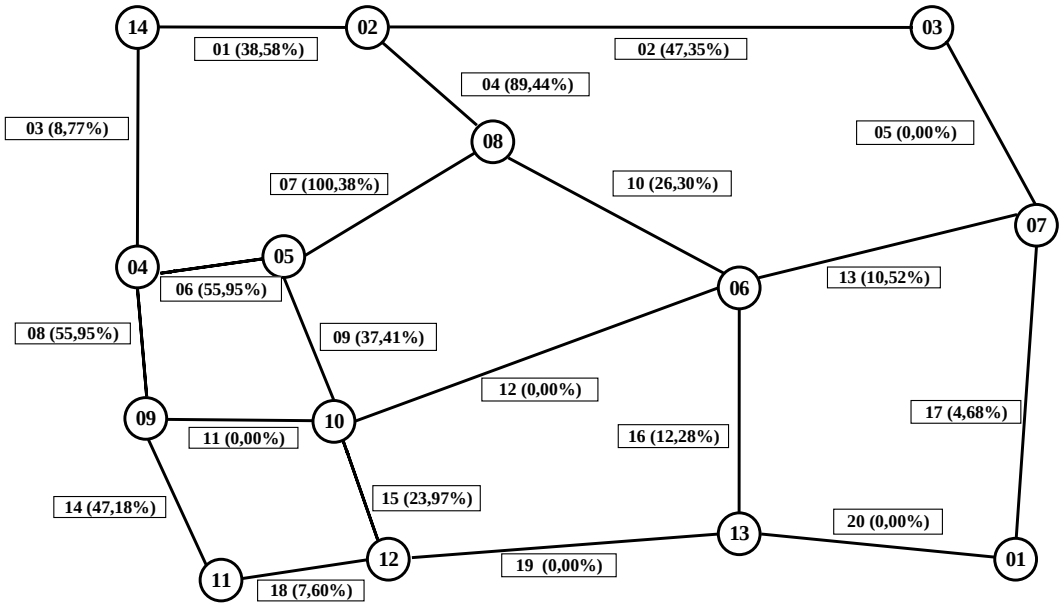


Рис. 1. Распределение нагрузки на ребра сети при использовании кратчайших маршрутов

Найденные кратчайшие маршруты, использованные для распределения ПД и повлиявшие на значения суммарной нагрузки в каждой линии, приведены в таблице. Нагрузка оценивалась по отношению к пропускной способности ребер (линий), равной суммарному канальному ресурсу

124,74 Мбит/с (63E1 при условии использования 1980 кбит/с из E1), с учетом дополнительной нагрузки от служебных полей протокольных блоков данных IP/MPLS/Ethernet (40 + 4 + 6 × 3) × 8 = 496 бит.

ТАБЛИЦА. Кратчайшие маршруты между КПУ

k	Маршрут (номера ОУС)	*k*	Маршрут (номера ОУС)
1	8 – 2 – 3	18	8 – 6 – 7 – 1
2	8 – 2 – 14	19	8 – 5 – 10 – 12
3	8 –5	20	8 – 5
4	8 – 5 – 4 – 9	21	8 – 5 – 10
5	8 – 6 – 7	22	8 – 6
6	8 – 5 – 10 – 12	23	8 – 5 – 4 – 9 – 11
7	8 – 6 – 13	24	8 – 5 – 10 – 12
8	8 – 5 – 10	25	8 – 8
9	8 – 5 – 4 – 9	26	8 – 2 – 14
10	8 – 5 – 10 – 12	27	8 – 5 – 4 – 9
11	8 – 6 – 13	28	8 – 5 – 10
12	8 – 5 – 10	29	8 – 6 – 7
13	8 – 2 – 3	30	8 – 6 – 13
14	8 – 2	31	8 – 6 – 7 – 1
15	8 – 6 – 13	32	14 – 4 – 5
16	8 – 5	33	14 – 4 – 9 – 11
17	8 – 2 – 14	34	11 – 12

Как видно из рис. 1 при распределении ПД в соответствии с кратчайшими маршрутами ребра сети оказываются загружены очень неравномерно. Например, ребро 7 загружено потоками данных, поступающими на узел 8, на 100,38 % (что фактически соответствует перегрузке), а другие ребра 4 и 10, через которые можно попасть в тот же узел 8, загружены лишь на 89,44 % и 26,30 %. Среди остальных ребер сети многие оказались вообще не загруженными (в частности, ребра 5, 11, 12, 19, 20).

С учетом использования механизмов инжиниринга трафика в программе ONEPLAN RPLS-DB TE было выполнено распределение ПД по нескольким маршрутам с целью более равномерного распределения нагрузки между ребрами сети. Результаты оптимизации распределения ПД представлены на рис. 2 в виде новых значений нагрузки на отдельные ребра сети. Как видно из рис. 2, теперь нагрузка распределена более равномерно.

В частности, три ребра, через которые поступает основная часть ПД на узел 8, загружены примерно одинаково на 71,64–72,86 %. Незагруженным осталось только одно ребро 20, задействовать которое из-за низкой нагрузки на соседние ребра оказалось нерационально.

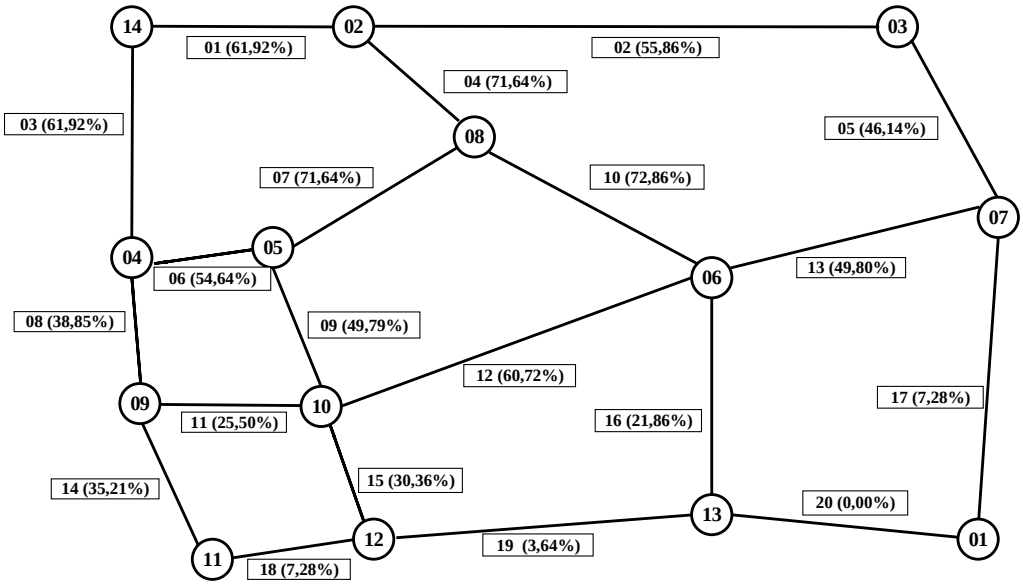


Рис. 2. Распределение нагрузки на ребра сети
после использования механизмов инжиниринга трафика

Вопросы перераспределения нагрузки и оптимальной маршрутизации являются острыми и актуальными в сфере военной связи. Исходя из проведенных исследований можно сделать вывод, что существуют отечественные программные комплексы, реализующие построение оптимальных маршрутов в инфокоммуникационных сетях связи специального назначения. В данной работе использовался ПК ONEPLAN RPLS-DB TE, применяющий механизмы инжиниринга трафика. Предложения по управлению потоками данных посредством ПК позволили повысить эффективность функционирования сети, проложив альтернативные маршруты, тем самым снизив нагрузку на всю сеть.

Список используемых источников

1. Rui Valadas Paulo Salvador. Traffic Management and Traffic Engineering for the Future Internet. First Euro-NFWorkshop, FITraMEn 2008. Porto, Portugal, December 2008.

2. Одоевский С. М., Кочешков А. К., Хоборова В. П. Оптимизация инжиниринга трафика на смежных уровнях сетевой архитектуры // Современное состояние и перспективы развития систем связи и РТО в управлении авиацией. VI МНТК : сб. науч. статей. Воронеж, 2017. С. 138–142.

3. Василевич Е. В., Одоевский С. М. Учебная информационная система моделирования телекоммуникационных сетей специального назначения (шифр NetSw). – Калининград: РГУ им. И. Канта, 2009. 47 с.

УДК 004.654
ГРНТИ 20.53.17

Приглашенный доклад

ОЦЕНКА КАЧЕСТВА ПОЛИТИК РАЗГРАНИЧЕНИЯ ДОСТУПА В ОБЛАЧНОМ ХРАНИЛИЩЕ, ОСНОВАННЫХ НА МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ ABAC

Д. С. Левшун[1,2], О. И. Пантюхин[3], И. Б. Саенко[1]

[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
[3]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Рассматривается проблема формирования политик разграничения доступа в облачном хранилище, основанных на модели управления доступом ABAC. Определены показатели качества политик разграничения доступа, характеризующих их свойства точности и целостности. Предложена методика оценки качества политик разграничения доступа в облачном хранилище на основе модели ABAC.

политика разграничения доступа, облачное хранилище, атрибут, оценка качества.

В настоящее время в критически важных инфраструктурах все чаще используются облачные хранилища. При этом заинтересованность злоумышленников в критически важных данных подобных систем обуславливает постоянный рост числа атак на них. Поэтому решение задач разграничения доступа, а также обнаружение и разрешение конфликтов в используемых ими политиках становится все более актуальным.

Оценка качества политик разграничения доступа в облачной инфраструктуре необходима для выявления необходимости принятия контрмер по противодействию возможным атакам на систему разграничения доступа. Как правило, эта оценка сводится к сопоставлению требуемой и результирующей схем разграничения доступа [1]. При этом требуемая схема разграничения доступа задается лицом, принимающим решения (ЛПР), а результирующая схема образуется на основании правил, свойственных выбранной модели контроля доступа.

В настоящей работе в качестве модели контроля доступа выбрана модель разграничения доступа на основе атрибутов ABAC (*Attribute-Based Access Control*). Данная модель контроля доступа представляет собой развитие моделей на основе списков доступа ACL (*Access Control List*) и на основе

ролей RBAC (*Role-Based Access Control*). Целью данной работы является выработка критериев оценки политик разграничения доступа в облачном хранилище, основанных на модели управления доступом ABAC.

В отличие от RBAC, в ABAC разграничение доступа пользователей обеспечивается атрибутами, а не ролями. Атрибуты, участвующие в формировании условий доступа, сгруппированы в три категории:

1) атрибуты субъектов доступа,

2) атрибуты информационных ресурсов,

3) атрибуты окружающей среды [2, 3].

Значения этих атрибутов участвуют в формировании правил, на основании которых принимается решение на разрешение или запрет доступа. Операции доступа относятся к информационным ресурсам и их атрибутам. В результате ABAC позволяет строить более гибкие схемы доступа, чем RBAC, которые отличаются способностью хорошо адаптироваться к высокой динамике изменения политики безопасности, свойственной облачным хранилищам [4].

Как в модели RBAC, так и в модели ABAC существует проблема формирования схемы разграничения доступа. Пусть даны множество пользователей (U), ресурсов (R) и операций (O), которые пользователи могут выполнять над ресурсами. Атрибуты разделяются на два типа – для пользователей (A_u) и ресурсов (A_r). Атрибут a пользователя или ресурс x может иметь пустое значение или множество значений из своего домена D_a. Это значение обозначается с помощью отношения $d(x, a)$. Правило $<e; o>$ в модели ABAC задается выражением, которое определяет условие применимости и выполняемое действие. Например, правило

$$\left\langle роль \in \{\text{'доктор'}, \text{'сестра'}\} \wedge ресурс \in \{ЗаписиПациента\}, read \right\rangle \qquad (1)$$

определяет, что только доктора или медицинские сестры имеют право читать записи о пациентах.

Проблема нахождения политики (схемы) разграничения доступа в модели ABAC формулируется следующим образом. Пусть имеются журнал событий L, состоящий из записей вида $<u, r, o, t>$, обозначающих тот факт, что пользователь u выполняет действие o над ресурсом r в момент времени t, пользователи U, ресурсы R, операции O, атрибуты A и отношение назначения атрибутов d. Тогда проблема нахождения (извлечения) политики ABAC определяется как поиск такой политики, которая максимизирует ее показатель качества [5].

Из этого определения следует вывод, что результат решения сформулированной выше проблемы во многом зависит от того, какие показатели выбраны для оценки качества политики. Чтобы определить эти показатели, необходимо в первую очередь выделить свойства, характеризующие политику ABAC. В [6] предлагается учитывать следующие основные свойства

политики: точность (*accuracy*), целостность (*integrity*) и доступность (*availability*). Точность определяет степень семантически и синтаксически правильного использования атрибутов и гарантирует, что атрибуты основаны на доверительных процессах измерения и отчетности. Целостность учитывает использование различных стандартов и протоколов безопасного распределения атрибутов между системами, позволяющих избежать нарушения целостности и конфиденциальности атрибутов. Доступность гарантирует, что обновление и поиск атрибутов обеспечивается своевременными действиями пользователя, который пользуется соответствующими атрибутами. Кроме того, учитывается отказоустойчивость и восстанавливаемость облачного хранилища. Некоторые атрибуты могут изменяться периодически или со временем. Так как доступность во многом определяется качеством хранилища, следует ограничиться рассмотрением первых двух свойств.

Для определения показателя, позволяющего оценить точность, представляется целесообразным использование универсальной матричной модели ABAC, предложенной в [7]. Матричная модель определяет матрицу доступа, в которой каждый ряд представляется парой, состоящей из субъекта и множества его атрибутов (S_i, $ATTS(S_i)$). Каждый столбец представляется парой, состоящей из объекта и множества его атрибутов (O_j, $ATTS(O_j)$). Тогда каждая ячейка ($[S_i : O_j]$) соответствует множеству прав доступа, которые субъект S_i может выполнять над объектом O_j, полагая, что выполняются условия некоторых политик доступа. Операция может быть выполнена субъектом над объектом только тогда, когда соответствующие права доступа, требуемые операцией, найдены в матрице доступа и атрибуты субъекта и объекта удовлетворяют множеству политик над операцией.

Пусть матрица доступа, задаваемая универсальной матричной моделью ABAC, обозначена как $\mathbf{M}_{\text{ABAC}}$, а матрица доступа, формируемая ЛПР, как $\mathbf{M}_{\text{ЛПР}}$. В ячейках матрицы $\mathbf{M}_{\text{ЛПР}}$ находятся права доступа субъектов по отношению к объектам, которые желает иметь ЛПР. Тогда в качестве показателя точности политики ABAC можно использовать

$$\Pi_{\text{ACC}} = \left|\mathbf{M}_{\text{ЛПР}} - \mathbf{M}_{\text{ABAC}}\right|, \qquad (2)$$

где операция $|\cdot|$ обозначает количество ненулевых ячеек в матрице.

Для определения показателя целостности можно воспользоваться подходом, согласно которому в качестве такового предлагается использовать взвешенную структурную сложность [8]. В этом показателе логические условия и операции в правилах снабжаются весами. В результате сложность правила $<e; o>$, имеющего вид (1), вычисляется как $WSC(e) + WSC(o)$, где WSC – вес логического условия e или операции o, определяемый как количество содержащихся в них атомарных элементов. Итоговый показатель целостности формулируется как сумма всех этих элементов:

$$\Pi_{\text{INT}} = \sum \left(WSC(e) + WSC(o) \right). \quad (3)$$

Предложенные показатели позволяют предложить следующую методику оценки качества политик разграничения доступа.

Шаг 1. Цикл по всем правилам, составляющим политику ABAC, и определение весовых коэффициентов для логических условий и операций. Вычисление итогового показателя целостности Π_{INT} в соответствии с (3).

Шаг 2. Преобразование политик ABAC в матрицу доступа $\mathbf{M}_{\text{ABAC}}$, соответствующую универсальной матричной модели ABAC. Данное преобразование также выполняется в цикле, организованном на шаге 1. Анализируется каждое правило, входящее в политику ABAC. Из правил извлекается информация об атрибутах субъектов и объектов и правах доступа субъектов над объектами. Эта информация помещается в соответствующие ячейки матрицы доступа $\mathbf{M}_{\text{ABAC}}$.

Шаг 3. Вычисление показателя точности Π_{ACC} в соответствии с (2). При этом полагается, что матрица $\mathbf{M}_{\text{ЛПР}}$ является априори заданной.

Предложенная методика позволяет оценить не только качество политик разграничения доступа, но и в целом безопасность ресурсов, содержащихся в облачном хранилище. Если в результате проведенной оценки показатель точности оказался больше нуля, то это сигнализирует о возможности реализации несанкционированного доступа (НСД) к облачным ресурсам, причем, чем выше показатель, тем выше вероятность НСД. Кроме того, этот факт может сигнализировать о возможности наличия противоречий в правилах политики доступа и необходимости верификации последней. Исследования в области верификации политик ABAC составляют направление дальнейших исследований.

Работа выполнена при финансовой поддержке проекта РФФИ № 18-07-01369 и частичной поддержке бюджетной темы № АААА-А16-116033110102-5.

Список используемых источников

1. Kotenko I., Saenko I. Improved genetic algorithms for solving the optimisation tasks for design of access control schemes in computer networks // International Journal of Bio-Inspired Computation. 2015. Vol. 7. No. 2. PP. 98–110.

2. Paci F., Squicciarini A., Zannone N. Survey on Access Control for Community-Centered Collaborative Systems // ACM Comput. Surv. 2018. Vol. 51, No. 1, Article 6, 38 pages.

3. Servos D., Osborn S.L. Current Research and Open Problems in Attribute-Based Access Control // ACM Comput. Surv. 2017. Vol. 49, No. 4, Article 65, 45 pages.

4. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. № 2 (25). С. 113–134.

5. Mocanu D. C., Turkmen F., Liotta A. Towards ABAC Policy Mining from Logs with Deep Learning // Proceedings of the 18th International Multiconference IS2015, 2015, pp. 124–128.

6. Hu V. C., Kuhn D. R., Ferraiolo D. F., Voas J. Attribute-Based Access Control // Computer, 2015, Vol. 48, Issue 2, pp. 85–88.

7. Zhang X., Li Y., Nalla D. 2005. An Attribute-Based Access Matrix Model // Proceedings of the 2005 ACM Symposium on Applied Computing. 2005, pp. 359–363.

8. Molloy I., Park Y., Chari S. Generative models for access control policies: applications to role mining over logs with attribution // Proceedings of the 17th Symposium on Access Control Models and Technologies (SACMAT), 2012, pp. 45–56.

УДК 004; 621.398
ГРНТИ 81.93.29

РАСПОЗНАВАНИЕ ВТОРЖЕНИЙ НАРУШИТЕЛЯ ПРИ УПРАВЛЕНИИ КИБЕРБЕЗОПАСНОСТЬЮ ИНФРАСТРУКТУРЫ ИНТЕГРИРОВАННОЙ ОРГАНИЗАЦИИ НА ОСНОВЕ НЕЙРО-НЕЧЕТКИХ СЕТЕЙ И КОГНИТИВНОГО МОДЕЛИРОВАНИЯ

В. А. Липатников, В. А. Тихонов

Военная академия связи имени Маршала Советского Союза С. М. Будённого

Способ управления кибербезопасностью инфраструктуры интегрированной организации с распознаванием вторжений и анализом динамики действий нарушителя на основе нейро-нечетких сетей и когнитивного моделирования. Функции алгоритма управления: наблюдение и выделение признаков цифровых потоков с протоколами передачи данных, поступающих в информационную сеть и распознавание вторжения, выбор и реализация способа защиты.

инфраструктура интегрированной организации, защита информации; нейро-нечеткие сети, когнитивное моделирование.

Целью кибербезопасности (КБ) является организация безопасности киберсреды, системы относящейся ко многим интегрированным организациям (ИО), использующим разнообразные компоненты и разные подходы к обеспечению безопасности. Для достижения цели необходимы механизмы управления КБ соответствующие быстро изменяющимся угрозам киберсреды и способные осуществлять проактивное управление. В целях по-

вышения эффективности обеспечения КБ инфраструктуры ИО за счет сокращения времени анализа динамики действий нарушителя предложен алгоритм прогнозирования на основе нейро-нечетких сетей и когнитивного моделирования

В [1] рассмотрен метод обеспечения КБ инфраструктуры с использованием модели прогнозирования временных рядов. Для управления КБ ИО предлагается внедрение распределенной интеллектуальной агентной системы обнаружения вторжений (АСОВ). Система является комплексной, состоящей из множества модулей, обеспечивающих повышение защищенности киберсреды ИО. Одним из процессов модуля прогнозирования АСОВ является процесс анализа данных на основе нейро-нечетких сетей и когнитивного моделирования. Для реализации процесса выбрана модулярная гибридная система прогнозирования временных рядов (МГСПВР), подробно описанная в работе [3]. Структурная схема МГСПВР представлена на рис. 1.

Рис. 1. Структурная схема модулярной системы прогнозирования временных рядов

Данная система за счет модулярности обладает дополнительной устойчивостью – даже если одних из составных модулей выходит из строя остальные продолжают выполнять свою работу. В основе лежат три основных модуля осуществляющих задачу прогнозирования: нейро-нечеткая сеть (ННС), нечеткая когнитивная карта (НКК) и нейронная сеть (НС), осуществляющая итоговый прогноз. В системе происходит параллельная обработка поступившей информации на гибридной ННС и НКК, что повышает как количественные, так и качественные характеристики, при этом результаты работы данных блоков проходят через этап верификации, подтверждающий адекватность прогноза. Оконечный блок, реализованный НС, выдает

результат прогноза, поступающий на вход внешних процессов модуля принятия решений нижнего уровня, модуля хранения данных и модуля оценки состояния защищенности ИС и внутренний процесс оценки прогноза.

Гибридная ННС, входящая в состав МГСПВР, представляет собой совокупность древовидного классификатора и карты Кохонена – рис. 2. С её помощью происходит анализ событий, происходящих в информационной инфраструктуре ИО, выявление и классификация возможных кибератак. Результатом работы гибридной ННС является количественные характеристики временного ряда – вероятность реализации прогноза. Подобная модель ранее успешно использовалась в работе [3] для обнаружения аномалий в сетевом трафике, но при этом в ней не учитывались качественные показатели прогнозирования.

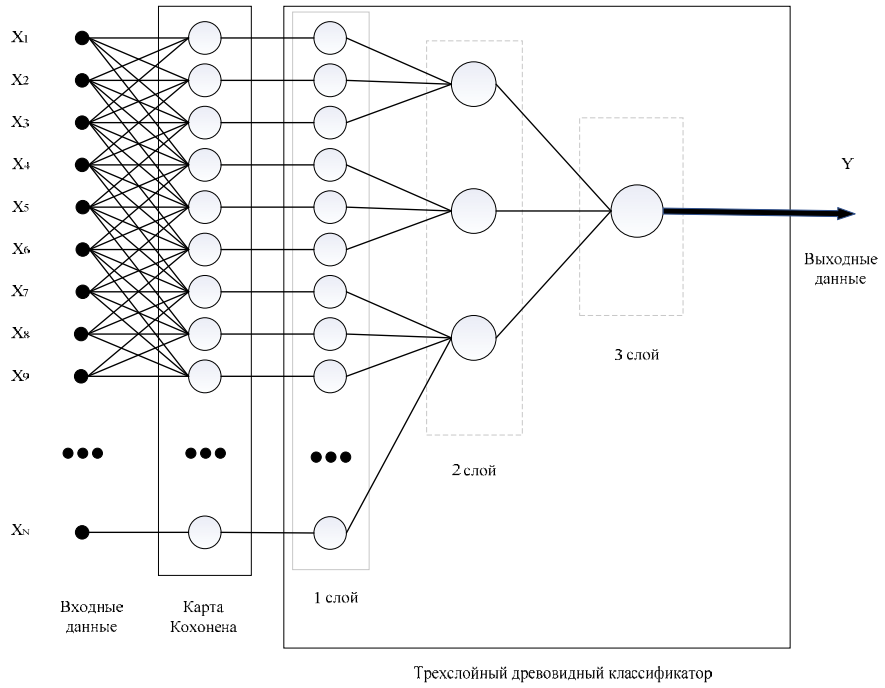


Рис. 2. Обобщенная схема модели обнаружения аномальных отклонений на основе нейронной сети

Для повышения качественной составляющей прогноза и определения наиболее вероятного графа атаки предлагается использовать нечеткие когнитивные карты. Нечеткая КК на рис. 3 представляет собой направленный и ориентированный граф, в котором ключевые факторы объекта представлены как вершины графа и называются концептами. Граф описывается {*Cij*,*Lij*,*Wij*}, где *Cij* – концепты, *Lij* – дуги графа, *Wij* – множество весовых коэффициентов, описывающих дуги графа.

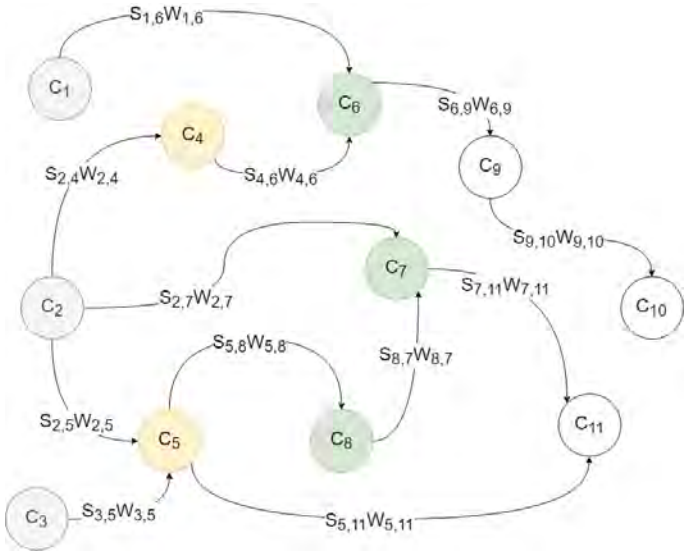


Рис. 3. Когнитивная карта, отображающая динамику ситуации с распознаванием вторжений и анализом действий нарушителя

Дуги графа являются причинно-следственными связями между вершинами и отображают влияние изменения одного фактора на другие. Связи с положительными знаками отображают, что при возрастании или убывании параметров, описывающих один концепт, параметры связанного с ним концепта так же возрастают или убывают. При отрицательных связях возрастание или убывании параметров одного концепта говорит об убывании или возрастании параметров связанного с ним концепта. Вес связи *Wij* определяет степень взаимного влияния между концептами.

В нечетких КК в отличие от обычных когнитивных картиспользуется теория нечетких множеств, описанная Лотфи Заде в 1965 г. Теория нечетких множеств позволяет использовать лингвистическую информацию в математических моделях. В НКК концепты представляют собой нечеткие переменные описывающие параметры фактора. Связи так же задаются в лингвистическом виде: «Сильно», «Среднее», «Мало».

Множество концептов *Cij* следует разделить на подмножества концептов, объединенных по описываемым свойствам системы. В соответствии с [4] угроза КБ определяется как совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. При этом безопасность информации – это состояние защищенности информации, при котором обеспечивается конфиденциальность целостность и доступность. Таким образом, целевыми концептами являются свойства информации – конфиденциальность, целостность и доступность, за дестабилизирующие концепты принимаются угрозы КБ. Под базовыми концептами предлагается использовать следующие совокупности переменных:

– описывающих состояние телекоммуникационной системы – текущие показатели параметров и настройки оборудования;

– описывающих состояние системы защиты информации – текущие показатели параметров и настройки средств защиты информации;

– уязвимости, существующие в информационной системе.

Подобное объединение концептов позволяет прогнозировать векторы атак отображающие действия нарушителя, объекты информационной системы на которые происходит КВ и результаты возможной реализации таких воздействий. В совокупности данная информация является качественной составляющей прогноза, что повышает эффективность и точность принятия решений. Для построения КК, отражающей динамику ситуации необходимо определить шкалы значений концептов и их приращений. Задача прогноза сводится к макстриангулярной композиции матрицы весов ивектора начальных приращений признаков и вычисляется по методу описанном в [4]. В качестве третьей составляющей МГСПВР используется сеть Хэмминга, представляющая собой совокупность нейронов из двух слоёв, имеющих по m нейронов, где *m* – число образцов. Нейроны первого слоя соединены со входами сети синапсами и образуют фиктивный нулевой слой. Нейроны второго слоя соединены между собой отрицательными обратными связями, единственная положительная обратная связь для каждого нейрона установлена со входом этого же нейрона рисунок. Модель НС реализует алгоритм поиска расстояния Хэмминга от поступившего входного сигнала до всех образцов и последующего выбора образца с минимальным расстоянием Хэмминга до неизвестного входного сигнала, в результате чего будет активизирован только один выход сети (рис. 4).

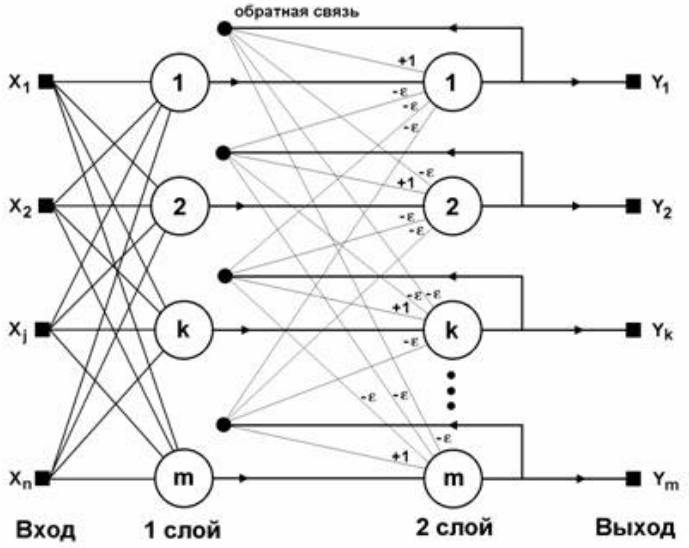


Рис. 4. Структурная схема поиска расстояния Хэмминга от поступившего входного сигнала до всех образцов

Найденное минимальное расстояние Хэмминга и выбор соответствующего ему образца, позволяет повысить точность прогнозирования, качество анализа действий нарушителя и осуществить итоговый прогноз развития атаки.

Практическая значимость заключается в том, что предложенный подход позволяет обеспечить КБ защищаемой инфраструктуры ИО на основе использования модели прогнозирования событий. Данные о событиях безопасности формируются на уровне инфраструктуры, подлежат предварительной обработке на уровне данных, распространяются с помощью уровня событий к требуемым элементам прикладного уровня и, в конечном итоге, окончательно обрабатываются элементами этого последнего уровня.

В отличие от [5, 6, 7] представлен способ распознавания вторжений нарушителя при управлении КБ инфраструктуры ИО на основе нейро-нечетких сетей и когнитивного моделирования. Применено использование модифицированных адаптационных алгоритмов. Разработаны модули модулярной системы прогнозирования временных рядов, реализующие алгоритм функционирования АСОВ.

Список используемых источников

1. Костарев С. В., Липатников В. А. Анализ состояния и динамики качества объектов автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2015. № 3 (89). С. 52–64.

2. Korshunov G. I., Lipatnikov V. A., Shevchenko A. A. Decision support systems for information protection in the management of the information network // Fuzzy Technologies in the Industry. FTI 2018. 23–25 October, 2018. Ulyanovsk (Russia). pp. 418–426.

3. Ярушева С. А., Аверкина А. Н., Федотова А. В. Модулярная модель прогнозирования временных рядов на основе нейро-нечетких сетей и когнитивного моделирования // Нечеткие системы и мягкие вычисления. 2017. Т. 12, № 2. С. 159–168.

4. Коршунов Г. И., Липатников В. А., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя // Информационно-управляющие системы. 2018. № 4. С. 61–72. doi:10.31799/1684-8853-2018-4-61-72.

5. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. Вып. 2 (45). С. 207–243.

6. Ivo Batina. Model predictive control for stochastic systems by randomized algorithms – Eindhoven: TechnischeUniversiteit Eindhoven, 2004.

7. E. Byres, J. Lowe. The myths and facts behind cyber security risk for industrial control systems // In ISA Process Control Conference, 2003.

УДК 004.421
ГРНТИ 49.33.29

АЛГОРИТМ УСТРАНЕНИЯ ПЕТЕЛЬ В СЕТИ ТАКТОВОЙ СЕТЕВОЙ СИНХРОНИЗАЦИИ

М. В. Лобастова, А. Ю. Матюхин

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

В статье рассматриваются вопросы организации тактовой сетевой синхронизации в сетях следующего поколения. Обосновывается использование технологии OTN для организации транспортной сети. Приводится описание метода обнаружения петель в сети синхронизации и текст кода программы для его реализации.

сети 5G, транспортные сети, технология OTN, тактовая сетевая синхронизация.

Сегодня отрасль телекоммуникаций стоит на пороге внедрения сетей мобильной связи пятого поколения. Ожидается, что в сети 5G значительно увеличится трафик за счет развития такого перспективного направления как интернет вещей. Эксперты считают, что скорость передачи данных увеличится до 10 Гбит/с, минимальная задержка не будет превышать 1 мс [1], максимальная плотность подключенных к сети устройств в городских условиях будет достигать 1 миллиона устройств/км^2, при этом должна обеспечиваться мобильность при скорости передвижения до 500 км/ч.

Несмотря на то, что еще не утверждены стандарты для сетей пятого поколения, ведущими производителями сформированы основные требования, предъявляемые к транспортному оборудованию независимо от топологии сети.

В первую очередь, транспортное оборудование должно быть «прозрачным» для всех клиентских сервисов. Эта прозрачность обеспечивается достаточной пропускной способностью, сохранением синхронизации фазы и времени, информация о которых содержится в клиентских сигналах, а также минимально вносимой задержкой.

Кроме того, необходимо учитывать, что внедрение сетей 5G будет происходить эволюционно, а это значит, что сеть должна включать в себя и низкоскоростные сервисы предыдущих поколений мобильной связи.

Одной из технологий, которая удовлетворяет предъявляемым требованиям, является технология OTN (*Optical Transport Network*). OTN позволяет объединить каналы различного типа, от устаревших протоколов до новей-

ших стандартов, через единый транспорт. Кроме того, технология OTN позволит интегрировать в оптическую сеть и новейшие протоколы и стандарты, которые еще не появились.

В качестве перспективного направления развития технологии OTN/OTH по ряду оценок принято считать разработку средств наноэлектроники и нанофотоники, стандартов ITU-T и т. д. для получения скоростных режимов передачи в одном спектральном канале 400 Гбит/с и 1 Тбит/с [2].

Одним из важных вопросов при построении сети связи с использованием технологии OTN является доставка сигналов синхронизации фазы и времени по сети OTN. Сеть синхронизации для 5G будет иметь распределенную систему. Носителем синхросигнала в OTN является сигнал OTUk (*Optical channel Payload Unit-k* – комплексно стандартизированный блок OPU уровня *k*, где $k = 1, 2, 3, 4$).

При построении сети синхронизации иерархия генераторов имеет три уровня: первый или высший уровень иерархии с первичным эталонным источником (ПЭИ); второй уровень, который задают вторичные задающие генераторы (ВЗГ); третий уровень, который задают генераторы сетевых элементов (ГСЭ).

Важным требованием при построении сети синхронизации является наличие альтернативных источников синхросигнала. При переключении с основного источника синхронизации на резервный также не должны образовываться петли синхронизации [3]. Сеть синхронизации описывается графом, в соответствие которому может быть поставлена матрица смежности.

Для обнаружения петель в сети синхронизации можно использовать метод, основанный на вычеркивании нулевых строк и столбцов матрицы смежности графа сети синхронизации.

В матрице смежности единицами обозначается наличие связей (основных и резервных) между узлами сети синхронизации, нулями – их отсутствие. Если какой-либо узел не синхронизирует ни один другой узел, ему будет соответствовать нулевая строка в матрице смежности. Если в матрице смежности есть нулевой столбец, значит, соответствующий этому столбцу узел не получает сигнал синхронизации от других узлов [4]. Следовательно, узлы, которым соответствуют нулевые строки и столбцы матрицы смежности, не участвуют в петлях синхронизации, и их из графа можно удалить.

Данный алгоритм можно описать следующим образом.

1. Для сети синхронизации строится направленный граф, в котором стрелками указываются возможные направления передачи синхросигнала в сети.

2. По графу составляется матрицу смежности.

3. Если в матрице присутствует нулевая строка или столбец, то данная строка вычеркивается с соответствующим ей столбцом, и наоборот.

4. Пункт 3 данного алгоритма повторяется до тех пор, пока не получится матрица без нулевых строк и столбцов.

5. Анализируя конечную матрицу, можно сделать вывод об отсутствии или наличии петель в сети.

Данный алгоритм был реализован с использованием программного обеспечения Mathcad.

Программа производит расчёты для сети, содержащей *n* узлов. Матрица смежности задается вручную. Для расчёта векторов весовых коэффициентов необходимо сформировать единичный вектор, размерности *n*. В программе это выполнено следующим образом:

$$B := (0A + 1)^{\langle 0 \rangle},$$

где A – матрица смежности графа сети, B – единичный вектор-столбец размерности n.

Выражение $A^{<0>}$ означает, что берется нулевой столбец вектора A, далее он обнуляется и к каждому его значению добавляется единица.

Далее рассчитываются векторы весовых коэффициентов. Для расчета вектора – столбца используется выражение:

$$Q := A \cdot B.$$

Для расчета вектора – строки используется следующее выражение:

$$D := D^T \cdot A.$$

Для определения номеров нулевых элементов вектора – столбца весовых коэффициентов используется цикл *for*. Цикл выполняется для элементов вектора - столбца весовых коэффициентов Q от 0 до Q–1. В программе имеется возвращаемая переменная *arg*, которая вначале обнуляется. А далее каждый из элементов вектора Q сравнивается с нулем. В том случае, когда некоторый элемент k вектора Q равен 0, номер этого элемента добавляется в вектор p (рис. 1).

```
p := | arg ← 0
     | for k ∈ 0.. rows (Q) − 1
     |   arg ← stack (arg , k + 1)  if (Q)_k = 0
     | submatrix (arg , 1, rows (arg) − 1, 0, 0) − 1
```

Рис. 1. Расчет вектора-столбца весовых коэффициентов

Для определения номеров нулевых элементов вектора - строки весовых коэффициентов так же используется цикл *for* (рис. 2).

Цикл выполняется для транспонированного вектора D от 0 до D^T–1. Если элемент вектора $D = 0$, то номер элемента этого вектора добавляется в вектор z.

```
z := | arg ← 0
     | for i ∈ 0.. rows(D^T) − 1
     |   arg ← stack(arg, i + 1) if (D^T)_i = 0
     | submatrix(arg, 1, rows(arg) − 1, 0, 0) − 1
```

Рис. 2. Расчет вектора-строки весовых коэффициентов

Для определения номеров всех нулевых строк и столбцов матрицы A необходимо объединить векторы p и z. В программе mathcad формируется вектор U из векторов p и z:

$$U := csort(stack(p, z), 0).$$

Вычеркивание строк и столбцов происходит в два этапа. Вначале производится вычёркивание нулевых столбцов, также с помощью цикла и операторов *for* и *if* (рис. 3).

```
S := | M ← 0·A^⟨0⟩
     | for i ∈ 0.. cols(A) − 1
     |   | Arg ← 0
     |   | for k ∈ 0.. rows(U) − 1
     |   |   | Arg ← Arg + 0 if i ≠ U_k
     |   |   | Arg ← Arg + 1 if i = U_k
     |   | M ← augment[M, (A)^⟨i⟩] if Arg = 0
     |   | M ← M if Arg = 1
     | submatrix(M, 0, rows(M) − 1, 1, cols(M) − 1)
```

Рис. 3. Вычеркивание нулевых столбцов в матрице смежности

В начале цикла обозначается возвращаемая переменная M которая представляет собой нулевой столбец размерности n. Данный столбец получен умножением нулевого столбца вектора A на 0. Цикл выполняется для столбцов матрицы A от нулевого до $n – 1$. Внутри этого цикла есть еще один цикл, который сравнивает номера столбцов матрицы A с элементами вектора весовых коэффициентов U. Этот цикл выполняется для всех элементов вектора U. В том случае, если номер столбца матрицы A не равен значению элемента вектора U, то данный столбец матрицы A добавляется

слева в матрицу *S*. В том случае, если номер столбца матрицы *A* равен значению элемента вектора *U*, то данный столбец матрицы *A*, не добавляется к матрице *S*, а расчет проводится для следующего столбца *A*.

Аналогичным образом построена программа для вычеркивания нулевых строк (рис. 4). Но вычеркивание будет производиться не для матрицы *A*, а для транспонированной матрицы *S*, полученной после вычеркивания нулевых столбцов из матрицы *A*.

$$
\begin{aligned}
S1 := \;& M \leftarrow 0 \cdot A1^{\langle 0 \rangle} \\
& \text{for } i \in 0..\text{cols}(A1) - 1 \\
& \quad Arg \leftarrow 0 \\
& \quad \text{for } k \in 0..\text{rows}(U) - 1 \\
& \quad\quad Arg \leftarrow Arg + 0 \;\text{ if }\; i \neq U_k \\
& \quad\quad Arg \leftarrow Arg + 1 \;\text{ if }\; i = U_k \\
& \quad M \leftarrow \text{augment}\left(M, A1^{\langle i \rangle}\right) \;\text{ if }\; Arg = 0 \\
& \quad M \leftarrow M \;\text{ if }\; Arg = 1 \\
& (\text{submatrix}(M, 0, \text{rows}(M) - 1, 1, \text{cols}(M) - 1))^{T}
\end{aligned}
$$

Рис. 4. Вычеркивание нулевых строк в матрице смежности

В результате выводится матрица *S1*, полученная вычёркиванием нулевых строк и столбцов матрицы *A*.

Если в матрице *S*1 появились новые нулевые строки или столбцы, то вычеркивание производится еще раз. Если же в матрице *S*1, нулевых строк и столбцов нет, то в сети есть петли с участием оставшихся после вычеркивания узлов. Судить о конфигурации петель по полученной матрице невозможно. Для устранения петель в сети синхронизации достаточно из каждой петли удалить по одному ребру.

Как показано в [4], данный метод позволяет снизить вычислительную сложность в n^2 раз. Проведение экспериментов с использованием разработанного программного обеспечения позволило убедиться в правильности полученной ранее оценки снижения вычислительной сложности.

Список используемых источников

1. Бородин А. С., Кучерявый А. Е. Сети связи пятого поколения как основа цифровой экономики // Электросвязь. 2017. № 5. С. 45–49.

2. Фокин В. Г. Когерентные оптические сети : учебное пособие / Сибирский государственный университет телекоммуникаций и информатики; каф. многоканальной электросвязи и оптических систем. Новосибирск, 2015. 372 с.

3. Лобастова М. В. Метод обнаружения замкнутых петель в сети синхронизации // Электросвязь. 2019. № 1. С. 29–32.

4. Лобастова М. В., Матюхин А. Ю. Аналитическое описание метода обнаружения замкнутых петель в сетях тактовой сетевой синхронизации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2018. С. 574–577.

УДК 004.522
ГРНТИ 49.33.29

VOICE ASSISTANT КАК ИНТЕРФЕЙС К СИСТЕМАМ УПРАВЛЕНИЯ ИНФРАСТРУКТУРОЙ 5G/IMT-2020

М. А. Маколкина, Н. А. Шыпота

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

Статья посвящена изучению проблем повышения эффективности работы с оборудованием при использования голосового помощника. Раскрыты основные особенности технологии управления системами голосом. Проанализированы позитивные и негативные аспекты внедрения голосового помощника. Приведено описание возможных случаев его применения.

инфраструктура 5G/IMT-2020, Voice Assistant , NFV, SDN.

Введение

Исследование проблем сетевой индустрии приобретает все большую актуальность. Потребность в инновационном подходе к развитию управления инфокоммуникационной инфраструктурой вызвана необходимостью в повышении эффективности профессиональной деятельности с использованием информационных приложений.

Сети связи пятого поколения или сети IMT-2020, согласно рекомендациям МСЭ-Т с точки зрения сетевых технологий, должны строиться на основе SDN/NFV технологий. Данные технологии позволяют абстрагироваться от уровня передачи данных (*Data Plane*) и оперировать уже так называемыми сущностями и объемами ресурсов. Управление при данном подходе реализуется как ряд приложений, работающих поверх северного интерфейса контроллера и оркестратора сети. В том числе, интеграция с уже имеющимися системами управления также происходит на данном уровне. Данный подход позволит разрешить вышеуказанные противоречия. В том числе предоставляет новые возможности взаимодействия в модели

«администратор-инфраструктура». Развитие технологий по усовершенствованию интерфейсов взаимодействия «человек-машина» в последнее время внесли в нашу жизнь новые возможности, например – голосовой помощник (*Voice Assistant*, VA). VA имеет большое значение в развитии человеко-компьютерного взаимодействия и ее определяющую роль на пути к следующей парадигме пользовательского интерфейса.

Постановка проблемы

Стоит отметить возникшее противоречие между существующим потенциалом автоматизации управления сетями, необходимостью повышения эффективности и мобильности их управления и недостаточной динамичностью, возможностями к оперативной адаптации и гибкостью активно действующих сервисов. Эффективная реализация их потенциала обеспечивается вычислительными возможностями и позволяет стабильно работать в условиях гипернагрузок [1].

В свою очередь, Voice Assistant имеет большое значение в развитии человеко-компьютерного взаимодействия и ее определяющую роль на пути к следующей парадигме пользовательского интерфейса. И использование VA в задачах инжиниринга систем позволит иначе посмотреть на процессы взаимодействия с инфраструктурой, в том числе оптимизировать OPEX. Однако, для обеспечения стабильности, безопасности данного решения существует ряд исследовательских задач, необходимых к рассмотрению.

Инфраструктурные технологии 5G/IMT-2020. SDN/NFV

В качестве сетевых технологий Международный Союз Электросвязи предлагает в рекомендации ITU-R M.2083-0 в качестве технологий сетевой инфраструктуры использовать работающие совместно такие технологии, как: Software-defined Networking (SDN)/Network Function Virtualization (NFV). Согласно концепций SDN/NFV, традиционное администрирование сети уже переходит в программную плоскость. Человек «отдаляется» от непосредственного конфигурирования систем. Системы управления с использованием программно-конфигурируемых сетей (SDN) могут содействовать решению вышеназванного противоречия.

Работа SDN с использованием разделенных плоскостей – плоскости управления и плоскости данных, делает ее незаменимой при модернизации архитектуры системы интегрированных информационных ресурсов.

В настоящее время попытки создания интеллектуального речевого интерфейса «человек-машина» все более интегрируются в реальную жизнь, а соответствующие системы стремятся занять свое надлежащее место в кабинах самолетов, рубках кораблей, мобильных телефонов и т. д [1].

Поиск оптимального решения данной проблемы привлекает внимание ученых. Электронные приборы как бытовые, так и используемые в различной профессиональной деятельности людей, продолжают «обрастать» все новыми многофункциональными кнопками, значения которых достаточно сложно быстро запомнить и эффективно использовать, особенно в условиях возможного дефицита времени. Предложенная технология позволит легко открывать необходимое приложение вместо длительного и трудоемкого процесса поиска нужных файлов в различных системных директориях компьютера. А также, поможет пользователям с ограниченными возможностями (например, с недостатками зрения и др.), облегчит работу с устройством в ситуациях, когда руки пользователя заняты [2].

VA (Voice Assistant-голосовой помощник)

Технология распознавания позволяет организовать одновременное распознавание команд в дикторозависимом режиме [1]. То есть, пользователь настраивает каждую команду на свой голос, прежде чем система начнет работать. Или использует некоторое количество команд в дикторонезависимом режиме. Как вариант, возможна работа без предварительной настройки системы в случае подготовки неизменного набора команд, так сказать, определенной базы эталонов этих команд.

В случае возникающих дефектов из-за помех или неразборчивости речи (шумы и т. д.), для корректировки поведения машины, его интеллектуализации, можно предложить следующие возможные варианты ее реакции:

– использовать режим молчания и не предпринимать никаких действий;

– сообщить пользователю о возможной ошибке и послать повторный запрос на команду;

– предложить помощь, озвучивая или визуализируя доступные в данном режиме команды.

Повысить эффективность позволяют заранее прописанные действия машины по интерпретации молчания пользователя:

– выполнить команду;

– не выполнять команду;

– другой вариант.

Принципиальная схема организации Voice Assistant с целью управления оборудованием SDN/NFV приведена на рис. (см. ниже).

Описание

Клиент общается с сервером, с помощью voice assistant.

Клиент, отправляя запросы с помощью интерфейса голосового ввода, может запросить любую информацию о состоянии и настройках облачных

сервисов, виртуальных машин и самой сети. На схеме данный способ взаимодействия отображен пунктирной линией. Также возможно управление сетью напрямую через оркестратор посредством голосового ввода с помощью voice assistant.

