СПбГУТ))) 95 лет

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

НТК ППС

65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов

ОСНОВНЫЕ НАУЧНЫЕ НАПРАВЛЕНИЯ:

- Инфокоммуникационные сети и системы
- Информационные технологии и программная инженерия
- Социальные технологии и экономика данных
- Радиоэлектронные системы и робототехника
- Кибербезопасность
- Сети связи специального назначения

СБОРНИК НАУЧНЫХ СТАТЕЙ

2025



ntk.sut.ru

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

65-Я НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА, НАУЧНЫХ РАБОТНИКОВ И АСПИРАНТОВ (НТК ППС 2025)

17–21 февраля 2025 года

Сборник научных статей

Том 2

Радиоэлектронные системы и робототехника

Кибербезопасность

Сети связи специального назначения

Санкт-Петербург

2025

УДК 001:061.3(082)
ББК 72 А43

65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025); сб. науч. ст.: в 3 т. / Под. ред. А. В. Рабина; сост. И. М. Татарникова: СПб.: СПбГУТ, 2025. Т. 2. 636 с.

Рецензент – доктор технических наук, профессор, директор института радиотехники и инфокоммуникационных технологий, заведующий кафедрой конструирования и технологий электронных и лазерных средств Санкт-Петербургского государственного университета аэрокосмического приборостроения Бестугин А. Р.

ПРОГРАММНЫЙ КОМИТЕТ

Председатель

Киричек Р. В., доктор технических наук, профессор, ректор СПбГУТ

Заместитель председателя

Рабин А. В., доктор технических наук, доцент, и.о. проректора по научной работе

Ответственный секретарь

Громова Н. Н., кандидат экономических наук, руководитель группы планирования научных исследований и аналитики СПбГУТ

Члены программного комитета

Елагин В. С., кандидат технических наук, доцент, и.о. декана факультета инфокоммуникационных сетей и систем СПбГУТ

Владыко А. Г., кандидат технических наук, доцент, декан факультета радиоэлектронных систем и робототехники СПбГУТ

Литвинов В. Л., кандидат технических наук, доцент, и.о. декана факультета информационных технологий и программной инженерии СПбГУТ

Зикратов И. А., доктор технических наук, профессор, декан факультета кибербезопасности СПбГУТ

Шутман Д. В., кандидат политических наук, доцент, декан факультета социальных технологий и экономики данных СПбГУТ

Гирш В. А., полковник, начальник военного учебного центра СПбГУТ

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ (СПбГУТ, Россия)

Председатель

Абилов А. В., первый проректор – проректор по учебной работе

Заместитель председателя

Окунева Д. В., проректор по проектной деятельности

Члены организационного комитета

Бобровский В. И., и.о. директора НИИ «Технологии связи»

Дружков К. В., и.о. директора департамента экономики и финансов

Ивасишин С. И., директор департамента организации и качества образовательной деятельности

Лысов А. Н., директор департамента по эксплуатации и развитию материально-технического комплекса

Зыкова Н. В., начальник управления информационно-образовательных ресурсов

Гребелина Н. В., начальник управления информатизации

В научных статьях участников конференции исследуются тенденции развития информационных технологий и телекоммуникационной отрасли, новейших достижений в науке и образовании. Предлагаются инновационные решения на основе информационных и коммуникационных технологий в образовании, науке, технике, экономике, социальной сфере и других областях.

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

ISBN 978-5-89160-370-7
ISBN 978-5-89160-372-1 (Том 2)

© СПбГУТ, 2025

СОДЕРЖАНИЕ

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА

Акимов С. В., Верхова Г. В. Концепция формирования децентрализованной киберфизической среды на базе принципов агентности, информационного самообслуживания и управляемой информационной открытости 10

Белоус К. В., Белов С. М., Михайлов В. Д., Шабанов А. П. Протоколы для построения систем малой автоматизации 15

Белоус К. В., Попугаев Д. Г., Шабанов А. П. Анализ ансамблевых и нейросетевых моделей искусственного интеллекта в систематизации оценки знаний обучающихся 20

Бойко И. А., Агейчик Н. О. Исследование адаптивных фильтров в антеннах беспилотных авиационных систем 26

Борисов С. В., Ланда А. Э., Остроумова Ю. С., Ханин С. Д., Шумаков П. П. К повышению эффективности обучения будущих специалистов физическим основам электроники 30