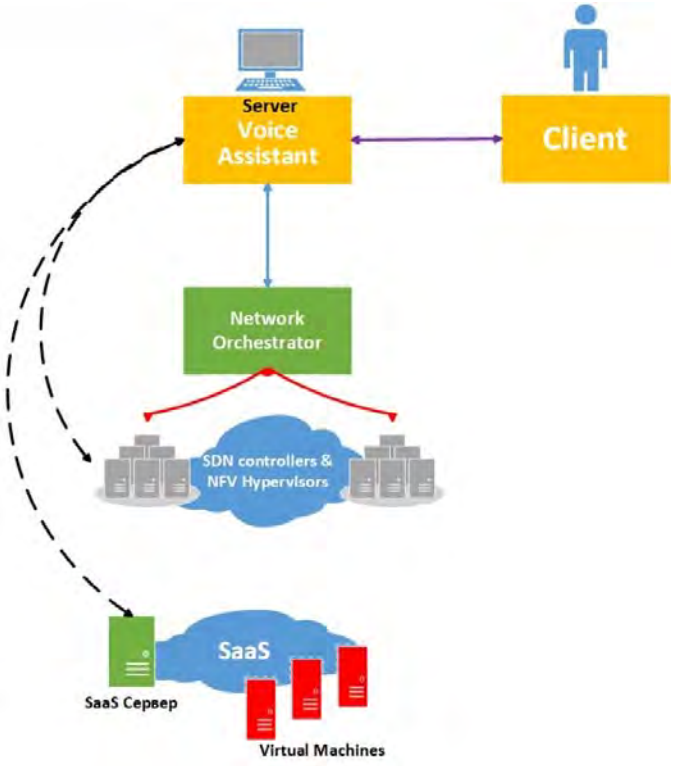


Рисунок. Схема взаимодействия Voice Assistant с инфраструктурой сетей 5G

Выводы

Традиционное администрирование в дальнейшем будет трансформироваться в программную область, что позволит разрабатывать новые подходы к мониторингу и управлению систем. Пользователь, не принимая участия в непосредственном конфигурировании систем, получает преференции в повышении эффективности и скорости взаимодействия с инфраструктурой. Перспективные исследования в области реализации VA как интерфейса к управлению телекоммуникационными системами лежат в плоскости обеспечения стабильности и достоверности принятия сообщений от устройства клиента и конфиденциальности работы.

Список используемых источников

1. Борисов В. А. Презентация «Голосовое управление ПК» [Электронный ресурс] // Красноармейск, 2010. URL: https://www.metod-kopilka.ru/page-4-1-13-29.html (дата обращения 28.03.2019).

2. Бабаринов С. Л., Будникова М. А. О распознавании речи [Электронный ресурс] // Научные ведомости. 2014. № 21 (192). URL: http://speech-soft.ru/index.php?a=inf&inf=rasp (дата обращения 28.03.2019).

УДК 004.056.2
ГРНТИ 20.53.23

ИССЛЕДОВАНИЕ ВОПРОСОВ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ РАЗВЕДЫВАТЕЛЬНЫХ АТАК

А. Д. Малько, Д. Д. Стародубова, А. А. Чечулин

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

Успешность реализации компьютерной атаки напрямую зависит от объёмов информации об атакуемой сети, получаемых злоумышленником при проведении разведывательных атак. Использование различных средств обнаружения и предотвращения вторжений, анализаторов сетевого трафика и межсетевых экранов позволяет усложнить возможность осуществления сбора информации о сети. Наибольшая защищённость сети достигается при использовании средств обеспечения безопасности в соответствии с методиками, описывающими комплексный подход к обеспечению защиты. В статье рассматриваются вопросы, связанные с описанием существующих алгоритмов и методик защиты компьютерных сетей от разведывательных атак.

информационная безопасность, разведывательные атаки, сбор информации, анализ сетевого трафика, защита информации, компьютерные сети.

В современном мире, основополагающим элементом успешной работы большинства организаций является обеспечение и поддержание высокого уровня безопасности своей компьютерной сети. Использование компанией общедоступных сервисов, а также высокая сложность внутренней сетевой инфраструктуры предоставляют дополнительные возможности для осуществления атак злоумышленниками. Помимо этого, скорость создания нового вредоносного программного обеспечения и использование уязвимостей нулевого дня, в совокупности с высокой доступностью рынка киберпреступности создают необходимость обнаружения и предотвращения атак на первых этапах их реализации.

В регулярном отчёте по исследованию вопросов информационной безопасности компании Positive Technologies аналитики указывают на то, что в IV квартале 2018 г. количество уникальных инцидентов возросло на 11 %, по сравнению с результатами аналогичного периода 2017 г., а также превышены показатели III квартала 2018 года на 7 % [1]. Также специалисты данной компании в своём исследовании отмечают, что наиболее распространённой уязвимостью на сетевом периметре является использова-

ние открытых протоколов передачи данных, что позволяет злоумышленникам осуществлять перехват и анализ трафика, и на основании полученной информации строить векторы своих атак [2].

Первым этапом проведения целенаправленных атак является осуществление разведывательных действий, направленных на поиск уязвимых точек в атакуемой сети. Существует два метода сбора информации о сети: активный и пассивный. При активном сборе используются программные средства и сетевые сканеры, позволяющие определить основные сведения о сети (IP-адреса, топологию сети, открытые порты и т. д.). Данный метод предоставляет наибольшее количество информации, необходимое для проведение последующих атакующих действий, однако этот способ имеет более высокие риски обнаружения средствами защиты [3].

В свою очередь, пассивный сбор подразумевает минимальные взаимодействия с сетью, что позволяет атакующему избежать выявления своего присутствия. При такой разведывательной атаке используются открытые источники информации, например, специальные ресурсы сети Интернет, предоставляющие информацию о DNS, открытых портах и используемых сервисах. Также с помощью описания вакансий компании могут быть получены сведения об используемом оборудовании и программном обеспечения цели атаки. В таблице приведены примеры информации, которая может быть получена при проведении разведывательной атаки.

ТАБЛИЦА. Информация, получаемая при разведывательных атаках

Информация о сети	Информация о хостах	Персональная информация	Информация о средствах защиты
– диапазон используемых IP-адресов; – топология сети; – доменные имена; – сведения о режиме работы сети и движении трафика.	– имена пользователей; – информация о паролях (размер, частота смены); – производитель оборудования; – версия операционной системы; – открытые TCP/UDP порты; – используемые сервисы.	– контактный телефон/e-mail; – данные банковских карт; – сведения о частной жизни (адрес проживания, места отдыха, личные данные).	– средства криптографической защиты; – средства физической защиты; – межсетевые экраны; – системы обнаружения и предотвращения вторжений.

Обнаружение наличия неправомерных действий с целью сбора информации о сети осуществляется на основании признаков атаки, которые могут различаться в зависимости от характеристик сети (параметров работы хостов и телекоммуникационного оборудования, а также типовых сценариев

взаимодействия между ними). Корректное и своевременное выявление признаков атак играет ключевую роль при расследовании инцидентов информационной безопасности. Наиболее вероятными признаками осуществления разведывательной атаки являются:

– отклонения в работе сетевых протоколов;

– эксплуатация уязвимостей с помощью общедоступных методов и средств проведения атаки;

– аномалии в типовых взаимодействиях в сети.

Используя вышеуказанные признаки, системы безопасности должны обнаруживать попытки проведения разведывательных действий в сети. Первый метод обнаружения основан на сведениях об общеизвестных атаках и их модификациях. Данный метод использует сигнатурный анализ, при котором осуществляется сопоставление параметров известной атаки с данными о сетевых взаимодействиях и работе протоколов в сети. Модель состояния сети составляется на основании анализа корректности запросов и ответов, а также учёта количества однотипных запросов в единицу времени. Системы обнаружения и предотвращения вторжений на основании данной модели могут обнаруживать попытки сканирования адресного пространства или портов транспортного уровня [4].

Вторым методом является обнаружение аномалий, заключающееся в сопоставлении обработанного сетевого трафика с установленными характеристиками нормального поведения, которые образуются на основе мониторинга сетевых взаимодействий в течение определённого промежутка времени. Информацией для описания нормального поведения являются объёмы трафика для каждого хоста в сети, типы и протоколы взаимодействия между ними, а также временно хранимые потоки данных. Использование двух описанных методов вместе позволяет повысить шанс обнаружения разведывательных действий в сети за счёт расширения списка признаков проведения атаки [5].

Для обеспечения максимального уровня защищённости сети рекомендуется совместно использовать средства обнаружения и предотвращения вторжений на отдельных хостах и в ключевых точках сетевого периметра, через которые проходят максимально возможные объёмы трафика. Помимо этого, объединение всех этих средств в систему под единым управлением, позволяющую централизованно хранить сведения о событиях, анализировать и обрабатывать их, значительно ускоряет и упрощает работу по борьбе с разведывательными атаками. Также единая система должна обрабатывать данные, получаемые с других средств защиты (межсетевых экранов, антивирусных программ и т. д.), и сопоставлять их с общей картиной событий безопасности.

Таким образом, проблема борьбы с разведывательными действиями является первым этапом защиты сетевой инфраструктуры от целевых атак.

Постоянное упрощение методов сбора информации и получаемые при этом объёмы данных представляют серьёзную угрозу при отсутствии грамотного внедрения средств защиты. Использование описанных методов обнаружения признаков атаки, а также внедрение системы централизованного мониторинга и управления событиями безопасности позволяет обеспечить высокую точность выявления потенциальных угроз и реагирования на них.

Работа выполнена при финансовой поддержке РФФИ (проект 18-37-20047) в СПИИРАН.

Список используемых источников

1. Отчёт компании Positive Technologies «Актуальные киберугрозы. IV квартал 2018 года». С. 3–6. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018-q4/

2. Отчёт компании Positive Technologies «Уязвимости корпоративных информационных систем, 2019». С. 7–8. URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/

3. Биячуев Т. А. Безопасность корпоративных сетей / Под ред. Л. Г. Осовецкого. СПб. : СПб ГУ ИТМО, 2004. 161 с.

4. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. 2016. Вып. 6 (49). С. 208–225.

5. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей. М. : Горячая линия-Телеком, 2016. 644 с.

УДК 004.056.2
ГРНТИ 20.53.23

ИССЛЕДОВАНИЕ МЕТОДИК И АЛГОРИТМОВ СБОРА ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СЕТИ

А. Д., Малько, Д. Д. Стародубова, А. А. Чечулин

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

Актуальность обеспечения информационной безопасности корпоративных сетей обусловлена высокими темпами роста компьютерных атак на них. Рост уровня сложности и быстрая адаптация атак к предпринятым мерам защиты вынуждают устанавливать строгие правила, чтобы получать уведомления о любых потенциальных нарушениях еще до их возникновения. Средства анализа и мониторинга сетевого трафика становятся необходимыми составляющими любой системы управления информационной безопасностью. Такие системы помогают повысить уровень защищенности сети

предприятия. В докладе представлены результаты исследования и сравнения существующих методик и алгоритмов сбора информации о сетевом трафике.

информационная безопасность, сетевые атаки, сетевой трафик, обнаружение аномалий.

На сегодняшний день, вопросы реагирования на компьютерные атаки являются актуальными, в силу роста количества компьютерных угроз, вызванных повсеместным использованием информационных технологий, сложность и размер сетевых инфраструктур которых, постоянно растёт [1]. А соответственно возрастает необходимость в усовершенствовании методов сбора информации в сетях для выбора мер адекватного реагирования на атаки.

В целях грамотного противодействия атакам необходимо разработать эффективную методику сканирования сети, которая позволит производить всесторонний анализ уязвимостей, реально отражающих потенциальные источники угроз.

Одним из самых распространенных на сегодня источником получения информации являются компьютерные сети, однако не существует общепринятого алгоритма и инструмента для мониторинга компьютерных сетей, и последующей нейтрализации угроз [2]. Существует ряд приемов, реализующих сканирование систем, но не позволяющих собирать полный спектр уязвимостей. Новизна работы состоит в масштабном отображении картины компьютерной сети, использованием нескольких методик в отношении одной сети, что дает максимальное представление исследуемого объекта, для дальнейшего построения модели объекта.

В целях грамотного планирования атаки необходимо иметь представление о возможных уязвимостях и характере их происхождения. В работе представлена классификация по источнику возникновения [3], так как в рамках данной статьи она является достаточно эффективной и оптимальной в силу ориентации на причину возникновения уязвимости.

Чем больше данных мы передаем, тем больший по объему перехват может совершить злоумышленник и тем больший вред он способен нанести [4]. Чтобы избежать данной проблемы, необходимо зашифровать информацию, причем сделать это с максимально возможной криптоустойчивостью и наименьшими временными затратами на данный процесс.

Уязвимости проектирования. Значительная часть уязвимостей возникает именно на этапе проектирования. Например, большая часть прикладных сервисов стека TCP/IP не предполагает использование шифрования данных при передаче по сети, что становится причиной передачи критичной информации по сети в открытом виде [5]. Отсутствие использования криптографических защитных механизмов на этапе проектирования позволяют злоумышленнику получить данные.

Уязвимости реализации так же являются не менее популярными и составляют важную часть уязвимостей. Уязвимости в драйверах позволяют в обход ограничений ОС выполнять код в режиме ядра и повышать привилегии запускаемого эксплойтом приложения до максимально что одна из функций драйвера не проверяет возвращаемое ей другой функцией значение и передает его дальше, результатом чего становится то, что получатель оперирует неправильным значением.

Уязвимости эксплуатации также могут являться следствием ошибок, допущенных при эксплуатации информационной системы, а именно: применение конфигураций по умолчанию, не точно установленные параметры защиты и прочие действия пользователей, связанных с некорректной работой по обеспечению безопасности.

В процессе разработки атаки возникает необходимость в сборе информации о сетевых объектах. Цели, конфигурация сети, действующие в ней сервисы и службы, конфигурации серверов, используемые для мониторинга – все эти параметры учитываются для дальнейшего выбора методики и других приемов сбора информации о сети.

Для сбора информации существуют достаточно методов, но в самом общем виде способы сбора о системе можно разделить на две группы: активные, предполагающие использование ключевых воздействий на систему и анализ откликов; а также пассивные, производящие использование информации, которая «добровольно» рассылается исследуемой системой. Активные методы сбора информации так же можно представить, как способы, требующие явного подключения к сетевым службам объекта сканирования и не нуждающиеся в подобном подключении. Последнюю группу методов также принято называть как предварительное изучение цели.

В процессе сбора данных об исследуемом объекте, могут быть получены сведения различного характера начиная от информации регистрационного и организационного характера до операционных систем узлов и используемых средствах защиты. Следует отметить, что в ходе сбора список необходимых для атаки ресурсов может включить в себя любую другую дополнительную информацию, которая может оказаться полезной для повышения эффективности дальнейшей работы.

Предварительно изучив алгоритмы сбора информации в исследуемой области были выделены основные приемы, позволяющие определить существующие угрозы сети и их потенциальные источники. На самом общем уровне можно говорить о таких этапах как: проверка физической доступности оборудования, проверка работоспособности служб и сервисов, запущенных в сети, детальная проверка не критичных, но важных параметров функционирования сети: производительности и загрузки, проверка параметров, специфичных для сервисов и служб данного конкретного окружения.

Проведя анализ существующих на настоящий момент методик сбора информации в сети, было выделено три лидера, которые включают в себя элементы, позволяющие максимально отразить компоненты сети и определить потенциальные источники угроз для эффективного проведения атаки. Наиболее простой и понятной является методика, разработанная кафедрой «Информационная безопасность» МГТУ им. Н. Э. Баумана. Другой, наиболее популярной является методика, утвержденная советом ЕС и являющаяся частью курсов по этичному хакингу (тест на проникновение). Обратим внимание еще на одну методику, представленную лабораторией Offensive security, которая является обладает предполагает использование новейших этических инструментов и техник взлома. На основе модулей, входящих в состав, рассмотренных выше методик была составлена таблица, которая отражает наиболее эффективную методику сбора информации о сети, которой стала EC-Council.

ТАБЛИЦА. Выбор наиболее эффективной методики сбора информации о сети

Методика / Модуль	Методика Университета им. Баумана	EC-Council	Offensive Security
Предварительный сбор информации о цели	+	+	+
Сканирование сети	+	+	–
Инвентаризация ресурсов		+	
Исследование уязвимостей	+	+	+
Перехват трафика в сети	+	+	–
Отказ в обслуживании		+	+
Перехват сессий		+	–
Обход систем обнаружения вторжений и межсетевых экранов	+	+	+

Таким образом, увеличение количества компьютерных атак, провоцирует необходимость усовершенствования методов сбора информации в компьютерных сетях для актуализации нейтрализующих данные атаки мер.

Список используемых источников

1. Максимова Е. А. Корнева В. А. Формализация действий злоумышленника при прогнозировании вторжений в корпоративную информационную систему // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства. Матер. II Всерос. науч.-практ. конф., Волгоград, 26 апреля 2013 г. Волгоград : Изд-во ВолГУ, 2013. С. 71–78.

2. 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. № 2. С. 100–108.

3. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

4. Кириллов Д. И., Красов А. В., Долгорук Ю. Г., Селиванов А. Е., Ушаков И. А. Основы информационной безопасности сетей и систем: учебное пособие. Часть 1. СПб.: СПбГУТ, 2012. 64 с.

5. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. № 1 (20). С. 27–56.

УДК 004.9
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ТРАФИКА И ФУНКЦИОНИРОВАНИЯ САМООРГАНИЗУЮЩИХСЯ СЕТЕЙ СВЯЗИ

А. В. Марочкина, А. И. Парамонов

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

В данной работе представлены результаты исследования трафика и функционирования самоорганизующейся сети, полученные с помощью имитационного моделирования. Для исследования были реализованы две имитационные модели в программах NS-3 и OMNeT++. В результате исследований получены зависимости качества обслуживания трафика и характеристик маршрутов от количества узлов сети.

самоорганизующиеся сети связи, Интернет вещей, протоколы маршрутизации.

Введение

Ключевой технологией Интернета вещей являются самоорганизующиеся сети. Они автоматически определяют логическую структуру сети с помощью различных методов маршрутизации. Выполнение таких процедур самоорганизации сети отражается на качестве обслуживания сети и объеме служебного трафика.

В общем, сети связи с изменяющейся во времени конфигурацией (количество узлов, связность) называются самоорганизующимися [1]. Информация в таких сетях передается по маршрутам, которые выбираются с помощью различных алгоритмов поиска оптимальных путей, удовлетворяющих определенному критерию (загруженность каналов передачи данных, их надежность, расстояние между транзитными узлами и др.) [2, 3].

Процедура выбора маршрутов, фактически, является процедурой определения конфигурации сети, т. е. решает основную задачу самоорганизации.

Изменение условий функционирования сети приводит к необходимости изменения маршрутизации трафика. Такими изменениями могут быть, например, изменение расстояний между узлами из-за их движения, изменение количества узлов сети из-за выхода из строя узлов или появления новых узлов сети, внешних помех, приводящих к изменению условий функционирования радиоканалов.

Поиск маршрутов связан с необходимостью передачи служебного трафика, который создает нагрузку на сеть и снижает ее основные показатели функционирования. В данной работе приведены результаты исследования показателей функционирования самоорганизующейся сети под влиянием ряда факторов.

Исследование выполнено с помощью имитационного моделирования в программах NS-3 [4] и OMNeT++ [5]. Полученные результаты позволили выявить закономерности в самоорганизующихся сетях связи.

Маршрутизация в самоорганизующихся сетях связи

Самоорганизующиеся сети поддерживают несколько типов маршрутизации, которые принято условно разделять на проактивную, реактивную, гибридную.

Проактивная или табличная маршрутизация представляет собой алгоритм, который постоянно обновляет информацию о состоянии топологии сети. Благодаря этой информации, каждый узел строит маршруты до всех остальных узлов, которые записываются в таблицу маршрутизации и используются при передаче информации от одного узла к другому. Табличную маршрутизацию поддерживают такие протоколы, как FSR, OLSR, DSDV, TBRPF.

Реактивная маршрутизация (маршрутизация по требованию) – это алгоритм построения маршрута при необходимости до определенного узла путем отправки по сети широковещательного сообщения и получение ответа-подтверждения от адресата. К реактивным протоколам относятся DSR, AODV, DYMO, MOR.

Маршрутизация, которая включает в себя хранение таблиц маршрутизации (элемент проактивного алгоритма построения маршрута) и опрос узлов по требованию (элемент реактивного алгоритма построения маршрута), называется гибридной. При таком типе построения маршрутов вся сеть разбивается на множество подсетей, которые взаимодействуют между собой с помощью реактивных алгоритмов, а информация между узлами внутри

каждой подсети передается с помощью проактивного алгоритма. Для гибридной маршрутизации используются следующие протоколы: ZRP, HSLS, HRPLS [6].

Сравнение выше указанных протоколов проводилось с помощью имитационного моделирования в программе Network simulator 3. Во время данного эксперимента выбирались протоколы, описанные в [7].

Также при моделировании было выбрано случайное расположение узлов в зоне обслуживания, источников и приемников трафика. Средняя скорость движения узлов была выбрана равной 1,5 м/с, модель движения – «случайная путевая точка». Время имитационного эксперимента – 150 с. Зона обслуживания представляет собой квадрат со стороной, определяемой по формуле:

$$W = d\sqrt{N} \text{ м},$$

где d = 100 м, N – число узлов сети.

В результате этого моделирования были представлены зависимости коэффициента доставки пакетов от размера сети (рис. 1) и времени доставки пакетов от размера сети (рис. 2).

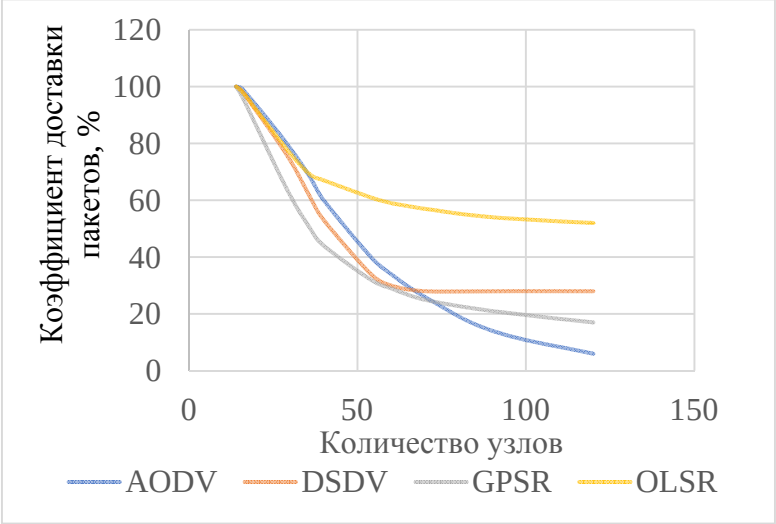


Рис. 1. Зависимость коэффициента доставки пакетов от размера сети

Из результатов, приведенных на рис. 2, видно, что с ростом количества узлов сети снижается коэффициент доставки пакетов, причем это характерно для всех рассматриваемых протоколов маршрутизации.

Среди рассмотренных протоколов наиболее быстро коэффициент доставки снижается при использовании протоколов AODV, GPSR и DSDV, хотя для последнего следует отметить некоторую стабилизацию коэффициента доставки на уровне около 30 %.

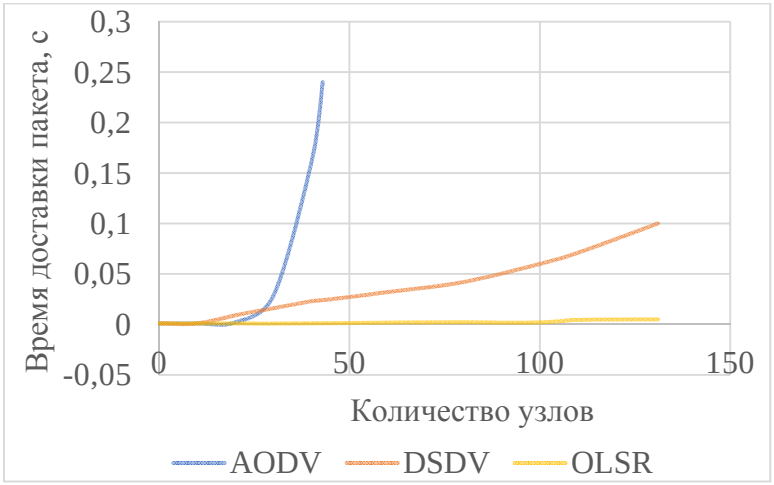


Рис. 2. Зависимость времени доставки пакетов от размера сети

Наибольшую устойчивость к росту количества узлов сети показал протокол OLSR – коэффициент доставки пакетов относительно стабилизируется на уровне около 55 %.

Исследование зависимости времени доставки пакетов от количества узлов сети также показало достоинства протокола OLSR. При его использовании время доставки незначительно увеличивалось с ростом количества узлов, в то время как для протоколов AODV и DSDV было существенным. В наибольшей степени время доставки возрастало при использовании протокола AODV.

Параметры маршрута в самоорганизующихся сетях связи

Основными параметрами оптимальности маршрута в самоорганизующихся сетях являются число транзитов и длина маршрута. Для анализа этих параметров в программе OMNeT++ была реализована имитационная модель сети со случайным распределением узлов, образованной 20, 50 и 100 узлами, расположенными на плоской поверхности в области, ограниченной квадратом 200×200 м. В результате обнаружены следующие закономерности, представленные на графиках ниже (рис. 3, рис. 4).

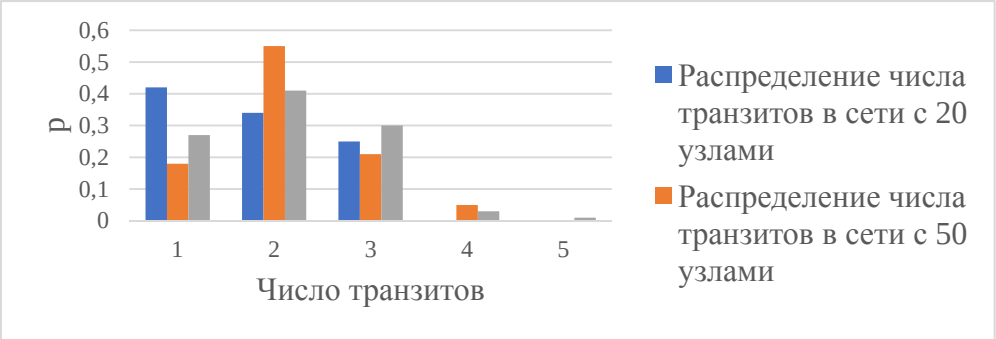


Рис. 3. Распределение числа транзитов в сети

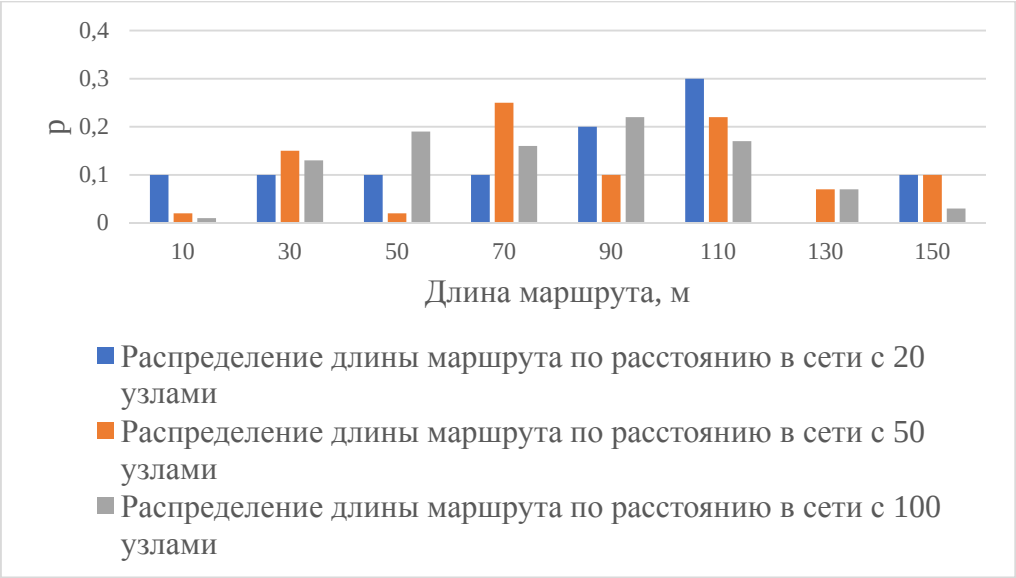


Рис. 4. Распределение длины маршрута по расстоянию в сети

Полученные результаты показывают, что длина маршрута является случайной величиной, причем ее распределения схожи при различном количестве узлов сети. С ростом количества узлов сети количество транзитных узлов в маршруте изменяется незначительно, это изменение, вероятно, обусловлено изменением связности сети [8]. Для длины маршрута, выраженной в единицах расстояния, характерны аналогичные свойства.

Заключение

Полученные результаты имитационного моделирования с использованием системы моделирования NS-3 показали, что наиболее стабильным протоколом по процентному соотношению доставленных пакетов и времени доставки пакетов является проактивный протокол OLSR. Вероятно, что эти преимущества обусловлены его принципом функционирования, который в рассмотренных условиях снижает загруженность сети. Результаты также показали, что реактивный протокол AODV уступает всем остальным протоколам по времени доставки пакетов, поскольку требует больше времени на установку маршрута, чем многие другие протоколы.

Разумеется, что полученные результаты справедливы только для условий функционирования сети, которые имели место в имитационном эксперименте.

Имитационная модель, реализованная в программе OMNeT++, позволила оценить распределение длин маршрутов доставки трафика и исследовать зависимость длины маршрута от количества узлов сети.

Список используемых источников

1. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. СПб. : БХВ-Петербург, 2013. 160 с.: ил. ISBN 978-5-9775-0900-8.

2. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Типография Любавич, 2011. 312 с.

3. Борисов Е. Г., Владыко А. Г., Парамонов А. И., Киричек Р. В. Самоорганизующиеся сети связи мультиагентных робототехнических систем // Актуальные проблемы защиты и безопасности: труды XIX Всероссийской научно-практической конференции РАРАН (4–7 апреля 2016 г.). М. : ФГБУ «РАРН», 2016. С. 210–217.

4. Network Simulator ns-3 [Электронный ресурс] // URL: https://www.nsnam.org (дата обращения 18.02.2019).

5. Discrete Event Simulator OMNeT++ [Электронный ресурс] // URL: https:// https://omnetpp.org (дата обращения 20.02.2019).

6. Павлов А. А., Датьев И. О. Протоколы маршрутизации в беспроводных сетях // Труды Кольского научного центра. Информационные технологии. Апатиты : КНЦ РАН, 2014. С. 64–75.

7. Метелёв А. П., Чистяков А. В., Жолобов А. Н. Протоколы маршрутизации в беспроводных самоорганизующихся сетях. // Вестник Нижегородского университета им. Н. И. Лобачевского. Нижний Новгород : ФГАОУ ВПО «ННГУ им. Н. И. Лобачевского», 2013. № 3 (1). С. 75–78.

8. Нуриллоев И. Н., Парамонов А. И. Модель связности для беспроводных сенсорных сетей // 71-я всероссийская научно-техническая конференция, посвященная дню радио. СПб. . : СПбГЭУ «ЛЭТИ» им. В. И. Ульянова (Ленина), 2016. С. 176–177.

УДК 004.71
ГРНТИ 49.33.29

СЕТЬ ИНТЕРНЕТА ВЕЩЕЙ КАК СЕТЬ С ДОПУСТИМЫМИ ЗАДЕРЖКАМИ

О. А. Махмуд, А. И. Парамонов

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

В статье приведены результаты анализа производительности мобильной одноранговой сети и протоколов маршрутизации сети с допустимыми задержками, используемых в Интернете вещей. Сеть MANET рассматривается как сеть с допустимыми задержками, в которой маршруты доставки не является стабильным, а имеют вероятностный характер. Доставка данных производится, когда возникает такая возможность вследствие движения узлов и изменения их взаимного положения. Приведены результаты анализа влияния движения узлов на вероятность доставки данных.

интернет вещей, ИВ, протоколы маршрутизации, сеть с допустимыми задержками.

Введение

Сети с допустимыми задержками (DTN, *Delay Tolerant Network*) – это мобильные сети, в которых маршрут между источником и получателем сообщения может отсутствовать в некоторый момент времени или на интервале времени. Доставка же сообщения производится за счет его физической транспортировки подвижными узлами или ожидания возможности создания маршрута доставки [1]. Характеристики DTN отличаются от традиционных сетей Ad Hoc [2], поэтому исследователи предлагают новые протоколы маршрутизации, которые лучше поддерживают проблемы DTN (мобильность, временное соединение, доставка с большой задержкой и т. д.).

Все схемы маршрутизации в DTN основаны на принципе Store-Carry-Forward (хранение-перемещение-отправка) [3]. В последнее время развивается несколько новых групп приложений, которые также требуют поддержки маршрутизации с задержкой. Интернет вещей (IoT) – это одна из этих новых областей. IoT соединяет дополненные датчиками физические объекты в любом месте в любое время для многих областей применения (промышленность, безопасность, военное назначение, умный дом и т. д.) [4]. Использование принципов устойчивой к задержке связи в IoT позволит смарт-объектам взаимодействовать между собой даже при нарушениях их соединений [5, 6].

Например, в случае приложений управления дорожным движением с ограниченной возможностью связи (на территориях с малой плотностью населения), транспортные средства, регистрирующие важную информацию о состоянии дороги и других транспортных средств, могут использовать принцип хранения / переноса данных до тех пор, пока они не будут доставлены получателю.

Несмотря на общеизвестные принципы, существующие схемы построения DTN должны быть адаптированы к приложениям IoT, чтобы соответствовать их конкретным требованиям, таким как: неоднородность, огромный объем передаваемых сообщений, протокол, основанный на информации, и т. д. Хотя существует множество интересных обзоров DTN. Целью данной работы является изучение возможностей и проблем в использовании стратегий DTN для Интернета вещей.

Принцип работы и анализ протоколов маршрутизации DTN

Для построения DTN известны различные протоколы маршрутизации. Некоторые из них основаны на сравнении узлов друг с другом, в то время как другие сосредотачиваются на внутренних свойствах сообщений, которые они передают и хранят. Существующие протоколы работают по-разному в зависимости от среды (прикладной области), в которой они находятся.

Известные протоколы DTN можно разделить на три категории:

– затопление (*Flooding*) – когда сообщения распространяются на все узлы при каждом контакте (возможности связи между узлами);

– ожидание (*Wait-and-forward*) – когда распространяется ограниченное количество сообщений;

– информированная переадресация (*Informed forwarding*) – где выбор узлов основан на ранее полученных знаниях.

Затопление *(Flooding*):- Epidemic (эпидемия) – это алгоритм стохастической маршрутизации для сетей DTN, где узел-источник отправляет сообщение всем своим соседям, которые затем отправляют сообщение всем своим соседям и т.д.

Ожидание (*Wait-and-forward*):- Spray and Wait – использует две стратегии пересылки. В первой стратегии, называемой Spray, распространяются копии L-сообщений. Узел-источник пересылает сообщение всем своим соседям, которые сохраняют сообщение в своем кэше, а затем пересылают сообщение. Если пункт назначения не может быть достигнут с использованием стратегии Spray, то узлы могут использовать стратегию ожидания: сообщение пересылается непосредственно к месту назначения, если один из узлов, имеющих сообщение в своем кэше, связывается с пунктом назначения.

Информированная переадресация (Informed forwarding):- PRoPHET – использование пересылки сообщений в соответствие с ожидаемой вероятностью доставки, основанной на анализе связи (связности).

Когда плотность узлов относительно мала, протоколы DTN превосходят протоколы MANET (мобильной одноранговой сети). С увеличением плотности скорость доставки протоколов DTN уменьшается. Это уменьшение более заметно при информированной пересылке и переполнении (*informed forwarding and flooding*), поскольку сообщения отбрасываются из-за ограничений размера памяти в узлах сети (длин очередей). Эти протоколы отправляют гораздо большее количество сообщений, чем протоколы «ожидание и пересылка» (*wait and forward*), следовательно, больше сообщений отбрасывается из-за перегрузки сети и коллизий.

Для протоколов MANET скорость доставки увеличивается с увеличением плотности узлов. Это увеличение более заметно на реактивных протоколах, потому что маршруты становятся более стабильными, и в случае изменения маршрута можно найти больше альтернативу. Подходы построения MANET и DTN увеличивают потребление энергии с ростом плотности узлов.

Протокол «Затопление» (*Flooding*) приводит к наибольшему увеличению трафика сети, так как этот протокол очень подвержен конфликтам.

Протокол «Информированная переадресация» *(Informed forwarding*) работает несколько лучше благодаря меньшему количеству отправляемых

сообщений, и как следствие, при его работе используется меньше памяти узлов сети (буферного пространства) и происходит меньше потерь сообщений.

Протоколу «Ожидание и пересылка» (*Waiting and forwarding*), в свою очередь, характерен плавный прирост трафика, поскольку в фазе пересылки сообщений используется постоянное количество копий.

Особенность модель сети IoT

Особенность IoT состоит в том, что Интернет-вещи могут оказаться в самых различных условиях: как в условиях сети сверхвысокой плотности, например, в условиях города; так и в сети малой плотности с ограниченной связностью, например, в условиях низкой плотности населения и отсутствия покрытия сетями беспроводной связи. Это можно дополнить возможностью внезапного изменения условий функционирования из-за различного рода происшествий (ЧС, аварийных ситуаций и т. п.). В тех и других условиях сеть IoT должна обеспечивать доставку данных.

К тому же различные условия функционирования или их изменения могут приводить и к изменению приоритетов функционирования IoT. Например, в нормальном режиме, целевыми параметрами могут быть такие как время доставки сообщения и расход энергии, но в случае ЧС и возникновении угрозы жизни людей, энергопотребление уже не следует рассматривать в качестве целевого параметра.

Иными словами, сеть IoT должна строиться согласно тем принципам, которые в нужное время обеспечивают максимум целевых характеристик, последние, в свою очередь также зависят от внешних условий и назначения сети. В частности, в определенных условиях, может быть оптимально построение сети IoT как сети с допустимыми задержками.

Как было отмечено выше, рассмотрение IoT как DTN приводит нас к рассмотрению принципов построения MANET, однако, особенность IoT в том, что это не абстрактная ad hoc сеть, а сеть с такими параметрами, при которых она иначе функционировать не может. Данный «режим» работы сети является вынужденным, обусловленным «стремлением» сети сохранить свою функциональность в «любых» условиях. Это такие условиями, когда относительно малое количество узлов сети могут «контактировать» между собой. Это может быть следствием влияния различных факторов (препятствия и помехи для распространения сигналов между узлами) или низкая плотность сети (удаленные территории и т. п.).

Представим транспортировку данных от узла к узлу некоторым гипотетическим протоколом, схожим с теми, которые были описаны выше, рис. 1.

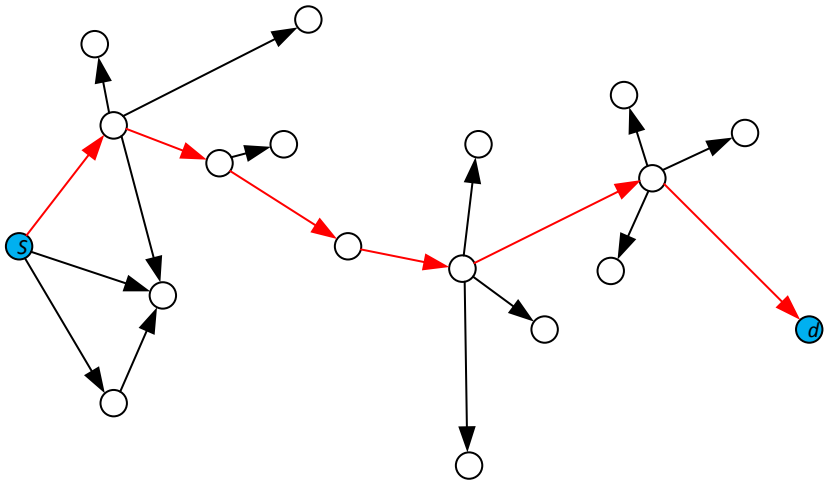


Рис. 1. Пример доставки данных в DTN

Для описания модели сети с нестабильной конфигурацией часто используют модель случайного графа [7]. В частности, во многих работах для описания сетей используется теорема Эрдеша-Реньи [8], которая позволяет оценить связность сети и среднюю длину маршрута.

В данном случае, особенность сети IoT состоит в том, что в рассмотренных условиях случайный граф следует считать сильно разряженным. В таких условиях, как показано в [8], упомянутая теорема дает завышенные оценки. В этой же работе показано, что для разряженного графа более адекватной оценкой является использование теоремы Боллобаша-Риордана.

Так в обычном графе (модель Эрдеша-Реньи) средняя длина пути составляет порядка $\tilde{g}(n) = \ln(n)$, в то время как для модели Боллобаша-Риордана это значение равно

$$g(n) = \frac{\ln(n)}{\ln(\ln(n))}.$$

На рис. 2 показана разница между этими двумя моделями.

Как видно из приведенного рисунка, средняя длина пути в разряженном графе существенно меньше, причем ее длина (в количестве тран-

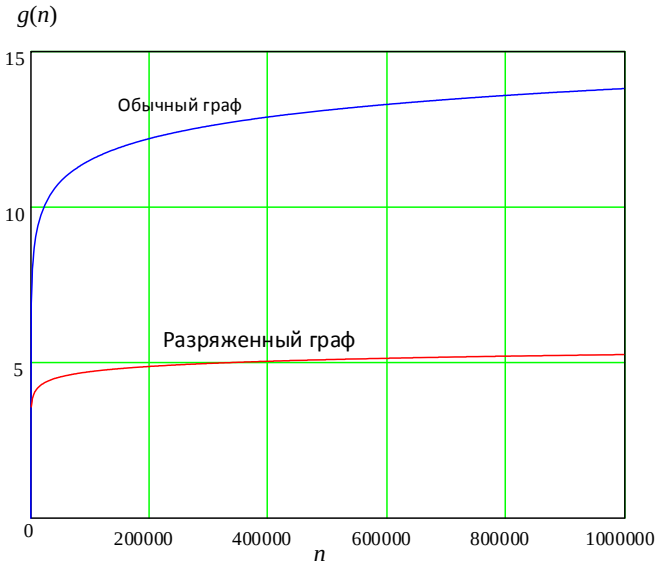


Рис. 2. Зависимость средней длины пути (в числе транзитов) от количества узлов сети

зитов) растет очень медленно с ростом количества узлов. Даже в сети из нескольких миллиардов узлов она не превышает 8 (8 приблизительно при 100 миллиардах).

Выводы

Результаты проведенного анализа и выбор модели для описания IoT говорит о том, что в сети, даже с очень большим количеством узлов (если сравнивать его, например, с количеством людей на земле), длина маршрута между узлами (в среднем) не превышает 8 транзитов.

Заметим, что это хорошо всем известное свойство социальных групп, которое часто выражают словами «мир тесен». Существует расхожее утверждение том, что любые два человека в мире «знакомы через 5–6 рукопожатий». Модель Боллобаша-Риордана очередное подтверждение этому.

Для IoT, в общем смысле, это означает, что маршрут между источником и получателем вполне возможен, даже при малой плотности узлов сети. Причем при изменении количества узлов сети в широких пределах, длина маршрута вполне реалистична.

Анализ известных протоколов показал, что использованные в них подходы поиска маршрутов могут быть использованы и в сетях IoT.

Список используемых источников

1. Jain, S., Fall, K., & Patra, R. Routing in a delay tolerant network // In Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications. ACM 2004, USA. pp. 145–158.

2. Кучерявый А. Е., Прокопьев А. В., Кучерявый Е. А. Самоорганизующиеся сети. СПб. : Любавич, 2011. 312 с.

3. Sathiaseelan, A., Trossen, D., Komnios, I., Ott, J., & Crowcroft, J. (2013). Information centric delay tolerant networking: an internet architecture for the challenged. Computer Laboratory Technical Report, UCAM-CL-TR-841.

4. Кучерявый А. Е. Интернет Вещей // Электросвязь. 2013. № 1. С. 21–24.

5. Гольдштейн Б. С., Кучерявый А. Е. Сети связи пост-NGN. С.Пб. : БХВ-Петербург, 2013. 160 с.

6. Кучерявый А. Е., Парамонов А. И., Кучерявый Е. А. Сети связи общего пользования. Тенденции развития и методы расчета. М. : ФГУП ЦНИИС, 2008. 290 с.

7. Колчин В. Ф. Случайные графы. М. : ФИЗМАТ ЛИТ, 2004. 256 с.

8. Райгородский А. М. Модели случайных графов. М. : МЦНМО, 2011. 136 с.

УДК 004.715
ГРНТИ 49.33.29

РАЗРАБОТКА АЛГОРИТМА МАРШРУТИЗАЦИИ, ОБЕСПЕЧИВАЮЩЕГО ЭФФЕКТИВНОЕ ФУНКЦИОНИРОВАНИЕ В УСЛОВИЯХ РЕКОНФИГУРАЦИИ ИЛИ ПРИ ОТКАЗАХ В СЕТИ

О. В. Моисеев, А. В. Яковлев

Академия Федеральной службы охраны Российской Федерации

В современных условиях гиперагрегации нагрузки, часто возникает задача необходимости поиска альтернативных путей передачи информации, а это ведет к прекращению информационного обмена на десятки секунд. В статье описаны вопросы повышения устойчивости сетей связи к отказам ее элементов за счет реконфигурации информационных потоков и повышения эффективности протоколов маршрутизации.

сеть связи, маршрутизация, граф, устойчивость.

Задача формирования структур сетей (формирование покрывающего дерева) решается путем разбиения множества вершин графа на непересекающиеся подмножества вершин с максимально связанными между собой каналами и минимальным суммарным весом ребер, проходящих между подмножествами полученных вершин. Следует отметить возможную противоречивость критериев разбиения графа – максимальная связность подмножеств вершин может не соответствовать минимальности весов граничных ребер и наоборот. В данной ситуации необходимо принятие того или иного компромиссного решения. Особенностью разработанного алгоритма является то, что он использует процедуру распознавания изоморфизма графов и средняя длина путей при заданном числе листьев будет минимальна. Предлагается деление сети на непересекающиеся участки с использованием триангуляции. В рамках исследований, проводимых с целью выполнения требований, предъявляемых к различным алгоритмам маршрутизации возможно синтезировать неравномерный граф для построения структуры сети с минимальной средней длиной процедуры поиска.

Будем рассматривать процедуру поиска по наименьшему расстоянию, с учетом количества исходов из вершины. В этом случае пространство поиска делится с помощью центроидов, координаты которых определяются на этапе разбиения исходного пространства телекоммуникационной сети.

Искомые вершины при этом являются центроидами нижнего уровня иерархии разбиения. Для ускорения времени поиска центроиды нижних уровней представляются центроидами верхних уровней.

Триангуляционное разбиение означает, что имеется стартовая вершина от которой ведется поиск, промежуточные и оконечные, таким образом все элементы сети делятся на три части. Число проверок (измерений) в корневой и промежуточных вершинах для бинарного дерева однозначно определяется полустепенью исхода вершин $S(X)$ [1], где X – вершина графа, так как в каждой такой вершине осуществляется измерение расстояний до каждой соседней вершины и выбор наименьшего из них. В случае триангуляционного разделения число измерений в корневой и промежуточных вершинах определяется степенью исхода из вершины.

Пусть исходный граф, задан матрицей инциденций $\|B\|$, где p – число промежуточных вершин в графе; m –число дуг; n – количество листьев.

Введем переменные $f_{RL}, R=\overline{1,n},\ L=\overline{1,m}$:

$$f_{RL}=\begin{cases}1, & \text{если } R\text{-ый путь проходит через } L\text{-ую дугу;}\\ 0, & \text{если } R\text{-ый путь не проходит через } L\text{-ую дугу.}\end{cases}$$

Тогда задача о минимальной сумме кратчайших путей из вершины X до всех листьев с весами дуг, определяемых вектором $\overrightarrow{H}_L=(H_1,H_2,H_3,...,H_n)$ формулируется следующим образом [2, 3]:

$$\sum_{R=1}^{n}\sum_{L=1}^{m}\overrightarrow{H_L}f_{RL}\to\min_{f_{RL}}\ \forall\ R=\overline{1,n},\ \ L=\overline{1,m} \tag{1}$$

при ограничениях:

$$\sum_{L=1}^{m}a_{xL}f_{RL}=1,\forall\ R=\overline{1,n}; \tag{2}$$

$$\sum_{L=1}^{m}a_{yL}f_{RL}=0,\forall\ R=\overline{1,n},L=\overline{1,m} \tag{3}$$

$$\sum_{L=1}^{m}a_{zL}f_{RL}=-1,\forall\ R=\overline{1,n},L=\overline{1,m}; \tag{4}$$

$$f_{RL}=0\text{ или }1 \tag{5}$$

Задача Штейнера является NP-полной. Большинство алгоритмов решения NP-полных задач на графах строятся на основе поиска, использующего метод ветвей и границ. Задача (1) при ограничениях (2)–(5) является задачей

поиска n кратчайших путей в графе от вершины *X* до *n* листьев с фиксированными весами дуг и может быть решена за полиномиальное время при помощи алгоритма Дейкстры, что дает нижнюю границу выражения на расширенном множестве.

Известно два основных типа поиска в дереве решений задачи в зависимости от того, как выбирается следующая задача для продолжения процесса ветвления: поиск в глубину и поиск в ширину, которые можно выполнять в алгоритме. Поиск в глубину более предпочтителен т. к. обеспечивает быстрое получение допустимого решения и экономное расходование ресурсов.

Алгоритм, обеспечивающий уменьшение времени сходимости для протоколов маршрутизации представлен на рис.

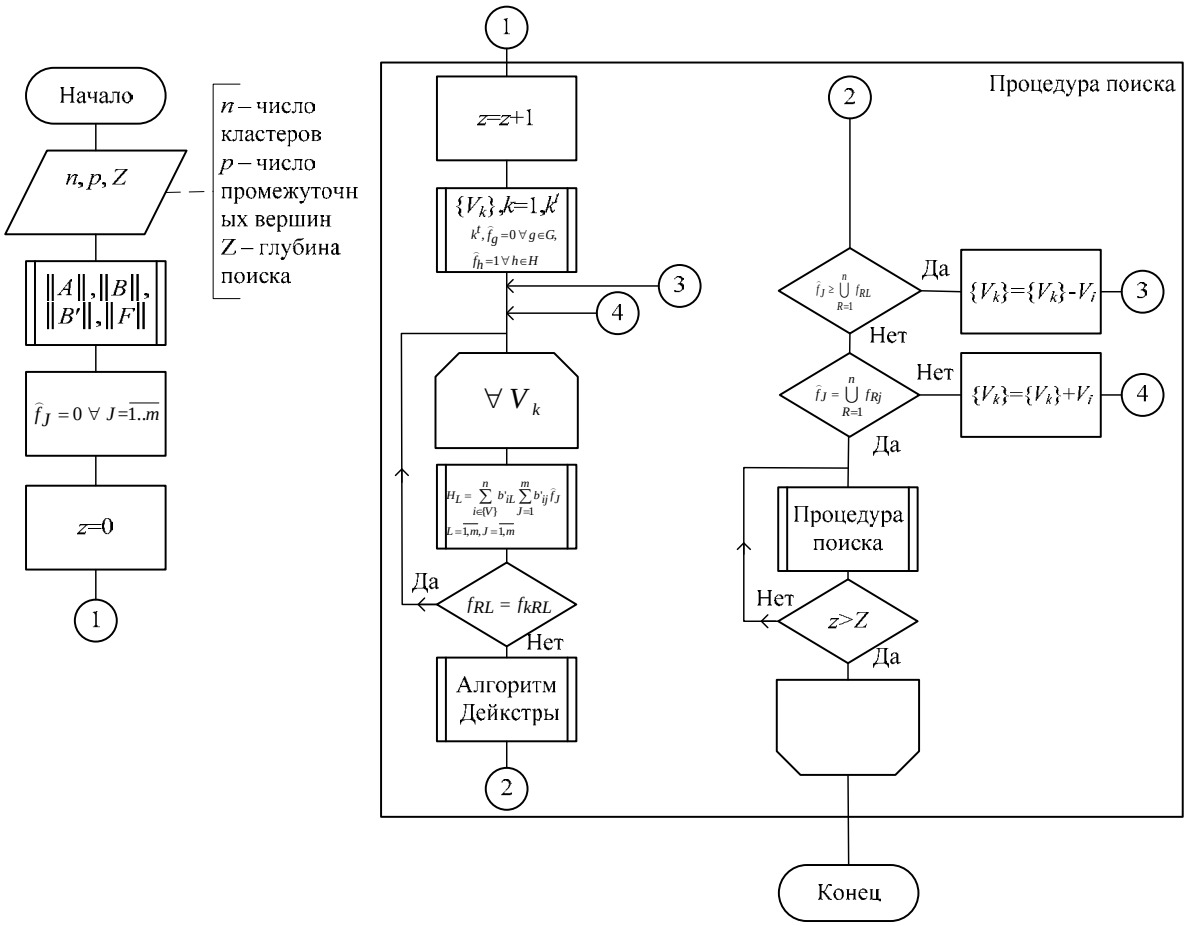


Рисунок. Схема алгоритма, обеспечивающего уменьшение времени сходимости для протоколов маршрутизации в условиях реконфигурации или при отказах в сети

Для решения задачи минимизации времени сходимости сети (многократный последовательный процесс) выбран алгоритм поиска в глубину,

что соответствует задаче поиска кратчайшего расстояния от одной из вершины графа до другой.

Исследование различных реализаций алгоритмов Дейкстры и алгоритма поиска в глубину показало, что алгоритм поиска в глубину имеет удовлетворительную точность при меньшем количестве итераций.

Список используемых источников

1. Моисеев О. В., Фам Т. Ф. Алгоритмы, обеспечивающие время сходимости протоколов маршрутизации в условиях реконфигурации или при отказах в сети // Системы управления и информационные технологии. 2017. № 4 (70). С. 45–50.

2. Моисеев О. В., Фам Т. Ф. Теоретико-графовая модель телекоммуникационной сети на основе триангуляционного разбиения // Телекоммуникации. 2018. № 2. С. 12–16.

3. Моисеев О. В., Кучук Г. Г. и др. Синтез структуры сети по критерию минимума средней длины процедуры поиска // Актуальные направления развития систем охраны, специальной связи и информации для нужд органов государственной власти Российской Федерации: материалы X Всероссийской научной конференции. – Орел : Академия ФСО России, 2017. С. 181–184.

УДК 004.492.2
ГРНТИ 81.93.29

ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ ОТ ПОПУЛЯРНЫХ АТАК НА ПРИМЕРЕ HTTP-ЗАГОЛОВКОВ ДЛЯ NGINX

Д. П. Морозов

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

Практически все типы веб-сайтов, начиная от одностраничных сайтов и заканчивая высоко нагруженными веб-приложениями, уязвимы для кибератак. Существуют различные способы защиты веб-приложений от кибератак. В данной статье рассматривается способ защиты на основе HTTP-заголовков для Nginx, позволяющий защитить веб-приложение от популярных видов атак.

атака, кликджекинг, clickjacking, межсайтовый скриптинг, Cross-Site Scripting, XSS, nginx, HTTP-заголовок.

По статистике за 2018 год были выявлены 6 наиболее популярных атак (рис. 1), направленных на пользователей веб-приложений, в частности атака «Cross-Site Scripting», которая составила 31,6 % от общего числа,

и атаки, с помощью которых можно получить доступ к данным или выполнить команды на сервере, – «SQL-injection», «Path Traversal», «Local File Inclusion», «Remote Command Execution», «Information leakage».

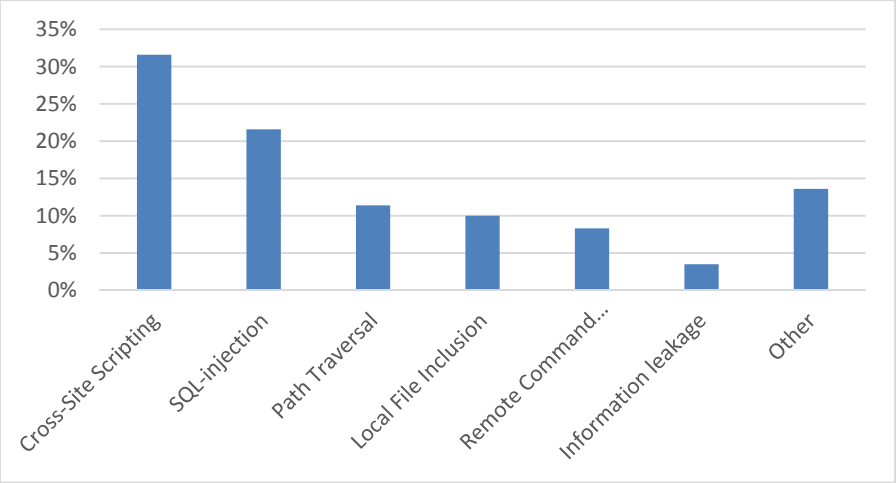


Рис. 1. Популярные виды атак на веб-приложения

Кликджекинг (*Clickjacking*) – механизм обмана пользователей интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже получить доступ к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу [3].

Атаку «Clickjacking» легко осуществить, если на сайте есть действие (рис. 2), активируемое с помощью одного клика [4].

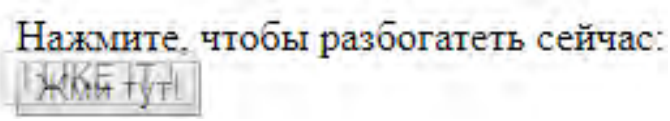


Рис. 3. Пример действия активируемого с помощью одного клика

Для предотвращения данной атаки необходимо добавить заголовок X-Frame-Options (рис. 3), который поддерживают все современные браузеры (рис. 4) [1]. Он разрешает или запрещает отображение страницы, если она открыта во фрейме, согласно параметрам таблицы 1 [2].

ТАБЛИЦА 1. Параметры заголовка X-Frame-Options

Значение параметра	Содержание
SAMEORIGIN	Позволяет загрузку контента в frame/iframe только если фрейм и страница, его загружающая, расположены на одном домене.
DENY	Запрещает загрузку контента в frame/iframe.
ALLOW-FROM	Допускает загрузку контента в фреймах только для определенного URI.

```
add_header X-Frame-Options "DENY";
```

Рис. 3. Пример заголовка X-Frame-Options

	Chrome	Edge	Firefox	Internet Explorer	Opera	Safari
Basic support	4	Yes	3.6.9	8	10.5	4
ALLOW-FROM	No	Yes	18	8	?	No
SAMEORIGIN	Yes *	?	Yes *	8	Yes *	Yes

Рис. 4. Поддержка браузерами заголовка X-Frame-Options

Межсайтовый скриптинг (*Cross-Site Scripting*) – тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода, который будет выполнен на компьютере пользователя при открытии им этой страницы, и взаимодействии этого кода с веб-сервером злоумышленника [3].

Пример кода уязвимой страницы представлен на рис. 5.

```
<input name="username" value="<? echo $_GET['username'] ?>">
```

Рис. 5. Код уязвимой страницы для атаки Cross-Site Scripting

Для атаки достаточно сформировать URL следующего вида (рис. 6).

```
http://www.server.com/index.php?username="><script>alert(document.cookie)</script>
```

Рис. 6. URL для атаки Cross-Site Scripting

В результате код страницы, подверженной атаке, примет следующий вид (рис. 7).

```
<input name="username" value=""><script>alert(document.cookie)</script>">
```

Рис. 7. Код страницы, подверженной атаке Cross-Site Scripting

Заголовок *CSP* (*Content Security Policy*) (рис. 8) позволяет запретить выполнение вредоносного кода при внедрении в страницу, содержит инструкции о загрузке контента из разрешенных источников [2]. Возможные параметры заголовка представлены в таблице 2 [2]. Поддержка браузерами представлена на рис. 9 [1].

ТАБЛИЦА 2. Параметры заголовка Content Security Policy

Значение параметра	Содержание
default-src	Загружать с определенного источника все.
script-src	Загружать с определенного источника только скрипты.
frame-src	Определяет допустимые источники для загрузки вложенных контекстов просмотра с использованием таких элементов, как <frame> и <iframe>

```
add_header Content-Security-Policy "default-src 'self';";
```

Рис. 8. Пример заголовка *Content Security Policy*

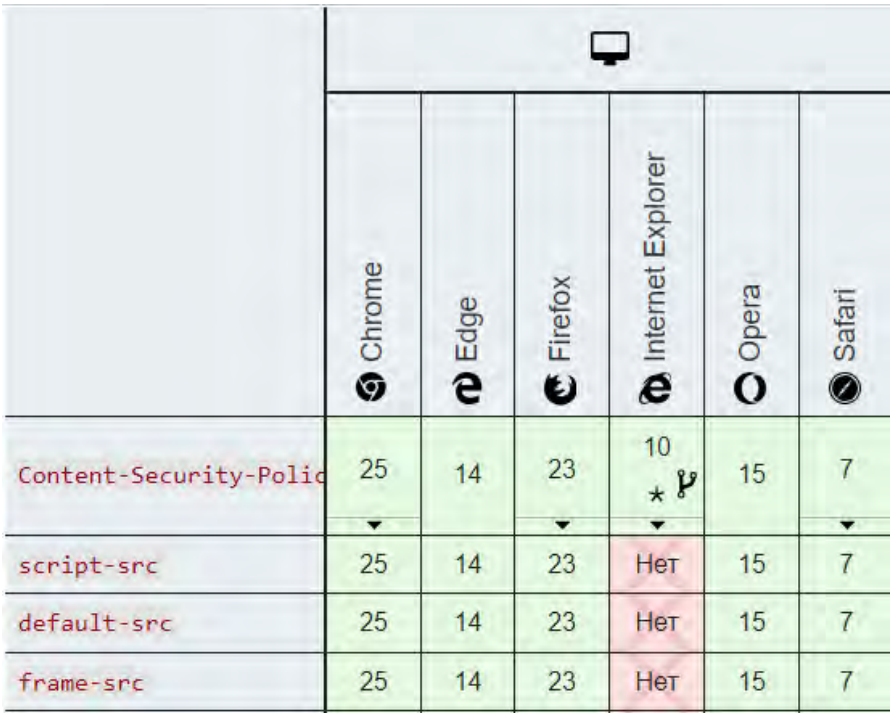


Рис. 9. Поддержка браузерами заголовка *Content Security Policy*

Один из вариантов использования параметра script-src – значение nonce-source, которое разрешает только определенные встроенные блоки

скриптов. Пример использования варианта с nonce-source представлен на рис. 10, 11.

```
Content-Security-Policy: script-src 'nonce-2726c7f26c'
```

Рис. 10. Параметр script-src со значением nonce-source

```
<script nonce="2726c7f26c">
  var inline = 1;
</script>
```

Рис. 11. Разрешенный встроенный блок скрипта с атрибутом nonce

Второй из возможных вариантов использования заголовка CSP – создание хеш-суммы (рис. 12, 13) из встроенных скриптов. CSP поддерживает sha256, sha384 и sha512.

```
script-src 'sha256-B2yPHKaXnvFWtRChIbabYmUBFZdVfKKXHbWtWidDVF8='
```

Рис. 12. Параметр script-src со значением sha256

```
<script>var inline = 1;</script>
```

Рис. 13. Пример скрипта для создания хеш-суммы

Список используемых источников

1. Веб-документация MDN. Протокол передачи гипертекста [Электронный ресурс]. URL: https://developer.mozilla.org/ru/docs/Web/HTTP (дата обращения 20.03.2019).

2. Блог компании HOSTING.cafe. Как использовать HTTP заголовки для предупреждения уязвимостей [Электронный ресурс]. URL: https://habr.com/ru/company/hosting-cafe/blog/315802 (дата обращения 22.03.2019).

3. Википедия, свободная энциклопедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki (дата обращения 24.03.2019).

4. Уязвимости веб приложений. Виды уязвимостей и способы их защиты [Электронный ресурс]. URL: http://ct-po.ru/blog/uyazvimosti-veb-prilozheniy-vidy-uyazvi (дата обращения 24.03.2019).

Статья представлена заведующим кафедрой СПбГУТ, кандидатом технических наук, профессором Л. Б. Бузюковым.

УДК 654.1
ГРНТИ 49.33.29

К ПРОГНОЗУ СРОКА СЛУЖБЫ СТРОИТЕЛЬНОЙ ДЛИНЫ ОПТИЧЕСКОГО КАБЕЛЯ МОДУЛЬНОЙ КОНСТРУКЦИИ

А. О. Нижгородов

Поволжский государственный университет телекоммуникаций и информатики

В представленной работе предпринята попытка прогноза срока службы оптического кабеля модульной конструкции с учетом случайного характера воздействий на оптическое волокно при производстве кабеля. В данной работе ограничились прогнозом срока службы оптического кабеля после приемки и поставки изделия на склад изготовителя.

оптическое волокно, оптический кабель, строительная длина, надежность, срок службы.

Задача прогноза срока службы оптического кабеля до настоящего времени является актуальной и представляет интерес как для производителей, так и потребителей кабеля [1, 2, 3]. В [1] автор рассматривает два основных подхода к прогнозу надежности оптических кабелей и дает обоснование применению в качестве ее более предпочтительной оценки именно срока службы изделия. На оценках срока службы оптического кабеля, введенного в эксплуатацию, базируются прогнозирующие стратегии технического обслуживания кабельных линий [2]. В [3] для определения оценок срока службы оптического кабеля в процессе эксплуатации предлагается комплексный подход, включающий анализ статистики повреждений кабеля на линии, данных мониторинга и результатов специальных измерений параметров кабеля, выполненных, в частности, импульсным рефлектометром обратного рассеяния Мандельштама-Бриллюэна. Вместе с тем, в отличие от оптического волокна, для которого рекомендуемые методики прогноза срока службы регламентированы и подробно описаны [4], для оптического кабеля утвержденных рекомендаций нет.

Рабочие функции, для которых собственно и предназначен оптический кабель, выполняет оптическое волокно, а все остальные элементы кабеля служат для защиты оптических волокон от внешних воздействий в целях обеспечения их работоспособности. Это позволяет полагать, что срок службы оптического кабеля определяется сроком службы оптического во-

локна в кабеле. В этом случае, для прогноза срока службы оптического кабеля можно воспользоваться методикой прогноза срока службы оптического волокна по результатам его испытаний под нагрузкой, рассматривая воздействия на оптическое волокно в процессе изготовления кабеля, строительства, а в последствии и эксплуатации кабельной линии, как испытания оптического волокна под нагрузкой. Для этого надо только знать характер воздействия, нагрузку на волокно и интервал времени, в течение которого она приложена. Очевидно, для процесса производства кабеля и, тем более, для процессов строительства и эксплуатации кабельных линий можно оперировать лишь с вероятностными оценками указанных параметров, определение которых требует выполнения достаточно большого объема статистических исследований.

Один из вариантов изложенного выше подхода к прогнозу срока службы оптического кабеля модульной конструкции был рассмотрен в работе [5]. Авторами были рассмотрены основные технологические процессы производства оптического кабеля. Предложена методики определения эквивалентных значений нагрузки и времени ее воздействия на оптическое волокно при изготовлении кабеля. Выполнен анализ характера воздействий и представлены средние значения нагрузок и интервалов времени при выполнении отдельных технологических операций. Представлены их эквивалентные значения для технологического процесса изготовления кабеля в целом. Осуществлено физическое моделирование нагрузок на оптическое волокно в процессе строительства. Представлен пример прогноза срока службы оптического кабеля на вновь построенной кабельной линии. При этом, время воздействия и нагрузка на волокно рассматривались как детерминированные величины. Безусловно, это справедливо для процесса испытания оптического волокна под нагрузкой, поскольку в данном случае нагрузка на волокно и время воздействия строго контролируются. Однако, в дальнейшем на последующих этапах производства кабеля, а тем более на стадии строительства и эксплуатации кабельной линии, эти величины в общем случае носят случайный характер.

В представленной работе предпринята попытка прогноза срока службы кабеля с учетом случайного характера воздействий на оптическое волокно при производстве кабеля. Поскольку рассматривались воздействия только при производстве кабеля, то ограничились прогнозом срока службы кабеля на складе хранения после приемки и поставки изделия на склад изготовителя.

В соответствие с предложенной в [5] методикой прогноза, базирующейся на детерминированной модели воздействий срока службы оптического кабеля определяется согласно известному выражению [4, 6]:

$$t_s = t_p \left(\frac{\varepsilon_p}{\varepsilon_s} \right)^n \left\{ \left[1 - \frac{\ln(1-F)}{N_p L} \right]^{\frac{1}{\alpha}} - 1 \right\}, \quad (1)$$

где t_s – срок службы волокна в кабеле; t_p – время испытания волокна под нагрузкой; ε_p – напряжение в волокне при испытании под нагрузкой; ε_s – эквивалентное напряжение в волокне после изготовления кабеля; L – длина кабеля; N_p – количество обрывов волокна в процессе испытаний; n – параметр статической усталости; α – параметр распределения Вейбулла; F – надежность прогноза.

Допустим, что остаточное напряжение в оптическом волокне после изготовления и приемки кабеля есть величина случайная и будем оценивать срок службы оптического кабеля, применяя формулу (1), методом статистических испытаний. В процессе испытаний для каждой реализации для заданных значений напряжения в волокне и надежности прогноза получаем оценку срока службы. Задавая некоторое пороговое значение срока службы кабеля будем оценивать вероятность его превышения по формуле:

$$P(t_s \geq t_{th}) = \frac{N(t_s \geq t_{th}) - N(\varepsilon_p \geq \varepsilon_s)}{N_c - N(\varepsilon_p \geq \varepsilon_s)},$$

где $P(t_s \geq t_{th})$ – вероятность того, что срок службы не менее заданного значения; $N(t_s \geq t_{th})$ – число испытаний, для которых срок службы не менее заданного значения; $N(\varepsilon_p \geq \varepsilon_s)$ – число испытаний, для которых выполняется условие $\varepsilon_p \geq \varepsilon_s$; N_c – общее число испытаний.

Здесь учитывали, что кабель с поврежденным оптическим волокном не пройдёт приемо-сдаточные испытания.

По результатам моделирования строим график зависимости вероятности от порогового значения срока службы кабеля. При моделировании полагали, остаточное напряжение волокна описывается законами распределения «с длинным хвостом», а именно законами распределения Парето и Вейбулла [7]. Плотность распределения Парето задается функцией:

$$f(x) = \frac{a}{b} \left(\frac{b}{x} \right)^{a+1},$$

где a – параметр формы, варьируемый в пределах от 1 до 2; b – мода распределения (минимальное значение случайной величины x).

Для распределения Вейбулла с параметрами a (может изменяться от 0 до 1) и β плотность распределения задается функцией:

$$f(x) = a \cdot \beta \cdot x^{a-1} \cdot \exp\left(-\beta \cdot x^{a}\right).$$

По описанному выше алгоритму в результате статистического моделирования были получены оценки срока службы строительной длины оптического кабеля на складе хранения после приемки и поставки изделия на склад изготовителя. Были получены зависимости надежности оценок срока службы от его минимальных пороговых значений. Моделирование было выполнено для двух законов распределений напряжения волокна – Парето и Вейбулла. Вычисления производились для ряда значений параметра a. В целях сравнения искомая зависимость была также рассчитана при условии, что напряжение в волокне есть величина детерминированная. Расчеты производились для строительной длины оптического кабеля L = 4 км. Как и в [5] полагали, что α = 0,04256.

Моделирование было выполнено для тех же параметров, для которых рассчитывался срок службы в работе [5]. А именно, при n = 13, ε_s = 0,1326 %. Результаты представлены на рисунке. Данные, полученные для детерминированной модели воздействий, достаточно хорошо согласуются с результатами, приведенными в статье [5]. Результаты моделирования, полученные для вероятностных моделей воздействий, как и ожидалось, демонстрируют уменьшение срока службы при учете случайного характера воздействий. Причем для распределения Парето – весьма существенное.

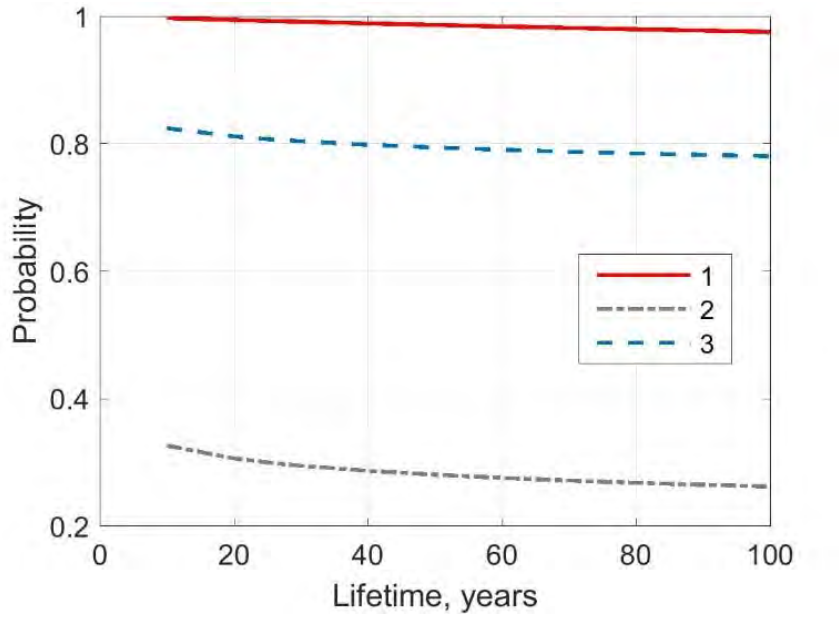


Рисунок. Вероятность того, что срок службы оптического кабеля не менее значения абсциссы. 1 – детерминированная модель; 2 – вероятностная модель (закон Парето); 3 – вероятностная модель (закон Вейбулла)

Можно полагать, что для детерминированной модели воздействий прогнозы дают завышенные оценки срока службы, а предложенные вероятностные модели – заниженные. Предложенные вероятностные модели достаточно грубые, базируются на статической модели и не учитывают случайные кратковременные динамические воздействия, которые, очевидно, могут возникать как при изготовлении кабеля, так и при строительстве и эксплуатации кабельной линии. Выбор параметров законов распределений был достаточно произволен. Вместе с тем, даже такие грубые модели наглядно демонстрируют необходимость учета случайного характера воздействий на волокно на разных стадиях работы с оптическим кабелем. По мнению авторов, общие идеи рассматриваемого в работе решения могут быть развиты и позволят получить модель, позволяющую учитывать при прогнозе срока службы оптического кабеля динамический характер случайных кратковременных воздействий на оптическое волокно в кабеле как на этапах его изготовления, так и на этапах строительства и эксплуатации кабельной линии.

Список используемых источников

1. Зеленяк-Кудрейко И. В., Коршунов В. Н., Ларин Ю. Т. Параметры надежности оптических кабелей // Электросвязь. 1994. № 1. С. 25–28.

2. Петров Ю.М. Надежность функционирования ВОЛС-ВЛ при низких температурах окружающей среды // Электросвязь. 1999. № 3. С. 14–15.

3. Ларин Ю. Т. Оптические кабели: М.: Престиж, 2006. 304 с.: ил.

4. Воронцов А. С., Коршунов В. Н., Цым А. Ю. Оценка долговечности ВОЛС // Электросвязь. 1999. № 2. С. 9–13.

5. Ларин Ю. Т. Сравнительный анализ двух подходов к надежности оптических кабелей// Наука и техника. 2009. № 2 (315). С. 3–7.

6. Бурдин В. А., Воронков А. А., Шафигуллин Л. Н. Эффективность применения прогнозирующих стратегий технического обслуживания ОК // Вестник связи. 2012. № 7. С. 5–8.

7. Воронков А. А., Шафигуллин Л. Н. Проблемы технической эксплуатации волоконно-оптических линий передачи // T-Comm: Телекоммуникации и транспорт. 2011. Т. 5. № 8. С. 40-43.

Статья предоставлена научным руководителем ПГУТИ, доктором технических наук, профессором, В.А. Бурдиным.

УДК 654.09, 519.21
ГРНТИ 49.37.33, 49.03.09, 27.35.30

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ВЕНТЦЕЛЬ-ОВЧАРОВА С РАВНОМЕРНОЙ ВЗАИМОПОМОЩЬЮ ДЛЯ СОВРЕМЕННЫХ СИСТЕМ NFV

А. И. Новиков, В. В. Фицов

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

Концепция NFV заключается в том, чтобы объединить несколько типов оборудования в одно устройство на базе унифицированной платформы. Такие центры обработки данных равномерно распределяют аппаратные ресурсы на заданное количество серверов. Вентцель и Овчаров описывали модель распределения аппаратных ресурсов, которая получила название «математическая модель с равномерной взаимопомощью». В статье будет рассмотрено применение модели Вентцель-Овчарова к центру обработки данных с поддержкой NFV. Система DPI может быть рассмотрена как виртуализированная сетевая функция.

NFV, DPI, Front-End, математическая модель, СМО, равномерная взаимопомощь, модель M/M/V.

Введение

В настоящее время можно выделить несколько наиболее актуальных проблем оператора связи: длительность внедрения новых услуг, большие затраты на обслуживание и обновление оборудования, адаптация системы под определённый вид или объем трафика. Данные проблемы может решить концепция *NFV* (*Network Function Virtualization*, виртуализации сетевых функций) [1, 2, 3, 4].

NFV – это способ виртуализации функций элементов сети оператора связи. Суть *NFV* состоит в том, чтобы реализовать сетевые функции программным путем, вместо того, чтобы использовать специализированное оборудование. Существует архитектура виртуализации сетевых функций, разработанная *ETSI* (*European Telecommunications Standards Institute*, Европейским институтом телекоммуникационных стандартов). Её основной особенностью является возможность оркестрации услуг (выделения виртуальных ресурсов тем или иным услугам по запросу). При этом достигается наиболее эффективное использование аппаратных ресурсов, а также ресурсов хранения и ресурсов сети. У концепции *NFV* есть побочное действие –

повышение нагрузки на оборудование. Можно адаптировать систему к повышенной нагрузке, путём добавления аппаратных средств. Возникает вопрос: какое число аппаратных ресурсов следует добавить для эффективной работы системы?

Математическая модель Вентцель-Овчарова

Значительный интерес представляет распределение аппаратных средств на основе данных математической модели обслуживания. В статье предлагается рассмотреть математическую модель Вентцель-Овчарова с равномерной взаимопомощью между каналами. Концепция данной модели заключается в том, чтобы объединять каналы в группы для совместного обслуживания заявок. У такой системы есть 3 режима работы (рис. 1):

Рис. 1. Граф состояний модели обслуживания с равномерной взаимопомощью

1. Количество заявок меньше максимального количества групп
2. Количество заявок больше максимального количества групп, но меньше количества каналов
3. Количество заявок больше количества каналов.

Первый режим работы подразумевает формирование групп каналов. В данном режиме система работает как классическая СМО, в которой за прибор обслуживания принимается группа каналов. Во втором режиме работы все возможные группы каналов уже сформированы и система начинает постепенно их расформировывать по мере поступления новых заявок.

Третий режим предусматривает постановку новопришедших заявок в очередь. Система переходит в режим работы классической СМО. Система выбирает режим работы в зависимости от количества находящихся в ней заявок.

Применение модели Вентцель-Овчарова

Рассмотрим применение модели Вентель-Овчарова к виртуализированной системе DPI (*Deep Packet Inspection*, глубокой инспекции пакетов). Такого рода системы применяются для накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. Система глубокой инспекции пакетов имеет распределенную архитектуру, но в данный момент нас интересуют подсистемы HF (*Hardware Filter*, аппаратный фильтр) и FE (*Front-End*). На вход аппаратного фильтра приходит поток пакетного трафика, который распределен не по закону Пуассона, а значит для такого потока заявок нельзя применять M/M/V. HF имеет экспоненциальный закон обслуживания заявок, и согласно исследованиям, создает новый поток заявок, распределенный по закону Пуассона [5]. Следовательно, мы можем использовать данную математическую модель на подсистеме Front-End. Так как система глубокой инспекции пакетов должна обрабатывать все заявки, то для упрощения расчетов, можем представить очередь как бесконечную. Следовательно, необходимо подвергнуть модель Вентцель-Овчарова изменениям. Предположим, что интенсивность обслуживания одной заявки группой каналов будет прямо пропорциональна количеству задействованных каналов. Принимая во внимание вышеупомянутые сведения о системе, можно получить интересующие формулы.

Расчетные формулы

Введем некоторые обозначения: n – количество каналов в системе, l – количество каналов в одной группе, h – максимально возможное количество групп. Для данной модели вероятность простоя системы (p_0):

$$p_0 = \left[\sum_{i=0}^{h} \frac{\alpha^i}{i!} + \frac{\alpha^h}{h!}\frac{\beta^{h+1}}{1-\beta}\right]^{-1},$$

где $\alpha = \frac{\lambda}{l\mu}, \beta = \frac{\lambda}{n\mu}$

Используя определения среднего времени ожидания и обслуживания, а также p_0, получаем:

$$\overline{t_{ож}} = \frac{\beta}{n\mu}\frac{\alpha^h}{h!}\beta p_0 \frac{1}{(1-\beta)^2},$$

$$\overline{t_{\text{обслуж}}} = \frac{1}{\sum_{i=1}^{h} il\mu + \sum_{j=h+1}^{n} n\mu}.$$

Основным показателем в данной статье является среднее время нахождения заявки в системе. Её мы получим, сложив среднее время обслуживания и среднее время ожидания:

$$\overline{t_{\text{сист}}} = \frac{1}{\sum_{i=1}^{h} il\mu + \sum_{j=h+1}^{n} n\mu} + \frac{\beta}{n\mu}\frac{\alpha^h}{h!}\beta p_0 \frac{1}{(1-\beta)^2}.$$

Результаты вычислений

Будем считать, что канал составляет 10 % от мощности CPU. Возьмем следующие значения в качестве исходных данных: 1 сервер (10 каналов), интенсивность обслуживания одного канала равна 300, в группе может находится максимум 2 канала. Тогда условием устойчивости системы будет являться неравенство: $\lambda < 3000$. Сравнение будет проводиться с классической СМО (M/M/V с бесконечной очередью). При различных значениях интенсивности входящего потока получим следующие значения среднего времени нахождения заявки в системе (табл. 1, рис. 2):

ТАБЛИЦА 1. Сравнение среднего времени нахождения заявки в системе двух моделей

	λ	1000	1500	2000	2500
модель Вентцель-Овчарова	$\overline{t_{\text{сист}}}$,с	$4{,}779*10^{-4}$	$4{,}994*10^{-4}$	$6{,}552*10^{-4}$	$1{,}723*10^{-3}$
Классическая СМО	$\overline{t_{\text{сист}}}$,с	$3{,}335*10^{-3}$	$3{,}357*10^{-3}$	$3{,}508*10^{-3}$	$4{,}309*10^{-3}$

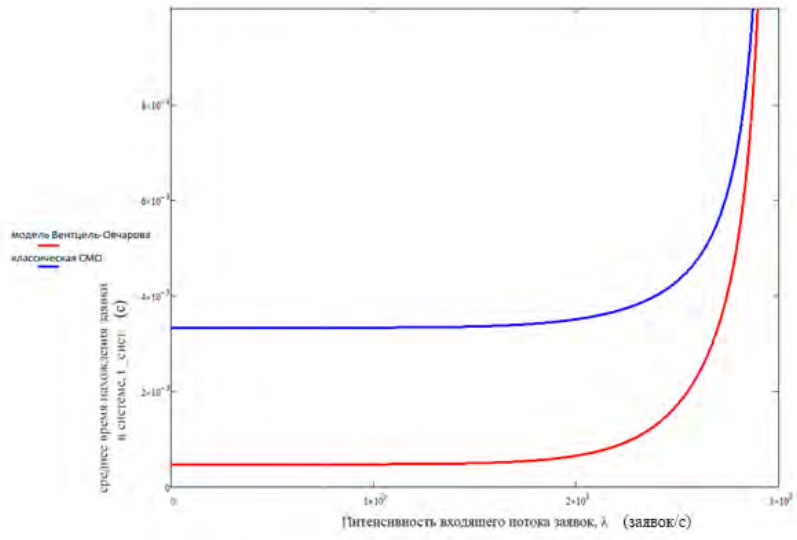


Рис. 2. Зависимость среднего времени нахождения заявки в системе от интенсивности входящего потока заявок

Можно привести другой пример, где ограничим среднее время пребывания заявки в системе. Пусть $\overline{t_{\text{сист}}} \leq 3{,}4 * 10^{-3}$ при $\lambda = 2000$. Тогда, исходя из приведенных формул, нам потребуется число каналов, приведенных в таблице 2.

Таблица 1. Сравнение требуемого количества каналов при ограничении среднего времени пребывания заявки в системе

СМО	Количество каналов	$\overline{t_{\text{сист}}}$, с
Вентцель-Овчарова	8	$2{,}2*10^{-3}$
Классическая	16	$3{,}334*10^{-3}$

Получается, что при использовании одинакового количества аппаратных ресурсов математическая модель Вентцель-Овчарова дает выигрыш в среднем времени нахождения заявки в системе почти на порядок относительно классической многоканальной СМО с ожиданием (при загруженности системы не более, чем на $\frac{2}{3}$).

Список используемых источников

1. Фицов В. В. Применение программного кода для оптимизации числа серверов DPI методом максимального элемента / Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция. СПб. : СПБГУТ, 2018 С. 650–656.

2. Вентцель Е. С. Исследование операций. М. : Советское радио, 1972. – 552 с.

3. Овчаров Л. А. Прикладные задачи теории массового обслуживания / Науч. ред. Е. С. Вентцель. М. : Машиностроение, 1969. – 324 с.

4. Вентцель Е. С. Теория вероятностей; 4-е изд. М. : Наука, 1969. – 576 с.

5. Зайцев В. С. Анализ свойств суммарного потока заявок на входе системы массового обслуживания / Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция. СПб. : СПБГУТ, 2018

Статья представлена заведующим кафедрой СПбГУТ, доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.891.3
ГРНТИ 50.41.25

ИНТЕГРАЦИЯ ПЛАТФОРМЫ 1С:ПРЕДПРИЯТИЕ 8 И НЕЙРОННОЙ СЕТИ ДЛЯ ДИАГНОСТИКИ КАРДИОЛОГИЧЕСКИХ ЗАБОЛЕВАНИЙ

Д. В. Окунева, М. В. Павшева

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

В данном докладе речь идет о машинном обучении нейронной сети на основе базы знаний кардиологических заболеваний, ее интеграции с платформой 1С:Предприятие 8 для объективной и быстрой постановки предварительного диагноза и направления на дальнейшую диагностику по результатам электрокардиограммы пациента.

нейронная сеть, платформа 1С:Предприятие, электрокардиограмма.

На сегодняшний день система программ «1С:Предприятие 8» внедрена в различные области человеческой деятельности, не является исключением и медицина. Существующие прикладные решения не раскрывают возможности платформы по решению задач машинного обучения, именно поэтому следует выделить применение нейросетевых решений как новый вектор развития программных продуктов 1С. С помощью стандартных средств платформы можно создать, обучить и использовать нейронную сеть в целях диагностики сердечно-сосудистых заболеваний на основе анализа электрокардиограммы.

Внедрение технологии машинного обучения позволит уменьшить время на установление промежуточного диагноза для дальнейшего назначения лечения или более глубокой диагностики.

Для решения поставленной задачи может быть использована многослойная нейронная сеть, созданная с помощью штатных механизмов платформы и встроенного языка 1С.

Искусственная нейронная сеть – это программная реализация нейронных структур человеческого мозга. Чтобы не углубляться в его сложное строение, достаточно сказать, что нейроны составляют огромную взаимосвязанную систему, способную передавать сигналы во внешнюю среду в зависимости от электрических или химических импульсов. Основу искусственной нейронной сети составляют искусственные нейроны, взаимосвязанные при помощи группы синапсов – однонаправленных входных связей, соединенных с выходами других нейронов, с которых сигнал возбуждения

или торможения поступает на синапсы следующих нейронов по аналогии с нервными клетками мозга [1].

Структура нейронной сети изображена на рис. 1. На данном этапе в её состав входят четыре слоя, которые состоят из 7, 10, 17 и 37 нейронов. Первый слой – входной, получает амплитуду и продолжительность зубцов, сегментов и интервалов комплексов сердечных сокращений и передает эти значения на следующий уровень без изменения. Второй и третий слои являются скрытыми и отвечают за нахождение отклонений от нормы значений исходных данных и выявляют нарушения, о которых свидетельствуют отклонения. Четвертый, выходной, слой отвечает за установление предварительного диагноза и дальнейшую передачу данных специалисту на согласование для назначения правильного лечения.

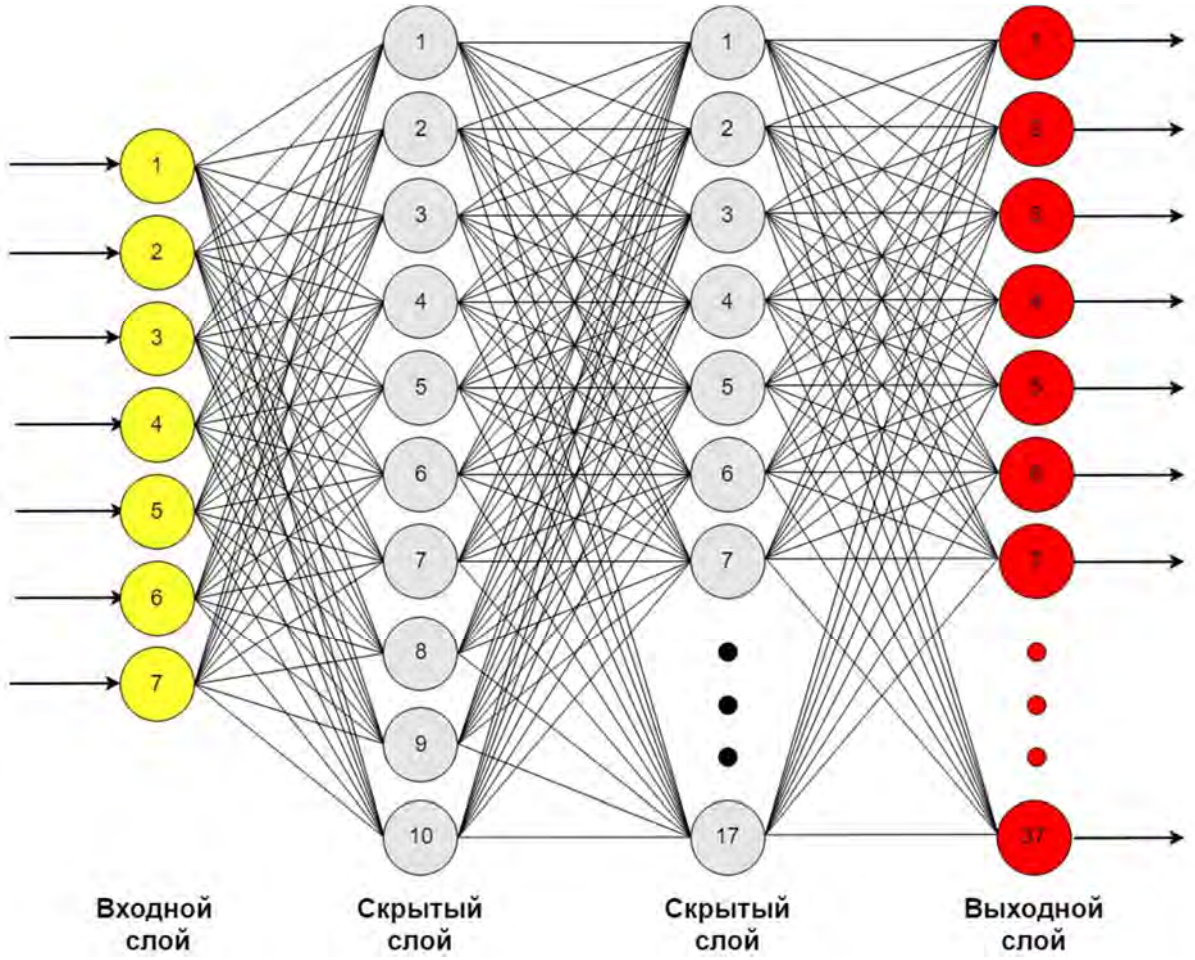


Рис. 1. Структура нейронной сети

Для корректной работы сети необходимо обеспечить правильное формирование двух основных параметров каждого нейрона: входных (INPUT) и выходных данных (OUTPUT). В случае входного нейрона: INPUT = OUTPUT. В остальных, в поле INPUT (1) попадает суммарная информация всех

нейронов с предыдущего слоя, после чего, она нормализуется с помощью функции активации (2) и попадает в поле OUTPUT (3).

$$INPUT = \sum_{j=1}^{n} w_{ij} * x_i, \quad (1)$$

где w_{ij} – веса, x_i – входные нейроны.

$$F_{activation}(INPUT) = \frac{1}{1-e^{-x}}, \quad (2)$$

$$OUTPUT = F_{activation}(INPUT). \quad (3)$$

Система «1С:Предприятие» состоит из технологической платформы и созданных на её основе прикладных решений. Для реализации многослойной нейронной сети создана конфигурация, позволяющая в пользовательском режиме либо заполнить данными и использовать созданную при помощи предопределённых элементов нейронную сеть, либо создать новую и применить для решения собственных задач.

Непериодический регистр сведений «Структура нейронной сети» предусмотрен для хранения данных, обеспечивающих корректную работу сети. В нём заданы связи нейронов, входы и веса. За процесс обучения отвечает команда «Обучить» на форме списка регистра сведений, схема работы которой представлена на рис. 2. В первую очередь случайным образом из промежутка чисел от 0 до 1 инициализируются веса синапсов. Затем подаются входные данные для проверки правильности работы сети. Если выведенный результат не соответствует ожидаемому, веса модифицируются в сторону увеличения или уменьшения в зависимости от величины разницы между идеальным и полученным значениями до тех пор, пока сеть не перестанет ошибаться.

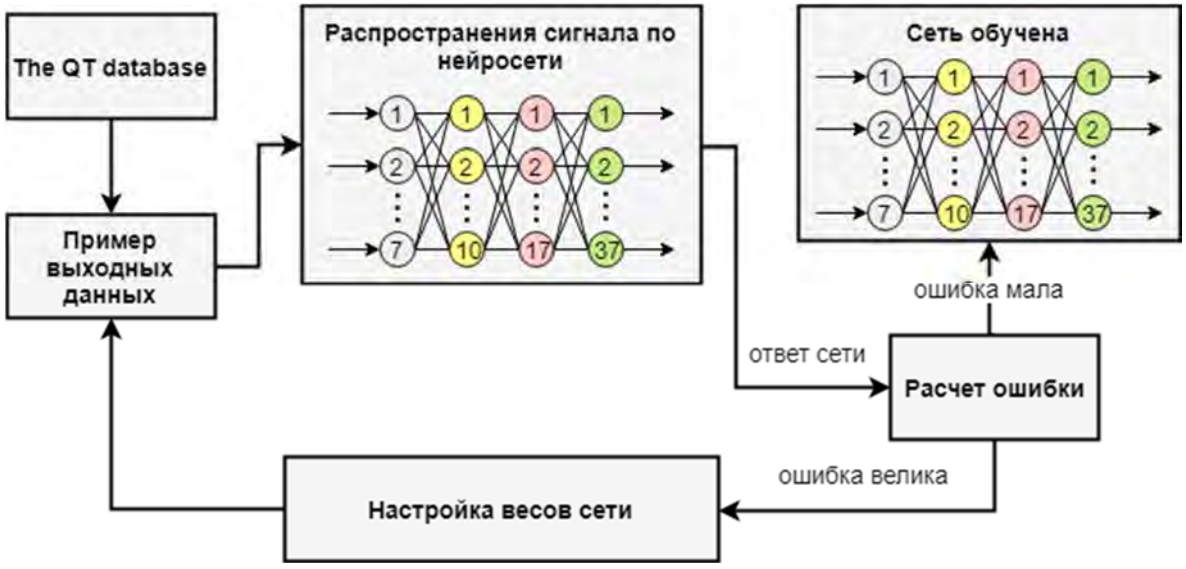


Рис. 2. Схема процесса обучения нейросети с учителем

Объекты конфигурации «Справочники» позволяют хранить в информационной базе данные, имеющие одинаковую структуру и списочный характер [2]. Справочник «Уровни сети» по умолчанию имеет четыре предопределенных элемента: «Первый уровень (вход)», «Второй уровень (скрытый)», «Третий уровень (скрытый)», «Четвертый уровень (выход)». Это обеспечивает четырехуровневую структуру сети. При появлении необходимости изменить количество слоев в сети следует воспользоваться кнопками «Создать», «Изменить» или «Удалить». Справочник «Нейрон» содержит единственный реквизит «Выход нейрона», ссылающийся на справочник «Виды входов сигналов». В этом реквизите указывается тип выходного сигнала нейрона для правильного соотношения с нужными весами следующего слоя.

Для хранения персональных данных пациентов в системе предусмотрен справочник «Пациенты», с помощью которого можно импортировать кардиограмму из ранее сохраненного файла, записанного электрокардиографом.

Расчет нейронной сети выполняется в обработке «Предварительная диагностика» с помощью механизма запросов (рис. 3). Однако следует иметь в виду, что с помощью запросов можно только прочитать нужную информацию из базы данных, но изменить ее и записать обратно нельзя – для этого нужно использовать средства встроенного языка [3].

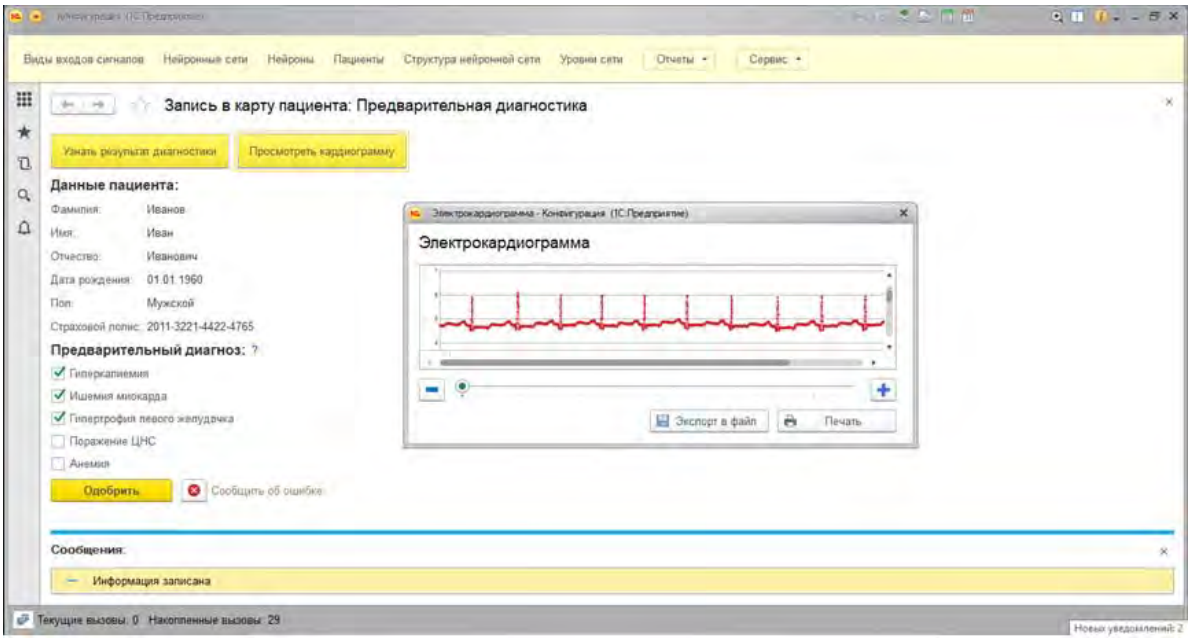


Рис. 3. Работа с результатами анализа нейронной сетью в пользовательском режиме

Для нелинейной нейронной сети невозможно произвести все расчеты в одном запросе из-за наличия функции активации. Путем внутреннего соединения информации из регистра сведений для входного уровня с данными

значений сигналов формируется временная таблица, содержащая входы и соответствующие им сигналы. Для расчета второго, третьего и четвертого уровня используется одинаковая логика запросов: внутренним соединением объединяются данные регистра для соответствующего уровня с временной таблицей входного уровня по виду входа, перемножаются веса на сигналы входов, применяется группировка по нейронам суммированием произведения весов на сигналы входов и применением функции активации.

Материалы и методы

Материалом для исследования послужили данные с открытого ресурса PhysioNet, который предлагает свободный веб-доступ к большому количеству зарегистрированных физиологических сигналов (*PhysioBank*). Для обучения нейронной сети была выбрана база данных The QT Database, которая содержит 105 пятнадцатиминутных отрывков двухканальных ЭКГ, в число которых входят как патологические записи, так и данные о пациентах без диагностированной болезни сердца. Преимуществом является наличие справочных аннотаций с отмеченным расположением границ формы сигнала.