Борисов С. В., Ланда А. Э., Остроумова Ю. С., Ханин С. Д., Шумаков П. П. Настройка преподавания физических дисциплин на обучение научным основам и методам современных технологий 36

Буснюк А. О., Кузенов С. Р., Лившиц А. И., Передистов Е. Ю., Зайцев Д. А. Разработка системы рециркуляции изотопов водорода, основанной на явлении сверхпроницаемости металлических мембран по надтепловым водородным частицам 42

Ваганов А. В. Устройство для автоматизированного контроля токсичности биологических жидких дисперсных сред 48

Верхова Г. В., Пермяков А. А. Разработка программного обеспечения с микросервисной архитектурой для определения допустимых областей размещения технических объектов на основе анализа геоданных 54

Верхова Г. В., Чернышов А. С. Исследование возможности применения большой языковой модели для решения задач пространственного анализа 58

Волостных В. А., Воробьев П. В. Анализ характеристик геомагнитных возмущений 63

Волынкин П. А. Аппаратно-программные решения расширения мобильного робототехнического комплекса ROBO-PICA средствами искусственного интеллекта 68

Глушанков Е. И., Ву Т. З. Исследование простых и комбинированных сверточных кодов в радиотехнических системах 74

Глушанков Е. И., Кондрашов З. К., Суденкова А. В. Синтез стохастических дифференциальных уравнений для моделирования случайных процессов в корреляционном приближении 80

Глушанков Е. И., Фам К. К. Исследования методов кодирования и многопозиционной модуляции в каналах с замираниями и эффектом Доплера 86

Деткова В. М., Долматова О. А. Интеграция инженерных задач в курс общей физики: повышение мотивации студентов технических вузов 92

Деткова В. М., Долматова О. А. Оценка эффективности преподавания физики: критерии, методы и инструменты обратной связи 98

Деткова В. М., Урванцева Н. Л., Шарихина Ю. В. Апробация методических указаний для выполнения лабораторной работы «Изучение явлений и законов волновой оптики. Двулучепреломление. Четвертьволновая фазовая пластинка» 104

Зайцева З. В. Разработка и создание виртуального лабораторного практикума по исследованию устойчивости активных четырехполюсников 111

Иванов В. Г., Алленов Д. С., Михайлов В. П., Чабаненко В. В. Анализ современных средств уничтожения беспилотных летательных аппаратов как архитектуры семантической интероперабельности обстановки на поле боя в тактическом звене управления 117

Коровин К. О., Алли Р. А. Методы распознавания объектов по спектрограммам в сетях сотовой связи 122

Коротин В. Е., Вторых В. С. Исследование процедуры эквалайзирования для компенсации искажений в рэлеевском канале с замираниями 128

Коротин В. Е., Вторых В. С. Исследование факторов формирования зон покрытия, характерных для радиосистем, использующих технологию OFDM 134

Кубалова А. Р. Микроволновый эллиптический фильтр с реализацией на микрополосковых резонаторах с четвертьволновыми инверторами сопротивлений 138

Ликонцев А. Н., Попов Д. С. Использование спутниковой связи VSAT для интеграции с платформой RIGSPACE в целях мониторинга буровых операций на удаленных нефтяных скважинах 142

Любимов А. Г. К вопросу решения задачи о многопродуктовом потоке в интеллектуальной системе поддержки принятия решений 149

Макаров Л. М. Информационная комплементарность топологических элементов полупроводников 157

Макогон В. П., Негурица А. А., Лукьяненко Д. И. Аккумуляторные батареи АБ-18 для Р-187-П1 «АЗАРТ»: современное решение для военных радиостанций 166

Никитин Ю. А. Моделирование цифровых преобразований при когерентном синтезе частот с помощью логических элементов 171

Остроумова Ю. С., Ханин С. Д. Структурная неоднородность неупорядоченных диэлектриков элементов электронной базы и их эксплуатационные характеристики 177

Павлов Ф. Ф. Избранные вопросы квантовой оптики: неоднозначность закона смещения Вина 183

Пантюхин О. И., Изотов Д. Ю., Яровой Р. В. Основные подходы к решению проблем распознавания медиаданных 191

Пантюхин О. И., Изотов Д. Ю., Яровой Р. В. Системы распознавания медиаданных: области применения и решаемые задачи 196