Заключение

1. Сформировано пространство информативных признаков, влияющих на выбор метода лечения заболеваний сердечно-сосудистой системы.

2. Разработан нейросетевой классификатор с помощью штатных механизмов платформы «1С:Предприятие 8». Рассчитаны показатели значимости параметров, которые имели наибольшее влияние на выбор метода дальнейшей диагностики.

3. Выполнено тестовое прогнозирование разработанной системы с использованием контрольной выборки базы данных «The QT Database».

Список используемых источников

1. Медведев В. С. Нейронные сети. Matlab 6. М. : Диалог-МИФИ, 2002. – 496 с.

2. Официальный сайт фирмы 1С [Электронный ресурс]. URL: http://v8.1c.ru

3. Хрусталева Е. Ю. Язык запросов «1С:Предприятия 8». М: ООО «1С-Паблишинг», 2013. – 369 с.: ил. – (Библиотека разработчика). ISBN 978-5-9677-1987-5.

УДК 004.732
ГРНТИ 50.39.27

СИСТЕМА ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ ВИРТУАЛЬНЫМИ ЛОКАЛЬНЫМИ ВЫЧИСЛИТЕЛЬНЫМИ СЕТЯМИ КОРПОРАТИВНОГО УРОВНЯ

И. Б. Саенко, А. М. Старков

Военная академия связи имени Маршала Советского Союза С. М. Буденного

Разработана система технологического управления виртуальными локальными вычислительными сетями, предназначенная для использования разработчиками и администраторами корпоративных информационных систем на стадиях проектирования, эксплуатации и реорганизации вычислительных сетей. Данная система позволяет синтезировать оптимальную схему построения виртуальных локальных вычислительных сетей, удовлетворяющую предъявляемым требованиям и обеспечивающую повышение пропускной способности и защиты от несанкционированного доступа к ресурсам сети.

корпоративная информационная система, виртуальная локальная вычислительная сеть, информационная безопасность, разграничение доступа.

Корпоративной информационной системе (КИС) присущи высокая динамичность вычислительных сетей (ВС) и резкие перепады информационной нагрузки на отдельных направлениях. Одним из перспективных способов решения существующего противоречия является применение технологии «виртуальной локальной вычислительной сети» (*virtual local area network* – VLAN, ВЛВС). Данная технология позволяет повысить пропускную способность ВС и защиту ресурсов сети от несанкционированного доступа (НСД) [1].

Актуальность разработки системы технологического управления ВЛВС корпоративного уровня (технология VLAN относится к уровню технологического управления) обуславливается отсутствием в настоящее время аналогичных решений, а также проектирование структуры сети разработчиками и администраторами КИС, основываясь только на собственном опыте и интуиции [1].

Основная задача технологического управления состоит в выработке и принятия решения по конфигурации ЛВС, с доведением данного решения до элемента сети, а также контролем его исполнения. Для решения задачи

по формированию управляющего воздействия $\Phi(t)$, обеспечивающего оптимальный вариант организации подсетей VLAN в КИС X и предъявляемые требования, предлагается следующая структура системы ТУ ВЛВС корпоративного уровня, представленная на рис. 1.

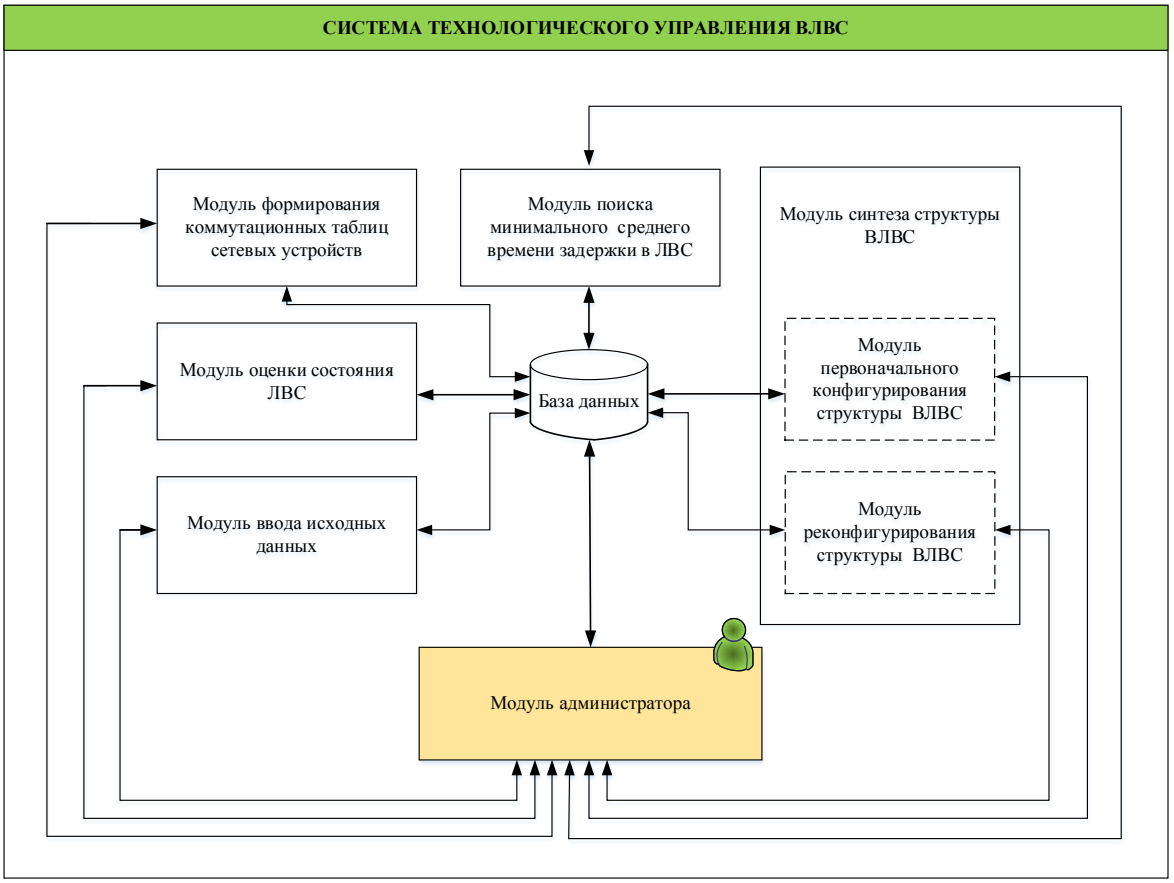


Рис. 1. Структура системы ТУ ВЛВС корпоративного уровня

Основополагающим элементом данной системы является «модуль администратора», который отвечает за взаимодействие и управление остальными модулями.

В связи с многократным использованием данных при их одноразовом вводе, а также обеспечения выработки решения по организации ВЛВС, в режиме времени близкому к реальному, в системе ТУ ВЛВС используется база данных (БД).

Первоначально в «модуле ввода исходных данных» производится задание топологической структуры сети вида: $G=\{A,B,C\}$, где $A=\{a_1,...,a_i\}$, $i=\overline{1,I}$ – множество вершин (узлов) графа, соответствующие множеству сетевых устройств, которые являются источниками и (или) приемниками информации при решении функциональных задач; $B=\{b_{mn}\}$ –

множество ребер (ветвей) графа между вершинами a_i и a_j, которые соединяют сетевые устройства; $C = \{c_{ij}\}$ – пропускная способность ребер (ветвей) графа, которые соединяют сетевые устройства (узлы). Также задается множество информационных потоков между узлами графа – $\Lambda = \{\lambda_{ij}\}$, характеризующее взаимосвязь абонентов в ЛВС с учетом передаваемой информации в единицу времени (λ_{ij} – информационный поток между *i*-м и *j*-м элементом сети) и булева матрица разрешенных информационных потоков $\mathbf{A}[n,n]$, $i, j = \overline{1,n}$, где при $a_{ij} = 1$ обмен между компьютерами *i* и *j* разрешен, в противном случае – невозможен. Кроме того, в данном модуле определяется администратором множество требований к ЛВС $TP_q = \{P_\lambda^{\text{Тр}}, Q_\lambda^{\text{Тр}}, K_{\text{нсд}}^{\text{Тр}}\}, q = \overline{1,Q}$, где $P_\lambda^{\text{Тр}}$ – подмножество требований к значениям вероятностей обмена заданными потоками сообщений в установленные сроки и с требуемым качеством $Q_\lambda^{\text{Тр}}$, $K_{\text{нсд}}^{\text{Тр}}$ – подмножество требований к значениям коэффициента защиты ресурсов ЛВС от НСД.

В «модуле оценки состояния ЛВС» система ТУ ВЛВС корпоративного типа собирает данные о состоянии сети и формирует множество выходных характеристик ЛВС $V = \{v_n\}, n = 1...N$, а также проверяет наличие отклонений текущего состояния сети от предыдущего состояния сети, записанного в БД. В случае отсутствия расхождений между двумя состояниями формируется оптимальный вариант – не реализовывать никаких управлений на данном промежутке времени, которое является одним из допустимых вариантов. При наличии отклонений текущего состояния сети от предыдущего состояния сети запускается «модуль синтеза структуры ВЛВС», который отвечает за синтез матрицы структуры построения VLAN $\mathbf{S}[n,k]$, показывающей распределение компьютеров по подсетям. Данная матрица формируется согласно следующему правилу: если $s_{ij} = 1 (i, j = 1,...,k)$, то компьютер *i* принадлежит подсети *j*, иначе подсеть *j* не охватывает компьютер *i*. Используемые методы обработки знаний при формировании данной матрицы, а также последовательность получения множества решений настройки VLAN $SC = \{\mathbf{S}_p\}$, $p = \overline{1,P}$, где *SC* – множество решений настройки VLAN, $\mathbf{S}_p$ – матрица структуры построения VLAN (особь в популяции), удовлетворяющая условию $\mathbf{A} = \mathbf{S}_p \otimes \mathbf{S}_p^{\text{T}}$, *P* – количество особей в популяции, изложены в [2].

«Модуль синтеза структуры ВЛВС» работает в двух режимах: первоначального конфигурирования структуры ВЛВС (выбирается в случае первоначального формирования структуры ВЛВС для КИС) и реконфигурирования структуры ВЛВС (выбирается в случае трансформации структуры КИС). При выборе одного из режимов запускается соответственно «модуль

первоначального конфигурирования структуры ВЛВС» или «модуль реконфигурирования структуры ВЛВС».

В «модуле поиска минимального среднего времени задержки в ЛВС» проводится поиск минимального значения среднего времени задержки в сети $\overline{T_{zf}}(k_f)$ на основании множества решений настройки VLAN (*SC*), полученного в результате работы «модуля синтеза структуры».

Нахождение минимального $\overline{T_{zf}}(k_f)$ осуществляется методом бинарного поиска [3] и на первом шаге из множества решений *SC* выбирается пять решений: $\mathbf{S}_p(k_{\min})$ – решение с минимальным количеством VLAN, $\mathbf{s}_p(k_{\max})$ – решение с максимальным количеством VLAN, $\mathbf{S}_p(k_{sr})$ – ближайшее решение со средним количеством VLAN, находящееся по формуле $k_{sr} = \frac{k_{\max} + k_{\min}}{2}$, а также ближайшие решения, являющиеся средними слева $\mathbf{S}_p(k_l)$ от $\mathbf{S}_p(k_{sr})$ и справа $\mathbf{S}_p(k_r)$ от $\mathbf{S}_p(k_{sr})$, находящиеся, соответственно, по формулам $k_l = \frac{k_{\min} + k_{sr}}{2}$ и $k_r = \frac{k_{man} + k_{sr}}{2}$. При этом все *k* являются целочисленными и, в случае получения дробного значения, округляются к ближайшему целочисленному значению. В случае отсутствия точных решений $\mathbf{S}_p(k_{sr})$, $\mathbf{S}_p(k_l)$ и $\mathbf{S}_p(k_r)$ находятся ближайшие к ним решения на множестве решений настройки VLAN *SC*.

На втором шаге производится настройка выбранных решений $\mathbf{S}_p(k_{\min})$, $\mathbf{S}_p(k_{\max})$, $\mathbf{S}_p(k_{sr})$, $\mathbf{S}_p(k_l)$, $\mathbf{S}_p(k_r)$ на разработанной имитационной модели и определение зависимостей среднего времени задержки в сети от количества настроенных VLAN $\overline{T_z}(k_{\min})$, $\overline{T_z}(k_{\max})$, $\overline{T_z}(k_{sr})$, $\overline{T_z}(k_l)$, $\overline{T_z}(k_r)$.

На третьем шаге среди полученных значений среднего времени задержки в ЛВС выбирается минимальное значение среднего времени задержки в сети $\overline{T_{zf}}$ при k_f количестве VLAN $\overline{T_{zf}}(k_f)$. Полученное k_f принимается за k_{sr}. Заново определяются $k_{\min}$ и $k_{\max}$, а также производится поиск значений количества VLAN слева (k_l)и справа (k_r) от k_{sr}. Делается переход ко второму шагу бинарного алгоритма.

Последовательность второго и третьего шагов алгоритма повторяется до тех пор, пока не будет найден локальный и глобальный минимум значения среднего времени задержки в сети $\overline{T_{zf}}$ при k_f количестве VLAN – $\overline{T_{zf}}(k_f)$, т. е. при проверке после второго шага выполняется условие $k_{\max} - k_{sr} = 1$ и $k_{sr} - k_{\min} = 1$. В соответствии с найденным значением ко-

личества VLAN k_f, при котором среднее время задержки в сети $\overline{T_{zf}}$ минимально, из множества решений настройки VLAN (*SC*) выбирается оптимальное, т. е. то, у которого максимальна функция пригодности при условии $k = k_f$.

«Модуль формирования коммутационных таблиц сетевых устройств» отвечает за выработку рекомендаций администратору ЛВС по настройке коммутационного оборудования в сети вида: $Rec(sw_j) = \langle port, \{x_k\} \rangle$, где $Rec(sw_j)$ – рекомендации по настройке sw_j коммутатора сети, $port$ – номер порта коммутатора sw_j, x_k – множество ВЛВС, к которым принадлежит a_i (АРМ, коммутатор) элемент сети, подключенный по данному порту $port$ к коммутатору sw_j. Множество подсетей VLAN $X = \{x_k\}$ строится на основании матрицы $\mathbf{S}[n,k]$, где столбец матрицы $\mathbf{S}[n,k]$ является подмножеством x_k.

Для формирования рекомендаций на первом шаге анализируется матрица разрешенных информационных потоков $\mathbf{A}[n,n]$, которая играет роль матрицы «АРМ-АРМ», на наличие выше главной диагонали элементов $a_{ij} = 1$ и формируется матрица требуемых взаимосвязей абонентов ЛВС вида $\mathbf{UR}[n,m]$, $i_{ur} = \overline{1,n}$, $j_{ur} = \overline{1,2}$ где $ur_{i_{ur}} = IN(a_i)$, $ur_{j_{ur}} = IN(a_j)$, $IN(a_i)$ и $IN(a_j)$ – идентификационные номера АРМ (a_i и a_j) в графе сети *G*.

На втором шаге для каждой пары элементов матрицы **UR** производится поиск кратчайшего пути из узла $IN(a_i)$ в узел $IN(a_j)$ при помощи алгоритма Дейкстры [3], для этого примем, что вес каждого ребра в графе *G* равен единице ($w_{ij} = 1$). В результате работы данного алгоритма сформируется множество кратчайших путей для каждой пары вершин $PG(IN(a_i), IN(a_j)) = \{IN(a_{i_G})\}$, $i_G = \overline{1, I_G}$.

На третьем шаге проводится формирование рекомендаций по настройке коммутаторов ($Rec(sw_j) = \langle port, \{x_k\} \rangle$) при помощи последовательного определения для каждого порта $(port)$ коммутационного устройства sw_j из множества кратчайших путей *PG* требуемой настройки VLAN x_k, $a_i \in x_k$.

Список используемых источников

1. Саенко И. Б., Старков А. М. Подход к моделированию виртуальных локальных вычислительных сетей в корпоративных информационных системах // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 1. № 1. С. 66–77.

2. Старков А. М., Саенко И. Б., Волков Д. В. Методика технологического управления виртуальными локальными вычислительными сетями специального назначения // Известия Тульского государственного университета. Технические науки. Тула : Тульский государственный университет, 2018. Вып. 12. С. 423–434.

3. Левитин А. В. Алгоритмы. Введение в разработку и анализ. М. : Вильямс, 2006. 576 с.

УДК 004.75
ГРНТИ 28.19.27

Приглашенный доклад

АРХИТЕКТУРА СИСТЕМЫ РАСПРЕДЕЛЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СКАНЕРОВ СЕТЕВОГО КОНТЕНТА ДЛЯ ЗАДАЧ ЗАЩИТЫ ОТ НЕЖЕЛАТЕЛЬНОЙ ИНФОРМАЦИИ

И. Б. Саенко, А. В. Федорченко

Санкт-Петербургский институт информатики и автоматизации Российской академии наук

Работа посвящена исследованию информационных ресурсов глобальной сети Интернет для реализации задач защиты от нежелательной информации. Целью исследований является разработка распределенной системы для обеспечения сканирования, загрузки и предварительной обработки сетевого контента. В работе исследуются условия обеспечения доступности сетевых ресурсов с учетом ограничительных мер и большого объема информации. В результате приводится разработанная архитектура системы распределенных интеллектуальных сканеров, обладающая свойствами масштабируемости, а также оперативности и гибкости выполнения, поставленных перед ней задач.

сеть Интернет, сетевой контент, распределенный сбор данных.

В настоящее время информационные войны и открытое распространение запрещенного контента в сети Интернет способствуют развитию методов защиты от информации, что делает данное научное направление особенно актуальным. Для решения проблемы ограничения доступа к противоречивой, вредоносной и незаконной информации, помимо задачи распознавания и классификации, предварительно следует выполнять задачи сканирования сети Интернет и загрузки сетевого контента для дальнейшего анализа. Ввиду наличия условно-неограниченного количества обрабатываемой информации для решения указанных задач предлагается использовать

интеллектуальные сканеры на основе параллельных и распределенных методов и технологий анализа данных. Таким образом, целью работы является разработка архитектуры системы распределенных интеллектуальных сканеров (РИС) для задач сбора и предварительной обработки нежелательной информации в сети Интернет.

Вопросы обнаружения информации и манипулирования ею в сети Интернет активно исследуются и обсуждаются в мировом научном сообществе. Задачи сканирования, поиска и обработки сетевого контента используются для различных процессов мониторинга и управления безопасностью, анализа связности и семантического поиска. В работах [1, 2, 3, 4] описываются подходы для различных задач сканирования, таких как: поиск открытых сетевых портов в сети интернет, сканирование содержимого сетевого трафика и др. В работах [5, 6, 7, 8, 9] описываются подходы и программные средства синтаксического разбора сетевого контента в виде человеко-читаемых текстов.

Помимо научных исследований в области оптимизации и развития задач сканирования, поиска и загрузки сетевого информационного контента, существует ряд проектов и программное обеспечение (ПО) с открытым исходным кодом, такие как [10, 11, 12]. Так, средство [10] предоставляет широкий функционал по сканированию как внутренней (Интранет), так и внешней (Интернет) информационно-телекоммуникационной сети с целью детектирования «живых» хостов и их характеристик (управляющая ОС, работающие сервисы, открытые порты, наименования и версии используемого ПО и многие другие).

Проект [11] ориентирован на широкомасштабное сканирование определенных портов глобальной сети Интернет с целью получения сведений о работе обслуживающих их сервисов на задаваемом множестве хостов. Явным преимуществом данного средства заключается повышенная оперативность сканирования всей сети интернет [3]. Однако наиболее острым недостатком является отсутствие поддержки протокола UDP, являющегося одним из основных протоколов передачи данных без гарантии в современных информационно-телекоммуникационных сетях.

Средство [12] предназначено для сканирования хостов, обеспечивающих работу веб-серверов с точки зрения их безопасности. Simple HTTP Scanner позволяет сканировать директории (пути домена) и файлы в них, а также другие признаки веб-серверов.

Ряд веб-сервисов [13,14] и программных средств [15, 16, 17, 18, 19] ориентированы на непосредственный целевой сбор информации из сети Интернет on-line и off-line режимах соответственно. В качестве входных данных, как правило, указывается адрес конечного домена, по которому располагается информационный ресурс.

Основными задачами системы РИС являются:

1) обнаружение сетевых ресурсов в сети Интернет;

2) загрузка сетевого контента в локальное хранилище информации (не является частью описываемой системы);

3) мониторинг изменения загруженных информационных объектов (страниц, ресурсов, их сетевых адресов и доменных имен).

В данной статье рассматривается архитектура компонента РИС только с точки зрения планирования и обеспечения загрузки сетевого контента для формирования обучающего и тестового набора данных. Однако общая концепция построения архитектуры компонента РИС при этом останется неизменной.

Основными проблемами задачи загрузки данных из сети Интернет являются: (1) их большой объем и (2) отсутствие гарантии их доступности. Первая проблема обусловлена условно-неограниченным и слабо-предсказуемым количеством данных в сети Интернет. Даже если имеется ограниченное количество ресурсов, необходимых для загрузки, объем содержащейся в них информации может динамически уменьшаться и увеличиваться (особенно, когда дело касается медиа- и авто-генерируемого контента). Вторая проблема связана с законодательными (сбор данных с заблокированных ресурсов) и внутриполитическими (ограничение автоматизированной загрузки ресурса межсетевым экраном) мерами по ограничению доступа к ресурсам сети Интернет, а также с различными случайными факторами (например, техническими причинами недоступности). Обе проблемы сводятся к техническим ограничениям пропускной способности сети и физическому расположению в пространстве Интернет каждого из сканеров.

Решение поставленных проблем предлагается реализовать за счет децентрализованного (логически и физически) анализа и сканирования ресурсов сети Интернет IR, а также загрузки сетевого контента с помощью компонентов РИС. На рисунке (см. ниже) представлена архитектура системы РИС, которая содержит:

1) сканеры S, полностью выполняющие вычислительный процесс;

2) сетевые ретрансляторы NR, позволяющие динамически распределять сетевую нагрузку;

3) модуль очередей загрузки;

4) сеть Интернет, предоставляющая сетевую доступность загружаемых ресурсов, а также обеспечивающая функциональность всех элементов архитектуры.

Интернет ресурсы не являются частью архитектуры, однако отображены для четкого представления организации доступа к ним (условно объединены в группу).

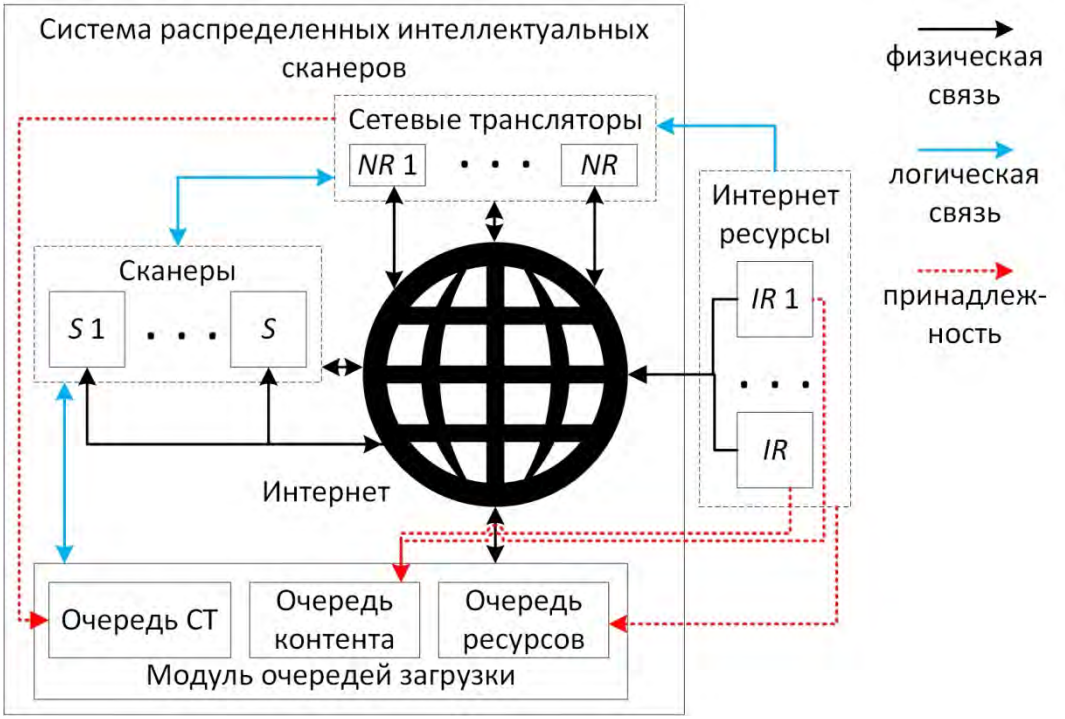


Рисунок. Архитектура системы распределенных интеллектуальных сканеров

Каждый интеллектуальный сканер *S* представлен самостоятельным вычислительным процессом. Общая группа сканеров условно обозначена для отображения логических связей с сетевыми ретрансляторами *NR* и модулем очередей загрузки. Каждый сканер, как и их общая группа, связан физическим каналом с сетью Интернет. Это объясняется возможностью их физического размещения как на отдельном устройстве с собственным сетевым каналом связи, так и параллельное выполнение на одном устройстве (сервере или кластере серверов). Аналогично, в общую группу условно объединены сетевые ретрансляторы *NR*. В свою очередь, модуль очередей загрузки является неделимым динамическим хранилищем. Он позволяет в реальном времени предоставлять сканерам информацию о тех *IR* и их объектах, которые требуется загрузить, а также информацию о расположении в сети Интернет сетевых трансляторов *NR*. Для сбора информации при обучении компонента аналитической обработки, очередь ресурсов является заполненной. Тогда как очередь сетевого контента наполняется при загрузке и анализе каждого из *IR*. Каждый сканер *S* может быть связан с одним и более сетевым транслятором *NR*. Вместе с тем, каждый транслятор *NR* может одновременно обслуживать более одного сканера. Также, ввиду распределенного удаления *NR* в сети Интернет, использующие их сканеры первоначального проверяют доступность загружаемого *IR* при первичном обращении. Такой подход позволяет планировать загрузку *IR* наиболее эффективным образом.

Таким образом, в результате проделанной работы была разработана архитектура системы РИС для выполнения сбора и предварительной обработки информации из сети Интернет для задач защиты от информации. Преимуществом представленной архитектуры системы РИС является децентрализованное и распределенное управление загрузкой сетевого контента за счет общих очередей загрузки, а также обратной связи от сетевых ретрансляторов. Стоит отметить, что каждый сетевой сканер S обеспечивает как самостоятельное принятие решения о выборе ретрансляторов для снижения сетевой нагрузки, так и принимает участие в формировании общего списка загрузки.

Работа выполнена при поддержке РНФ (грант № 18-11-00302).

Список используемых источников

1. Leonard D., Loguinov D. Demystifying Service Discovery: Implementing an Internet-Wide Scanner // Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. Melbourne, Australia, November 01 30, 2010. P. 109–122.

2. Moscola J., Lockwood J., Loui R. P., Pachos M. Implementation of a Content-Scanning Module for an Internet Firewall // Proceedings of the 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines. Napa, CA, USA, April 9 11, 2003.

3. Durumeric Z., Wustrow E., Halderman J. A. ZMap: Fast Internet-wide Scanning and Its Security Applications // Proceedings of the 22nd USENIX Security Symposium. Washington, D.C., USA, August 14–16, 2013. P. 605–619.

4. Durumeric Z., Adrian D., Mirian A., Bailey M., Halderman J. A. A Search Engine Backed by Internet-Wide Scanning // Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, Colorado, USA, October 12–16, 2015. P. 542–553.

5. Petrov S., McDonald R. Overview of the 2012 Shared Task on Parsing the Web // Notes of the First Workshop on Syntactic Analysis of Non-Canonical Language (SANCL), 2012. Vol.59.

6. Zhang Z., He B., Chang K. C. Understanding Web query interfaces: best-effort parsing with hidden syntax // Proceedings of the 2004 ACM SIGMOD international conference on Management of data. Paris, France, June, 13 18, 2004. P. 107–118.

7. Ovrelid L., Skjaerholt A. Lexical categories for improved parsing of web data // Proceedings of the 24th International Conference on Computational Linguistics (COLING 2012). Mumbai, India, 8 15 December, 2012. P. 903–912.

8. Khan M., Dickinson M., Kubler S. Towards Domain Adaptation for Parsing Web Data // Proceedings of Recent Advances in Natural Language Processing. Hissar, Bulgaria, 7–13 September, 2013. P.357–364.

9. Zhang W., Engelen R. A Table-Driven Streaming XML Parsing Methodology for High-Performance Web Services // Proceedings of the 2006 IEEE International Conference on Web Services (ICWS'06). Chicago, IL, USA, 18-22 September, 2006. P. 197–204.

10. Nmap Free Security Scanner [Электронный ресурс] // URL: https://nmap.org/ (дата обращения 25.02.2019).

11. The ZMap Project [Электронный ресурс] // URL: https://zmap.io/ (дата обращения 25.02.2019).

12. Simple HTTP Scanner [Электронный ресурс] // URL: https://sourceforge.net/projects/shttpscanner (дата обращения 25.02.2019).
13. WEBSITE DOWNLOADER. A Free Tool By Wayback Machine Downloader [Электронный ресурс] // URL: https://www.waybackmachinedownloader.com/website-downloader-online (дата обращения 25.02.2019).
14. Web Downloader [Электронный ресурс] // URL: https://web-downloader.en.softonic.com (дата обращения 25.02.2019).
15. HTTrack WEBSITE COPIER [Электронный ресурс] // URL: https://www.httrack.com (дата обращения 25.02.2019).
16. SurfOffline 2.2 Website downloader [Электронный ресурс] // URL: http://www.surfoffline.com (дата обращения 25.02.2019).
17. Website eXtractor [Электронный ресурс] // URL: http://www.esalesbiz.com/extra (дата обращения 25.02.2019).
18. SiteSucker [Электронный ресурс] // URL: http://ricks-apps.com /osx/sitesucker/index.html (дата обращения 25.02.2019).
19. Blue Squirrel [Электронный ресурс] // URL: http://www.bluesquirrel.com/products/grabasite/ (дата обращения 25.02.2019).

УДК 004.032.24
ГРНТИ 20.15.05

АНАЛИЗ ВОЗМОЖНОСТЕЙ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ «АКТИВНЫХ СЕРВЕРНЫХ СТРАНИЦ» ДЛЯ РЕАЛИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

И. Б. Саенко, Д. С. Шаповалов

Военная академия связи имени Маршала Советского Союза С. М. Буденного

Рассматриваются возможности построения автоматизированной информационной системы с использованием модели обработки данных на основе технологии «активных серверных страниц». Детально рассматриваются отдельные характеристики ключевых процессов, влияющих на функционирование системы. Приводятся результаты экспериментальной оценки возможных способов реализации модели и даются рекомендации по их применению в системе.

автоматизированная информационная система, модель обработки данных, веб-программирование.

В настоящее время практически в каждой автоматизированной информационной системе (АИС) достаточно острым является вопрос сбора, обработки, хранения и выдачи различного рода информации. Существующий уровень пользовательских услуг характеризуется увеличением размера поступающего потока данных, что связано с ростом многозадачности процессов управления, увеличением количества хостов и объема информации. Автоматизированная система учета научной работы (АСУНР), рассматриваемая в качестве примера, в полной мере отвечает данной характеристике. Трафик, который необходимо фиксировать в этой системе, имеет разнородных характер за счет наличия большого количества имеющих свою специфику органов управления научно-исследовательской работой. Кроме того, возникает необходимость перекрестного учета информации при взаимодействии различных органов управления друг с другом. Таким образом, при рассмотрении АСУНР речь идет о распределенной системе обработки информации [1, 2].

В результате возникает острая необходимость разработки соответствующих информационных технологий, поддерживающих полный функционал общеязыковой среды исполнения, богатый инструментарий, быстрое понимание основ разработки программистом, достойную скорость исполнения проекта. Одним из направлений решения этой проблемы видится применение технологии «активных серверных страниц» (англ. *Active Server Pages*, ASP). Поэтому целью настоящей работы является разработка модели обработки данных на основе технологии «активных серверных страниц» и оценки эффекта ее практической реализации в АСУНР.

Общая последовательность функционирования «активных серверных страниц» выглядит следующим образом. Клиент – должностное лицо (ДЛ), с удаленного рабочего места (РМ) посылает запрос на *ASP*-страницу на сервер АИС. Сервер принимает запрос и приступает к его обработке. Обработка запроса начинается с определения запрашиваемого файла с расширением asp, после чего сервер работает с содержимым этого файла через обработчик *ASP*: интерпретирует и выполняет вставки *ASP*-кода, содержащего обращения к источникам данных. Примерами таких вставок, являются «%*Response.Write*%» и «%*Data*()%». Таким образом, на сторону РМ ДЛ отправляется гипертекстовая страница (HTML) без *ASP*-кода. Иными словами, копирование серверных сценариев клиентом невозможно, т.к. обозреватель получает лишь результаты их выполнения [3, 4].

Реализация данной модели возможна следующими способами:

1) способ «ВК» – использование валидации и специально созданного класса для замены элемента управления (контроля);

2) способ «НН» – неиспользование валидации и специально созданного класса;

3) способ «НК» – неиспользование валидации, но использование специально созданного класса;

4) способ «ВН» – использование валидации, но неиспользование специально созданного класса.

Валидация (контроль ввода), являющаяся первой составляющей эксперимента, играет важную роль при оптимизации работы многий сложных приложений. Однако, в некоторых случаях, могут применяться и другие варианты обеспечения эффективной работы приложения. В рассматриваемом примере АИС контроль ввода данных подразумевает, что клиент выбирает в выпадающем списке символ по умолчанию для его ввода в базу данных (БД). Данная проблема решается установкой флага запрета на отображение некорректного символа.

Вторая составляющая эксперимента заключается в том, что заголовок регистрационных данных будет отображаться без использования меток либо каких-то дополнительных контролов. Для реализации данной идеи создается следующий специальный класс «*Head*»:

```
public class Head
{ public string Text { get;set;}
  public Head (string text)
   {
      this.Text = text; }}
```

В папке программы *App_Data* размещается текстовый документ *TextFile*.txt с содержимым:

```
<div>
<p><%REG%></p>
</div>
```

Код для преобразования виртуального адреса файла в физический добавляется в папку *Page_Load*, после чего выполняется следующая замена:

```
string filename = Server.MapPath(@"App_Data\TextFile.txt");
      output = File.ReadAllText(filename);
      Head h = new Head("Регистрация");
      output = output.Replace("<%REG%>", h.Text);
```

Заголовок в разметке выводится при помощи кодовой вставки *<%=output%>* [2, 3, 4].

Оценка работы приложения, реализующего рассматриваемую модель, производилась на ЭВМ следующей конфигурации: Intel(R) Pentium(R) CPU

B960 @ 2.20 GHz 2.20 GHz, ОЗУ 4 Гб, ОС Windows Server 2012 R2 Standard, ×64, Visual Studio 2010 версии 10.0.30319.1 RTMRel, Microsoft.NET Framework версии 4.5.52282 RTMRel 2010. Использовалась программа «Монитор ресурсов», версия 6.3.9600. Интервал измерений в каждом эксперименте составлял 60 секунд. В табл. 1 представлены результаты сравнительной оценки способов реализации модели.

ТАБЛИЦА 1. Сравнение способов реализации модели

Загружаемый набор данных, Кб	Вариант	Объем данных для процесса, Кбайт	
		sqlservr.exe	WebDev.WebServer40.exe
Общий	ВН	22424	35160
Выделение		71128	38976
Рабочий		62064	53352
Общий	НК	22028	34980
Выделение		71524	38676
Рабочий		61001	52928
Общий	НН	22321	35124
Выделение		71328	38416
Рабочий		61940	52788
Общий	ВК	22528	34924
Выделение		71624	38692
Рабочий		62196	52856

Из проведенных экспериментов видно, что применение рассмотренных выше способов реализации модели отражается на загрузке процесса локального веб-сервера и среды конфигурирования. Из таблицы 1 видно, что применение валидации уместно при наличии небольшого приложения. Что касается больших программных продуктов, то рекомендуется внимательно изучать структуру проекта, чтобы найти эффективные способы обхода валидации, где это возможно.

В таблице 2 представлены данные загрузки центрального процессора (ЦП) при различных способах реализации модели, снятые программой «Монитор ресурсов».

Использование способа с применением классов в обход стандартных контролов приводит к появлению выраженных скачков в загрузке ЦП (способы ВК и НК, табл. 2), с контролами – к концентрированной загрузке. Какой вариант лучше использовать – это зависит от конкретной задачи. С точки зрения безопасности, рационально остановиться на варианте ВК,

так как интервал загрузки небольшой. За столь малый промежуток времени вредоносный трафик сможет нанести вред системе с меньшей вероятностью.

ТАБЛИЦА 2. Сравнение загрузки ЦП

Вариант	Количество выраженных скачков загрузки ЦП
ВН	2
НК	4
НН	1
ВК	3

Таким образом, в результате разработки и практической реализации модели обработки данных в АИС на основе технологии «активных серверных страниц» видно, что в зависимости от тех или иных условий необходимо использовать определенный способ ее реализации. Правильный подход будет напрямую влиять на работу веб-сервера, среду конфигурирования, управления, доступа и разработки его компонентов, сочетающую в себе элементы Analysis Manager, Enterprise Manager и Query Analysis. Кроме того, с учётом связи данных процессов со службами Reporting Services, Integration Services и другими, приоритет анализа и учёта предложенных способов в ходе всех этапов разработки приобретает значительный вес.

Дальнейшие направления исследований связываются с интеграцией модели «активных серверных страниц» в модель веб-сервера.

Список используемых источников

1. Шаповалов Д. С., Хазиев Н. Н. Проектирование программного обеспечения с использованием стандартов UML // Труды ЦНИИС. Санкт-Петербургский филиал. 2017. Т. 1 (4). С. 141–146.

2. Котенко И. В., Саенко И. Б., Полубелова О. В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации // Труды СПИИРАН. 2013. N 2 (25). С. 113–134.

3. Беллиньясо М. Разработка веб-приложений в среде ASP.NET 2.0: задача – проект – решение. М. : «Диалектика», 2007.

4. Экспозито Д. Знакомство с технологией Microsoft ASP.NET 2.0 AJAX. СПб. : Питер, 2007. 321 с.

УДК 621.39
ГРНТИ 49.33.29

ПРОЦЕДУРА АКТИВАЦИИ ONU В СЕТЯХ NG-PON2

А. Р. Салтыков, В. Д. Ястребов

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

В настоящей статье рассматриваются процессы активации, при которых неактивный ONU подключается или переподключается к сети NG-PON2. Процедура активации включает в себя три этапа, в частности: изучение параметров, получение серийного номера и выбор диапазона. Во время фазы изучения параметров ONU получает рабочие параметры, которые необходимы в восходящем потоке. На этапе получения серийного номера OLT обнаруживает новый ONU (по серийному номеру) и назначает ему идентификатор.

ONU, PON, процессы активации, NG-PON2.

Активация ONU обеспечивается сходимостью передачи мультиплексирования с разделением по времени и длине волны (TWDM-TC) и определяется рекомендацией [1]. В стандарте NG-PON2 есть два варианта канала PLOAM. Опция внутри полосы является классической передачей сообщений PLOAM, а опция вспомогательного канала управления и контроля (*auxiliary management and control channel,* AMCC) является обязательной для ONU, которые не соответствуют указанным пределам калибровки для данной длины волны восходящего канала (рис., см. ниже).

Состояние *O*1 – начальное состояние: ONU находится в этом состоянии, когда он включен. В этот момент происходит сканирование и калибровка нисходящего канала. Устройство также может перейти в это состояние при деактивации или при включенной аварийной остановке. Передатчик выключен, и ранее установленные параметры, такие как ONU-ID, профили пакета и выравнивающая задержка, должны быть удалены. Затем запускается машина синхронизации (рис.). Подсостояние *O*1.1 называется Off-Sync. В этом состоянии ONU пытается синхронизироваться в нисходящем направлении. Как только синхронизация завершена, ONU переходит к следующему подсостоянию, *O*1.2, известному как изучение профиля [2, 3]. Когда достаточно информации было собрано, ONU оценивает длину волны нисходящего канала. Если канал подходит для активации, ONU продолжает процесс и переходит в следующее состояние. Однако, если он не подходит,

ONU ищет альтернативный канал и возвращается к подсостоянию *O*1.1, сохраняя информацию о системе и канале, но отбрасывая информацию о профиле пакета.

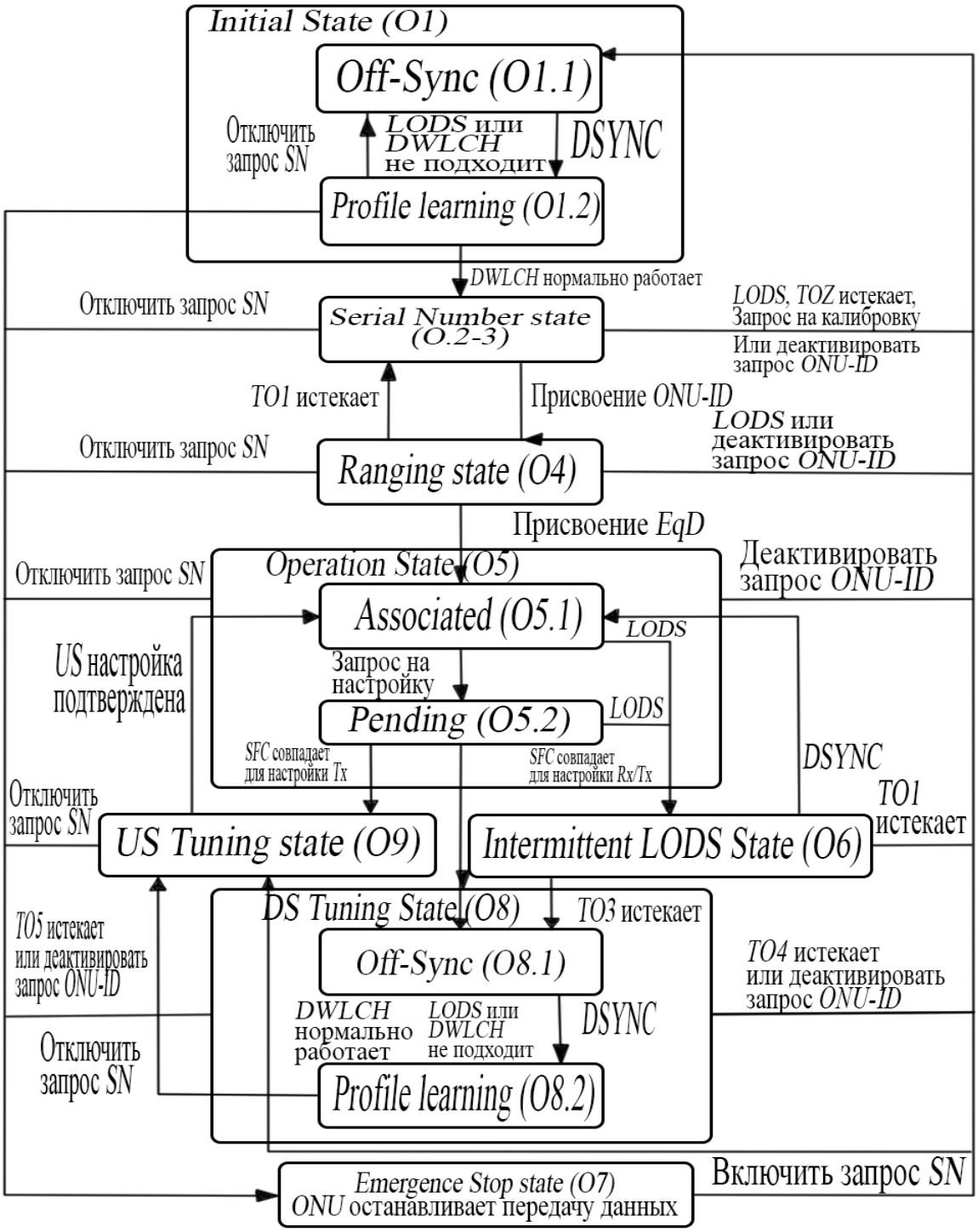


Рисунок. Процесс активации ONU в NG-PON2

Состояние *O*2-3 – состояние серийного номера: в этом состоянии ONU активирует свой передатчик и пытается настроить длину волны восходящего канала в соответствии с длиной волны нисходящего канала. Как только ONU удовлетворяет минимальным требованиям к точности калибровки для требуемой длины волны восходящего канала, он получает запрос, известный как внутриполосное разрешение SN, для отправки серийного номера. Сообщение «Серийный номер ONU» отправляется в ответ на этот запрос. Однако если ONU не соответствует минимальной точности калибровки, он получает запрос на отправку номера типа AMCC. В этом случае сообщение PLOAM ONU с серийным номером AMCC отправляется в ответ на этот запрос. Затем ONU ожидает ответа от OLT, который может быть в форме сообщения Assign ONU-ID, сообщения PLOAM запроса калибровки и регулировки длины волны *Tx*. В зависимости от принятого сообщения или запроса ONU либо остается в этом состоянии и настраивает передатчик, возвращается в исходное состояние *O*1, чтобы другой канал TWDM мог быть откалиброван, или переходит в следующее состояние и продолжает процесс активации. В этом состоянии ONU запускает таймер обнаружения, называемый TOZ. Если этот таймер истекает без ONU, получающего ответ от OLT, он возвращается в состояние *O*1. В этом случае устройство отбрасывает всю накопленную информацию о системе, канале и профиле пакета.

Состояние *O*4 – состояние ранжирования: в этом состоянии ONU отвечает на разрешение ранжирования. Если он получает разрешение на ранжирование профиля пакета из предыдущего сообщения PLOAM профиля пакета, передается пакет FS, несущий сообщение PLOAM регистрации. Как только ONU получает сообщение Ranging Time с выравнивающей задержкой, он переходит в следующее состояние. В этом состоянии запускается таймер *TO*1 с рекомендуемой продолжительностью 10 секунд. Если время таймера истекает, ONU удаляет выделенный ONU-ID вместе со всеми ранее установленными параметрами и возвращается в состояние *O*2-3, сохраняя при этом собранную информацию профиля.

Состояние *O*5 – рабочее состояние: в этом состоянии ONU уже обрабатывает кадры в нисходящем направлении и передает пакеты в восходящем направлении в соответствии с инструкциями от OLT. Это конкретное состояние делится на два подсостояния. Точкой входа этого состояния является *O*5.1, которая называется Associated.

ONU связан с конкретным каналом TWDM, и сообщение «Нет настройки Tuning ControlPLOAM» ожидает обработки. Другое подсостояние, *O*5.2, называется Pending. Хотя ONU завершает восходящую передачу блоков SDU, фрагментация которых уже началась в предыдущем подсостоянии, он выполняет дальнейшую фрагментацию, если необходимо, и передает любые нефрагментированные блоки SDU [4].

Состояние *O*6 – прерывистое состояние LODS: ONU может достичь этого состояния из состояния *O*5 в случае потери синхронизации в нисходящем направлении. При входе в это состояние устройство включает таймер.

Когда защита длины волны канала (*wavelength channel protection*, WLCP) включена, таймер *TO*3 включен. Если WLCP выключен, таймер *TO*2 включается. Если нисходящий сигнал восстанавливается до истечения любого из двух таймеров, ONU возвращается в состояние *O*5. Однако по истечении таймера *TO*2 ONU переходит в исходное состояние *O*1. В другом случае, если таймер *TO*3 истекает, ONU переходит в состояние *O*8.

Состояние *O*7 – состояние аварийной остановки: ONU переходит в это состояние, если получает сообщение «Disable Serial Number» с включенной опцией «Disable». В этом случае он отключает лазер. Тем не менее, он поддерживает работу нисходящей синхронизирующей машины и анализирует секцию PLOAM нисходящих кадров FS (однако в этот момент запрещено передавать любые нисходящие данные или отправлять любые восходящие данные). Если ONU получает сообщение «Disable Serial Number» с включенной опцией «enable», он возвращается в состояние *O*1.

Состояние *O*8 – состояние настройки в нисходящем направлении: в этом состоянии ONU пытается восстановить передачу с использованием нового канала TWDM, в то же время поддерживая конфигурацию уровня TC, за исключением его профилей пакета. В этом состоянии используется таймер *TO*4. Когда он истекает, ONU возвращается в исходное состояние *O*1 и сбрасывает конфигурацию уровня TC. В подсостоянии *O*8.1, также известном, как Off-Sync, ONU настраивает свой приемник и пытается синхронизироваться с нисходящим сигналом. Как только он синхронизируется, он перемещается в подсостояние *O*8.2, известное как Изучение профиля. В этом состоянии он анализирует кадр подуровня кадрирования в нисходящем направлении (FS) и начинает сбор информации о системе, канале и профиле пакета [4].

Когда будет собрано достаточно информации, ONU оценит длину волны нисходящего канала. Если этот канал подходит для активации, ONU продолжает процесс активации и переходит в следующее состояние. Однако, если он не подходит, ONU ищет альтернативный канал и возвращается к подсостоянию *O*8.1, сохраняя информацию о системе и канале, но отбрасывая информацию о профиле пакета.

Состояние *O*9 – состояние настройки восходящего потока: пока ONU находится в этом состоянии, он ожидает обратной связи от OLT и выполняет точную настройку своего передатчика. Впоследствии он переходит в состояние *O*5. В этом состоянии таймер *TO*5 запускается. Если этот таймер истекает, ONU возвращается в исходное состояние.

Список используемых источников

1. Recommendation G.989.3. 40-Gigabit-Capable Passive Optical Networks (NG-PON2): Transmission Convergence Layer Specification. ITU-T, Geneva, Switzerland, 2015. 250 p.

2. Luo Y., Zhou X., Effenberger F., Yan X., Peng, G., Qian Y., Ma Y. Time- and wavelength-division multiplexed passive optical network (TWDM-PON) for next-generation PON stage 2 (NG-PON2) // IEEE Journal of Lightwave Technology. Feb. 2013. Vol. 31. Iss. 4. PP. 587–593.

3. Micolta J. C. V. Analysis of Performances and Tolerances of the Second Generation Optical Networks (NG-PON2) for FTTH Systems. 2014.

Nesset D. NG-PON2 Technology and Standards // IEEE Journal of Lightwave Technology. 2015. Vol. 33, Iss. 5. PP. 1136–1143.

4. Bertignono L., Ferrero V., Valvo M., Gaudino R. Photon ranging techniques for upstream signalling in TWDM-PON during ONU activation // IEEE Journal of Lightwave Technology. April 2015. Vol. 34. Iss. 8. PP. 2064–2071.

Статья представлена заведующим кафедрой СПбГУТ, кандидатом технических наук, доцентом С. Ф. Глаголевым.

УДК 004.056
ГРНТИ 81.93.29

РАЗРАБОТКА ЗАЩИЩЕННОГО ВЕБ-ИНТЕРФЕЙСА ДЛЯ УПРАВЛЕНИЯ УСТРОЙСТВАМИ В СЕТИ

А. И. Таргонская, А. Ю. Цветков

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

В век стремительного развития информационных технологий удаленное управление являются неотъемлемой частью в работе с различным оборудованием. Несмотря на наличие большого числа реализаций клиент-серверных программ удаленного управления, подавляющее большинство существующих решений не удовлетворяет требованиям больших современных кампаний. Такие компании в наибольшей степени ощущают необходимость в наличии единой системы управления сетью, ввиду большого количества физически удалённых филиалов и обширного штата сотрудников технической поддержки. Исходя из это было принято решение разработать достаточно простую единую централизованная систему управления устройствами сети с наличием базы данных пользователей и возможностью частичного делегирования полномочий.

веб-разработка, удаленное управление, информационная безопасность.

В век стремительного развития информационных технологий удаленное управление являются неотъемлемой частью в работе с различным оборудованием. Многочисленные реализации данной технологии применяются практически повсеместно. Удалённое управление позволяет решить целый спектр различных задач: от исправления бытовых ошибок некомпетентных пользователей персонального компьютера до поддержания сложных сценариев с наличием множества сетевых устройств. Учитывая современные тенденции все больше работодателей предлагает ИТ-специалистам возможность удаленной работы, само наличие которой подразумевает необходимость использования программного комплекса удалённого управления. Однако особенной популярностью удалённое управление пользуется в рядах персонала технической поддержки. Данная категория специалистов использует удалённое управление повсеместно, по понятному ряду причин: далеко не все обслуживаемые точки находятся в физической доступности и не всегда целесообразно пересекать относительно большие расстояния для решения проблем, которые, чаще всего, можно решить удалённо.

Появление протоколов удалённого управления во многом обусловлено широким распространением компьютерных сетей и стремительно растущим количеством конфигурируемого оборудования. В наши дни, несмотря на большое количество различных протоколов удалённого управления, особенную популярность приобрели протоколы telnet и ssh [1].

Протокол Telnet (*teletype network*) считается одним из первых стандартизованных протоколов удалённого доступа. Telnet – многопользовательский клиент-серверный протокол прикладного уровня, что подразумевает наличие клиентской реализации для управляющего устройства и соответственно серверной для управляемого устройства. Фактически Telnet является простой эмуляцией терминальной сессии без наличия каких-либо механизмов безопасности, что является довольно серьёзным недостатком. Механизм работы Telnet строится на поддержании управляющей дуплексной TCP сессии, в которой осуществляется передача команд терминалу удалённой системы и возврат результата их выполнения.

Однако, когда речь заходит о безопасном управлении устройствами предпочтение, в большинстве случаев, отдают протоколу SSH (*Secure Shell*), так как он обеспечивает шифрование всего трафика. SSH дословно переводится как «безопасная оболочка», что в полной мере отражает принципы его работы.

Несмотря на наличие большого числа реализаций клиент-серверных программ удаленного управления, подавляющее большинство существующих решений не удовлетворяет требованиям больших современных кампаний. Такие компании в наибольшей степени ощущают необходимость в наличии единой системы управления сетью, в виду большого количества

физически удалённых филиалов и обширного штата сотрудников технической поддержки.

Исходя из это было принято решение разработать достаточно простую единую централизованная систему управления устройствами сети с наличием базы данных пользователей и возможностью частичного делегирования полномочий.

Основными достоинствами которой будут:

- интуитивно-понятный интерфейс;
- централизованное управление;
- кроссплатформенность (Работа прямо из браузера);
- разграничение прав доступа.

Так как разрабатываемое веб-приложение должно быть защищенным необходимо ознакомиться с наиболее популярными уязвимостями. Ссылаясь на Open Web Application Security Project (OWASP), который является открытым проектом обеспечения безопасности веб-приложений, можно выделить 10 самых опасных рисков (уязвимостей) веб-приложений [2].

1. Внедрение кода.
2. Некорректная аутентификация и управление сессией.
2. Межсайтовый скриптинг.
3. Нарушение контроля доступа.
4. Небезопасная конфигурация.
5. Утечка чувствительных данных.
6. Недостаточная защита от атак.
7. Подделка межсайтовых запросов.
8. Использование компонентов с известными уязвимостями.
9. Недостаточное журналирование и мониторинг.

Учитывая каждую уязвимость были разработаны методы борьбы с ними для дальнейшего внедрения в веб-интерфейс и представлены в таблице [3, 4, 5, 6].

Схема работы разрабатываемого приложения представлена на рис. 1 (см. ниже).

Оболочкой интерфейса является WEB сервер, которые обрабатывает запросы от клиентов, SQL и SSH сервера. SQL сервер хранить все необходимые данные, к примеру, такие как учетные данные пользователей. Тем временем, SSH выступает как ретранслятор. То есть, принимает и отправляет запросы от Web сервера и конечных устройств. Все запросы между собой передаются по защищенным протоколам:

ТАБЛИЦА. Веб-уязвимости и методы борьбы с ними

Уязвимость	Описание	Решение
Инъекции	Это уязвимости,	Экранирование запросов

Уязвимость	Описание	Решение
	возникающие при передаче не проверенных данных интерпретатору.	
Проблемы аутентификации и проверки сессий	При аутентификации и проверке сессии злоумышленники могут перехватить ключи или токены сеанса	Использование secure cookie. При атрибуте secure cookie передаются только по защищенному каналу
Межсайтовый скриптинг	При XSS передается JS код в какое-либо поле и браузер его выполняет	Необходимо использовать методы, работающие напрямую с текстом
Проблемы контроля доступа	Ошибки в коде приложения открывают доступ к секретным данным для не авторизованных пользователь	Распределение прав доступа к файлам в соответствии с задачами пользователь решает эту проблему
Неверная конфигурация	Неверная конфигурация ставит под угрозу безопасность приложения	Настройки безопасности должны разрабатываться, реализовываться и постоянно поддерживаться
Незащищенные конфиденциальные данные	Многие сайты не защищают конфиденциальные данные пользователя и передают их в открытом виде	Использование защищенных протоколов, таких как HTTPS, SSH, WSS
Недостаточная защита от атак	Большинство приложений не имеют базовых возможностей по обнаружению, предотвращению и реагированию на атаки	Необходимо включать обнаружение, протоколирование и блокирование попыток несанкционированных действий
Подделка межсайтовых запросов	Атака CSRF позволяет заставить браузер жертвы отправить определенный HTTP запрос, включая куки, файлы сеанса и другую информацию	Способом защиты является токен. Под токеном подразумевается случайный набор байт, который сервер передает клиенту, а клиент возвращает серверу
Использование компонентов с уязвимостями	Использование приложений и API с известными уязвимостями могут подорвать защиту приложений	Своевременное обновление программного обеспечение и проверка на уязвимости с помощью общеизвестных баз данных уязвимостей (например, CVE)

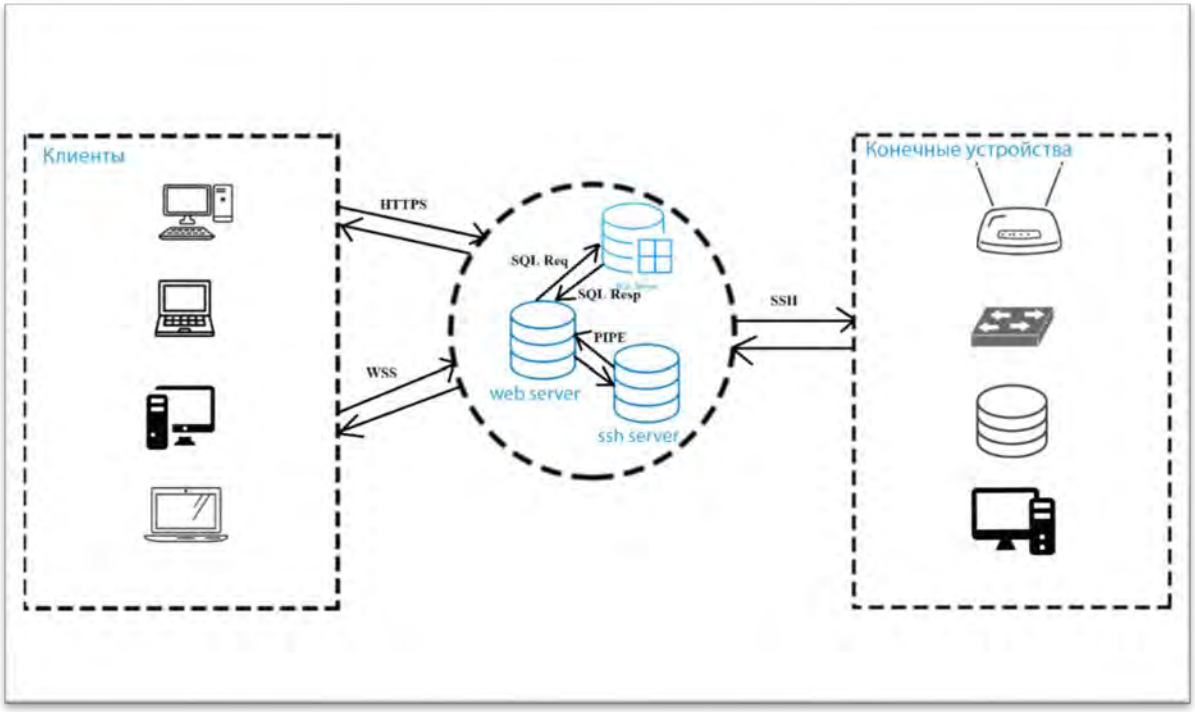


Рис. 1. Схема работы веб-интерфейса

– HTTPS (*HyperText Transfer Protocol Secure*) – защищенный протокол HTTP для защиты передачи данных. Данные шифруются с помощью SSL/TLS.

– WSS (*WebSocket Secure*) – протокол связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени.

– SSH (*Secure Shell*) – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.

На рис. 2 (см. ниже) представлен графический интерфейс веб-ресурса, где необходимыми элементами является интерактивное меню, окно командной строки, список подключенных машин и окно личного кабинета с текущими оповещениями [7].

В настоящее время веб-интерфейс реализован только частично. Дальнейшими задачами является разработка возможности работы с несколькими рабочими машинами одновременно, поддержка протокола SFTP для работы с файлами удаленной машины, авторизация клиентов по ключу и балансировка нагрузки с помощью кластера серверов.

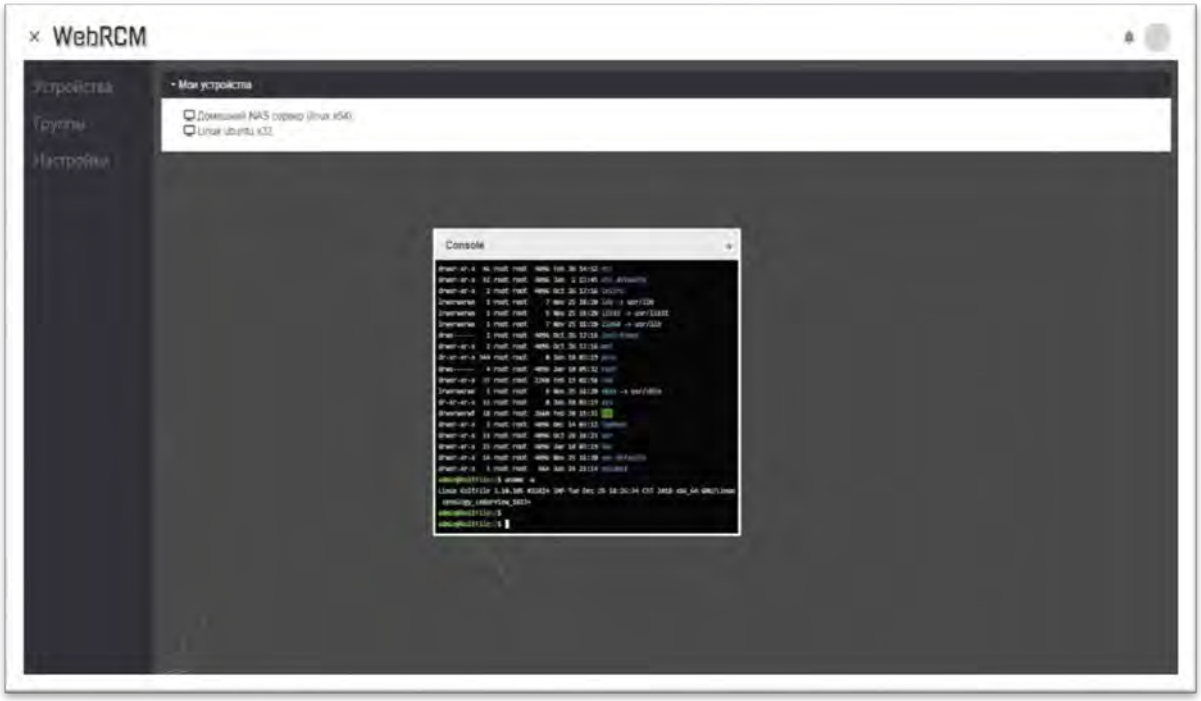


Рис. 2. Начальная реализация графического веб-интерфейса

Список используемых источников

1. Эндрю Таненбаум. Компьютерные сети. 5-е изд. М. : Питер, 2012. 960 с.

2. Linux Open Source Software Technologies [Электронный ресурс]. URL: https://losst.ru/ (дата обращения 20.02.2019).

3. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Материалы конференции Региональная информатика (РИ-2016) : сб. науч. тр. 2016. С. 168–169.

4. Котенко И. В., Ушаков И. А. Модели NOSQL баз данных для мониторинга кибербезопасности // 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. 498–501.

5. 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.

6. Дешевых Е. А., Ушаков И. А., Чечулин А. А. Интеграция SIEM-систем с системами корреляции событий безопасности, основанных на технологии больших данных // Материалы 9-й конференции по проблемам управления. Информационные технологии в управлении (ИТУ-2016) : сб.науч.тр. / Председатель президиума мультиконференции В. Г. Пешехонов. 2016. С. 684–687.

7. Мигель Гринберг. Разработка веб-приложений с использованием Flask на языке Python. М. : ДМК Пресс, 2016. 272 с.

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

УДК 004.451
ГРНТИ 81.93.29

ПРОЕКТИРОВАНИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОПЕРАЦИОННОЙ СИСТЕМЕ

В. И. Темченко, А. Ю. Цветков

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

Операционная система – специально организованная совокупность программ, которая управляет ресурсами системы (ЭВМ, вычислительной системы, других компонентов информационно-вычислительной системы) с целью наиболее эффективного их использования и обеспечивает интерфейс пользователя с ресурсами. Под безопасностью ОС будет пониматься такое состояние ОС, при котором невозможно случайное или преднамеренное нарушение функционирования ОС, а также нарушение безопасности, находящихся под управлением ОС, ресурсов системы. Поскольку большинство ОС обладают дефектами с точки зрения обеспечения безопасности данных в системе, что обусловлено выполнением задачи обеспечения максимальной доступности системы для пользователя, то задачей данной работы будет создание такой модели информационной безопасности для операционной системы, чтобы максимально предотвратить любое преднамеренное или непреднамеренное воздействие на ОС как снаружи, так и изнутри.

операционная система, угрозы для ОС, уязвимости, модель безопасности.

Введение

В нашем мире угрозы безопасности информационным системам являются неотъемлемой частью жизни. Потому поддержание безопасности данных систем на должном уровне является важной задачей. С учетом роста силы различных типов угроз, увеличением числа уязвимостей и других проблем, необходимо решение, которое охватит максимальное число задач. В данная статья представляет один из видов информационных систем, а конкретно – операционные системы. Данный вид встречается и используется повсеместно, что наводит о важности данных систем. Соответственно вторжение в штатную работу операционной системы может нанести непоправимый ущерб всему, что связано с работой данных систем. Модель, которая будет представлена в рамках данной статьи должна охватить весь спектр необходимых условий, который обеспечит отказоустойчивость операционной системы, но также сохранит возможность работать с данной системой не ощущая неудобств, связанных с защитой системы [1].

Механизмы обеспечения защиты операционной системы

Существуют различные методы защиты операционных систем (далее ОС), которые нацелены на ту или иную проблему.

Но необходимо понимать, что такое механизмы защиты операционной системы – это все средства и способы сохранения работоспособности ОС и защиты данных, функционирующие в составе ОС.

Механизмы можно разделить на:

– Программные решения (Антивирусные программы, Программные межсетевые экраны, Системы защиты информации).

Антивирусные программы – это специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Программный межсетевой экран – это программный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Среди задач, которые решают программные межсетевые экраны, основной является защита отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.

СЗИ обеспечивают защиту и целостность данных от НСД в процессе их хранения и обработки. Является комплексом защитных средств для информационных систем. Данный комплекс оснащен также возможностью ведения аудита для осуществления полноценного контроля за «жизнью» операционной системы. Также позволяет использовать аппаратные идентификаторы в качестве опознавания пользователей (токены, смарт-карты, usb-накопители и т. д.).

– Аппаратные решения (Модули доверенной загрузки).

Делают почти тоже, что и аппаратные идентификаторы, только управляют запуском операционной системы (запуск не будет произведен пока не предъявлен ключ запуска – по аналогии с автомобилем) [2].

Нарушения безопасности операционной системы

Данная часть рассматривает не все атаки, а только их основные виды. В статье классификация немного отличается от тех, что можно обычно встретить.

– Несанкционированный доступ (НСД). Сюда могут входить как преднамеренное, так и непреднамеренное воздействие. То есть, тот кто не должен иметь доступа к той или иной части ОС, данным, элементам управления

ОС и прочему, получает такой доступ. Чаще всего именно такой характер носит большинство нарушений безопасности ОС. Сюда также включено физическое воздействие.

– Кража данных. Данное нарушение также чаще всего подразумевает использование полученной информации для последующего получения НСД. Но и не только.

– Воздействие любого вида на ОС. Тут чаще всего производятся атаки с целью уничтожить, повредить данные, ОС или вычислительную систему целиком (то есть аппаратные повреждения) [3].

Данные нарушения безопасности чаще всего производятся при помощи:

– вирусных атак;
– сетевых атак;
– прямого физического контакта;
– неосторожности использования;
– уязвимостей в программном обеспечении.

Также, данные виды атак и нарушения безопасности производятся в совокупности, а не по отдельности, для большей вероятности успеха [4].

Рис. 1 и рис. 2 показывают исследование по типам атак, нарушающие безопасность операционной системы. Берутся 2 часто используемые и известные ОС – Windows 10 и Linux (рассматривается конкретно ядро, из-за того, что трудно определить частоту использования различных оболочек). Статистика получена за 2017 год.

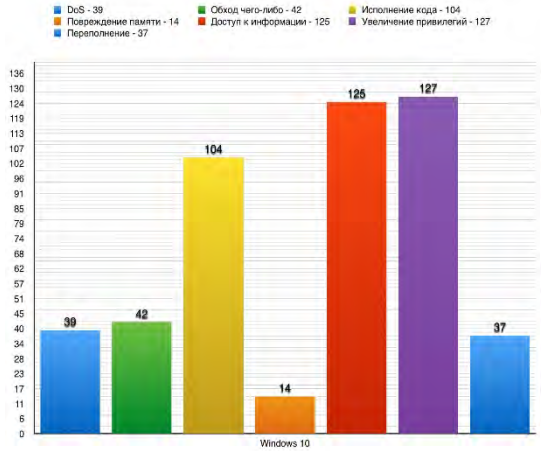


Рис. 1. Атаки на Windows 10

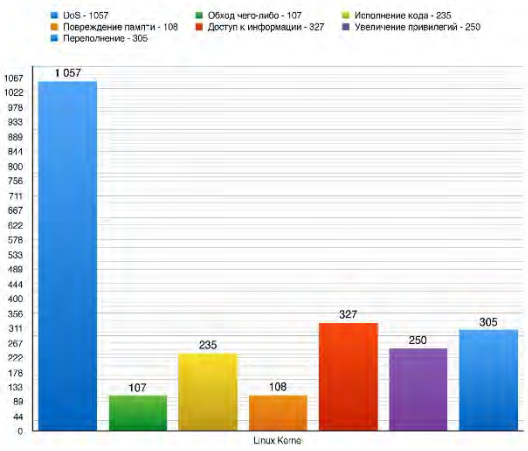


Рис. 2. Атаки на Linux

Уязвимостей много, как мы видим, сотни, а то и тысячи. Вот основные виды уязвимостей, которые рассматриваются в нашем анализе:

– DoS (*Denial of Service* / отказ в обслуживании) (эксплойт уязвимости приводит к DoS устройства);

– обход чего-либо (например, пароля для входа в систему);

– исполнение кода (возможность злоумышленником выполнить какую-то команду на устройстве жертвы);

– повреждение памяти;

– доступ к информации (имеется в виду секретная информация, полученная за счет уязвимости);

– увеличение привилегий (в частности для вредоносного ПО);

– переполнение (буфера) – уязвимость программного обеспечения, связанная с неправильным использованием памяти и отсутствием жёсткого контроля от подсистемы программирования или операционной системы[5].

Windows до сих пор многими людьми считается самой уязвимой ОС. Но такая ОС как Android (666 уязв.) показывает, что это уже не так. По данным Windows 10 содержит 255 уязвимостей.

Linux Kernel – ядро операционной системы, основа ОС семейства Linux. Несмотря на большое количество уязвимостей, обнаруженных за период с 1999 по 2017 год, Linux не так популярна среди киберпреступников. А все связано с ее малым распространением в мире. Рассматривая отдельно уязвимости, выяснится, что при оценке влияния на работу системы – данные уязвимости оказывают крайне малое воздействие [6].

Модель защиты операционной системы

В данном разделе на рис. 3 показана разработанная модель защиты ОС. На ней разграничены все аспекты, связанные с ОС. Для каждого применяется свое решение, чтобы обеспечить максимальный уровень соотношения безопасности и удобства, при этом сохраняя целостность системы.

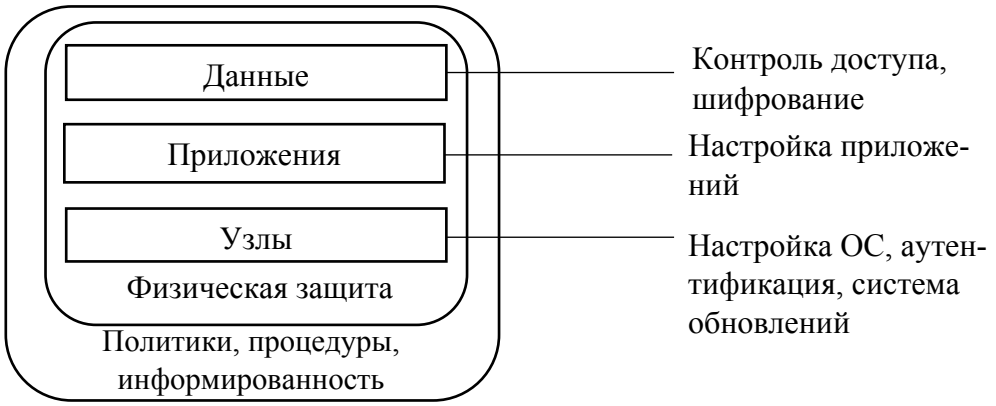


Рисунок 3. Модель защиты операционной системы

1. Создание решений по защите систем, начинается не с технических средств. Важным аспектом являются меры организационного характера, определяющие правила работы пользователей. В данном случае речь идет о разработке политики безопасности, которая будет состоять из соответствующих регламентов, инструкций и других документов.

2. При возникновении потенциально возможной угрозе физического НСД к компьютеру, все другие меры будут бесполезны. Необходимо применить комплексный подход по защите от НСД (использовать аппаратные средства совместно с программными СЗИ от НСД, представленные ранее, и не забывать блокировать или выключать ОС).

3. Этот пункт о защите операционной системы и ее сервисов, но не о прикладном ПО. Существуют следующие пробелы в безопасности на уровне узла:

Уязвимости ОС, также упомянутые ранее, зная которые, злоумышленник может нарушить управляемость системы, получить доступ к компьютеру, выполнить иные деструктивные действия. Уменьшить риски можно с помощью своевременных и регулярных обновлений ОС, и программных средств, представленных ранее.

4. Уровень приложений – это ПО, выполняющиеся на узлах сети. К ним относятся дополнительные службы, например, почтовые или как Microsoft Office. Риски в плане безопасности включают в себя:

– Незащищенность приложений (уязвимость ПО от версии к версии).

– Конфигурации приложений по умолчанию (стандартная конфигурация далеко не всегда является безопасной).

5. Уровень данных – это данные, которые непосредственно хранятся на компьютерах. К нему относятся файлы данных, файлы приложений, базы данных и доменные службы Active Directory, и т. д. То есть риски чрезвычайно высоки. Их уменьшение по НСД к данным может выполняться различными способами. К примеру использование разрешений файловой системы NTFS и общих папок, где к файлам имеют доступ только легитимные пользователи. Однако, при наличии физического доступа к компьютеру, такого метода защиты будет очевидно недостаточно. Поэтому для обеспечения конфиденциальности необходимо шифровать данные [7].

Заключение

Представленная модель произвела охват необходимого спектра обеспечения отказоустойчивости и удобства, за счет 5 приведенных элементов. Контроль данных с помощью встроенных средств ОС и СЗИ, приложений за счет их правильной конфигурации, самой системы за счет обновления её и сопутствующих приложений, также физическая защита с помощью аппаратных решений, СЗИ и созданных политик безопасности.

Список используемых источников

1. Танненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб. : Питер, 2015. – 1120 с.

2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие. М. : ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

3. Котенко И. В., Ушаков И. А. Модели NOSQL баз данных для мониторинга кибербезопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2018. С. 498–501.

4. Красов А. В., Савинов Н. В., Ушаков И. А. Использование инфраструктуры, ориентированной на приложения компании Cisco Systems Inc. в современных сетях ЦОД // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. 2017. С. 453–457.

5. Дешевых Е. А., Ушаков И. А., Чечулин А. А. Интеграция SIEM-систем с системами корреляции событий безопасности, основанных на технологии больших данных // Информационные технологии в управлении (ИТУ-2016) : материалы 9-й конференции по проблемам управления / Председатель президиума мультиконференции В. Г. Пешехонов. 2016. С. 684–687.

6. Уязвимости операционных систем. Часть I [Электронный ресурс]. URL: https://habr.com/ (дата обращения 12.04.2019).

7. Безопасность операционных систем [Электронный ресурс]. URL: https://works.doklad.ru/ (дата обращения 12.04.2019).

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

УДК 654.9, 681.5
ГРНТИ 19.31, 20.53.19, 49.37.33

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ДЕКОМПОЗИЦИИ СЕРВЕРА FRONT-END В СИСТЕМЕ ГЛУБОКОЙ ИНСПЕКЦИИ ПАКЕТОВ (DPI) ПО ВРЕМЕНИ ОБРАБОТКИ ЗАЯВОК

В. В. Фицов

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

В данной статье описывается идея декомпозиции сервера Front-End в системе DPI. Для проверки теоретических предпосылок разделения СМО для обработки заявок с длительным временем обслуживания и заявок с малым временем обслуживания используется имитационное моделирование. Критерием оценки работы системы DPI было выбрано общее время, проведенное заявками в Front-End (включая время в очереди). Даны результаты исследования, выявляющие условия при которых декомпозиция целесообразна. Особенностью работы является сама идея декомпозиции сервера Front-End в системе DPI, а также проверка теоретических идей, с помощью имитационного моделирования.

DPI, Front-End, СМО, очереди, QoS, имитационное моделирование (ИМ), GPSS, экспоненциальное распределение, распределение Вейбулла.

Введение

Система DPI (*Deep Packet Inspection*, глубокой инспекции пакетов) распознает приложения по потоку пакетов, для управления потоками этих приложений согласно политикам оператора. Наибольшее время затрачивается на анализ, который проводится на сервере Front-End (FE). В данной статье рассмотрена идея декомпозиции сервера FE, в надежде снизить время анализа данных в системе DPI в целом. Декомпозиция сервера FE предлагает унифицировать величину времени обработки заявок, путем вынесения дополнительных действий в отдельный сервер.

Декомпозиция была исследована с помощью имитационной модели (ИМ) в среде GPSS World. ИМ стандартной системы DPI описана в [1]. ИМ DPI с декомпозицией сервера Front-End была создана для этой работы.

Зависимость длины очереди от вариации времени обслуживания

В [2] Башарин Г. П. в ходе анализа очередей модели M/M/1 с бесконечной очередью обнаруживает, что условная средняя длина очереди имеет максимальное значение, когда обслуживается заявка с максимальным средним временем обслуживания. Системы с большой вариацией времени обслуживания невыгодны по сравнению с системами с меньшим разбросом значений времени обслуживания. Наличие в приборе заявки с малой интенсивностью обслуживания, приводит к образованию более длинной очереди. Разделение СМО на несколько СМО обрабатывающих однородные по времени обслуживания заявки, приведет к повышению производительности, сократив среднюю длину очереди.

Для увеличения производительности системы и уменьшения средней длины очереди целесообразно предоставлять преимущество заявкам с меньшим средним значением времени обслуживания [2]. Действительно альтернативным решением может быть введение приоритетного обслуживания тех заявок, которые требуют меньшего времени для обслуживания. Однако если в системе важно, как можно скорее обработать поступившую заявку, требующую длительного времени обслуживания, то приоритетное обслуживание заявок с меньшим временем обслуживания будет создавать дополнительные задержки в обслуживании.

Декомпозиция сервера Front-End системы DPI

Описание основных серверов DPI дано в [1]. После проведения анализа пакетов приложения на FE (с большим временем обслуживания), нужно вы-

полнить одно или несколько взаимодействий (с малым временем обслуживания) для завершения обслуживания заявки. Front-End взаимодействует со всеми основными серверами DPI. Если применить приоритетное обслуживание, то будут быстрее завершаться проанализированные заявки, но будут задерживаться в очереди непроанализированные заявки.

После определения приложения, от которого поступает трафик, на системе DPI применяются соответствующие политики. Таким образом, с момента пропуска трафика до момента применения политик возникает задержка коррекционных действий. Одной из составляющих этой задержки являются: время, проведенное заявками в очереди на FE, время, потраченное на обработку заявок при ее анализе, время на обработку последующих необходимых взаимодействиях FE с другими серверами для завершения обслуживания проанализированных заявок. В исследовании оценивалось суммарное время, затраченное всеми заявками на сервере FE. В случае декомпозиции FE на две СМО, оценивалось суммарное время, затраченное всеми заявками на обеих СМО, выполняющих функции FE.

Имитационная модель системы DPI с декомпозицией сервера Front-End

Обычно пакетный трафик описывают такие распределения, как Парето, Вейбулловское и др. Однако в процессе длительных исследований, собранных в [3] оказалось, что наиболее близки мультифрактальное брауновское движение, а затем распределение Вейбулла. Для описания процесса обработки в основном применяют экспоненциальное распределение. Поэтому в ИМ был задан поток поступления заявок на аппаратный фильтр DPI с распределением Вейбулла, а закон обработки заявок на каждом из серверов был выбран экспоненциальным.

Для упрощения результатов математическое ожидание (МО) времени обработки заявок было выбрано целочисленным. Модуль генерации заявок каждые 5 мс в GPSS описывается как GENERATE (WEIBULL(1, 5, 1, 1)), а обработка заявки (анализ потока приложения) в сервере FE в течение 2000 мс как ADVANCE (Exponential(1,20,2000)). Всего генерировалось по 10 000 заявок. Согласно заданным в ИМ вероятностям, 20 % заявок поступают на FE. ИМ выдает следующие значения: нагрузка на FE, общее число поступивших заявок, число заявок, заставших систему свободной, среднее время ожидания в очереди. Чтобы получить время обработки заявки устройством в ИМ потребовалось вводить дополнительную переменную. После простых вычислений были получены (табл.): число заявок, попавших в очередь, суммарное время ожидания всех заявок на FE, суммарное время обработки всех заявок на FE, общее время заявок в FE.

ТАБЛИЦА. Результаты моделирования

Параметр	FE	FE-Sum	FE-A	FE-I
МО появления новой заявки, мс	5			
Нагрузка, Эрл	0,696	–	0,735	0,064
Всего заявок, шт	3443	–	2028	3417
Заявок ожидало, шт	0	–	0	237
Суммарное время ожидания, мс	0	18,012	0	18,012
Среднее время обработки, мс	1234,449		2191,665	1,129
Суммарное время обработки, мс	4250208	4448554	4444697	3857,793
Суммарное время в системе, мс	4250208	4448572	4444697	3875,805
Отношение сумм. вр. FE к FE-AI, раз	0,96			
МО появления новой заявки, мс	3			
Нагрузка, Эрл	0,970	–	0,960	0,083
Заявок ожидало, шт	3095	–	1842	282
Суммарное время ожидания, мс	4013522	2905535	2905506	28,482
Суммарное время обработки, мс	4285712	4357239	4353806	3433,92
Суммарное время в системе, мс	8299234	7262774	7259312	3462,402
Отношение сумм. вр. FE к FE-AI, раз	1,14			
МО появления новой заявки, мс	2			
Нагрузка, Эрл	0,970	–	0,972	0,084
Суммарное время в системе, мс	17816129	14822778	14820042	2735,261
Отношение сумм. вр. FE к FE-AI, раз	1,20			
МО появления новой заявки, мс	1			
Нагрузка, Эрл	0,974	–	0,970	0,088
Суммарное время в системе, мс	21637473	16249742	16247746	1996,366
Отношение сумм. вр. FE к FE-AI, раз	1,33			

Чтобы получить такие же данные о системе DPI, в случае декомпозиции сервера FE, была разработана новая ИМ (рис. 1).

Функции FE были разделены между FE-Analyse (FE-A) и FE-Interworking (FE-I). FE-A проводит только длительную по времени первичную обработку заявки (анализ потока приложения). После этого результат анализа и идентификатор потока передается в FE-I. Который осуществляет взаимодействие с другими серверами DPI по мере необходимости. При декомпозиции мы получаем две СМО. Поэтому для сравнения двух видов систем DPI,

среднее время очереди и среднее время обработки заявок FE-A и FE-I будут просуммированы.

Чтобы исключить влияние аппаратного фильтра, ему была задана достаточная производительность, чтобы не создавать больших очередей.

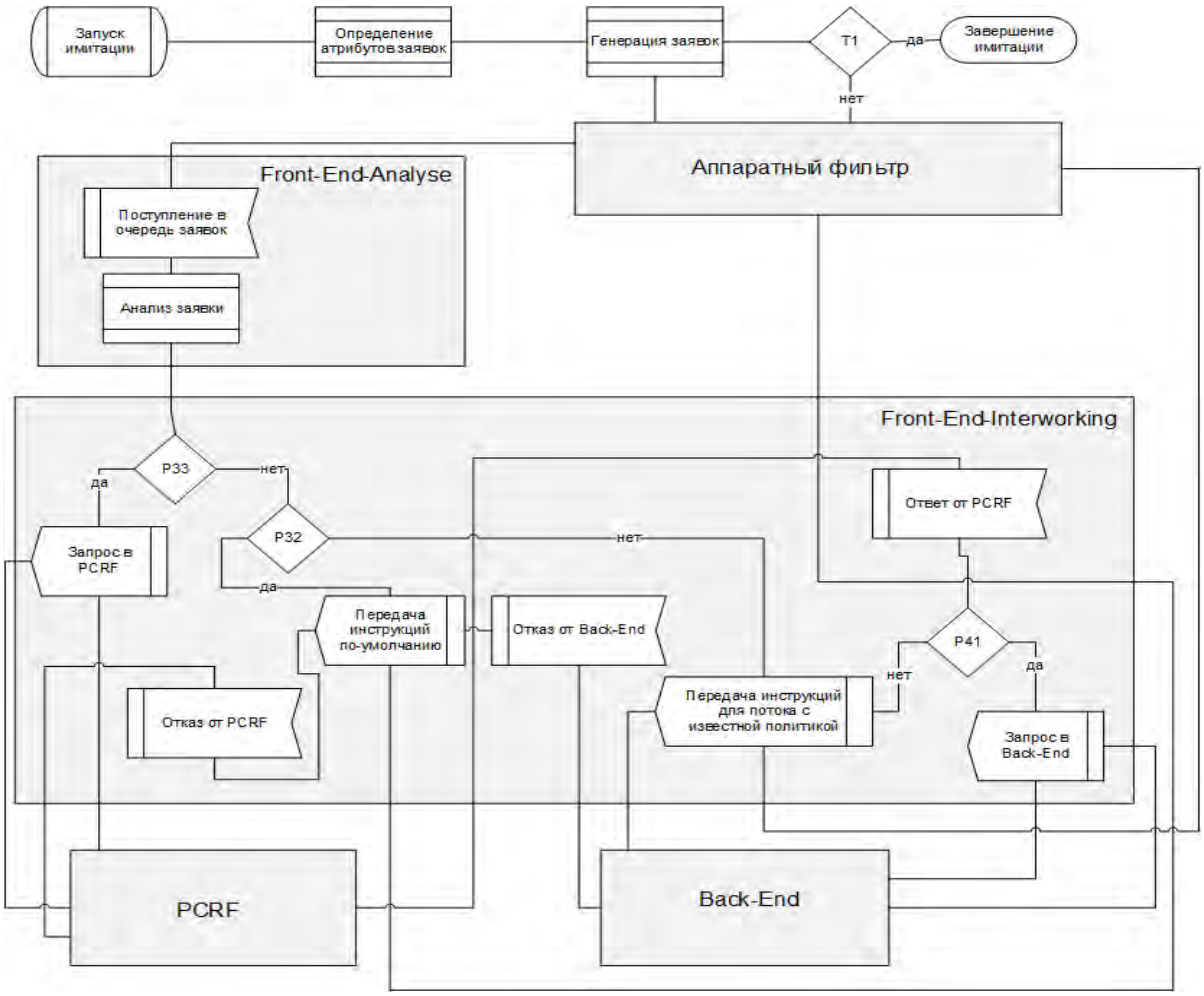


Рис. 1. Алгоритм имитационной модели системы DPI с декомпозицией сервера Front-End

Данные проведенных моделирований

Число серверов FE было задано как: 101 FE, 100 FE-A и 1 FE-I. Время анализа – 2000 мс, а время прочих задач взаимодействия – 10 мс. При одинаковых условиях и поступлении в систему DPI новых заявок раз в 5 мс, DPI без декомпозиции сервера FE тратит времени на обработку всех заявок на 4 % меньше, чем DPI с декомпозицией (табл.). Очередь на серверах анализа отсутствует, а очередь на FE-I мала. С увеличением интенсивности поступления заявок на DPI, возрастают очереди.

Согласно [2] время очереди зависит от вариации времени обслуживания. Исследование показало, что при близких условиях работы FE и FE-A

время очереди больше для сервера без декомпозиции при высоких значениях очереди (нагрузка порядка 0,96 Эрл) (табл.). Большая длина очереди и высокое время ожидания оказывают существенное влияние на суммарное время (рис. 1), которое провели все заявки в сервере FE. Таким образом, сервер без декомпозиции тратит времени на обработку всех заявок на 14–33 % больше (табл., рис. 2), чем сервер с декомпозицией.

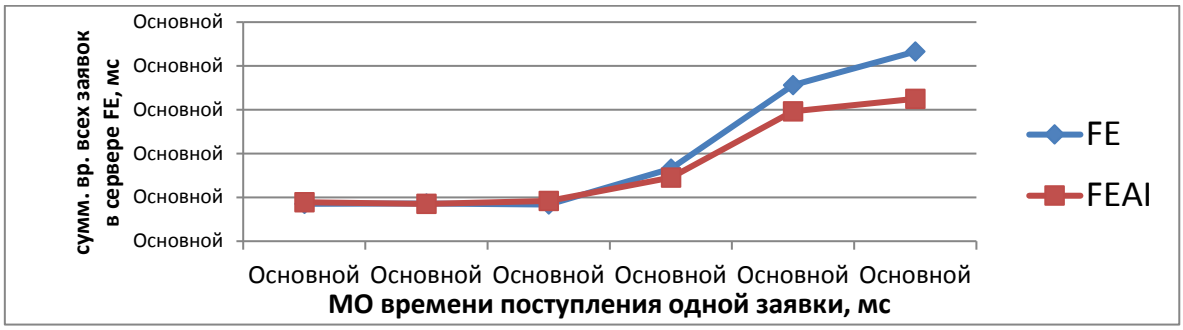


Рис.2. Зависимость общего суммарного времени,
проведенного заявками в сервере Front-End от нагрузки на него

Было выявлено несколько важных факторов, влияющих на эффективную работу с очередями сервера Front-End с декомпозицией. Во-первых, с ростом нагрузки на сервер анализа, возрастают очереди и при близких параметрах FE и FE-A, время в очереди в системе с декомпозицией оказывается меньше. Во-вторых, чем больше различие во времени обслуживания длительных и быстрых заявок, тем эффективнее сервер с декомпозицией. Для рис. 2 время обслуживания отличается в 2000 раз. В-третьих, чем больше в системе DPI доля быстрых заявок, тем более эффективна декомпозиция. В исследовании доля быстрых заявок взаимодействия составила около 70 % от числа заявок анализа (табл.). Такое значение определено вероятностями ИМ. Например, при равном числе быстрых и длительных в обслуживании заявок, сервер с декомпозицией тратит времени на обслуживания заявок в 2 раза меньше.

Целесообразность декомпозиции

Проведенное исследование подтвердило теоретические предпосылки, о зависимости средней длительности очереди, от величины вариации времени обслуживания. Декомпозиция FE действительно повышает производительность DPI, однако только при работе с большими очередями и прочих условиях, описанных выше. В приведенном в таблице примере расчета выигрыш составил 33 % по суммарному времени нахождения всех заявок в сервере. В режиме работы без больших очередей, выгоднее использовать все аппаратные мощности в едином сервере Front-End. В случае, когда до-

бавить аппаратные мощности в сервер FE невозможно, применение дополнительного сервера FE-I увеличит производительность системы, и снизит длительность очереди в случае ее возникновения.

Список используемых источников

1. Фицов В. В. Имитационная модель системы DPI на основе программного обеспечения GPSS World // Актуальные проблемы инфотелекоммуникаций в науке и образовании. V Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб. : СПбГУТ, 2016. – С. 539–545.

2. Башарин Г. П., Харкевич А. Д., Шнепс М. А. Массовое обслуживание в телефонии // Наука, 1968. С. 141–194.

3. Christian Grimm, Georg Schluchtermann IP Traffic Theory and Performance // Springer, 2008. P. 497.

Статья представлена научным руководителем (СПбГУТ), доктором технических наук, профессором Б. С. Гольдштейном.

УДК 004.056.53
ГРНТИ 50.05.17

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ АТАК ТИПА ПЕРЕПОЛНЕНИЯ БУФЕРА НА ОПЕРАЦИОННЫЕ СИСТЕМЫ СЕМЕЙСТВА MICROSOFT

А. Ю. Цветков

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

Программа состоит из сложного набора правил, следующих за определенным потоком выполнения, который в конечном итоге сообщает компьютеру, что делать. Поскольку программа действительно может делать только то, для чего она предназначена, уязвимости в безопасности – это недостатки или недоработки при разработке программы или среды, в которой работает программа. В некоторых случаях эти уязвимости являются продуктами очевидных ошибок разработчика, но есть некоторые менее очевидные ошибки, которые породили более сложные методы эксплуатации.

уязвимость, стек вызовов, кадр (фрейм) стека, адрес возврата, шелл-код.

С развитием информационных технологий становятся все более значимой безопасность программного обеспечения (ПО). Сложное ПО часто

используется в работе критической инфраструктуры. Ошибки в функционировании таких программ приводят к серьезным последствиям, а целенаправленная эксплуатация ошибок злоумышленниками способна привести к еще большему ущербу. Ошибки, использование которых может привести к намеренному нарушению целостности системы и вызвать её неправильную работу, называют уязвимостями. Многие крупные IT-компании не только поддерживают исследования в области поиска ошибок и уязвимостей программного обеспечения, но и внедряют самые передовые технологии в жизненный цикл разработки программ, с целью сокращения ошибок в выпускаемом ПО и снижения издержек, связанных с обнаружением и исправлением ошибок [1, 2, 3, 4, 5, 6].

Принцип атаки переполнения буфера основан на использовании программных ошибок, позволяющих вызвать нарушение границ памяти и аварийное завершение приложения или выполнить произвольный бинарный код от имени пользователя, под которым работала уязвимая программа. Если программа запущена с правами администратора, то данная атака позволит получить полный контроль над компьютером жертвы.

Помимо контроля со стороны злоумышленника, атака переполнения буфера может привести к чтению или модификации секретных переменных, располагающихся в адресном пространстве уязвимого процесса. [7, 8, 9, 10].

Обычно с переполнением буфера связывают такие языки программирования, как C, C++, Assembly. Данные языки не обеспечивают встроенную защиту от перезаписи данных в любой части памяти и не проверяют, что данные, записанные в буфер, находятся в переделах границ данного буфера. C – высокоуровневый язык программирования, но он предполагает, что программист несет ответственность за целостность данных.

Переполнение буфера в программе может вызвать одно из последствий [11]:

– программа выдает неверные данные;
– аварийное завершение программы;
– программа изменяет логику своего поведения, выполняя незапланированные действия;
– нет никаких последний.

Методы использования уязвимости переполнения буфера зависят от архитектуры, операционной системы и области памяти. Например, эксплуатация в куче заметно отличается от использования в стеке вызовов. Прежде чем исследовать переполнение буфера, необходимо исследовать несколько понятий, используемых при эксплуатации данной атаки.

Современные операционная система (ОС) пользуются схемой, которая называется виртуальной памятью [12]. При этой схеме прямое соответствие между адресом памяти и физическим участком RAM (*Random Access*

Memory) отсутствует. Программы и процессор работают в виртуальном адресном пространстве. ОС Windows использует модель сплошной памяти (*flat memory*). Это означает, что память появляется в программе как единое непрерывное адресное пространство. Каждому процессу в операционной системе предоставляется виртуальное адресное пространство и принадлежит оно только ему. Адресное пространство каждого процесса имеет, по крайней мере, три сегмента [13, 14]:

– сегмент кода или *.text* (содержит команды из программы, которые будут исполняться процессором);

– сегмент данных или *.data* (содержит данные, т. е. переменные);

– сегмент стека или *call stack.*

Стоит отметить, что существует понятие соглашение о вызове (*calling convention*) функций. Это соглашение является стандартизированным методом для функций, которые должны быть реализованы и вызываться машиной. Оно также определяет метод, который компилятор устанавливает для доступа к подпрограмме [10, 12].

В архитектуре x86 стек растёт от больших адресов к меньшим, то есть новые данные помещаются перед теми, которые уже находятся в стеке. Стек содержит по одному фрейму (области данных) для каждой процедуры, в которую уже вошла, но из которой еще не вышла программа. В стековом фрейме процедуры хранятся ее входные параметры (аргументы), а также локальные и временные переменные, не содержащиеся в регистрах [13]. Помимо этого, стековый фрейм содержит обратный адрес возврата и указатель кадра стека (*frame pointer*).

Указатель стека (*stack pointer*) – это изменяемый регистр, общий для всех вызовов. Указатель кадра для данного вызова функции – это копия указателя стека, когда функция еще не была вызвана. Когда размер кадров стека может различаться, например, при вызове различных функций, выталкивание кадра из стека не является фиксированным декрементом указателя стека. При возврате функции указатель стека вместо этого восстанавливается в указатель кадра, который содержит значение указателя стека непосредственно перед вызовом функции.

Шелл-код (*shellcode*) – это небольшой фрагмент кода (двоичный исполняемый код), используемый в качестве полезной нагрузки при использовании уязвимости программного обеспечения. Он называется «shellcode», потому что он обычно запускает командную оболочку, из которой злоумышленник может управлять уязвимой машиной, но любой фрагмент кода, который выполняет подобную задачу, можно назвать шелл-кодом. Есть два типа шелл-кода: удаленный и локальный. Локальный тип используется злоумышленником, который имеет ограниченный доступ к машине, но может использовать уязвимость, например, переполнение буфера, в более высоко привилегированном процессе на этом компьютере. Если

он успешно выполнен, шелл-код предоставит злоумышленнику доступ к машине с теми же более высокими привилегиями, что и целевой процесс.

В некоторых случаях атакующий не может узнать значение адреса возврата, чтобы точно перейти к шелл-коду. Однако есть метод, который позволяет указать примерный адрес возврата без высокой точности. Метод «NOP-sled» – самый старый и наиболее известный способ успешного использования переполнения буфера стека [15]. Он решает проблему поиска точного адреса буфера, эффективно увеличивая размер целевой области. Для этого большие секции стека повреждены машинной инструкцией no-op (NOP или *no operation*, т.е. отсутствие операции). В конце данных, полученных от злоумышленника, после инструкций no-op злоумышленник помещает инструкцию для выполнения относительного перехода в верхнюю часть буфера, где находится шелл-код. Этот метод требует, чтобы злоумышленник угадал, где в стеке NOP-sled вместо сравнительно небольшого шелл-кода.

Этот метод также позволяет размещать шелл-код после перезаписанного обратного адреса на платформе ОС Windows. Поскольку исполняемые файлы в основном основаны на адресе 0x00400000, а x86 – архитектура Little-endian, последний байт обратного адреса должен быть нулевым, он завершает копию буфера и после него ничего не записывается. Это ограничивает размер шелл-кода размером буфера.

Динамические библиотеки (DLL, *Dynamic Link Library*) находятся в областях памяти с высокими значениями адресов (выше 0x01000000) и имеют адреса, содержащие нулевые байты, поэтому этот метод может удалить нулевые байты (или другие запрещенные символы) из перезаписанного обратного адреса. Используемый таким образом метод часто называют «DLL Trampolining» или трамплин (рис.).

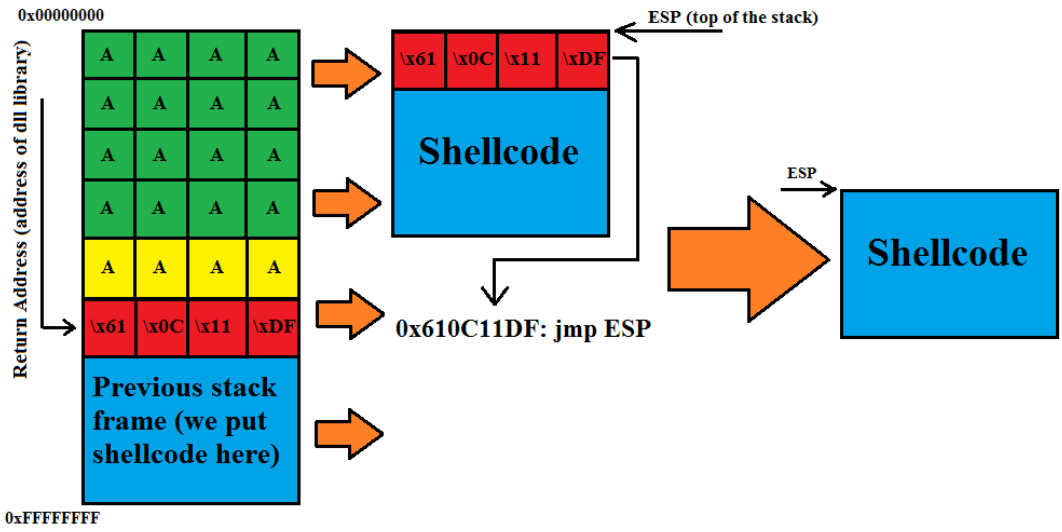


Рисунок. Принцип действия метода прыжка по регистру с помощью DLL трамплина

Переполнение буфера уже давно является известным в сфере компьютерной безопасности. И несмотря на то, что первая программа, использующая данную уязвимость, была в далеком 1988 году, даже сейчас эта уязвимость остается актуальной. Из-за одной маленькой ошибки со стороны разработчика ПО могут возникнуть катастрофические трудности. Использование переполнения буфера позволяет злоумышленнику контролировать процесс или заменять его внутренние переменные, что может привести к большим потерям информации

Список используемых источников

1. Котенко И. В., Ушаков И. А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Региональная информатика «РИ-2016» : материалы конференции. 2016. С. 168–169.

2. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

3. Крылов К. Ю., Ушаков И. А., Котенко И. В. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28–30 октября 2015 г. Материалы конференции. СПб. : СПОИСУ, 2015. С. 75–76.

4. Гельфанд А. М., Пестов И. Е., Катасонов А. И., Рязанцев К. С. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8. С. 91–97.

5. Красов А. В., Штеренберг С. И. Разработка методов защиты от копирования по на основе цифровым водяным знакам внедряемых в исполняемые и библиотечные файлы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция. 2013. С. 847–852.

6. Красов А. В., Трегубов Ю. А. Кодовое зашумление при вложении информации в исполняемый файл методом семантической замены эквивалентных инструкций // Телекоммуникационные и вычислительные системы : тр. конф. 2015. С. 108–111.

7. Штеренберг С. И., Красов А. В. Варианты применения языка ассемблера для заражения вирусом исполнимого файла формата elf // Информационные технологии и телекоммуникации. 2013. Т. 1. № 3. С. 61–71.

8. Цветков А. Ю. Исследование существующих механизмов защиты операционных систем семейства linux // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т. 2018. С. 657–662.

9. 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 (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция : сб. науч. ст. в 4-х т.2018. С. 570–573.

10. Хогланд Г., Мак-Гроу Г. Взлом программного обеспечения: анализ и использование кода : пер. с англ. М.: Издательский дом «Вильяме», 2005. 400 с.

11. Падарян В. А. Автоматизированный метод построения эксплойтов для уязвимости переполнения буфера на стеке // Труды Института системного программирования РАН. 2014. Т. 26. Вып. 3. С. 127–144.

12. Таненбаум Э., Бос Х. Современные операционные системы, 4-е изд. СПб. : Питер, 2015. 1120 с.

13. Таненбаум Э., Остин Т. Архитектура компьютера, 6-е изд. СПб.: Питер, 2013. 816 с.

14. Буйневич М. В., Щербаков О. В., Израилов К. Е. Структурная модель машинного кода, специализированная для поиска уязвимостей в программном обеспечении автоматизированных систем управления // Проблемы управления рисками в техносфере. 2014. № 3 (31). С. 68–74.

15. Эриксон Дж. Хакинг: искусство эксплойта : пер. с англ., 2-е изд. СПб. : Символ-Плюс, 2010. 512 с.

Статья представлена научным руководителем (СПбГУТ), кандидатом технических наук, доцентом А. В. Красовым.

УДК 004.428.2
ГРНТИ 50.41.25

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В КЛИЕНТ-СЕРВЕРНОМ JAVA ПРИЛОЖЕНИИ ДЛЯ УЧЕТА И АВТОМАТИЧЕСКОЙ ПРОВЕРКИ ЛАБОРАТОРНЫХ РАБОТ

А. Ю. Цветков, М. Е. Шалаева, М. А. Юрченко

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

В современной системе образования уже не обойтись без использования информационных технологий, в частности систем автоматизации учебного процесса. Данные системы в основном строятся по модели клиент-серверного приложения. Во время разработки клиент-серверных автоматизированных систем разработчикам необходимо внедрять механизмы обеспечения безопасности во избежание неправомерного доступа к передаваемой по сети информации и для защиты серверных приложений от различных видов атак.

TLS, обфускация, права доступа, java.

В данной статье рассмотрены основные механизмы обеспечения информационной безопасности клиент-серверных приложений на языке Java на примере программы для автоматизации учебного процесса. Системы

для автоматизации учебного процесса обычно нуждаются в обеспечении механизмов информационной безопасности.

В клиент-серверных автоматизированных системах существуют различные типы угроз информационной безопасности. Среди них можно выделить следующие виды угроз:

– прослушивание канала связи атакой «человек посредине», спуфинг сетевых пакетов;

– статический анализ декомпилированного исходного кода клиентского приложения (реверс-инжиниринг);

– несанкционированный доступ к привилегированным функциям сервера;

– внедрение в программное обеспечение сервера [1].

В целях противодействия указанным угрозам будут использованы следующие механизмы информационной безопасности:

– TLS (англ. *transport layer security* — Протокол защиты транспортного уровня);

– обфускация скомпилированных классов Java-приложений;

– модели распределения прав доступа;

– защита от вредоносного кода при тестировании пользовательских программ при помощи безопасного загрузчика классов.

В настоящие время существует множество различных технологий, позволяющих обеспечить безопасность как программного кода, так и канала передачи информации между приложениями [2, 3, 4, 5, 6].

Любое сетевое приложение, данные в котором передаются по сети между различными узлами, должно обеспечивать средства для защиты передаваемой информации. Самым распространенным на данный момент протоколом защиты данных, передаваемых по сети, является TLS [7]. Он использует асимметричные алгоритмы шифрования для синхронизации ключей шифрования симметричных алгоритмов, которыми непосредственно шифруются все пакеты данных. Также он обеспечивает проверку подлинности при помощи сертификатов.

Для усложнения процесса статического анализа декомпилированного программного кода приложения на java в большинстве случаев используют механизм обфускации скомпилированных классов, но существуют и другие методы [5]. Процесс обфускации заменяет все идентификаторы объектов на непонятные для человека случайные последовательности символов, тем самым затрудняя анализ декомпилированного кода.

Обфускация может увеличить время вскрытия приложения, однако, не обеспечивает полной защиты от анализа, так как обфусцированный код все равно можно проанализировать, постепенно восстанавливая идентификаторы по их смысловому значению в контексте программы.

Для противодействия несанкционированному доступу к привилегированным функциям сервера были реализованы следующие модели распределения прав доступа.

DPS (*distributed permission system*) – распределенная система контроля доступа к различным функциям админ-панели в системе, основанная на уровневой модели контроля доступа.

Каждому администратору присваивается определенный уровень доступа и каждому возможному действию в админ-панели присваивается минимальный требуемый уровень доступа для выполнения данного действия. В таблице 1 представлена диаграмма прав на различных уровнях доступа в системе и их описания. Каждый уровень включает в себя все права всех предыдущих уровней.

ТАБЛИЦА 1. Уровни доступа в системе

Уровень	Название	Права
1	Смотритель	students.view, labs.view, courses.view
2	Помощник преподавателя	messages.view, groups.update, students.update
3	Преподаватель	students.create, students.delete, groups.create, groups.delete, messages.create, messages.delete, labs.change_state
4	Старший преподаватель	courses.change_state, common.massive
5	Администратор	server.reload_dps, server.reload_crs, server.reload_plugins

Уровневая модель контроля доступа хотя и работает достаточно быстро в сравнении с другими моделями контроля доступа, но имеет один значительный недостаток. Она не обладает достаточной гибкостью настройки для того, чтобы подходить под любую ситуацию. Для решения проблемы недостаточной гибкости была реализована новая система контроля доступа в системе – DPSX (*distributed permission system eXtended*).

DPSX основывается на ролевой модели контроля доступа и работает с теми же правами, что и DPS, но позволяет задавать все возможные комбинации этих прав для различных администраторов и называть эти комбинации определенными ролями. Каждому администратору вместо числа уровня доступа теперь назначается числовой идентификатор роли из базы данных, в которой прописан список доступных ему прав.

Кроме того, в глобальных настройках DPSX можно выбирать режим интерпретации правил – режимы черного и белого списка:

- В режиме белого списка администраторы имеют доступ только к тем правам, которые перечислены в ролях.

• В режиме черного списка администраторы не имеют доступа только к тем правам, которые перечислены в ролях.

В таблице 2 приведен пример таблицы ролей для системы DPSX в режиме белого списка.

ТАБЛИЦА 2. Примеры ролей для DPSX в режиме белого списка

Роль	Права
Смотритель	students.view, labs.view, courses.view
Помощник преподавателя	students.view, labs.view, courses.view, messages.view, groups.update, students.update
Преподаватель	students.view, labs.view, courses.view, messages.view, groups.update, students.update, students.create, students.delete, groups.create, groups.delete, messages.create, messages.delete, labs.change_state

Система распределения прав на курсах, CRS (*course role system*), является логическим развитием системы DPSX. Однако, она не полностью заменяет DPSX, а только лишь дополняет ее в одной из частей системы.

Разделение лабораторных работ в системе на несколько параллельных курсов внутри одного и того же сервера послужило предпосылкой для создания системы контроля доступа с учетом курсов, которой и стала CRS. Система CRS оперирует только лишь правами labs.* и messages.*, т. к. они непосредственно зависят от выбранного курса. Проверка доступа происходит в несколько этапов и работает после проверки DPSX.

Алгоритм принятия решения по правам labs.* и messages.*:

1. DPSX проверяет наличие у администратора этого права вообще в системе.

2. CRS проверяет наличие соответствия администратора определенной роли по данному курсу и считывает идентификатор роли в случае успеха.

3. CRS проверяет наличие указанного права в списке прав роли администратора на данном курсе.

Все перечисленные выше системы контроля доступа записывают каждое произведенное успешное и неуспешное действие в лог действий администраторов с целью возможности изучения недавней активности. Для реализации была выбрана библиотека Log4j версии 1.2.17 [8].

Также система предоставляет возможность автоматической проверки результатов выполнения лабораторных работ, отправляемых на сервер студентами. Одной из самых больших сфер применения этой системы тестирования является проверка корректности работы программ на языке Java.

Для проверки программ тестировочный сервис непосредственно запускает пользовательские программы. При таком устройстве пользовательская

программа может получить полный доступ к системе и причинить вред серверу, поэтому необходимо реализовать механизмы защиты от таких атак.

Первым таким механизмом было ограничение времени работы пользовательской программы для предотвращения ее зависания до момента перезагрузки сервера во избежание постоянного потребления ресурсов программой.

В целях предотвращения доступа программы к потенциально опасным классам был реализован собственный безопасный загрузчик классов, разрешающий использовать только определенный список классов, задаваемый в дескрипторах лабораторных работ.

Для того, чтобы злоумышленник, каким-либо образом получивший доступ к серверу и его базе данных, не смог прочесть пароли пользователей из нее, все пароли при создании аккаунтов проходят через одностороннюю криптографическую хеш-функцию, после чего вернуть их в прежний вид уже не представляется возможным без перебора всех возможных паролей.

Однако, данный метод не полностью защищает от вскрытия паролей, потому что существуют радужные таблицы. Радужная таблица – это специальный вариант таблицы поиска для обращения криптографических хеш-функций, использующий механизм разумного компромисса между временем поиска по таблице и занимаемой памятью [9].

Для того, чтобы усложнить создание таких таблиц, необходимо добавлять к каждому паролю случайную строку, называемую солью. Соль хранится в защищенном месте внутри самого сервера и используется каждый раз при создании пароля для аккаунтов или проверке присланного пользователем пароля на совпадение с паролем из базы данных.

На основе вышеизложенного, в качестве мер противодействия от атак в среде, где злоумышленником может являться обучающийся, внедрены следующие механизмы:

- Механизмы распределения прав доступа (DPS, DPSX, CRS) для предотвращения неправомерного доступа к просмотру, изменению, удалению, созданию лабораторных работ, студентов, групп студентов, курсов в системе.
- Безопасный загрузчик классов, предназначенный для контроля выполнения пользовательских программ в системе тестирования и предотвращения доступа к запрещенным классам и функциям.
- Ведение журнала учета совершаемых операций в системе, для отслеживания потенциально опасных действий.
- Обфускация скомпилированного Java байт-кода для затруднения статического анализа клиентского приложения и вскрытия сетевого протокола.
- Защита сетевого соединения при помощи протокола TLS 1.2 для защиты от прослушивания и изменения сетевых пакетов.

• Применения криптографических хеш-функций над паролями пользовательских аккаунтов с использованием соли.

Они позволят обеспечить необходимый уровень безопасности [3], но при рассмотрении других возможных моделей злоумышленников, могут потребуется модификации.

Список используемых источников

1. Гельфанд А. М., Пестов И. Е., Катасонов А. И., Рязанцев К. С. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2018. № 8. С. 91–97.

2. Котенко И. В., Левшун Д. С., Чечулин А. А., Ушаков И. А., Красов А. В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29–38.

3. Крылов К. Ю., Ушаков И. А., Котенко И. В. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2015). 28–30 октября 2015 г. Материалы конференции. СПб. : СПОИСУ, 2015. С. 75–76.

4. Хомяков И.Н., Красов А.В. Возможность скрытого вложения информации в байт-код Java // Информационные технологии моделирования и управления. 2014. № 2 (86). С. 185–191.

5. Красов А. В., Шариков П. И. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47–50.

6. Krasov A. V., Arshinov A. S., Ushakov I. A. Embedding the hidden information into java byte code based on operands' interchanging // ARPN Journal of Engineering and Applied Sciences. 2018. V. 13. No 8. PP. 2746–2752.

7. ГОСТ СТБ 34.101.65–2014 «Информационные технологии и безопасность. Протокол защиты транспортного уровня (TLS)».

8. Maven Repository: Apache Log4j [Электронный ресурс]. URL: https://logging.apache.org/log4j/2.x/ (дата обращения 25.12.2018).

9. Радужная таблица [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D0%B4%D1%83%D0%B6%D0%BD%D0%B0%D1%8F_%D1%82%D0%B0%D0%B1%D0%BB%D0%B8%D1%86%D0%B0 (дата обращения 27.01.2019).

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

УДК 004.056
ГРНТИ 81.96

АУТЕНТИФИКАЦИЯ КЛЮЧЕЙ, РАСПРЕДЕЛЯЕМЫХ МЕТОДОМ ДИФФИ-ХЕЛЛМАНА, НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ УНИВЕРСАЛЬНЫХ ХЭШ-ФУНКЦИЙ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

В. А. Яковлев

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

Проводится исследование способа аутентификации ключей для мобильных устройств, распределяемых методом Диффи-Хеллмана в условиях применения злоумышленником атаки «человек-посередине». Предполагается, что пользователи A и B, формирующие сеансовый ключ, имеют предварительно распределенные случайные цепочки бит ***a*** *и* ***b*** *соответственно, полученные либо от некоторого источника, либо сгенерированные в ходе реализации сценария «близкой аутентификации» на основе данных, полученных от магнитометров или акселерометров из состава мобильных устройств. Злоумышленник не имеет доступа к этим цепочкам. Ключ (значение Диффи-Хэллмана – DH) разделяется на N блоков по m бит эти блоки кодируются помехоустойчивым (T, N)-кодом, имеющим кодовое расстояние D. Аутентификация ключа (DH-значений) осуществляется путем формирования аутентификаторов длиной ν бит, к каждому блоку с использованием универсального класса хеш-функций. Хеш-функция задается ключем, который является подблоком длиной 2m бит случайных цепочек* ***a*** *или* ***b.*** *Получены соотношения для расчета вероятности ложного отклонения значения DH и вероятности не обнаружения навязывания ложного значения DH в зависимости от параметров m, ν, N, T, D. Сформулирована задача оптимального выбора параметров, минимизирующих длину цепочек* ***a*** *и* ***b.***

метод Диффи-Хеллмана, аутентификация, универсальные хэш-функции, помехоустойчивые коды.

Перспективным способом обеспечения ключами мобильных устройств (смартфонов) для осуществления конфиденциальной связи является метод Диффи-Хеллмана [1]. Однако для предотвращения атаки человек-посередине необходимо, чтобы данные, которыми обмениваются корреспонденты, были аутентифицированы. Для аутентификации целесообразно использовать дополнительные последовательности, генерируемые корреспондентами на основе данных, полученных от магнитометров или акселерометров, встроенных в смартфоны, при близком взаимном расположе-

нии мобильных устройств. Протокол формирования ключа на основе магнитометрических данных MagPairing предложен в [2]. В [3] проведен анализ стойкости такого протокола в условиях активного нарушителя и показано, что данный протокол не является стойким к атаке «человек посередине». В [4] был предложен способ аутентификации для метода Диффи-Хеллмана на основе магнитометрических данных, с использованием аутентифицирующих помехоустойчивых кодов (АП-кодов), обеспечивающий устойчивость к атаке человек посередине. В данной статье продолжено исследование способов аутентификации данных, распределяемых по методу Диффи-Хэллмана на основе использования, случайных двоичных цепочек бит, полученных от магнитометров или акселерометров, и применения универсальных хэш-функций в сочетании с помехоустойчивым кодированием.

Рассмотрим двух пользователей мобильной сети связи, назовем их Алиса (*A*) и Боб (*B*), которые вырабатывают совместный ключ, используя метод Диффи-Хеллмана [1]. Для этого пользователи *A* и *B*, согласуют параметры: p и g, где p – просто число, а g – элемент конечного поля $GF(p)$, порождающий группу, имеющую большой порядок. Далее выполняется следующий протокол.

1. Алиса генерирует элемент $x \in (1, p-1)$, вычисляет $X = g^x(modp)$ и посылает его Бобу.

2. Боб генерирует элемент $y \in (1, p-1)$, вычисляет $Y = g^y(modp)$ и посылает его Алисе.

3. Алиса вычисляет ключ $K = Y^x(modp)$.

4. Боб вычисляет ключ $K = X^y(modp)$.

Легко видеть, что ключи, найденные Алисой и Бобом, равны $K = g^{yx}(modp) = g^{xy}(modp)$.

Будем далее величины *X*, *Y*, которые передаются по открытым каналам, называть значениями Диффи-Хеллмана (DH-значениями).

Пусть пользователи сети (*A* и *B*) имеют двоичные предварительно распределенные последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$ соответственно. Символы в последовательностях равновероятны и взаимно независимы.

Обозначим вероятность несовпадения бит в последовательностях $\boldsymbol{a}$ и $\boldsymbol{b}$ – $p_m = P(a_i \neq b_i)$, где i = 1, 2...L – номер символа в последовательностях.

Предполагаем, что злоумышленник *E* во время процедуры получения (выработки) аутентифицирующих последовательностей легальными пользователями (сопряжении смартфонов) отдален от них, поэтому вероятность совпадения бит в последовательности $\boldsymbol{e}$, которую может сформировать нарушитель, и последовательности бит законного пользователя равна $p_e = P(a_i \neq e_i) = 1/2,\ i$ = 1, 2...L.

Для защиты от атаки человек-посередине пользователи *A* и *B* используют следующую схему аутентификации.

Пользователь *A* разделяет DH-значение *X* на *N* блоков длиной *m* бит. На основе универсального класса хэш-функций [6] вычисляется аутентификатор ***w*** длиной *v* бит для каждого блока. Представим блок ***u,*** как элемент поля $GF(2^m)$ и пусть ключ аутентификации $k=(k_0,k_1)$, где k_0, $k_1 \in GF(2^m)$ – элементы $GF(2^m)$, выбираются как непересекающиеся блоки последовательности ***a***. Тогда $w=[u\times k_0+k_1]_v$ – аутентификатор для блока ***u*** [6]. Знаки $\times,+$ обозначают соответственно умножение и сложение в конечном поле $GF(2^m)$, $\lfloor\bullet\rfloor_v$ «усечение», то есть выбор *v* левых ли правых элементов последовательности в квадратных скобках. Для аутентификации каждого следующего блока значения DH, выбираются новые блоки в последовательности **a.**

Корреспондент B для каждого принятого блока значения DH на основе ключей k_0 и k_1, полученных как блоки длиной *m* символов из последовательности ***b*** вычисляет аутентификатор ***w′***. Аутентификатор ***w′*** сравнивается с аутентификатором ***w***, полученным по каналу связи. Если ***w=w′***, то блок ***u*** аутентифицирован. Если ***w≠w′***, то блок ***u*** не аутентифицирован. DH-значение считается аутентифицированным в целом, если среди *N* принятых блоков не аутентифицированы не более чем Δ блоков($1 \le \Delta \le N$).

После аутентификации DH-значений корреспонденты формируют общий сеансовый ключ.

Защищенность системы аутентификации будем оценивать:

P_f – вероятностью ложного отклонения DH-значения в отсутствие навязывания, P_d – вероятностью не обнаруживаемого навязывания.

P_f может быть оценена, как вероятность суммы событий, состоящих в том, что в последовательности из *N* блоков из-за несогласованности аутентифицирующих последовательностей оказываются не аутентифи-цированными Δ + 1 и более блоков.

$$P_f = \sum_{i=\Delta+1}^{N} C_N^i p_b^i (1-p_b)^{N-i},$$

где p_b – вероятность несовпадения ключей (k_0,k_1), выделенных их последовательностей ***a*** и ***b.*** Если несовпадения бит в ***a*** и ***b*** подчиняются закону Бернулли, то $p_b = 1-(1-p_m)^{2m}$.

Для оценки вероятности P_d рассмотрим стратегии две навязывания нарушителя.

Первая стратегия. Нарушитель реализует атаку человек посередине. Для этого он делает подмену *X* на *X'* и заменяет аутентификаторы в каждом блоке.

Обозначим через *D* количество блоков, в которых отличается *X* и *X'*. Тогда, учитывая, что вероятность успешного навязывания ложного

аутентификатора длиной v символов при исспользовании универсальных хэш-функций равна $P_s = 1/2^v$ [6] можно записать:

$$P_d = \sum_{i=0}^{\Delta} C_D^i (1/2^v)^{D-i} (1-1/2^v)^i \sum_{j=0}^{\Delta-i} C_{N-D}^{ij} p_b^j (1-p_b)^{N-D-j}$$

где первая сумма характеризует вероятности фиксации на приеме i ложных аутентификаторов $(1 \le \Delta \le N)$, которые обнаруживаются и D-i ложных аутентификаторов, которые не обнаруживаются, вторая сумма – сумма вероятностей несовпадения j $(0 \le j \le \Delta - i)$ аутентификаторов (местного и принятого), за счет несовпадения блоков в аутентифицирующих последовательностях $\boldsymbol{a}$ и $\boldsymbol{b}$.

Вторая атака. Нарушитель ставит кратковременную цель – навязать любое ложное сообщение *X'*, зная что в дальнейшем он не сможет сформировать общий ключ ни с *A* ни с *B*. Но при этом он существенно затягивает процедуру аутентификации. Для выполнения такой атаки нарушителю достаточно сформировать ложное значение *X'*, отличающееся от *X*, хотя бы в одном блоке.

Предотвращение такой атаки возможно, если нарушитель будет вынужден формировать ложное сообщение, отличающееся от истинного, на число блоков большее порога Δ. Для этого DH-значение, передаваемое от *A* к *B*, закодируем q-ичным (T,N)-кодом с кодовым расстоянием $D > \Delta$, где N – число информационных символов. Далее, каждый m-блок аутентифицируем с помощью универсальных хэш-функций. На приемной стороне легальный пользователь проверяет является ли принятое сообщение кодовым словом, а затем выполняет проверку аутентификаторов принятых блоков.

Выражения для вероятности ложного отклонения ключа и вероятности необнаруженного навязывания в этом случае:

$$P_f(code) = \sum_{i=\Delta+1}^{T} C_T^i p_b^i (1-p_b)^{T-i},$$

$$P_d(code) = \sum_{i=0}^{\Delta} C_D^i \left(\frac{1}{2^v}\right)^{D-i} \left(1-\frac{1}{2^v}\right)^i \sum_{j=0}^{\Delta-i} C_{T-D}^{ij} p_b^j (1-p_b)^{T-D-j}.$$

В качестве q-ичного ($q = 2^m$) (T,N)-кода можно выбрать расширенный код Рида-Соломона с параметрами $D = T - N + 1$, $T = 2^m$ [7].

На рис. приведены зависимости P_f и P_d от Δ при различных значениях v и $p_m = 0{,}01$ для следующих параметров: длина DH-значения $n_0 = 256$ бит, длина блока аутентификации $m = 6$. Значения DH кодируются (T,N)-кодом

Рида-Соломона $T = 2^m = 64$, $N = 43$, минимальное кодовое расстояние кода $D = 22$.

Видим, что выбрав $\Delta = 14$ и $v = 4$, можно получить значения вероятности ложного обнаружения навязывания и вероятности навязывания не более 10^{-5}. Для формирования (проверки) аутентификаторов расходуется $L = 2mT = 12 \cdot 64 = 768$ бит аутентифцирующей последовательности.

Для выбора параметров системы аутентификации необходимо решить оптимизационную задачу, которую можно сформулировать следующим образом: заданы длина DH-значения – n_0 бит; допустимая вероятность ложного отклонения $P_f^{\text{доп}}$; допустимая вероятность навязывания $P_d^{\text{доп}}$; вероятность ошибки на бит в аутентифицирующих последовательностях – p_m.

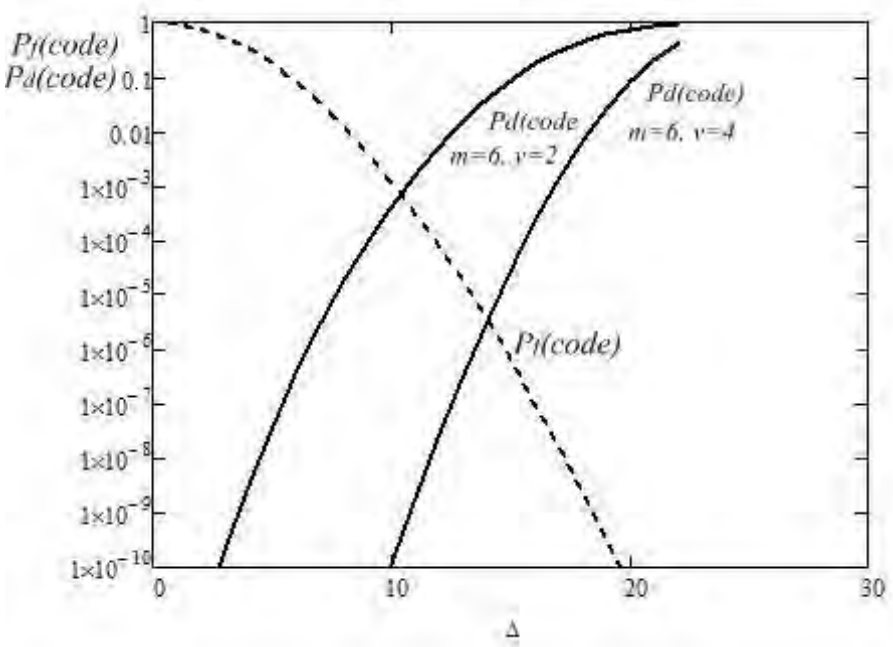


Рисунок. Зависимости P_f и P_d от Δ
при длинах аутентификатора $v = 2$, 4 и $p_m = 0{,}01$ для РС кода (64,43)

Требуется выбрать: длину кода T и кодовое расстояние D; длину блока m; длину аутентификатора $v \le m$; порог схемы аутентификации Δ; такие, что при выполнении условий: $P_f \le P_f^{\text{доп}}$, $P_d \le P_d^{\text{доп}}$ минимизируются: длина кода T, длина аутентифицирующей последовательности $L = 2mT$, суммарная длина аутентификаторов – Tv.

Решение задачи оптимизации автор рассматривает как важное направление дальнейших исследований.

Список используемых источников

1. Diffe M., Hellman M. New directions in cryptography. IEEE Trans. Inf. Theory. 1976. vol. 22, no. 6, pp. 644–654.

2. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. no. 6, pp. 1304–1319.

3. Roy N., Choudhury R.R. Ripple I: Faster Communication through Physical Vibration // Proc. USENIX Symp. Netw. Syst. Design Implement. 2016. pp. 671–675.

4. Яковлев В. А., Зуева Е. О. Анализ уязвимости протокола распределения ключей на основе магнитометрических данных Magpairing // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция (АПИНО-2018) : сб. науч. ст. СПб. : СПбГУТ, 2018. С. 396–401.

5. Яковлев В. А., Зуева Е. О. Разработка способа помехоустойчивой аутентификации для протокола распределения ключей Диффи-Хеллмана на основе магнитометрических данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция (АПИНО-2018) : сб. науч. ст. СПб. : СПбГУТ, 2018. С. 401–406.

6. Коржик В. И., Яковлев В. А. Основы криптографии : учебное пособие. СПб. : ИЦ Интермедиа, 2016.

7. MacWilliams F. J., Sloane N. J. The Theory of Error – Correcting Codes. New York: North-Holland. 1977.

A N N O T A T I O N S

PLENARY MEETING

Bagdasarian A., Butenko V. Telecommunications Environment in the Era of Information Society: Intelligent Devices and Materials of Functional Electronics. – PP. 5–14.
Receiving considerably new possibilities of promising technologies involves solving a number of fundamental and applied problems in the search for new physical principles of generation, transmission, reception and processing of information using modern micro and nano – technologies.
Key words: information society, telecommunication environment, functional electronics, intelligent devices, opal matrices.

Gekht A., Gogol A. To the 150th Anniversary of the Electronic Television's Founder Birthday: Milestones of B. L. Rosing's Biography and Scientific Work. – PP. 14–19.
This article's goal is not only describe the most important milestones of B. L. Rosing's scientific biography, but also to clarify the situation with the scientist's burial place. There is a point of view, according to which, the memorial created in 2005, is just a cenotaph and the real tomb remains in extremely neglected form. The authors of this paper responsibly claim that the above position is fatally flawed. Using B. L. Rosing's reburial video as their proof, the authors prove that the scientist remains were transferred from the old burial place to the current grave at the Vologda Cemetery in Archangelsk, Russia.
Key words: electronic television, B. L. Rosing.

INFORMATION AND COMMUNICATION NETWORKS AND SYSTEMS

Abdusalamov R., Anufrenko A., Mordvinova O., Fomkin R. The Influence of Elements of the Transport Network with Carrier Ethernet Technology on the Propagation Delay of the Traffic. – PP. 20–24.
Transport network connection Carrier Ethernet can be based on different architectures with a huge number of elements. When passing traffic in the directions of the transport network inevitably there are various kinds of delays associated with its processing in each node of the network, as well as its distribution over the network. To ensure the required quality of user service, it is necessary to be able to take into account in detail the impact of the functioning

of the elements of the transport network on the delay of traffic passing through it. This is facilitated by the development of appropriate simulation models of the functioning of the Carrier Ethernet transport network.
Key words: node delay, transport communication network, Carrier Ethernet, simulation, aggregation node.

Abdusalamov R., Fomkin R. Analysis of the Probability of Packet Loss in the Router's Buffer, Taking Into Account the Fractality of Traffic. – PP. 25–28.
The article studies the dependence of traffic fractality on the router BZU in the main queuing systems. Network traffic is considered as the system under study, where there are flashes or spikes at various time intervals. A relevant conclusion about the feasibility of increasing the capacity of BZU in order to reduce the impact of traffic fractality.
Key words: self-similar traffic, traffic fractality, Hurst index, BZU-buffer storage device.

Avramenko V., Bochkarev D., Malikov A. Analysis of the Problem of Investigating Computer Incidents in Infocommunication Systems. – PP. 29–32.
There are many various prerequisites for the occurrence of computer incidents in modern infocommunication systems. Diversity and the heterogeneity of information security events creates new requirements for the systems of analysis and rapid response to computer incidents.
Key words: the information security, computer incident, artificial intelligence, artificial neural network.

Ageev S., Ivanov A., Kolomeets M., Komashinsky V., Kotenko I. The Architecture of the Computer Network Visualization System Based on Touch Screens and Augmented Reality. – PP. 33–36.
The use of touch screens in conjunction with augmented reality systems in support systems and decision-making based on visual analytics allows for a more efficient analysis of the state of a computer network compared to conventional LCD displays. To share them, it is necessary to develop such an architecture that will allow visualizing and managing data in real time on several types of devices at once: a touch screen, an LCD display and augmented reality glasses. The paper proposes a concept of architecture support systems and decision-making based on visual analytics, which implements several methods of presenting information on different devices.
Key words: visual analytics, systems architecture, information security, touchscreens, augmented reality.

Akishin V., Kislyakov S., Terentyev D. Implementation of IoT Elements in the Mechanisms of Measuring the Customer Experience of the Telecom Operator`s Client. – PP. 37–41.
Currently, Telecom operators (and other B2C market participants) are increasingly interested in the introduction and development of mechanisms for measuring customer loyalty in order to control the churn and increase the profit received from each client. Therefore, approaches to achieve these goals, based on the customer experience management - customer impressions from contact with the company throughout the whole client life cycle, are becoming more popular. The rapid development of the concept of the Internet of Things provides new opportunities

in terms of customer experience management (CEM). This paper discusses possible solutions of CEM/IoT to improve the accuracy of identification of telecom operator`s customer.
Key words: customer experience management, Internet of Things.

Alekseeva D., Bylina M. Experimental Investigation of DWDM Integrated Optical Multiplexer. – PP. 42–46.
Nowadays the most promising technology for transport networks is dense spectral multiplexing with optical multiplexers (MUX) and demultiplexers (DEMUX). The best characteristics have integrated optical MUX/DEMUX based on an Arrayed-Waveguide Grating (AWG). In this work we investigate the parameters of 40-channel AWG DEMUX with 100 GHz channel spacing: their insertion loss and transition attenuation to the Far End Crosstalk (FEXT).
Key words: fiber-optic communication, division multiplexing, demultiplexing, AWG, DWDM.

Al-Sweity M., Muthanna A. S. Research of Modern Methods of Video Traffic Acceleration Using Edge Cloud Computing. – PP. 47–50.
It is expected that by 2021, 80 % of the world's Internet traffic will be video, so video acceleration is a requirement for better performance (QOE). There are many ways to model video traffic; in this article we will look at the latest and most common models. We also study and analyze the latest mechanisms and methods developed for video acceleration. In addition, video acceleration is analyzed in terms of 5G based on the ITU and 3GPP specifications announced.
Key words: IoT, 5G, MEC, Mobile-Edge Computing.

Andreev V., Bourdine A., Burdin V., Eremchuk E. Simulation of a Few-Mode Fiber Optic Link with Compensation of Chromatic Dispersion and Differential Mode Delay at the Physical Level. – PP. 51–55.
The paper presents the results of simulation modeling of a two-mode fiber-optic link with compensation of chromatic dispersion and differential mode delay at the physical level. The simulation was carried out on the basis of the solution of a system of coupled nonlinear Shadinger equations by Fourie split-step method. The model of a few-mode fiber optic link took into account the nonlinearity, dispersion, differential mode delay, and random mode coupling.
Key words: few-mode optical fibers, mode coupling, differential mode delay, chromatic dispersion, system of coupled nonlinear Schrödinger equations, errors probability.

Andreeva E., Valyukhov V., Kuptsov V. Hight-Quality Video Transmission Over Fiber-Optic Network with CWDM-Technique. – PP. 56–60.
A set of modulator and demodulator for studio-quality image transmission with the use of optical signal frequency technique for fiber-optic CWDM-systems was developed, investigated and successfully installed. The fiber-optic CWDM-channel for transmission of the full color high-quality television image with sound is realized in the operating network.
Key words: fiber-optic video systems.

Andreeva E., Valyukhov V., Kuptsov V., Sumkin V. Fibre Optics CWDM Security System. – PP. 60–65.
Fiber-optic video network of the manufacturing enterprise using CWDM method is presented. The application of the CWDM-method significantly increases both the profitability of the newly created systems and optimize the expansion of segments of existing systems. Ultra-bandable cable is selected for enterprise network segments. The scheme of technological control of one of segments is given as an example.
Key words: videosystems, security systems, fiber-optic cables.

Andreeva O., Polyakov P. Model of the "Down Direction" Channels of the Basic Station of UMTS Signals. – PP. 66–69.
The UMTS standard belongs to the third generation of cellular standards (3G). The main difference from the previous standards is the introduction of wide-band code division multiple access technology. The UMTS standard is the basis of the work of the largest communication providers in Russia, such as MTS, Beeline and Megafon. The standard allows you to maintain data transfer rates at a theoretical level of up to 21 Mbps, which allows to conduct video conferencing sessions via a mobile terminal, perform fast downloads of music and video content, and access the Internet. In this paper, we consider a model of a generator of UMTS signal for the "down direction" *channel. The proposed principle of modeling allows us to simplify the imitation of the ether environment.*
Key words: IPTV, caching, TV, time-shifted, the proxy.

Andrianov V., Vinogradova O. Development of a Methodology for Protected Control of Working Time Records for Public Service Employees. – PP. 70–75.
At all stages of information technology development, it was obvious that data stored and processed electronically must be protected, but initially external threats were given priority. Today, the problem of protection against internal threats is also gaining a significant turn, as with the development of these technologies and their gradual introduction into an increasing number of companies, and as a result, an increase in awareness of existing problems. In addition, it is also important to imply in the state services the availability of systems that ensure reliable work of employees, who may be potential violators for time-tracking control systems consisting of the listed information protection systems.
Key words: DLP, SIEM, data protection, cryptography, authentication.

Arbuzov N., Prudnikov S., Cleaver V., Shipulin S. Biometrics in access control. – PP. 76–81.
This article is devoted to the introduction of biometric recognition methods.It is known that biometric recognition methods are used by people in everyday life. So we know people we know by face, voice, gait, etc. the Police identify criminals by fingerprints, too, for a long time. This method is convenient, reliable, practical. And for many years biometric technologies have been used in ACS. Everyone understands what it is, how they work. But, surprisingly, until now it has not entered into mass practice. According to recent surveys, only 11 % of installers use biometric technology more or less regularly at their facilities.
Key words: electronic means of human biometric identification, controller, ACS, access control systems, authentication, integration, algorithms and software, verification (confirmation).

Arepiev P., Kalyashov E., Saveleva A., Tarlykov A. Building of Various Pixel Masks for Objects with Neural Network Based on U-Net Architecture. – PP. 81–85.
The article presents a process of construction and optimization of neural network to build pixel level masks of different shape – circular, rectangular, convex hull. Training data generation process and description of changes in network design for various object scales support are given. Results of the network against a model example are also provided.
Key words: convolutional neural network, u-net, training, data generation.

Arepiev P., Kalyashov E., Tarlykov A., Shvidkiy A. Testing of Generalization Ability of a Segmentation Neural Network Trained with a Limited Synthetic Dataset of Airplanes. – PP. 86–90.
The article investigates applicability of a convolutional neural network trained with a limited synthetic dataset for objects' segmentation against various backgrounds. Synthetic data generation technic and a method to prepare additional training data with the help of the network itself are given. Results of the network against a model example are also provided.
Key words: convolutional neural network, training, data generation.

Astakhova T., Vorobieva D., Kolbanev M., Shamin A. Estimation Model of Data Delivery Time in Wireless Sensor Networks. – PP. 90–93.
Exploring ways to save energy with individual devices to increase the time that they function for wireless sensor networks without recharging the battery is one of the primary tasks of recommendations Y. 3001 Future Networks. A model for estimating the probability of message delivery time is built, which improves the accuracy of assessing the quality of the wireless sensor network.
Key words: wireless sensor network, probability-energy characteristics, message delivery time, signal power at the transmitting antenna.

Astakhova T., Vorobieva D., Kolbanev M., Shamin A. Characteristics of Energy Consumption of Smart Things. – PP. 93–97.
Probability-energy characteristics which depend on the spatial parameters of the network and the technical characteristics of the sensor devices, allowing to determine the interdependence of energy and information parameters, as well as providing an opportunity to estimate the lifetime of the sensor network are investigated in this paper.
Key words: wireless sensor network, probability-energy characteristics, radio signal power, distribution density, Poisson field of points, distribution, network topology, smart things, energy efficiency of transmission.

Balueva A., Desnitsky V. Approach to Detection of Denial-of-Sleep Attacks in Cyber-Physical Systems on the Base of Machine-Training Methods. – PP. 97–103.
The paper analyzes possible types of attacks in the field of information security of cyber-physical systems and analyzes the available literature in the field. A problem of the vulnerability of Internet of Things devices in wireless networks to attacks aimed at depleting energy resources are considered. Several types of traffic and conducted a visual analysis of normal and attacking traffic are regarded. An approach to detecting the depletion of energy resources

in cyber-physical systems on the base of machine learning methods is proposed. The effectiveness of the proposed solution is confirmed by an example of identifying the attacking traffic by using Python language and Anaconda distribution.
Key words: information security, energy depletion attacks, analysis, Internet of things, cyber-physical systems, machine learning.

Baranova D., Saenko I., Smirnov E. Monitoring of Information Activity in Social Networks. – PP. 103–107.
Possible ways to solve the problems of combating harmful influence in social networks today is the convergence of socio-humanitarian and technical Sciences. Therefore, when we consider the issues of detection and counteraction of illegal activity, we investigate both humanitarian and technical aspects. The paper describes the optimization approach of ant colony. This is a polynomial algorithm used to find approximate solutions of the optimal path in the graph, proposed in the 70s of the 20th century by the American sociologist for the analysis of networks. It is assumed that the ant algorithm will identify the source of unwanted information in the social network.
Key words: social network analysis, social graphs, ant algorithm, Ant Colony Optimization, information activity, harmful influence.

Batenkov K. Multipolar Communication Network Reliability Analysis Based on Minimum Cross Sections Method. – PP. 108–112.
The paper considers an approach to the analysis of the reliability of multi-pole communication networks based on the method of minimum cross sections. The essence of this method of calculating the probability of incoherence is reduced to the formation of all possible combinations of sections, so that each combination contains all the elements of the graph included in the combined sections, as well as the calculation of the probability of the existence of combinations and their alternating summation.
Key words: communication networks, reliability, availability factor, method of full enumeration of typical states.

Batenkov K., Korolev A., Mironov A. Multipolar Communication Network Reliability Analysis Based on Minimum Cross Sections Method. – PP. 113–116.
It is emphasized that it is necessary to provide a known compromise between the maximum accuracy of the mathematical description of the functioning of the MSS, which leads to the complexity of the analysis apparatus and the availability of its use by the engineering and technical staff. It is illustrated that the implementation of a fully accessible link of the ICJ equal access strategy to service resource-intensive and low-resource applications are served with different quality (the probability of loss of applications in the first flow of requirements is lower than in the second resource-intensive).
Key words: multiservice communication network, heterogeneous traffic, analytical model, Kaufman-Roberts method.

Bakhtin D., Volkogonov V., Stasyuk V. Model of Protection Against Backdoors with a Following Analysis and Evaluation of Incidents. – PP. 117–123.
In modern distributed information systems (hereinafter – RIS), various types and characteristics of unauthorized access and data leakage prevail. For example, attack of the "back door" and the exploit. In the article discusses model of protection against backdoors with a following analysis and evaluation of incidents. It is proposed to develop and implement a model in a distributed information system.
Key words: backdoor, exploit, unauthorized access, distributed information systems, inform. security.

Bahtin U., Bushuev S., Kolomeets M., Komashinsky N., Kotenko I. Computer-Human Interaction Algorithms for Touch Screens in a Computer Network Visualization System. – PP. 123–127.
In modern computer network monitoring systems, the number of types of information sources that are becoming difficult to manage is extremely rapidly growing. Thus, it becomes necessary to develop new methods of data management within the framework of support and decision-making systems and, in particular, within the framework of visual analytics systems for monitoring network security. The paper discusses the implementation of cimputer-human interaction algorithms based on touch screens for controlling computer network state analysis systems. The considered algorithms allow using gestures to control the modes of drawing a computer network, movements between levels of the OSI model, as well as control the processes of filtering and scaling information.
Key words: touchscreens, cimputer-human interaction, information security, visual analytics.

Belozertsev I., Elagin V., Onufrienko A. The Impact of Blockchain Technology on Network Probability-Time Characteristics. – PP. 127–132.
Due to the increased popularity of blockchain technology applications, there are the problem of impact of this technology to the network characteristics and how does the technology affect the network. In this article, the authors introduce a definition of the term blockchain, describe the services implemented by this technology and its scope. The authors indicate basic features of the network required for guarantee quality of service during provision and transfer for different type of traffic, determine the network scheme working with blockchain transactions and the dependence of network characteristics on application parameters.
Key words: blockchain, QoS, Quality of service, distributed registry.

Belozertsev I., Elagin V., Onufrienko A. Models of QOE Ensuring for OTT Services. – PP. 132–137.
This article discusses the main models that contribute to improving the quality of OTT services. The main parameter for quality assessment was chosen QoE-Quality of Experience. An analysis was made of a number of factors that directly affect the assessment of QoE. The second part of the article deals with models that can provide the necessary level of quality for OTT services. These models were divided into three groups: traffic-based models, application-based models, and speed-based models. The main task of the study is to find optimal solutions to ensure the quality of OTT services.
Key words: OTT Services, QoE, MOS.

Belozor A., Goldstein A. Application of Chaos Theory to Forecast Customer Churn. – PP. 137–143.
The solution to the problem of forecasting customer churn is relevant for all telecom operators. Customer churn can be attributed to chaotic processes, because many of the factors determining the churn do not depend on the operator and cannot be determined and described in advance. The report describes the possibilities of applying the mathematical apparatus of the theory of chaos to predict the churn of the telecommunication operator.
Key words: churn, chaos theory, customer experience management (CEM), customer relationship management (CRM), OSS/BSS systems.

Berezina E., Yakovlev V. Shor's Algorithm for Factorization Attack of the Module of Cryptosystem of RSA is Analyzed. – PP. 143–148.
The Quantum Shor's algorithm is consists of five steps. Four of this steps, which are performed on a quantum computer, is analyzed. The computational rate of this algorithm is based on a fundamental property of the quantum parallelism, which allows quantum computers to compute a multivariable function simultaneously. An example of factorization attack on the module of the cryptosystem RSA by this method is given. The problems of creating a simulator of quantum computing for the Shor's algorithm, which is supposed to be used to study attacks on the cryptosystem of the RSA in the educational process, are highlighted.
Key words: the RSA cryptosystem, quantum Shor's algorithm, the attack of module factorization.

Bobrova K., Kanaev A., Saharova M. Analysis of NFV-Based Multiservice Networks Architecture Development Problems. – PP. 149–154.
Research analysis of NFV technology applicability revealed contradictions between different approaches and ETSI GS NFV-SWA 001 V1.1.1 (2014-12) standard in terms of NFV-based multiservice networks architecture development. Report provides comparative analysis of solutions proposed by several researchers and NFV architecture guidelines regulated by ETSI. Step-by-step transition from using nodes of existing multiservice network to a new NFV-based multiservice networks architecture has been also proposed. Detected contradictions and NFV-based multiservice network architecture development problems determine relevance of further research and improvement variants for many different industries application.
Key words: multiservice network (MSN), Network Function Virtualization (NFV), Management and Orchestration (MANO), Telecommunication Management Network (TMN).

Borisenko N. The Design of “Lightweight Ciphers” Using Substitutions with a Trivial Inertia Group with Respect to Affine Transformations. – PP. 154–159.
The adopted national standards and guidelines do not solve fully the emerging problems for an ensuring information security in protecting of high-speed information flows especially in the cases mass encryption with the Internet of things. One of the ways to solve these problems is the use of so-called "lightweight cryptography", that defines a subset of such ciphers, that achieving the same unbreakability as in classical ciphers, but require minimum resources, energy consumption and time of execution. Instead of fixed substitutions using common for conventional ciphers it is proposed to use their affine-equivalent analogues given by some random rule, depending on the key. We analyze S-boxes that have a trivial inertia group with respect to affine transforms.

Key words: block ciphers, substitutions (*S*-boxes), coordinate Boolean functions, affine equivalence of *S*-boxes, inertia group.

Bokhan I., Krasov A., Ushakov I. Comparative Analysis of SDN Solutions from Leading Manufacturers. – PP. 160–163.
In the rapidly developing world of network technologies, such an innovative network architecture as SDN attracts a lot of attention. The article discusses SDN solutions from the leading companies in the field of network technologies – Cisco Systems (Cisco ACI) and VMWare (VMWare NSX), and will be compared between these projects.
Key words: software-defined networking, SDN, Cisco ACI, VMWare NSX.

Branitskiy A., Vanchakova N., Doynikova E., Kotenko I., Krasilnikova N., Saenko I., Tishkov A. Common Approach to the Determination of Destructive Information Impacts and Negative Personal Trends of Young Generation Using the Techniques Based on Neural Networks for Internet Content Processing. – PP. 164–167.
The paper describes the developed common approach to the identification of destructive informational impacts and negative personal tendencies of the younger generation using the methods of neural network processing of Internet content. Currently, the Internet space is the main envionment for the dissemination of destructive information effects. Therefore, it is important to monitor and identify destructive informational impacts and negative personal tendencies of the young generation when interacting with the Internet space. The proposed approach includes a method for determining the features and criteria for identifying destructive content and destructive impact in the Internet; the method of revealing signs of destructiveness of Internet users based on information on their personal pages in social networks; methodology for monitoring and identifying destructive information impact in the Internet through the use of methods of neurocomputer and neural network processing of Internet content.
Key words: destructive impact, destructive content, social networks, neural networks.

Branitskiy A., Doynikova E., Kuzmina V., Saenko I., Chechulin A. Analysis of CVSS Metrics System in Order to Develop Attack Graph Algorithm. – PP. 167–72.
Article is devoted to development of an algorithm in order to develop attack graph. Algorithm developed based on analysis of CVSS v.3. metrics system. Work of algorithm and final graph are considered on example of a test computer network.
Key words: graph attack, CVSS, computer network, computer security.

Burdin A., Burdin V., Zhukov A. Simulation of 10GBase-LX Optical Signal Transmission over Multimode Optical Fibers with Extremely Enlarged Core Diameter and Reduced Differential Mode Delay. – PP. 172–177.
This work present some results of simulation IEEE 802.3ba 10GBase-LX optical signal transmission over 100 μm core MMFs with earlier on designed special refractive index profile, providing selected mode staff differential mode delay reducing down to 256 ps/km at the wavelength 1310 nm.
Key words: multimode optical fibers, differential mode delay.

Butsenko M. Organizing and Evaluating of Voice Transmission Quality Via IP Protocol on Android Devices. – PP. 178–182.
The article considers an example of a programatic phone development, based on OS Android and the open LibLinphone library. The mobile app provides user connection service, used in information exchange via SIP protocol. There has been conducted a test of voice transmitting utilizing PESQ protocol, calculated the bandwidth, required for the programatic phone.
Key words: ip-telephony, sip, android, VoIP.

Bylina M. Review and Comparative Analysis of Reflectometric Methods for Measuring Parameters of Cable Communication Lines. – PP. 182–187.
The classification of reflectometric methods by the type of probe signal used is given. A comparative analysis of various methods on the complexity of implementation, scope and information content. The advantages and disadvantages of each considered method are revealed. Recommendations on the use of various reflectometric methods for solving specific measurement problems are formulated.
Key words: two-wire communication line, reflectometry, reflectometer, time domain reflectometry, frequency domain reflectometry, time-frequency domain reflectometry.

Bylina M., Glagolev S., Semenov A. New Methodology and Results of the Calculation of the Linear Capacity of Two-Wire Circuits. – PP. 187–192.
The known G. Howe's method for calculating the linear capacity of two-wire circuits is analyzed. It is shown that its use leads to an underestimated result. A new method for calculating the linear capacity, based on the actual distribution of the linear charge density over the surface of the conductors, is proposed. The results of the calculation of the linear capacity of various two-wire circuits, confirming the effectiveness of the proposed method are presented.
Key words: two-wire communication line, balanced circuit, capacity per unit length, G. Howe method, linear capacity, linear charge density.

Bylina M., Reznikov B. Methods and Results of Interferential Filters Calculation. – PP. 193–197.
The paper discusses the matrix method for calculating multilayer structures that underlies optical interference filters. A method for calculating structures based on transfer matrices and scattering matrices is proposed. The results of the calculation of the filter, which is a two-layer structure, are given.
Key words: optical interference filters, radiation filtering, layered media, multilayer structures, frequency characteristics.

Valieva K., Vitkova L., Chechulin A. Preparatory Processing of Information Objects in the Monitoring Systems of the Internet. – PP. 197–201.
Today main information data flows are directed to the person from the Internet. Society is immersed in the information sphere, a process of digitalization has strong tendency to progress. The methods of collecting which are used in modern monitoring systems were created when flows and capacity of data were much less than nowadays. The authors are researching present approaches, methods and algorithms, are searching ways of improvements. The main aim of the research is to find characteristics and evaluation of information objects' parameters,

which would help to provide the prioritization of tasks for the monitoring systems of the Internet.
Key words: monitoring, big data, information object, class of information objects, data model.

Vasyliv N., Esalov K., Kislyakov S., Pupcev R. Comparative Analysis of Neural Network Models Relating to the Problem of Forecasting the Load of a Contact Center. – PP. 201–205.
The work is devoted to the study of the neural network model for predicting the number of incoming calls to the call center. To calculate the parameters of the model, a machine learning method was applied using real input contact center loads. The urgency of the task posed in the report is determined by the understanding of the number of operators that must be "in place" in order to ensure the proper quality of service of the call center. To do this, we need to predict the number of incoming calls in advance. The paper provides a comparative analysis of various models for predicting incoming calls based on various mathematical methods.
Key words: call center, operator, neural networks, LSTM, forecasting.

Venediktov A., Volkogonov V. The Main Types of Threats to Compromise Openflow Channels in SDN. – PP. 206–209.
In the architecture proposed by SDN networks, the control plane and the data plane for data transmission devices are separated, which leads to the transformation of the original closed network architecture into a more open one. From this it follows that the proposed architecture is subject to various specific types of attacks. Realizing threats in a software-configured network can lead to the compromising of various components, such as OpenFlow controllers, physical or virtual switches, control systems, and applications. This article presents an analysis of the main types of threats when the Openflow channel is compromised and measures that contribute to counteracting them.
Key words: SDN, SDN architecture, software-defined networks, Openflow.

Vitkova L. The Place and Role of Monitoring and Counteraction Unwanted Information in Social Networks. – PP. 209–212.
With the high level of distribution of social networks and the lack of clear legal mechanisms to control them, political opponents, international terrorist and extremist organizations, criminal structures are aware of the opportunities that they can use to influence the user. Modern approaches to the detection of illegal information on the Internet in General and in social networks in particular need to be improved taking into account the change of the "communication model" of the modern user. The paper presents a model of user communication. Possible ways to improve the monitoring and counteraction system taking into account the presented model are described.
Key words: monitoring, counteraction, unwanted information, social network analysis, communication model.

Vitkova L., Gamidov T., Doynikova E., Dudkina O., Kushnerevich A. The Analysis of Features of the Industrial Internet of Things for Formation of a System of Security Metrics. – PP. 212–217.
Article is devoted to the analysis of features of the industrial Internet of things, the existing methods and information security standards, for the purpose of formation the system of security metrics for the industrial Internet of things.
Key words: internet of things, risk assessment, vulnerabilities, information security, security assessment techniques.

Vitkova L., Desnitsky V., Zhernova K., Chechulin A. Review of Human-Computer Interaction for Network Security. – PP. 218–223.
The paper presents an analysis of ways of human-computer interaction in modern software tools for network security. As an example, several security information and event management systems (SIEM systems) and traffic analyzers are considered from the point of view of user and program interaction both from the user side and from the program side. Ways of implementing human-computer interaction in these software tools are compared with each other, their advantages and disadvantages are determined. On the basis of the analysis performed, an assessment is made of the effectiveness of human-computer interaction in modern software tools for network security.
Key words: human-computer interaction, information security, SIEM-systems, user interfaces, graphical user interface, text-based user interface.

Vitkova L., Doynikova E., **Kotenko I.** Model of Responses Against Unwanted, Questionable and Malicious Information on the Internet. – PP. 223–227.
The goal of the research consists in the development of the model of responses against unwanted, questionable and malicious information on the Internet. The paper considers different responses against unwanted, questionable and malicious information and outlines their types. The classification of responses via different parameters is defined. The parameters include information type, an information distribution channel, target audience, an efficiency and way of counteraction. Besides, the set of metrics for the responses is proposed. The model is constructed considering outlined classes and their features, i.e. qualitative characteristics of the responses, and outlined metrics, i.e. quantitative characteristics of the responses. The paper also describes the place of the developed model in the common approach of countering unwanted, malicious and questionable information.
Key words: unwanted, questionable and malicious information, responses, model, Internet.

Vitkova L., Kotenko I., Fedorchenko A., Hinenzon A. Distributed Data Collection and Processing In Systems of Monitoring of Information Space Social Networking. – PP. 228–232.
One of the most important areas that qualitatively change the structure of information security of the state in recent years is the involvement of the population in social networks. At the same time, the constant growth of the volume and variability of data obtained from social networks requires new approaches to building the architecture of the monitoring system and decision support to counter the spread of illegal information. In this paper, the authors propose a General approach and a conceptual scheme of the architecture of such a system, taking into account the dynamics of social networks. It is assumed that the use of the proposed architecture will improve the effectiveness of protection against unwanted information.

Key words: social network monitoring, monitoring system architecture, social network analysis, distributed algorithms and systems.

Vitkova L., Kuraeva A., Pronoza A., Chechulin A. Analysis of Methods of Identification and Evaluation Pages of Opinion Leaders in Social Networks. – PP. 233–237.
The aim of the study is to analyze the available methods and techniques for detecting opinion leaders in the space of social networks. The basis of the experiment, the results of which are described in the work, were taken indicators of involvement of users of the network "Vkontakte", such as "view", "comment" and "like". At the same time, the authors propose to divide opinion leaders and their enthusiastic users into clusters. Today, the mechanisms of control over the information space of social networks do not fully meet the criteria that are assigned to them. It is assumed that the allocation of such clusters will improve the efficiency of the system of monitoring and combating unwanted information.
Key words: leaders, "view", "comment", "like", cluster, counteraction.

Vladimirov S., Kognovitsky O. Decoding of Gordon–Mills–Welch Pseudorandom Sequences Using the Dual Basis. – PP. 238–242.
The paper presents an algorithm for determining the initial states of the shift registers that form the composite wideband Gordon–Mills–Welch (GMW) pseudorandom sequences using the dual basis of Galois field. The proposed algorithm allows one to determine arbitrary initial states of shift registers, which expands the possibilities of using composite wideband GMW sequences for solving various problems when transmitting information via communication channels with noise.
Key words: Gordon–Mills–Welch sequences, shift register, dual basis, error probability.

Vladimirov S., Malasherifov V. Development of Hardware Model of a Radio Channel with Intentional Interference for Studying of Error-correcting Codes – PP. 243–246.
The paper presents the implementation of a hardware model of a radio channel with noise for the study of error-correcting codes within the framework of the DTSMS data transmission simulation system developed at the Department of Communication Networks and Data Transmission of SPbSUT. The requirements for the developed radio channel model are given, the hardware configuration of the transceiver and control modules is selected, and the interface of interaction with the DTSMS core system is worked out.
Key words: simulation modeling, DTSMS modeling system, radio channel, radio frequency transceiver, error-correcting coding.

Vladimirov S., Mukhametshina D. Maximum Length Cyclic Codes Decoding Method Based on Reverse Matrix Using Soft Solutions – PP. 246–251.
The paper presents a maximum-length codes decoding method based on a decoding method using k-element linearly independent combinations using soft solutions based on weight patterns. Decoding errors of different multiplicities were analised to obtain a table of weight patterns for the maximum length code (7, 3). The scenario of using the proposed decoding method is given.
Key words: maximum length code, soft decoding, M-sequence, decoding by linearly independent combinations.

Vlasova I., Nikitin B., Sergeev A. Estimation of the Dispersion Length of the Regeneration Section in SDH Systems. – PP. 251–257.

In the design of fiber optic lines in the modern regulatory and technical literature, there are several approaches to assessing the dispersion lengths of elementary cable sections. Each of them determines the maximum length of fiber optic lines and imposes restrictions on the speed of optical information transmission. Due to the increase in speed and the desire to increase the length of the cable line, there are new influencing factors that cannot be ignored in the engineering calculations of the projected or reconstructed communication line. In addition, when performing calculations, it is necessary to take into account both the type of optical radiation source and its spectral characteristics, which, even if available, are given in a form that requires some recalculation.

Key words: dispersion, dispersion compensation, group delay time, equipment compatibility, LFM parameters, accumulated dispersion, total dispersion, FOCL length, maximum permissible dispersion.

Volkov A., Kovalenko V., Muthanna A. S. Research of Approaches to Managing Multi-Layer Cloud Structure. – PP. 257–262.

The number of Internet of Things devices continuously increases every year. The amount of traffic generated is also increasing. Therefore, in new generation of networks – 5G, the MEC technology is used to reduce the load and reverse delays. The architecture of MEC is based on multi- layered cloud structure, but the official international documents do not define the principle at which architecture level the computing cloud is selected to control the processing of user data. Therefore, in this article, we propose to compare three architectures for managing the choice of a computing cloud. A multi-layered cloud structure is proposed for implementation on the OpenStack platform.

Key words: IoT, 5G, MEC, OpenStack, cloud computing.

Volkogonov V., Gelfand A., Derevyanko V. The Relevance of Automated Control Systems. – PP. 262–266.

Automated control systems (ACS) play an important role in the modern world. They allow you to increase productivity, as well as optimize the management process. ACS monitors all the main activities, but also perform the function of planning and forecasting. Their appearance greatly improves and simplifies the management processes.

Key words: automated control systems, object control, process control, technologies.

Volkogonov V., Gelfand A., Karamova M. Safety of Personal Data at Their Processing in Information Sstems of Personal Data. – PP. 266–270.

For realization of constitutional right of citizens on personal privacy, a personal and family secret by the Government of the Russian Federation established requirements to safety of personal data at their processing with use of the automation equipment. It is important to note that now works on safety of personal data at their processing are an integral part of works on creation of the corresponding information systems.

Key words: providing, safety, personal data.

Volkogonov V., Kazantsev A., Katasonov A., Orlov G. Analysis of Security Wi-Fi Networks. – PP. 270–275.
Wi-fi networks are widespread in the modern world, in fact, they have become an important communication tool due to their flexibility, efficiency and low cost, on the other hand they transmit data using radio waves, which are usually sensitive to eavesdropping. Many protocols are used to ensure security. Of these, we'll focus on WEP and WPA, which are still widely used. Using these protocols, there is a chance of intercepting the necessary number of packets to recover the secret key. This article searches for the best way to protect wireless networks in order to reduce the average number of interception packets needed to recover the private key.
Keyword: Wi-Fi, Network, Security, WPA.

Volkogonov V., Lomakin A. Open data of the State Agency and Problems for Ensuring Security of Information. – PP. 275–279.
Data of actions and financial operations of the government. They are the guarantor of the transparency of work and development of the organization. This article discusses issues of security in the field of BIG Data. The article reveals the concepts and characteristics of big data and open data.
Key Words: Big data, open data, Information security, Federal Service for Technical and Export Control.

Volkogonov V., Preobrazhenskiy A., Ushakov I. Vulnerability of Software Defined Networking. – PP. 279–284.
SDN (Software Defined Networking) – the architecture that divides the function of control plane, it determines where the network traffic will go, and the function of flow forwarding that transmits traffic to the desired location. In SDN networks, the main functions of routers and switches are transferred to the Central network controller, which greatly simplifies the monitoring of the network status and the application of network policies. Because of its centralized management system, SDN has great potential and a number of significant advantages over traditional network architecture, which provide more effective ways to counter network threats. The article describes the architecture of SDN and OpenFlow Protocol. Also it presents the potential threats of SDN-networks from the point of view of information security.
Key words: SDN, Vulnerability of SDN, OpenFlow.

Volostnykh V., Gvozdev Y., Karganov V. Modeling of Information Systems of Organizations. – PP. 284–289.
The creation and modernization of information systems requires an assessment of their effectiveness. One of the most important indicators of the effectiveness of information systems of the organization is the security of the processed information and the security of the system from potential impacts, which determines the need to simulate information systems operating in security threats. Among the most important stages determining the success of modeling are the choice of indicators for evaluating the effectiveness of information systems. The article discusses approaches to the selection of indicators and criteria for assessing the effectiveness of information systems of organizations, as well as approaches to the construction of a mathematical model of the information system of the organization functioning in a crisis situation.
Key words: information security, information system, modeling, performance evaluation indicators.

Volostnykh V., Gvozdev Y., Kononov P. Analysis of Regulatory Legal Documents to Ensure Information Security of the Organization. – PP. 289–293.
The most important factor in ensuring the security of the organization is to ensure information security. Ensuring information security is determined by a number of regulatory legal documents. The main document is the Doctrine of information security of the Russian Federation, approved by the President of the Russian Federation in 2016. One of the factors of information security of the organization is the protection of information and information systems from possible threats. The article deals with the regulatory legal and guidance documents regulating the order of information security in organizations.
Key words: information security, information protection, legislation of the Russian Federation.

Volostnykh V., Gvozdev Y., Kononov P. Analysis of the Structure of the Manual the Protection of Personal Data in Higner Education. – PP. 294–298.
The problem of personal data security in higher education institutions is relevant today. Due to the large volume of processed personal data, high growth rates of Informatization of education, increase in potential threats to the security of personal data, ensuring the security of personal data should be based on an integrated approach. Ensuring the protection of personal data is determined by a number of regulatory legal documents. The main document is the Federal law № 152-FZ of 27.07.2006 "On personal data". The article analyzes the structure of management of personal data protection in higher education institutions.
Key words: protection of information, personal data, processing of personal data.

Volshchukov M., Kovyarova D. The Provision of Cloud-Based Services on NGN/IP Networks – PP. 298–302.
At the present time, information technology has started to unite a large number of different information systems. They become interpenetrating, in this connection new opportunities arise. Providing services to consumers is one of the most urgent tasks in the world of information technologies. With the advent of a large number of diverse systems, services and technologies, the problem of their interaction, integration and use arises. Optimize information resources and manage them more flexibly with a variety of technologies, in particular today, to solve such problems, the technology of cloud computing is widely used.
Key words: cloud computing, network infrastructure, technology, NGN/IP, heterogeneous environment, information system, IT.

Vorontcov D., Zhmurov V., Parashchuk I. Analysis of Vulnerabilities of Input Device and Reading Device Identification Signs. – PP. 303–307.
The problems of choosing the input devices and reading the identification signs and vulnerabilities of these devices in accordance with the proposed classification are considered.
Key words: device of input of identification signs, device for reading of identification signs, vulnerability, classification, control of an object, unauthorized access, limited access.

Gavrilyuk V., Chechulin A. Analysis of Trends of Informational Threats and Vulnerabilities. – PP. 307–311.
In this article will be analyzed main changes of informational vulnerabilities in different vendor's products. In this work will be used open vulnerability database of National Institute

of Standards and Technology (Common Platform Enumeration, Common Vulnerabilities and Exposures, etc.). As main criteria have been chosen: average threat level, which functions, software or hardware are under risk. Refer to results of this analyze will be made conclusions about the trends of vulnerabilities and possible problems of informational security.
Key words: Vulnerabilities, security analysis, informational security, threats, software, hardware.

Gaifulina D., Khavanskaya E., Chechulin A. Development of a Complex Algorithm for Websites Classification to Detect Inappropriate Content on the Internet. – PP. 312–317.
The paper is devoted to the research of the task of classification of websites to detect inappropriate content on the Internet. We present the results of experiments to analyze website classification algorithms based on different aspects of the source data and different machine learning methods. We identify and justify the need for joint use of classification algorithms. We present complex algorithm to websites classification bases on the simultaneous use of different aspects of websites. We present the experimental evaluation of the results of the proposed algorithm.
Key words: inappropriate content, prohibited information, Internet, Data Mining, machine learning, information protection, website classification.

Hamidov T., Desnitskiy A., Dudkina O., Sakharov D. Methods and techniques for analysis of unwanted information in social networks. – PP. 317–320.
Social analysis has been used for a long time, even before the advent of computer networks and the Internet. For example, telephone or physical surveys are also social analysis. With the development of the Internet and social networks such as VK.com Odnoklassniki.ru, personal information of users began to move to social networks, so there are more opportunities and tools for the analysis of public information. In this paper, we study methods and techniques of social network analysis that can be used in systems of monitoring and combating unwanted information. Due to the high level of digitalization of society, the immersion of the individual in the information space of social networks, the research topic is relevant.
Key words: SNA, the node, network, DNA, measurement, relations, undirected graph, directed graph, search, people, structure, relationships.

Ganyushin A., Elagin V. Analysis of Blockchain Technology and its Scope. – PP. 321–325.
The impetus for the emergence of the blockchain was the crisis of 2008, when people lost faith in traditional financial institutions and instruments. There is a need for payment instruments that are independent of politically involved issuing centers and not burdened by cross-border restrictions, as well as not requiring unconditional trust on the part of the participants. As a result, Bitcoin appeared, and with it the blockchain. Later it became clear that the blockchain can be used not only for cryptocurrency. Blockchain is a system of distributed decentralized storage of registries with increased confidence in ensuring the integrity of information.
Key words: blockchain, public blockchain, private blockchain, smart contract.

Gashkov R., Kanaev A., Tukmachev V. Engineering Methods of Calculating the Optical Characteristics of the Transport Communication Network Based on WDM. – PP. 326–328.
When designing a transport communication network based on WDM, you should determine the requirements for it based on the purpose for the network. Subsequently, it will determine

the design process, technical efficiency and economic expedience of the decisions made. The article discusses standard methods for calculating the characteristics of optical channels and existing problems of calculations. In addition, it contains the rationale for the creation of an engineering method for calculating optical channels.
Key words: transport network, WDM – wavelength-division multiplexing, optical channels, optical path elements.

Gelfand A., Kosov N., Krasov A., Orlov G. Protection for the Distributed Refusals in Service (DDoS) in Cloud Computing. – PP. 329–334.
With information technology development, cloud computing develops and increases the amount of vulnerabilities, using which it is possible to get access to the protected information. One of the possible attack is DDoS-attack, using which it is possible to overload service of the cloud computing. In article the principles of work of cloud computing and options of protection against DDOS-of the attacks are considered.
Key words: DDOS, information technology, attack, cloud.

Glagolev S., Leshchev P. Experimental Study of Losses in Fusion Connections Optical Fibers. – PP. 334–339.
In the early stages of the development of fiber-optic communication, the attenuation coefficient of optical fibers was on the order of several dB/km and the connection loss in tenths or even units of decibels did not seem excessive. Currently, the minimum attenuation coefficient in fibers with a pure quartz core is 0.16 dB/km, and the typical value is 0.2 dB/km. Connection loss of 0.2 dB reduces the permissible length of the optical line by 1 km. The smallest losses of the order of hundredths of dB / km are provided by the welding of optical fibers with modern welding machines. However, low losses are achieved by careful adherence to the welding technology and preparation of the welded optical fibers. This paper is devoted to the issues of experimental measurement of losses in welded joints with various violations of the technology of fiber preparation.
Key words: optical fiber welding, welding machine, fiber loss, optical reflectometer, preparation for welding.

Goldstein A., Kormanovskaya A. Customer Experience Evaluation Using Fuzzy Cognitive Maps. – PP. 340–345.
The current competitive situation in the telecommunications market forces operators' companies to rethink their approach to business and direct their development vector not towards services, but towards customers and their satisfaction. In this regard, companies are actively introducing the concept of Customer Experience Management into their business processes. This concept includes a set of methods, processes and technologies that allow you to manage customer experience. The customer experience itself is formed from a huge number of different factors that are formed in the interaction of the client with the company. And one of the most important aspects in the proper construction of the process of interaction with the client is the cumulative analysis of customer experience. This paper reviews customer experience using fuzzy cognitive maps.
Key words: Customer Experience, Customer Experience Management, cognitive maps, fuzzy logic.

Goldstein A., Terentev D. The Evaluation of Using the Chaos Theory Methods to Predict the Load of Contact-Center. – PP. 345–351.
In today's market, contact centers remain effective tools for interaction with customers. The most important problem in this case is to maintain the optimal quality of service. An integral part of this process is to predict the load on the contact center, followed by scheduling for employees, which allows to achieve the required quality of service and optimize staff costs. This article investigates the possibility of using methods of chaos theory prediction to solve this problem, provides a comparative analysis of their effectiveness.
Key words: chaos theory, forecasting, contact center, WFM.

Goldstein A., Shestakova A. Forecasting with Application of Neural Network in the Class OSS. – PP. 351–356.
The class OSS control systems are especially in demand for the companies, which underscore customer focus of their business and are working in the conditions of the high competitiveness and dynamics. It give tools for the detailed analysis of root causes of the current situation in the company. The class OSS control systems in combination with neural networks become the most powerful tool for business. The ability of neural network to study make it the most attractive tool. Such parameters as outflow of clients, loyalty of clients, and calculation of the optimal number of call center operators can be subject to the forecast in the sphere of telecommunications.
Key words: OSS, neural networks, loyalty, outflow of clients, probability of adoption of the offer, call center operators.

Gordeev I., Model M., Muthanna A. S. Development of a Software Package for Training in Building Software-Defined Networks SDN. – PP. 356–360.
This article discusses the issue of training in the construction of modern SDN networks. To build and maintain software-defined networks in existing conditions, we need trained specialists with the necessary set of theoretical knowledge and practical skills. In order to solve this problem, the authors of the article propose a software package that provides an opportunity to study the theory, pass testing, and also to model SDN networks. With the help of the developed software package, a site was created that allows you to study the basic principles of building and operating SDN networks, apply the knowledge gained to build virtual program-configured networks, and also test yourself using testing.
Key words: Software-Defined Networks, SDN, learning

Gofman M., Kornienko A. Covert Data Transmission Through Air Audio Channel by Watermarked Audio Signals. – PP. 361–365.
A method of digital marking of audio signals is being developed, which is focused on covert data transmission through an airborne audio channel. The embedded digital marker occupies the entire audible frequency range. Each digital marker carries one bit of information. The decision on the value of the transmitted bit is made on the basis of the sign of the central value of the mutual correlation function. The low computational complexity of the proposed labeling method makes it possible to use it for the wireless exchange of information between ordinary smartphones.
Key words: steganography, audio watermarking, covert data transmission.

Grebenshchikova A., Elagin V. Architecture of Network-Slicing-Based 5G System. – PP. 365–370.
5G networks are expected to be able to satisfy users' different QoS requirements. Network slicing is a promising technology for 5G networks to provide services tailored for users' specific QoS demands. SDN has been widely accepted as a promising technique to implement network slicing on the basis of network functions virtualization (NFV). The virtualized cloud of access networks and CN have the advantages of physical resource pooling, distribution of software architectures, and centralization of management. Due to the diversity of 5G application scenarios, new mobility management schemes are greatly needed to guarantee seamless handover in network-slicing-based 5G systems.
Key words: architecture, network slicing, 5G, SDN, NFV.

Grishin I., Mikheeva S., Podgornaya K. Analysis of the Development Perspective of 5-th Generation Communications Networks in Russian Federation. – PP. 370–374.
The article attempts to analyze the prospects for the introduction of fifth-generation communication networks in the territory of the Russian Federation. Issues such as the dependence of the field of telecommunications on foreign equipment and software, as well as the associated risks arising from the introduction of fifth-generation communication networks, are considered. The issues of providing mobile operators with the necessary frequency bands and the cost of implementing networks by operators are considered.
Key words: 5G networks, eMBB, mMTC, URRLC.

Dementev V., Elagin V. Communication Networks on High-Speed Highways of Railways. – PP. 374–379.
This article presents the main features of building communication networks on high-speed highways, for example, the specificity of highways of railway transport, a distinctive feature of which is the high speed of rolling stock, as well as a large amount of user and service traffic.
Key words: communication networks, switching, routing, transponder.

Denisov N., Meshalkin V. State-of-the-Art Review of Microstrip Antenna Arrangements of Wireless Networks. – PP. 380–384.
In article the review of the most widespread types of small-sized printing microstrip antennas is given. Their design is considered, the analysis of characteristics is given, comparison of different types of printing microstrip antennas is carried out. For more complicated kinds of printed microstrip antennas analytical relations for their resonant frequencies are given.
Key words: antenna, microstrip antenna, wireless network, wireless communication.

Desnitsky V., Dumenko P. Analysis of Information Security Violations in Mobile Applications. – PP. 384–390.
The paper analyzes violations in the field of information security of modern mobile applications, current methods of software protecting code and data, the main types of attacks and vulnerabilities as well as the most important aspects of developing secure mobile applications running on Android operating system. These aspects include a local data storage requirement; requirements for authentication and session management; network communication require-

ments; and resistance to reverse engineering. Analysis of key components of the mobile ecosystem and ensuring the protection of critical user data is given. The effectiveness of the proposed solutions is confirmed by an example of the task of protecting Java code by the use of Android Studio development environment.
Key words: information security, mobile applications, critical data, Android OS.

Desnitsky V., Zuev I., Karelsky P., Kovtsur M. Analysis of Dissemination Channels in the Social Network Twitter. – PP. 390–395.
Social networks are becoming increasingly common as a subject of analysis. Events and data from networks are investigated to obtain previously unknown information. You can use various tools to create a data set, even use the standard MS Office Suite. The article is devoted to the collection and analysis of data on distribution channels in the social network Twitter.
Key words social network analysis, social graphs, ant algorithm, Ant Colony Optimization, information activity, malicious influence.

Dinh D., Kirichek R. Development of Interaction Models Among Unmanned Aerial Vehicles in Flying Emergency Services Networks. – PP. 395–400.
The success of any searching and rescuing operation depends on the equipment and the time required finding the missing person. The use of unmanned aerial vehicles (UAVs) can increase the effectiveness of these operations. There are various solutions based on UAVs that are able to detect a missing person with the help of computer vision systems, infrared sensors and the detection of mobile phone signals. Thus, in order to increase the efficiency of resource use and reduce the cost of the search for missing people, this article presents interaction models among UAVs in flying emergency services networks.
Key words: unmanned aerial vehicle, search and rescue operation, flying network, emergency services.

Diorditsa V., Tcvetkov A. Means of Protection Against Attacks Type of Buffer Overflow on the Window OS. – PP. 400–405.
Modern operating systems are a fairly extensive set of protective tools against various types of vulnerabilities, but there are vulnerabilities, the complete elimination of which is not possible. One such vulnerability is buffer overflow. Critically dangerous vulnerability, known since the early 70s, actively exploiting hackers today.
This paper examines the problems of the vulnerability of modern programs, the study of the structure of computer memory, the buffer overflow attack algorithm, well-known defense mechanisms and systems to prevent overflow attacks.
Key words: information security, buffer overflow, operating system protection, computer memory, application vulnerabilities.

Doynikova E. Model for Forecasting Cyberattack Goals Based on the Neuro-Fuzzy Networks. – PP. 405–408.
The paper is devoted to the task of cyberattack goals forecasting. A general approach is described and a forecasting model based on the neuro-fuzzy network is proposed. Different classes of attack goals are outlined. On the basis of the security metrics, a set of features that characterize cyberattack goals is formed. The paper describes the first implementation of the

components of prototype for cyberattack goal forecasting using the proposed model, as well as the results of experiments.
Key words: cyberattacks, neuro-fuzzy networks, cyberattack goals, security metrics.

Dotsenko S. Using Optical Amplifiers to Maintain a Quasi Soliton Mode in Optical Single-Mode Fiber with Losses. – PP. 408–413.
It is known that the use of quasi-soliton propagation modes of pulses having the form of a hyperbolic secant makes it possible to increase the length and speed of transmission of a fiber-optic communication system. However, with increasing distance, the quasi-soliton mode in single-mode optical fibers with losses is destroyed. To maintain it, discrete optical amplifiers can be used to compensate for attenuation in the amplifying portions of the linear optical fiber path. The article is devoted to the study of the quasi-soliton mode of operation in a long-haul line with several amplifying sections and the optimal choice of the parameters of this line. The results of theoretical studies were verified by simulation.
Key words: fiber-optic communication lines, solitons, optical amplifiers, optical fiber.

Dobryanskiy V., Kushnir D. Blockchain Based Authentication in Cyber-Physical Systems. – PP. 414–418.
The fourth industrial revolution continues to actively influence production systems, they are smarter, interconnected, self-organizing, decentralized and flexible. However, good prospects, predictable opportunities for introducing various technologies for Industry 4.0, are associated with various problems. The security of cyber-physical systems (CSP) is of paramount importance, since its components actively interact with the physical world, and a security breach can lead to various technological disasters.
Key words: CSP, blockchain, authentication, Industry 4.0, information security.

Dunaytsev R., Kolevatyh Y. Building Outdoor Wi-Fi Networks. – PP. 418–423.
In this paper, we consider the features of building outdoor Wi-Fi networks. Experimental data are provided to determine signal attenuation due to the presence of green spaces between the source and the receiver. A comparative analysis of software products for radio planning of wireless networks is carried out in terms of their applicability for planning outdoor Wi-Fi networks, such as: the ability to take into account three-dimensional terrain and surrounding buildings, as well as additional attenuation introduced by trees and bushes.
Key words: IEEE 802.11, outdoor Wi-Fi, WLAN, radio planning.

Dunaytsev R., Lebedeva N. On the Efficiency of Wireless Site Surveys. – PP. 423–428.
Wireless site surveys can be conducted in one of the two modes: continuous or stop-and-go. The choice of site survey mode, as well as the route through the facility on which a WLAN is deployed, affect the complexity of the site survey and the accuracy of the results. This paper provides a comparative study of the above-mentioned modes on the example of a WLAN deployed at Saint-Petersburg State University of Telecommunications. Based on the results obtained, recommendations are given for conducting efficient site surveys in large facilities.
Key words: Wi-Fi, wireless site survey, WLAN, access point.

Dyubov A., Kovalenko A. The Current State and Prospects of Development of Optical Access Networks. – PP. 428–433.
Recently, optical access networks are the most dynamically developing segment of the telecommunications market. One of the characteristic signs of the continuous development of the access network market is from year to year improved data transmission and networking technologies designed to meet the growing needs of users. If on transport networks (trunk lines), the transition to an optical fiber is in full swing, then on optical access networks, the transition to an optical fiber is getting closer and closer to the end user.
Key words: PON, FTTx, Active Ethernet, Micro SDH, network development prospects.

Elagin V., Ivanov I. MPLS-TP capabilities and SDN integration. – PP. 434–437.
The MPLS network was developed to send various types of traffic in 2001. The main idea when creating MPLS is to speed up packet transmission through routing mechanisms. After the time lapse, telecom operators operating MPLS noticed that the base MPLS lacked control and management mechanisms. In 2009, the International Telecommunication Union and the Engineering Council of the Internet proposed the new MPLS-TP protocol, which eliminated the shortcomings and satisfied the desires of the operators. With the development of virtualization and the advent of SDN, there was a need to combine two advanced technologies MPLS-TP and SDN, for the transport networks of the operator.
Key words: MPLS-TP, SDN, OpenFlow, FlowTable.

Elagin V., Illarionov V. Investigation of Traffic in Data Networks on Land Transport. – PP. 437–442.
Data networks on land transport are becoming increasingly popular due to the fact that users are able to access the Internet in terms of personal mobility, available and free for each passenger.
Key words: session, traffic, network, busy hour.

Elagin V., Nevzorov Y. Analysis of the Use of MPTCP Protocol for Broadband Access Services in Mobile Networks. – PP. 443–448.
This article proposes to solve the applied task of organizing a communication channel for a mobile subscriber with the QoS level necessary for organizing audio and video broadcasting with minimal delay and with a maximum level of quality, while the subscriber is in dense urban areas without using expensive network or satellite equipment, with a high load of the network infrastructure of mobile operators. Based on the conditions of the task, it is proposed to provide the necessary QoS by organizing multi-threaded Internet access using MultiPath TCP (MPTCP).
Key words: MPTCP, Multi Path TCP, data aggregation.

Zhernova K., Kolomeets M., Chechulin A. Review of Human-machine Interaction Methods in Systems for Counteracting Doubtful and Undesirable Information. – PP. 449–454.
Different systems for counteracting doubtful and undesirable information can be used in different ways of presenting results and human-machine interaction with the received information. These methods are used to manage data and perform such operations as filtering and emphasizing certain data areas for the user. The paper will consider the main methods of human-

machine interaction used in software and hardware systems for counteracting doubtful and undesirable information such as parental control systems, information resource reputation determination systems and web resource classification systems. The paper also produces their comparative analysis and recommendations for use.
Key words: human-machine interaction, information security, systems for counteracting doubtful and unwanted information, user interfaces, graphical user interface, text-based user interface.

Zarubin A., Kalyashov E., Koval A., Tarlykov A. Semantic Segmentation of Synthetic Images with a Neural Network Based on U-Net Architecture. – PP. 454–458.
The article investigates usage of convolutional neural network based on U-Net architecture for semantic segmentation of various classes of objects against random backgrounds. Training set generation with synthetic data and network training process are described. Model results are provided too.
Key words: convolutional neural network, semantic segmentation, data generation.

Zakharov M., Kirichek R., Safronova E., Times K. The Use of Model Networks to Reduce Engineering Time. – PP. 459–461.
A significant part of the design time of telecommunication equipment takes the process of configuration of the equipment according to the requirements of TK. To reduce the time of equipment configuration and, accordingly, the design time, it is proposed to use model networks to emulate the developed virtual complexes of telecommunications equipment with the ability to upload configuration files. The EVENG emulator is considered as an environment for emulation.
Key words: model networks, engineering of communication networks, EVENG.

Izrailov K., Tatarnikova I. An Approach to Analyzing the Security of a Software Code from the Standpoint of its Form and Content. – PP. 462–467.
The article proposes an approach to the study of vulnerabilities of the program, based on the representations of the life cycle of the it, as well as on philosophical categories - form and content. The static and dynamic properties of vulnerabilities derived from the analysis are declared. The prerequisites for the emergence of qualitatively new effects from the interaction of several vulnerabilities in the program are described. An example is given of one of these effects from the standpoint of anthropomorphism, namely, «parasitism» of one vulnerability over another.
Key words: information security, vulnerability, program code, program representation, life cycle, anthropomorphism, form, content.

Imankul M. Problems of Safety and Compatibility Are in IoT. – PP. 467–472.
IoT (Internet of Things)-solutions increase efficiency and security and provide real-time decision-making. Their implementation is hampered by the lack of architectural templates describing communication protocols tailored to specific industries. With the introduction of IoT, cybersecurity problems increase, as each new connection of a physical device to the IoT network can become a source of security threats.
Key words: edge computing, blockchain, information security, Internet of Things.

Kalyashov E., Saveleva A., Tarlykov A. Segmentation of Real Objects with Neural Network Trained on Synthetic Data. – PP. 472–476.
The article describes a method to train convolutional neural network with synthetic data for pixel level segmentation of real objects. Common descriptions of synthetic data generation, training process and optimization are given. Segmentation results for high quality images and low quality video are also provided.
Key words: convolutional neural network, training, synthetic data, segmentation.

Kalyashov E., Shvidkiy A., Tarlykov A. Finding Plane Orientation Parameters with Neural Network. – PP. 476–481.
The article investigates task of finding plane orientation parameters from image data. Different training approaches for various neural architectures with synthetic data are described. Test results are provided for several model examples.
Key words: convolutional neural network, training, regression, data generation.

Kandziouba E. Optimization of Symmetric Cable for Long Ethernet by Economic Criteria. – PP. 481–487.
In the construction of access networks and information systems of real estate can be used optical and symmetrical electrical cables. The use of the latter, despite the shorter transmission distance, provides a number of advantages, including the possibility of remote power terminal equipment. In such circumstances, it seems relevant to work out such a design of these products, which provides an increase in the range compared to the typical UTP cables values.
Key words: cable tract, impedance, working attenuation, optimization, long “Ethernet”.

Kanivets Z., Kulik V., Makolkina M. Examination of Traffic from Virtual Reality Application. – PP. 488–492.
Augmented reality is one of the most popular and rapidly developing technology at the moment. The subject of the research in this article is the traffic characteristics of Augmented Reality applications. Based on the findings, conclusions were drawn about the general nature of the traffic of Augmented Reality applications.
Key words: Augmented Reality, AR, traffic analysis.

Kirilova K., Tsvetkov A. Existing Rootkit Realization Methods Analysis. – PP. 492–497.
With information technologies evolving and spreading all over the world, cyber threats are widely spreading as well. Users and administrators of computers systems often face different malware, such as viruses, trojans, rootkits, etc. UNIX kernel-mode rootkits have much more privilege than user-mode ones, therefore they can use their own effective methods to hide in the system.
Key words: linux, kernel modules, malware analysis, rootkits.

Kirichek R., Mitskovskii D. The Method of Applying Network Steganography to Transfer Identifiers in Heterogeneous Communication Networks. – PP. 497–502.
In today's world, information is the most common resource, which sometimes has great value. Of course, in order to establish communication in complex systems of connections between

multiple users, a well-established, reliable system that can ensure reliable data transfer between users, as well as its complete confidentiality, if necessary, is required. With the advent of more powerful computing technology, steganographic methods of data protection are becoming more relevant, but they often involve access to the source data. In the absence of such access, this problem is solved by applying the methods of network steganography.
Key words: network steganography, packet header, RSTEG-steganography, flags.

Kirichek R., Reutova D. Methods of Identification of Objects of Augmented Reality. – PP. 502–507.
The technology of augmented reality is one of the most perspective directions in the field of information technologies today. Its rapid development involves increase in quantity of digital objects that in turn asks problems of their identification. In this article possible methods of identification of objects of augmented reality on the basis of architecture of digital objects are considered.
Key words: DOA, digital object, augmented reality.

Kirichek R., Sazonov D. Digital Object Architecture as an Approach to Identification the Devices of the Internet of Things. – PP. 508–513.
In this paper the analysis of the possibility of building a system for identifying devices of the Internet of things based on the architecture of digital objects is reviewed. The created model of the resolution system as a queuing system is presented. The optimization experiment is performed and optimal configuration is obtained. Possible improvements of the resolution algorithm are proposed.
Key words: Internet of Things, Digital Object Architecture, Digital Object Identification, Handle System, queuing system.

Kirichek R., Sklyarova M. Analysis of Communication Network Technologies 2030. – PP. 513–518.
The concept of communication networks 2030 was announced in July 2018 and represents a set of technologies and applications that are not included in the 5G / IMT-2020 network. The article discusses the possibilities of technology development up to 2030 in various spheres of life. Requirements for data transfer speeds, ultra-small network delays, new methods for processing data arrays, etc.
Key words: Internet of things, tactile internet, latency.

Kirichek R., Filin E. Models of Interaction between Unmanned Vehicles with VANET Infrastructure for Network Support. – PP. 518–523.
The development of technologies related to unmanned vehicles and technical infrastructure contributes to the emergence of new solutions, ideas and models. In this connection, it is necessary to monitor the research work. The publication provides an overview of the existing technological solutions that exist at the moment.
Key words: Unmanned Vehicles, Connected and Autonomous Vehicle (CAV), Vehicular Cloud (VC), Vehicle-to-Everything (V2X).

Kovaykin Y., Lebedev P., Prokofev O. Method Improve the Stability Control System Data Network on the Basis of the Protection to Technological Traffic. – PP. 523–528.
The article discusses the theoretical aspects of building network management system, the model of interaction between the controlling and controlled systems, methods for managing the cryptographic routers which are build along a two-segment architecture, as well as technical proposals for improving the data transmission network management system by protecting the configuration traffic.
Key words: data network, cryptographic router, configuration traffic, two-segment architecture.

Kovtsur M., Kozmyan A., Tverdohlebova Y. Analysis of the RADIUS Authorization Mechanism for IP-TV Services. – PP. 528–532.
Security is one of the most important aspects of data transmission networks. Controlled access to the network, authorization and user authentication are often provided with an AAA server. IP-TV is a technology of digital television in data networks using the IP protocol, a new generation of television. Usually IP-TV broadcasts utilize multicast traffic to deliver the content to clients as well as user authorization and authentication. This study examines client authorizations for accessing an IP-TV service using a RADIUS server by presenting the authorization process model.
Key words: authorization, IP-TV, graph, IGMP, multicast, RADIUS.

Kovtsur M., Lueke P. Development of an Attendance Accounting System on a Scale of a University. – PP. 532–537.
One of the most common tasks in every organization of any kind, is to track and constantly check the attendance of their employees/workers. Technologies such as RFIDs and web applications are used every day in almost every organization. This article describes the concept of implementing a student attendance accounting system using web technologies and RFID systems. It focuses on two possible approaches; one of them based on a web infrastructure, leveraging the power of client-server's applications with web authentication, and another one based on RFID technologies and wireless data transmission. For each implementation, a full analysis is done, with strengths and weaknesses from a security, costs, and difficulty of implementation perspective. Possible attacks directed at the system are determined.
Key words: Accounting, RFID, attendance, Web.

Kovtsur M. **Simanov M.** Analysis of User's Authorization Methods in the IEEE 802.11 Collective Access Networks. – PP. 537–541.
These days the IEEE 802.11 wireless networks are widely distributed for the guest network access. The number of launched networks increases every year. Therefore it is necessary to pay special attention to the user authorization coordination. The existing methods of wireless guest network access, their classification and the relevant solutions for each type of the network access are presented in the research. According to such characteristics as user connection time, cost of implementation and operation, network size and project payback recommendations on the relevant solution choice are introduced.
Key words: authorization, Wi-Fi, guest access, wireless networks, IEEE 802.11.

Kozmyan A., Tverdohlebova Y., Ushakov I. Comparative Analysis of Non-Relational Databases. – PP. 542–546.
The article contains comparative analysis of the most popular non-relational databases based on a number of evaluation criteria. Apache Cassandra, HBase and MongoDB which are taking leading positions according to various industry trends were chosen for the study. NoSQL databases are designed for specific data models and have flexible schemas that allow to develop modern applications. NoSQL databases are widely used due to ease of development, functionality and performance at any scale.
Key words: NoSQL, Apache Cassandra, HBase, MongoDB, performance, databases.

Kolomeets M., Chechulin A. Models and Algorithms for the Implementation of Visual Interfaces to Identify and Counter Undesirable, Questionable and Harmful Information. – PP. 547–551.
Visualization models allows one to build graphical data display structures in such a way that the user can easily perceive information in comparison with a regular tabular or textual representation. Various models and visualization algorithms in an abstract graphical form can be used in the implementation of information counteraction systems, namely in support and decision-making subsystems. The paper discusses models and algorithms for implementing visual interfaces in such systems for identifying and counteracting unwanted, questionable and harmful information such as parental control systems and Internet resource classification systems.
Key words: visual analytics, information counteraction, visualization models, information security.

Komashinsky N., Kotenko I. Analysis of Models and Systems of Parallel Processing of Events for the Detection of Information Security Incidents. – PP. 551–556.
The paper analyzes the existing models and systems for parallel processing of information security events. The possibilities and estimates of the effectiveness of parallel data processing with the aim of detecting computer attacks based on the functional approach are considered. Based on the results of the analysis, the specification of the main stages of the parallel event processing process and the scheme of their implementation as part of the information security event processing system are presented.
Key words: information security, parallel processing of security events, computer attack, functional approach, security event analysis.

Komashinsky N., Kotenko I. An Intrusion Detection Model with the Use of Signature Methods and Big Data Technologies. – PP. 556–561.
Based on the analysis of various classes of parameters of modern information systems, a model for detecting malicious activity using signature methods is proposed. This model specifies ways to increase the efficiency of processing large traffic flows in high-speed data networks in order to detect patterns of malicious activity. Signature methods are represented by Snort rules and are adapted for processing input data using big data technology. The developed prototype of the detection system is presented and a preliminary assessment of its performance indicators is carried out.
Key words: abnormal activity, traffic, Snort, signature methods, sensor, big data, Hadoop.

Kondratenko V., Muratov E., Sleptsov M. Vibro-Acoustic System of Distributed Sensors "Dunay". – PP. 562–568.
The Dunay system allows real-time detection, classification and identification of potentially dangerous events on the linear part of the pipeline with an accuracy of 1 meter without the need to deploy field sensors: as a sensitive element in these systems is the fiber optic cable. It should be noted that the system operates autonomously in a fully automatic mode, that is, it does not require operator intervention (only if it is necessary to confirm the reliability of the detected event).
Key word: fiber optic sensor, fiber optic cable, optical reflectometer, detection of effects.

Kotenko I., Ovramenko A., Ushakov I. Architecture and Program Prototype of Insider Detection System in Computer Network Based on Big Data Technologies. – PP. 568–572.
The work is devoted to the development of a software prototype of an insider detection system for the timely detection of potential violators of information security. The proposed architecture and the implemented software prototype of the insider computer network detection system are considered.
Key words: Big Data, UBA, UEBA, information security, NoSQL.

Kotenko I., Pelevin D., Ushakov I. General Technique of Computer Network Insider Detection Based on Big Data Technology. – PP. 572–576.
The article discusses the general method of analyzing user behavior in the corporate environment for further use in conjunction with Big Data technologies to identify insiders in computer networks.
Key words: Big Data, UBA, UEBA, NoSQL, information security.

Kotenko I., Tushkanova O. A Version of the System Architecture for Analyzing Information Objects on the Internet Using Parallel Computing. – PP. 577–580.
The paper proposes a variant of the developed intelligent system for analytical processing of digital network content, which provides the implementation of data processing methods and algorithms, primarily in the context of the task of multidimensional evaluation and categorization of information objects on the Internet, for example, websites, according to their semantic content. Information objects usually contain a large amount of content represented by heterogeneous data, and have a complex structure, so the task of analyzing such objects should be attributed to the Big Data , respectively, for its timely solution the use of parallel computing is required.
Key words: information object, analytical processing system, classification problem, parallel computing.

Kotenko I., Tynymbaev B. Architecture of Advanced UEBA System for Cloud Service Providers. – PP. 581–585.
The benefits of User and Entity Behavior Analytics (UEBA) systems for cloud service providers are analyzed. A description of a class of systems called Cloud Access Security Brokers is given, and their connection with analytical systems of the UEBA class is shown. The scheme of interaction with information security event sources is described, examples of mathematical models

of user behavior analysis and possible areas of application of a potential UEBA system in the field of cloud technologies are given.
Key words: information security, security analytics, user behavior models.

Kotenko I., Tynymbaev B. Review of UEBA Class Solutions. – PP. 585–590.
The review of current decisions in the field of User and Entity Behavior Analytics (UEBA) class systems is carried out. We consider both commercial solutions and research papers in the field of user and entity behavior analytics, including those reflecting threat detection scenarios, models and algorithms for calculating the rating of user profiles. On the basis of the research carried out, a model of the promising UEBA class system is proposed.
Key words: information security, user behavior analytics, UEBA systems, information security.

Krasov A., Gelfand A., Kazantsev A., Katasonov A. Formation and Control of Security Operations Center (SOC) for Efficient Using in Practice. – PP. 590–595.
Technical development of potential security threat for organizations demands improvement of systems which provide companies' information security. In consequence the question about formation of efficient Security Operations Center (SOC) arises. There is lack of information about methods of SOC's formation for using in real conditions (or methods are poorly described) in the open sources. The article is devoted to elaboration of methods of formation and control of efficient Security Operations Center (SOC).
Key word: Security Operations Center, SOC.

Krasov A., Radynskaya V., Tasiuk A. Kerberos, Data Protection in Big Data. – PP. 596–601.
Working with big data is a big responsibility. As the volume of data grows and the number of applications and platforms accessing this data increases, new vulnerabilities emerge that need to be addressed.
Many protocols used on the Internet, do not provide any security. Tools to steal passwords from the network are often used by attackers. Therefore, applications that send an unencrypted password over the network are extremely vulnerable. Worse, other client-server applications rely on the client program to be "honest" about the identity of the user who uses it. Other applications rely on the client to limit its actions to what it is allowed to do without any other enforcement action on the server side. The article is devoted to the methods of big data protection using the Kerberos Protocol.
Key words: Kerberos, big data, data protection, cryptography, authentication.

Krasov A., Savinov N., Tokareva K., Ushakov I. Analysis of Diversion SDN Security Policies. – PP. 602–605.
This article discusses security threats, such as bypassing predefined mandatory policies by rewriting stream records and eavesdropping data by inserting fraudulent stream records. This article has developed security solutions for the above security issues.
Key words: security, SDN, controller, application, switch, OpenFlow, policies, application profile.

Krasov A., Ushakov I., Fedorov V. Comparative Analysis of Existing SDN Network Monitoring Solutions. – PP. 606–611.
This article discusses the issues of monitoring SDN networks in order to ensure security and increase the resiliency of these networks, also provides an overview of the work of SDN. The main features, operating principles and some distinctive features of the existing SDN monitoring solutions are reviewed, and a comparative analysis of the considered technologies is given.
Key words: SDN, networks, monitoring, analysis, security.

Krasov A., Ushakov I., Shchiptsov D. Analysis of Vulnerabilities and Relevant Decisions in the Field of SDN Security. – PP. 611–616.
Software-defined network (SDN) is a new approach to building data networks in which the level of network management is separated from data transmission devices and is implemented by software. The article provides a brief overview of the security issues of SDN and their solutions.
Key words: information security, SDN, OpenFlow protocol, software-configured networks.

Kraubner A., Meshalkin V. Types of Crossovers are for Finding the Optimal Routes of Delivery of Messages of Nerworks with Genetic Algorithm on the Model of Whitley. – PP. 616–620.
The problem of meeting the requirements for timely delivery of documentary telecommunication messages is considered. The complexity of the route is determined by the number of recipients (sources) and their spatial distribution. Of the set of discrete optimization problems, the most suitable is the traveling salesman problem. It was proposed to use the Whitley model of the genetic algorithm for the solution. The aim of the work is to study and select the most appropriate types of crossovers to solve the traveling salesman problem on the model of the Wheatley genetic algorithm. The article describes the most suitable types of crossovers to solve the traveling salesman problem using genetic algorithms based on the Whitley model. The results of the tests and a comparative analysis of the effectiveness of the proposed crossovers are presented.
Key words: genetic algorithms, Whitley model, crossover, genetic operator, documentary telecommunication, traveling salesman problem, unmanned aerial vehicles, tactical control link.

Kuznetsov V., Malyarov M. EDFA as a Broadband Emission Source. – PP. 620–626.
This article discusses the possibility of obtaining a broadband and uniform spectrum with a high-power level, based on the erbium-doped fiber amplifier. Amplified spontaneous emission sources have a number of advantages and can be used in several areas of science and technology. Investigation of relationship between the width, uniformity, emission spectrum power and such EDFA's parameters as type and active fiber length, saturation parameter, power level and number of pump-sources is carried out in the simulation program.
Key words: EDFA, spectral range, amplified spontaneous emission.

Kuznetsova A., Sakharov D. Review of the State of Research Information Security and the Use of SIEM-Systems. – PP. 626–631.
In article the question of ensuring information security at the enterprise with the application of SIEM (Security Information and Event Management) allowing to analyze and register threats

to security of information in real time is considered. Use of this technology is relevant and perspective technology for crucial infrastructures as allows to achieve almost full automation of process of identification of threats, thereby having placed emphasis on timely identification of incidents of safety of infrastructure and significant reduction of possible losses. The description and the main characteristics of a SIEM-system, the analysis of security with information security of the enterprises, relevance of introduction of these systems and their shortcomings is provided in article.
Key words: information security, SIEM systems.

Kuzmin M., Rogov S. Laboratory Setup for Optoelectronic Information Processing Systems Study and Development. – PP. 631–636.
The description of the optical-digital setup for carrying out laboratory works on the basics of Fourier optics and optical information processing is provided. Along with the educational application, the setup makes possible scientific research and physical modeling of new devices for signal and image processing tasks in various purpose systems.
Key words: laboratory works, optical processing of images and signals, spatial light modulator, liquid-crystal matrix, optical Fourier processor, joint transform correlator.

Kuzmin M., Rogov S. Optical Processors with Parallel Signals Input into a Liquid-Crystal Matrix. – PP. 636–640.
The performance of optical information processing systems with parallel (line-by-line) input of signals into a liquid-crystal spatial light modulator with electronic control was evaluated. It is shown that using parallel input allows in some cases to increase the performance of known optical systems to a level that is by an order of magnitude higher than the speed of digital devices of similar purpose.
Key words: liquid-crystal spatial light modulator, parallel information processing, performance of optical processors, multichannel systems, spectral analysis of signals, optical correlators.

Kulik V., Sleptsova N. Development and Examination of Semantic Compatibility Models of Various Platforms and Services of the Internet of Things. – PP. 641–645.
This article examines the compatibility of data formats of various platforms and the Internet of Things. The authors examined various methods to ensure the semantic compatibility of IoT platforms and services. On the basis of the obtained data, conclusions were made about the general nature of the traffic of multimedia applications.
Key words: video surveillance, "Smart City", IP, RTP, RTCP, RTSP, video traffic.

Kulikova A., Saenko I. The Choice of Document Oriented DBMS for Storing Personal Data. – PP. 646–650.
The problem of the organization of storage of the personal document oriented data in electronic form is considered. Comparative analysis of program tools for solving this problem is carried out. The choice of MongoDB DBMS as the most acceptable non-relational tool for personal base of the document oriented data is proved. The main possibilities of MongoDB DBMS are in details considered and examples of implementation of documentary data bases on its basis are given.
Key words: document, database management system, collection, replication.

Lebedeva N., Odoevsky S., Khoborova V. Proposals for data management in the infocommunication special appointment's network by means of traffic engineering. – PP. 651–654.
Proposals for managing data streams in a special-purpose infocommunication network using traffic engineering technologies are considered. An example of modeling a communication network is given, and the effect of network load redistribution using ONEPLAN RPLS-DB TE software is shown.
Key words: traffic engineering, software package, data streams, channel resource.

Levshun D., Pantjuhin O., Saenko I. Assessment of the Quality of Access Control Policies in a Cloud Storage Based on the ABAC Access Control Model. – PP. 655–659.
The problem of the formation of the access control policies in a cloud storage based on the ABAC access control model is considered. Quality indicators of the access control policies characterizing their property of accuracy and integrity are defined. The quality assessment technique for the access control policies in a cloud storage based on the ABAC model is offered.
Key words: access control policy, cloud storage, attribute, quality assessment.

Lipatnikov V., Tikhonov V. Recognition of Offenders Actions in the Management of Cyber Security of the Integrated Organization Infrastructure on the Basis of Neuro-Fuzy Networks and Cognitive Modeling. – PP. 659–664.
The method of managing the cybersecurity infrastructure of an integrated organization with intrusion recognition and analysis of the dynamics of actions of the offender based on neuro-fuzzy networks and cognitive modeling. Functions of the control algorithm: monitoring and highlighting features of digital streams with data transfer protocols entering the information network and intrusion detection, selection and implementation of a protection method.
Key words: infrastructure of the integrated organization, information security; neuro-fuzzy networks, cognitive modeling.

Lobastova M., Matukhin A. An algorithm to eliminate loops in the clock network synchronization networks. – PP. 665–670.
The paper deals with the issues of clock network synchronization organization in next-generation networks. Also we show the use of OTN technology for the transport network organization. A description of the loopdetect method in the synchronization network and the text of the program code for its implementation are given.
Key words: 5g networks, transport networks, OTN technology, clock network synchronization.

Makolkina M., Shypota N. Voice assistant as an interface to 5g/imt-2020 infrastructure management systems. – PP. 670–673.
The article is devoted to studying the problems of increasing the efficiency of work with equipment when using a voice assistant.
The main features of voice control systems technology are revealed. Analyzed the positive and negative aspects of the introduction of voice assistant. The description of the possible cases of its use.
Key words: infrastructure 5G/IMT-2020, Voice Assistant, NFV, SDN.

Malco A., Starodubova D., Chechulin A. The Research about the Protection of Computer Networks from Reconnaissance Attacks. – PP. 674–677.
The success of a computer attack directly depends on the amount of information about the attacked network received by the malicious actor during reconnaissance attacks. The use of various intrusion detection and prevention tools, network traffic analyzers and firewalls makes it difficult to gather information about the network. The greatest level of network security can be achieved by using security tools in accordance with techniques that describe an integrated approach to providing protection. The article discusses issues related to the description of existing algorithms and methods for protecting computer networks from reconnaissance attacks.
Key words: information security, reconnaissance attacks, information gathering, network traffic analysis, information protection, computer networks.

Malco A., Starodubova D., Chechulin A. The Research of Methods and Algorithms of Collection Information in a Computer Network. – PP. 677–681.
The relevance of information security support of corporate networks is caused by the high growth rates of the computer attacks on them. The increase in the level of complexity and fast adaptation to attacks to the measures of protection are forced to set strict rules to receive notifications on any potential violations even before their emergence. Data analysis and network traffic monitoring is becoming the necessary part of any system information security management. Such systems help to increase the level of security of the enterprise network. Results of a research and comparison of the existing techniques and algorithms of collection of information about network traffic are presented in the report.
Key words: information security, network attack, network traffic, anomaly detection.

Marochkina A., Paramonov A. Research of Traffic and Function of Self-Organizing Communication Networks. – PP. 681–686.
This paper presents the results of a self-organizing communication network traffic and functioning study, obtained by using simulation modeling. For this research, two simulation models were implemented in ns3 and OMNeT ++ programs. Through this research we obtained the dependence of the quality of the traffic service and the characteristics of routes on the amount of network nodes.
Key words: self-organizing communication networks, Internet of Things, routing protocols.

Mahmud O., Paramonov A. Internet of Things Network as Delay Tolerant Network. – PP. 686–691.
This article presents analysis performance of Mobile Ad-hoc Network (MANET) and network routing protocols with Delay Tolerant Network (DTN) used in the Internet of Things (IoT). The MANET network is considered as a DTN, in which routes used to traffic are not stable, but has a probabilistic character. Data delivery is made, when such an opportunity arises due to the movement of nodes and changes in their relative position. The results are given analysis the node movement impact on the probability of data delivery.
Key words: Internet of Things, IoT, Routing protocols, Delay Tolerant Network, DTN.

Moiseev O., Yakovlev A. Development of a Routing Algorithm that Ensures Efficient Operation in Reconfiguration or Network Failures. – PP. 692–695.
In modern conditions of hiperaggregation load is often nessary to search for alternate ways of information transfer, and this leads to cessation of information flow for tens of seconds. The article describes the issues of improving the stability of communication networks to failures of its elements due to reconfiguration of information flows and improving the efficiency of routing protocols.
Key words: telecommunication network, routing, graf, stability.

Morozov D. Web Application Protection Against Popular Attacks on the Example of HTTP Title for Nginx. – PP. 695–699.
Almost all types of websites, ranging from single-page sites and ending with highly loaded web applications are vulnerable to cyber attacks. There are various ways to protect web applications from cyber attacks. This article discusses a way to protect HTTP-based headers for Nginx, which allows you to protect a web application from popular types of attacks.
Key words: attack, clickjacking, Cross-Site Scripting, XSS, nginx, HTTP header.

Nizhgorodov A. To Predict the Lifetime of the Construction Length of Optical Cable to the Modular Design. – PP. 700–704.
In the present work, we attempt to predict the lifetime of the cable, taking into account the random nature of the effects on the optical fiber during cable production. In the work were limited to the prediction of cable lifetime after acceptance and delivery of the product at the manufacturer's warehouse.
Key words: optical fiber, optical cable, manufactured length, reliability, lifetime.

Novikov A., Fitsov V. Using the Mathematical Model Ventzel-Ovcharov with a Uniform Mutual Help for Modern Systems NFV. – PP. 705–709.
The concept of NFV (Network Function Virtualization) is to combine several types of hardware into a single device based on a unified platform (data center). Such data centers evenly distribute hardware resources to a given number of servers. Wentzel and Ovcharov described a model of distribution of hardware resources, which was called "mathematical model with uniform mutual aid." The article will consider the application of the Ventzel-Ovcharov model to the data center with NFV support. The DPI (Deep Packet Inspection) system can be considered as a virtualized network function.
Key words: NFV, DPI, Front-End, mathematical model, queueing system, uniform mutual help, model M/M/V.

Okuneva D., Pavsheva M. Integration of the 1C: Enterprise 8 Platform and Neural Network for the Diagnosis of Cardiac Diseases. – PP. 710–714.
The subject is a machine learning of a neural network based on the cardiac disease knowledge bases and its integration with the 1C: Enterprise 8 platform for an objective and quick diagnosis and determine further diagnosis based on the patient's electrocardiogram.
Key words: neural network, 1C: Enterprise platform, electrocardiogram.

Saenko I., Starkov A. Technological Management System for Enterprise-Level Virtual Local Area Networks. – PP. 715–720.
The system of technological management of virtual local area networks intended for use by developers and administrators of corporate information systems at stages of design, operation and reorganization of computer networks is developed. The system allows you to synthesize the optimal scheme of creation of virtual local area networks, meets the requirements and provides increased bandwidth and protection against unauthorized access to network resources.
Key words: corporate information system; virtual local area networks, information security; access control.

Saenko I., Feforchenko A. Architecture of System of Distributed Intelligent Scanners of Network Content for Protection Against Unwanted Information. – PP. 720–725.
The paper is devoted to the study of information resources of the global Internet for the implementation of the tasks of protection against inappropriate information. The goal of the research is to develop a distributed system for scanning, downloading and preprocessing network content. The paper examines the conditions for ensuring the availability of network resources, taking into account restrictive measures and a large amount of information. As a result, the developed architecture of the distributed intelligent scanners system is presented, possessing scalability properties, as well as efficiency and flexibility in performing the tasks assigned to it.
Key words: global Internet, network content, distributed data collection.

Saenko I., Shapovalov D. Analysis of Opportunities of Using the "Active Server Pages" Technology for Automated Information Systems Implementation and Operation. – PP. 725–729.
The possibilities of creation of the automated information system with use of the data processing model based on the "Active Server Pages" technology are considered. Separate characteristics of the key processes influencing on the operation are considered in details. Results of the experimental assessment of possible ways of the model implementation are given and recommendations about their application in this system are made.
Key words: automated information system, data processing model, web programming.

Saltykov A., Yastrebov V. Activation Process of ONU in NG-PON2 Networks. – PP. 730–734.
This article reviews the activation process that describes the steps in which an inactive ONU connects or reconnects to a PON. The activation process includes three phases, specifically: parameter learning, serial number acquisition and ranging. During the learning parameter phase, the ONU acquires the operational parameters that are needed in the upstream transmission. During the serial number acquisition phase, OLT discovers a new ONU (by serial number) and assigns an ONU identifier (ONU-ID) to it.
Key words: ONU, PON, activation process, NG-PON2, ONT.

Targonskaya A., Tcvetkov A. Development of a Secure Web Interface for Remote Control of Devices on the Network. – PP. 734–739.
In a century of rapid information technology development remote control are an integral part in work with the different equipment. Despite existence of a large number of implementations of client-server programs of remote control, the vast majority of existing solutions does not

meet requirements of big modern campaigns. Such companies most feel need available of a single system of network management, in view of a large number of physically remote branches and extensive staff of technical support. Proceeding from it the decision to develop rather simple uniform centralized management system by devices of network with availability of the database of users and a possibility of partial delegation of powers was made.
Key words: web development, remote control, information security.

Temchenko V., Tsvetkov A. Designing of Information Security Model in the Operating System. – PP. 740–745.
Operating system (hereinafter referred to as OS) is a specially organized set of programs that manages system resources (computer, computing system, other components of information computing system) in order to use them most effectively and provides a user interface with resources. By OS security, we mean an OS condition in which accidental or deliberate disruption of the functioning of the OS is impossible, as well as a security violation under the control of the OS system resources. Since most operating systems have defects in terms of ensuring data security in the system, which is caused by the task of ensuring maximum system availability for the user, the task of this work will be to create an information security model for the operating system to prevent any intentional or unintended effects on the operating system as outside and inside.
Key words: Operating system, OS threats, vulnerabilities, security model.

Fitsov V. Research Efficiency of Front-End Server Decomposition in the Deep Packet Inspection System (DPI) at the Processing Time Criterion. – PP. 745–751.
This article describes the idea of decomposing a Front-End server in DPI system. For test theoretical results of the QS separation for the processing of requests with a long service time and with a short service time used simulation modeling. The criterion for evaluating the performance of the DPI system was the requests total time in the Front-End (including the time in the queue). The results of studies that reveal the conditions, under which decomposition is appropriate. A feature of the work is idea of decomposing the Front-End server in DPI system, as well as testing theoretical ideas through simulation modeling.
Key words: DPI, Front-End, *QS*, queues, QoS, simulation modeling, GPSS, exponential distribution, Weibull distribution.

Tcvetkov A. Analysis of Methods Buffer Overflow Attacks by Operating System Family Microsoft. – PP. 751–756.
The program consists of a complex set of rules that follow a specific thread of execution that eventually tells the computer what to do. Because a program can only do what it's designed to do, exploits flaws in the development of the program or the environment in which the program runs. In some cases, these exploits are products of obvious developer errors, but there are some less obvious errors that have spawned more complex methods of exploitation.
Key words: exploit, call stack, frame, return address, shellcode.

Tsvetkov A., Shalaeva M., Yurchenko M. Ensuring Security in Client-Server Java Application for Accounting and Automatic Verification of Laboratory Works. – PP. 756–761.
In the modern education system, it is impossible to do without the use of information technologies, in particular, automation systems for the educational process. These systems are mainly based on the client-server application model. During the development of client-server automated systems, developers need to implement security mechanisms to prevent unauthorized access to information transmitted over the network and to protect server applications from various types of attacks.
Key words: TLS, obfuscation, access rights, java.

Yakovlev V. Authentication Keys that Are Distributed by the Diffie-Hellman Method Based on the Use Universal Hash-Function and Error-Correction Codes. – PP. 762–767.
*We study the protocol of keys authentication that are distributed by Diffie-Hellman method between mobile devices when an intruder used a man-in-the-middle attack. It is assumed that users A and B, who form the session key, have pre-distributed random sequences of bits **a** and **b**, respectively, obtained either from some source or generated during the implementation of the "near authentication". This scenario is based on data obtained by magnetometers or accelerometers from mobile devices. The attacker does not have access to these sequences. The Diffie-Hellman value (DH-value) is divided into N blocks of m bits each; these blocks are encoded with the error correction (T, N) -code having a code distance D. Authentication DH-values is performed by generating authenticators length of v bits for each block using the universal class of hash-functions. The hash function is specified by a the key, that is a subblock lenght of 2m bits taken from random sequences **a** or **b**. Relations are obtained to calculate the false rejection probability of the DH-value and the probability of false deception DH-value depending on the parameters m, v, N, T, D. The problem of optimal choice for parameters minimizing the length of the chains **a** and **b** is formulated.*
Key words: Diffie-Hellman method, authentication, universal hash functions, error-correction codes.

АВТОРЫ СТАТЕЙ

АБДУСАЛАМОВ
Ренат Сейдбалаевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, pain527@mail.ru

АВРАМЕНКО
Владимир Семенович — кандидат технических наук, доцент, профессор кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, vsavr@yandex.ru

АГЕЕВ
Сергей Александрович — кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, serg123_61@mail.ru

АКИШИН
Владимир Андреевич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, системный аналитик ООО «НТЦ АРГУС», v.akishin@argustelecom.ru

АЛЕКСЕЕВА
Дарья Денисовна — студентка группы ИКТФ-76м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, darya_alex_den@mail.ru

АЛЬ-СВЕЙТИ
Малик — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ma_sweity@mail.ru

АНДРЕЕВ
Владимир Александрович — доктор технических наук, профессор, Заслуженный деятель науки Российской Федерации, президент Поволжского государственного университета телекоммуникаций и информатики, andreev@psati.ru

АНДРЕЕВА
Елена Ивановна — кандидат физико-математических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andreeva.elena@sut.ru

АНДРЕЕВА Ольга Марковна — кандидат технических наук, доцент кафедры радиотехнических систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), AndreevaLETI@yandex.ru

АНДРИАНОВ Владимир Игоревич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.i.andrianov@gmail.com

АНУФРЕНКО Александр Викторович — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, leroi88@mail.ru

АРБУЗОВА Наталья Эдуардовна — инженер ПТО 1 категории ООО «Холдинговая компания СевЗапСтрой», prud2000@mail.ru

АРЕПЬЕВ Павел Александрович — студент группы ИКТМ-72м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavellsda@mail.ru

АСТАХОВА Татьяна Николаевна — кандидат физико-математических наук, доцент кафедры информационных систем и технологий Нижегородского государственного инженерно-экономического университета, ctn_af@mail.ru

БАГДАСАРЯН Александр Сергеевич — академик НАН Республики Армения, доктор технических наук, профессор, главный научный сотрудник Института радиотехники и электроники им. В. А. Котельникова РАН, bagdassarian@mail.ru, bas@niir.ru

БАЛУЕВА Анастасия Владимировна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, _tonys_@mail.ru

БАРАНОВА Дарья Николаевна — аналитик Информационного агентства GloryStory, 9302100@mail.ru

БАТЕНКОВ Кирилл Александрович — доктор технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

БАХТИН Юрий Евгеньевич — аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук, bakhtin@comsec.spb.ru

БАХТИН Дмитрий Витальевич — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drivan289@gmail.com

БЕЛОЗЕРЦЕВ Илья Алексеевич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilya.belozercev@outlook.com

БЕЛОЗОР Ангелина Михайловна — студентка группы ИКТК-55 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, belozor.am@yandex.ru

БЕРЕЗИНА Елизавета Олеговна — студентка группы ИКТЗ-53 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, berezinaelizaveta@icloud.com

БОБРОВА Ксения Борисовна — старший техник отдела перспективных сетевых технологий научно-исследовательского центра ОАО «Радиоавионика», студентка группы АС-401-3 кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, atorina141@yandex.ru

БОРИСЕНКО Николай Павлович — кандидат технических наук, доцент, советник генерального директора АО «Региональный центр защиты информации «ФОРТ», npbor@yandex.ru

БОХАН Илья Витальевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, megalit5000@yandex.ru

БОЧКАРЕВ Дмитрий Александрович — слушатель Военной академии связи им. Маршала Советского Союза С. М. Буденного, d.a.bochkarev@yandex.ru

БРАНИЦКИЙ Александр Александрович — кандидат технических наук, научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, branitskiy@comsec.spb.ru

БУРДИН Антон Владимирович — доктор технических наук, доцент, главный научный сотрудник НИЛ кафедры «Линии связи и измерения в технике связи», профессор кафедры «Линии связи и измерения в технике связи» Поволжского государственного университета телекоммуникаций и информатики, bourdine@psuti.ru

БУРДИН Владимир Александрович — доктор технических наук, профессор, заведующий кафедрой «Линии связи и измерения в технике связи» Поволжского государственного университета телекоммуникаций и информатики, burdin@psati.ru

БУТЕНКО Валерий Владимирович — доктор технических наук, генеральный директор ФГУП Научно-исследовательского института радио, butenko@niir.ru

БУЦЕНКО Максим Артурович — оператор научной роты Военной академии связи им. Маршала Советского Союза Буденного, buts94@yandex.ru

БУШУЕВ Сергей Николаевич — доктор технических наук, профессор АО «Научно производственное предприятие ТЕЛДА»; bsn@telda.ru

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bylinamaria@mail.ru

ВАЛИЕВА Кристина Альбертовна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kristinavalievaa@gmail.com

ВАЛЮХОВ Владимир Петрович — доктор технических наук, профессор института физики, нанотехнологий и телекоммуникаций Санкт-Петербургского политехнического университета Петра Великого, Valyukhov@yandex.ru

ВАНЧАКОВА Нина Павловна — доктор психологических наук, заведующая кафедрой педагогики и психологии факультета последипломного образования Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, nvanchakova@gmail.com

ВАСЫЛИВ Назар Иванович — студент группы ИКТС-83м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nazarvasyliv1@gmail.com

ВЕНЕДИКТОВ Андрей Дмитриевич — студент группы ИКТБ-78м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, andrey_venediktov@live.ru

ВИНОГРАДОВА Ольга Михайловна — ведущий специалист по кадрам отдела кадров Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vin2407@mail.ru

ВИТКОВА Лидия Андреевна — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича; научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, vitkova@comsec.spb.ru

ВЛАДИМИРОВ Сергей Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirov.opds@gmail.com

ВЛАСОВА Ирина Владимировна — старший преподаватель кафедры фотоники и линии связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlasova-1245@yandex.ru

ВОЛКОВ Артем Николаевич — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, artem.n@5glab.ru

ВОЛКОГОНОВ Владимир Никитич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimir.volkogonov@gmail.com

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, руководитель специальной группы отдела технической защиты информации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича; старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, ra1alo@mail.ru

ВОЛЩУКОВ Матвей Юрьевич — ассистент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, neve75@mail.ru

ВОРОБЬЕВА Дарья Михайловна — аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dashuta83@gmail.com

ВОРОНЦОВ Дмитрий Михайлович — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, 23esn2008@rambler.ru

ГАВРИЛЮК Владимир Андреевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirgavr96@gmail.com

ГАЙФУЛИНА Диана Альбертовна — младший научный сотрудник лаборатории кибербезопасности и постквантовой криптографии Санкт-Петербургского института информатики и автоматизации Российской академии наук; студентка Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, gaifulina@comsec.spb.ru

ГАМИДОВ Тимур Октаевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dakota4126@gmail.com

ГАНЮШИН Алексей Сергеевич — студент группы ИКМ-71з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, markcrew@mail.ru

ГАШКОВ Роман Сергеевич — аспирант кафедры «Электрическая связь» Петербургского государственного университета путей сообщений имени Александра I, gashkovrom@bk.ru

ГВОЗДЕВ Юрий Васильевич — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, caraim@yandex.ru

ГЕЛЬФАНД Артем Максимович — аспирант, ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, amgelfand@mail.ru

ГЕХТ Антон Борисович — кандидат исторических, доцент кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a.geht@yandex.ru

ГЛАГОЛЕВ Сергей Федорович — кандидат технических наук, доцент, заведующий кафедрой фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glagolevsf@yandex.ru

ГОГОЛЬ Александр Александрович — доктор технических наук, профессор, заведующий кафедрой телевидения и метрологии, советник ректора Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, al.gogol@mail.ru

ГОЛЬДШТЕЙН Александр Борисович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, agold@niits.ru

ГОРДЕЕВ Илья Михайлович — студент группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, derllya@mail.ru

ГОФМАН Максим Викторович — кандидат технических наук, доцент кафедры «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I, maxgof@gmail.com

ГРЕБЕНЩИКОВА Александра Андреевна — студентка группы ИКТМ-82м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sgreben1@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

ДЕМЕНТЬЕВ Владислав Геннадьевич — студент группы ИКМ-71з ИКС Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladislavdmntv@gmail.com

ДЕНИСОВ Николай Денисович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, gigantizm94@mail.ru

ДЕРЕВЯНКО Владимир Сергеевич — студент группы ИКТЗ-54 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirderevyanko@bk.ru

ДЕСНИЦКИЙ Василий Алексеевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, vasily.desnitsky@mail.ru

ДИНЬ Чыонг Зюи — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, din.cz@spbgut.ru

ДИОРДИЦА Вячеслав Николаевич — студент группы ИКБ-51 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dior.slavik@gmail.com

ДОБРЯНСКИЙ Виталий Валериевич — студент группы ИКТБ-78м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dobryanskiyvv@gmail.com

ДОЙНИКОВА Елена Владимировна — кандидат технических наук, старший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, doynikova@comsec.spb.ru

ДОЦЕНКО Сергей Эдуардович — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 0472895@gmail.com

ДУДКИНА Ольга Сергеевна — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dudkinaole4ka.ru@mail.ru

ДУМЕНКО Павел Игоревич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha-dumenko@yandex.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

ДЮБОВ Андрей Сергеевич — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, blip@bk.ru

ЕЛАГИН Василий Сергеевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.elagin@spbgut.ru

ЕРЕМЧУК Евгения Юрьевна — аспирант кафедры «Линии связи и измерения в технике связи» Поволжского государственного университета телекоммуникаций и информатики, eremchuk1989@yandex.ru

ЕСАЛОВ Кирилл Эдуардович — ассистент кафедры инфокоммуникационных систем, начальник Научно-образовательного центра «Исследование проблем инфокоммуникационных технологий и протоколов» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yk@iks.sut.ru

ЖЕРНОВА Ксения Николаевна — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, zhernova@comsec.spb.ru

ЖМУРОВ Владислав Дмитриевич — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, 23esn2008@rambler.ru

ЖУКОВ Александр Евгеньевич — аспирант кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, aadron@bk.ru

ЗАРУБИН Антон Александрович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, проректор по информатизации, azarubin@sut.ru

ЗАХАРОВ Максим Валерьевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaharov.spbgut@gmail.com

ЗУЕВ Игорь Павлович — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zuyev.i.p@mail.ru

ИВАНОВ Александр Юрьевич — доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, alexander.y@mail.ru

ИВАНОВ Игорь Николаевич — студент группы ИКТК-56 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, igvanov1728@gmail.com

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Konstantin.Izrailov@mail.ru

ИЛЛАРИОНОВ Виталий Владимирович — студент группы ИКМ-71з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vit-illarionov@yandex.ru

ИМАНКУЛ Манат Насиркызы — кандидат технических наук, доцент кафедры вычислительная техника и программное обеспечение Казахского агротехнического университета им. С. Сейфуллина, mimankul57@gmail.com

КАЗАНЦЕВ Алексей Анатольевич — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Farvest.ax@yandex.ru

КАЛЯШОВ Евгений Владимирович — инженер-программист научно-образовательного центра «Лаборатория программирования» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, ekalyshov@gmail.com

КАНАЕВ Андрей Константинович — доктор технических наук, профессор, заведующий кафедрой «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, kanaev@pgups.ru

КАНДЗЮБА Евгений Владимирович — аспирант кафедры многоканальные телекоммуникационные системы Московского технического университета связи и информатики, ekandziouba@gmail.com

КАНИВЕЦ Злата Сергеевна — студентка группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zkanivec@gmail.com

КАРАМОВА Марина Руслановна — студент группы ИКТЗ-54 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, karamovamarina2198@gmail.com

КАРГАНОВ Виталий Вячеславович — кандидат технических наук, доцент, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, vitalik210277@mail.ru

КАРЕЛЬСКИЙ Павел Владимирович — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pasha.karelscky@yandex.ru

КАТАСОНОВ Александр Игоревич — студент группы ИКБ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksasha716@yandex.ru

КИРИЛОВА Ксения Сергеевна — студентка группы ИКТЗ-54 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksen_98@mail.ru

КИРИЧЕК Руслан Валентинович — доктор технических наук, доцент кафедры сетей связи и передачи данных 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 ООО «НТЦ АРГУС», s.v.kislyakov@gmail.com

КОВАЙКИН Юрий Владимирович — кандидат технических наук, доцент, заместитель начальника кафедры сетей связи и систем коммутации Военной академии связи им. Маршала Советского Союза С. М. Буденного, Klyv.77@yandex.ru

КОВАЛЕНКО Вадим Николаевич — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kovalenkovadim1996@gmail.com

КОВАЛЕНКО Алексей Павлович — студент группы ИКМ-72 з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alesha-kovalenko@mail.ru

КОВАЛЬ Альбина Радиковна — аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича akoval@sut.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

КОВЯРОВА Дарья Сергеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dariakova97@gmail.com

КОГНОВИЦКИЙ Олег Станиславович — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kogn@yandex.ru

КОЗЬМЯН Александр Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avk96@list.ru

КОЛБАНЕВ Михаил Олегович — доктор технических наук, профессор кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), mokolbanev@mail.ru

КОЛЕВАТЫХ Яна Олеговна — студентка группы ИКТГ-74м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yana.rein552@gmail.com

КОЛОМЕЕЦ Максим Вадимович — младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук; аспирант кафедры безопасности информационных технологий Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, kolomeec@comsec.spb.ru

КОМАШИНСКИЙ
Владимир Ильич — доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, kama54@rambler.ru

КОМАШИНСКИЙ
Николай Александрович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, nckkm@yandex.ru

КОНДРАТЕНКО
Владимир Степанович — доктор технических наук, профессор, заведующий кафедры оптических и биотехнических систем и технологий МИРЭА-Российского технологического института, Kondratenko@mirea.ru

КОНОНОВ
Павел Александрович — начальник отдела технической защиты информации Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kononov.pa@spbgut.ru

КОРМАНОВСКАЯ
Анастасия Александровна — магистрант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Stacy35@mail.ru

КОРНИЕНКО
Анатолий Адамович — доктор технических наук, профессор, заведующий кафедрой «Информатика и информационная безопасность» Петербургского государственного университета путей сообщения Императора Александра I, kaa.pgups@yandex.ru

КОРОЛЕВ
Александр Васильевич — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

КОСОВ
Никита Алексеевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kosov.n.a@mail.ru

КОТЕНКО
Игорь Витальевич — доктор технических наук, профессор, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, ivkote@comsec.spb.ru

КРАСИЛЬНИКОВА Наталья Валерьевна — кандидат психологических наук, доцент кафедры педагогики и психологии факультета последипломного образования Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, NataljaKrasilnikova@yandex.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov@inbox.ru

КРАУБНЕР Алексей Константинович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Будённого, leha.kraubner@yandex.ru

КУЗНЕЦОВ Вячеслав Сергеевич — ассистент, аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, slava_kuznetsov@inbox.ru

КУЗНЕЦОВА Александра Дмитриевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lev.0897@mail.ru

КУЗЬМИН Михаил Сергеевич — аспирант кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ranlitik@gmail.com

КУЗЬМИНА Вероника Игоревна — магистрант кафедры системного программирования Санкт-Петербургского государственного университета, avrinika@gmail.com

КУЛИК Вячеслав Андреевич — ассистент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vslav.kulik@gmail.com

КУЛИКОВА Анастасия Сергеевна — курсант Военной академии связи им. Маршала Советского Союза С. М. Будённого, ana7stasiya.kulikova @yandex.ru,

КУПЦОВ Владимир Дмитриевич — кандидат технических наук, доцент института физики, нанотехнологий и телекоммуникаций Санкт-Петербургского политехнического университета Петра Великого, vdkuptsov@yandex.ru

КУРАЕВА Анна Маевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, annkrr4@gmail.com

КУШНЕРЕВИЧ Алексей Геннадьевич — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, kushnerevich@comsec.spb.ru

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

ЛЕБЕДЕВ Павел Владимирович — адъюнкт кафедры сетей связи и систем коммутации Военной академии связи им. Маршала Советского Союза С. М. Буденного, spirit-angel@yandex.ru

ЛЕБЕДЕВА Надежда Александровна — студентка группы ИКТУ-58 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lebedeva.na.97@bk.ru

ЛЕБЕДЕВА Наталия Николаевна — курсант учебной группы 2592, Военной академии связи им. Маршала Советского Союза С. М. Будённого, vaxnencenco@gmail.com

ЛЕВШУН Дмитрий Сергеевич — младший научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук; аспирант Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, levshun@comsec.spb.ru

ЛЕЩЕВ Петр Михайлович — студент группы ИКМ-72з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, leshchevpm@gmail.com

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно исследовательского центра Военной академии связи имени Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛОБАСТОВА Мария Викторовна — ассистент, аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mlobastovabk1@rambler.ru

ЛОМАКИН Артур Юрьевич — студент группы ИКТБ-78м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Airisu.Zero.AMV@gmail.com

ЛУЕКЕ Патрик Эрман — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, scanf555@gmail.com

МАКОЛКИНА Мария Александровна — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makolkina@list.ru

МАЛАШЕРИФОВ Виталий Валентинович — студент группы ИКТУ-58 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vitas1997@yandex.ru

МАЛИКОВ Альберт Валерьянович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, mkv.vas@yandex.ru

МАЛЬКО Алексей Дмитриевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, malkoad@mail.ru

МАЛЯРОВ Максим Владимирович — студент группы ИКТО-52 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maxim.malyarov2014@yandex.ru

МАРОЧКИНА Анастасия Вячеславовна — студентка группы ИКТИ-75м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasiy1996@mail.ru

МАТЮХИН Александр Юрьевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Matukhin@list.ru

МАХМУД Омар Абдулкарим — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mahmood_omar@list.ru

МЕШАЛКИН Валентин Андреевич — кандидат технических наук, доцент НИО-4 НИЦ Военной академии связи им. Маршала Советского Союза С. М. Будённого, vova7dima@yahoo.com

МИРОНОВ Александр Егорович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, pustur@yandex.ru

МИХЕЕВА Светлана Николаевна — студентка группы ИКТУ-68 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ms.mixeewa@mail.ru

МИЦКОВСКИЙ Денис Юрьевич — студент группы ИКТЗ-64 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denism1111198@gmail.com

МОДЕЛЬ Михаил Викторович — студент группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, modelmv97@gmail.com

МОИСЕЕВ Олег Владимирович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, yakovlev.al@mail.ru

МОРДВИНОВА Оксана Васильевна — старший преподаватель кафедры математики и инженерной графики Военной академии связи им. Маршала Советского Союза С. М. Буденного, mordvinova_o_v@mail.ru

МОРОЗОВ Денис Павлович — инженер-программист кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, morozoff.py@gmail.com

МУРАТОВ Элзар Мээрбекович — аспирант Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elzar.muratov@yandex.ru

МУТХАННА Аммар Салех Али — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ammarexpress@gmail.com

МУХАМЕТШИНА Дина Фаиловна — студентка группы ИКТГ-74м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, undinakamec@gmail.com

НЕВЗОРОВ Юрий Анатольевич — студент группы ИКТМ-82м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yuriy@nevzoroff.com

НИЖГОРОДОВ Антон Олегович — аспирант кафедры линий связи и измерений в технике связи Поволжского государственного университета телекоммуникаций и информатики, anton.socol2017@yandex.ru

НИКИТИН Борис Константинович — кандидат технических наук, доцент кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nbk117@mail.ru

НОВИКОВ Антон Игоревич — студент группы ИКТК-55 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, it.novikov.anton@yandex.ru

ОВРАМЕНКО Александр Юрьевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ovr-sasha@yandex.ru

ОДОЕВСКИЙ Сергей Михайлович — доктор технических наук, профессор кафедры сетей связи и систем коммутации Военной академии связи им. Маршала Советского Союза С. М. Будённого, odse@rambler.ru

ОКУНЕВА Дарина Владимировна — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, darina_okuneva@mail.ru

ОНУФРИЕНКО Анастасия Валентиновна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, anastasia.4991@mail.ru

ОРЛОВ Григорий Александрович — студент группы ИКБ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grigory.a.orlov@gmail.com

ПАВШЕВА Мария Владимировна — студентка группы ИКПИ-51 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, masha110.97@mail.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, p_oleg99@mail.ru

ПАРАМОНОВ Александр Иванович — доктор технических наук, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alex-in-spb@yandex.ru

ПАРАЩУК Игорь Борисович — доктор технических наук, профессор, Заслуженный изобретатель РФ, профессор кафедры автоматизированных систем Военной академии связи им. Маршала Советского Союза С. М. Буденного, shchuk@rambler.ru

ПЕЛЁВИН Дмитрий Владимирович — студент группы ИКТЗ-54 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nor808@yandex.ru

ПОДГОРНАЯ Ксения Александровна — студентка группы ИКТУ-68 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksenia.podgornaya@mail.ru

ПОЛЯКОВ Павел Олегович — студент группы 6101 Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В. И. Ульянова (Ленина), polyakovos.pro@gmail.com

ПРЕОБРАЖЕНСКИЙ Александр Ильич — студент группы ИКБ-51 Санкт-Петербургского государственного университета телекоммуникации им. проф. М. А. Бонч-Бруевича, preobrazhenskyalexandr@mail.ru

ПРОКОФЬЕВ Олег Дмитриевич — курсант Военной академии связи им. Маршала Советского Союза С.М. Буденного, O.ivanov.spb@yandex.ru

ПРОНОЗА Антон Александрович — аспирант Санкт-Петербургского института информатики и автоматизации Российской академии наук, pronoza@gmail.com

ПРУДНИКОВ Сергей Владимирович — старший преподаватель кафедры защищённые системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, prud2000@mail.ru

ПУПЦЕВ Ринат Игоревич — ассистент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rinat.pupcev@gmail.com

РАДЫНСКАЯ Виктория Евгеньевна — инженер кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, radynskaya.v@gmail.com

РЕЗНИКОВ Богдан Константинович — магистрант, инженер кафедры фотоники и линий связи, техник кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rznkff@gmail.com

РЕУТОВА Дарья Олеговна — студентка группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, doreutova@gmail.com

РОГОВ Сергей Александрович — доктор физико-математических наук, профессор кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sarogov@mail.ru

САВЕЛЬЕВА Анастасия Андреевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saa@spbgut.ru

САВИНОВ Никита Владимирович — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nick.cavin191@gmail.com

САЕНКО Игорь Борисович — доктор технических наук, профессор 31 кафедры Военной академии связи им. Маршала Советского Союза С. М. Будённого; ведущий научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук, ibsaen@mail.ru

САЗОНОВ Дмитрий Данилович — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dim-saz@yandex.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

САФРОНОВА Елена Алексеевна — студентка группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elena_safronova_97@mail.ru

САХАРОВ Дмитрий Владимирович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, d.sakharov@rkn.gov.ru

САХАРОВА Мария Александровна — кандидат технических наук, доцент кафедры «Электрическая связь» Петербургского государственного университета путей сообщения Императора Александра I, zuvakamariya@mail.ru

СЕМЕНОВ Андрей Борисович — доктор технических наук, профессор Национального исследовательского Московского государственного строительного университета, andre52.55@mail.ru

СЕРГЕЕВ Алексей Николаевич — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, a32@bk.ru

СИМАНОВ Михаил Сергеевич — студент группы ИКТБ-78м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Simanov157@gmail.com

СКЛЯРОВА Мария Всеволодовна — студентка группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mashaskl@mail.ru

СЛЕПЦОВ Михаил Алексеевич — кандидат технических наук, заместитель генерального директора ООО «Т8», sma@t8.ru

СЛЕПЦОВА Наталья Павловна — студентка группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sleptsovanp1997@gmail.com

СМИРНОВ Евгений Витальевич — студент Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, john.1.9.98@mail.ru

СТАРКОВ Артем Михайлович — адъюнкт Военной академии связи имени Маршала Советского Союза С.М. Буденного, kadet58v@mail.ru

СТАРОДУБОВА Дарья Дмитриевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, starodubova.95@mail.ru

СТАСЮК Владислав Валерьевич — студент группы ИКТБ-88м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlad030397@gmail.com

СУМКИН Владимир Радомирович — старший преподаватель кафедры фотоники и линий связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sumkinv@mail.ru

ТАРГОНСКАЯ Алина Игоревна — студентка группы ИКБ-51 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, targonskaya.ai@gmail.com

ТАРЛЫКОВ Алексей Владимирович — начальник научно-образовательного центра «Лаборатория программирования» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, atarlykov@gmail.com

ТАСЮК Александр Андреевич — магистрант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexsandric7@gmail.com

ТАТАРНИКОВА Ирина Михайловна — ведущий специалист отдела организации научной работы студентов Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, itatarnikova@list.ru

ТВЕРДОХЛЕБОВА Юлия Владимировна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yulia.tverdohlebova@yandex.ru

ТЕМЧЕНКО Владислав Игоревич — студент группы ИКБ-51 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sspman2603@gmail.com

ТЕРЕНТЬЕВ Даниил Александрович — студент группы ИКТК-55 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, terentyevdaniel@gmail.com

ТЕРЕНТЬЕВ Денис Александрович — студент группы ИКТК-55 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, terentyevdenis7@gmail.com

ТЕСАКОВ Вячеслав Юрьевич — генеральный директор ООО «Равелин», tesakov@ravelinspb.ru

ТИМЕЦ Кристина Анатольевна — студентка группы ИКТУ-57 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kris_tim97@mail.ru

ТИХОНОВ Валерий Александрович — оператор научной роты научно исследовательского центра Военной академии связи имени Маршала Советского Союза С. М. Буденного, valery_tikhonov@mail.ru

ТИШКОВ Артем Валерьевич — кандидат физико-математических наук, заведующий кафедрой физики, математики и информатики Первого Санкт-Петербургского государственного медицинского университета им. И. П. Павлова, artem.tishkov@gmail.com

ТОКАРЕВА Ксения Александровна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tokarevaksu@inbox.ru

ТУКМАЧЕВ Владимир Флюрович — инженер института по проектированию сигнализации, централизации, связи и радио на железнодорожном транспорте «Гипротранссигналсвязь» − филиал АО «Росжелдорпроект», v.tukmachev@mail.ru

ТУШКАНОВА Ольга Николаевна — кандидат технических наук, научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, tushkanova@iias.spb.su

ТЫНЫМБАЕВ Болат Айткожинович — докторант Евразийского национального университета им. Л. Н. Гумилева, tynymbaevba@gmail.com

УШАКОВ Игорь Александрович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

ФЕДОРОВ Валерий Алексеевич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, fedvalera25@gmail.com

ФЕДОРЧЕНКО Андрей Владимирович — младший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук, fedorchenko@comsec.spb.ru

ФИЛИН Егор Дмитриевич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского университета государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filin.ed@mail.ru

ФИЦОВ Вадим Владленович — старший преподаватель кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, noldi@iks.sut.ru

ФОМКИН Роман Константинович — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, Roma_95_17@inbox.ru

ХАВАНСКАЯ Эльвира Рустамовна — студентка Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, elvirochka1995@mail.ru

ХИНЕНЗОН Александра Витальевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Khinenzon.av@gmail.com

ХОБОРОВА Вера Петровна — адъюнкт кафедры сетей связи и систем коммутации Военной академии связи им. Маршала Советского Союза С. М. Будённого, khoborova.vera@yandex.ru

ЦВЕТКОВ Александр Юрьевич — аспирант, старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alexander.tsvetkov89@gmail.com

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук; доцент кафедры защищенные системы связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chechulin@comsec.spb.ru, andreych@bk.ru

ШАЛАЕВА Мария Евгеньевна — студентка группы РТ-61 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shalaeva98@bk.ru

ШАМИН Алексей Анатольевич — кандидат экономических наук, доцент кафедры инфокоммуникационных технологий и систем связи Нижегородского государственного инженерно-экономического университета, ngiei-spo@mail.ru

ШАПОВАЛОВ Дмитрий Сергеевич — курсант Военной академии связи имени Маршала Советского Союза С. М. Будённого, dimah1996@mail.ru

ШВИДКИЙ Артем Александрович — начальник научно-образовательного центра «Программно-определяемые системы» Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shvidkiy@sut.ru

ШЕСТАКОВА Анастасия Алексеевна — студентка Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nastya28011995@rambler.ru

ШИПУЛИН Сергей Владимирович — начальник подразделения Управления Роскомнадзора по Северо-Западному федеральному округу, prud2000@mail.ru

ШЫПОТА Николай Александрович — магистрант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ksarn.kelben@gmail.com

ЩИПЦОВ Даниил Игоревич — студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, danila.igorevich@gmail.com

ЮРЧЕНКО Михаил Андреевич — студент группы ИКТЗ-54 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, polsit@yandex.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, viyak@bk.ru

ЯКОВЛЕВ Алексей Викторович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, yakovlev.al@mail.ru

ЯСТРЕБОВ Владислав Денисович — студент группы ИКТО-51 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, blakkheart66@mail.ru

АВТОРСКИЙ УКАЗАТЕЛЬ

СПбГУТ)))