Прокофьев П. А. Методика оценки качества геоинформационного программного обеспечения 201

Седышев Э. Ю., Болдырев Е. А., Иванищева Е. Ф., Макаров А. А., Федоров С. И. Устройства СВЧ на планарных нерегулярных линиях 205

Седышев Э. Ю., Глухов Н. И., Котов Г. А., Федоров С. И. Спиральные антенны на конической поверхности в составе ФАР 214

Седышев Э. Ю., Федоров С. И. Использование нерегулярных линий при синтезе спиральных антенн 218

Симонина О. А., Бобровский А. В. Расчет минимально возможного расстояния между радиоэлектронными средствами в беспроводных сетях высокой плотности 223

Симонина О. А., Кокин С. А. Варианты реализации приемников для сверхширокополосных систем импульсного радио с временными скачками 228

Скалецкая И. Е., Урванцева Н. Л., Шарихина Ю. В. Апробация методических указаний для выполнения лабораторной работы «Изучение явлений и законов волновой оптики. Поляризация света. Закон Малюса. Закон Брюстера» 233

Ткачев Д. Ф., Мурачев Г. И. Разработка методики частотного регулирования и управления ветроэнергетическими системами 240

Ткачев Д. Ф., Парфенов М. С., Фукалов В. А. Разработка прототипа опорно-поворотного мехатронного модуля сканирующего лазерного дальномера мобильного робота 246

Фёдоров П. Н., Галушко И. В., Кудрявцева Ю. А., Следевский К. Н. Результат анализа методов измерения коэффициента шума усилителя для адаптивной антенной решетки, расположенной на БПЛА 251

Фёдоров П. Н., Галушко И. В., Кудрявцева Ю. А., Титков И. Е. Способ борьбы с активными помехами в радиотехнических системах с использованием адаптивных антенных решеток 255

Чуднов А. М., Деркач А. Е. Задачи оптимизации структуры сети ретрансляторов на базе беспилотных летательных аппаратов для повышения устойчивости передачи данных 261

КИБЕРБЕЗОПАСНОСТЬ

Аксенов К. Д. Разработка метода нейросетевой стеганографии для встраивания медицинских данных пациента в изображения **268**

Альотум Ю. М. А. Биометрические данные и их возможности достижения многофакторной аутентификации методом одноразового пароля **275**

Бабков И. Н. Аудит информационной безопасности - как метод повышения защищенности организации **282**

Бударный Г. С. Методика противодействия декомпиляции исполняемых файлов KOTLIN **288**

Васильев Н. А., Лещинский Б. С., Ситдиков Д. С. Применение искусственного интеллекта для анализа уязвимостей в сетевых протоколах **294**

Гаврилов И. В., Баранов Д. А. Применение технологии блокчейн в системах электронного документооборота **300**

Гаврилов И. В., Морозов В. О., Хрущев И. А. Прототип системы защищенной IP-телефонии на основе реализации криптографических алгоритмов **306**

Жернова К. Н. Архитектура программного прототипа визуализации данных безопасности для анализа с помощью нейронных сетей **311**

Иванов Д. В., Налимов К. Г. Анализ и классификация угроз информационной безопасности в системах искусственного интеллекта **314**

Иванов Д. В., Налимов К. Г. Противодействие угрозе отравления данных систем искусственного интеллекта путем применения механизмов предварительного анализа обучающих данных **320**

Израилов К. Е. Основные этапы авторской методологии реверс-инжиниринга машинного кода в интересах поиска в нем уязвимостей **326**

Киселёв Н. Н., Смирнов С. Н. Оценка влияния на изменение расходов в области защиты информации в электросетевой компании регионального уровня в связи с вступлением в силу 01.09.2024 Положений федерального закона № 185-ФЗ ОТ 13.07.2024 «О внесении изменений в федеральный закон «об электроэнергетике» **332**

Ковцур М. М., Дрепа В. Е. Формирование показателей качества систем определения местоположения беспроводных устройств семейства стандартов IEEE 802. 11 **339**

Копылов С. А., Горбачев П. Н., Романюк П. Р. О некоторых аспектах применения методов маркирования видеоданных **344**

Копылов С. А., Кощенко К. Б. Обзор методов поведенческой аутентификации **349**

Копылов С. А., Чертовских И. А. Применение методов машинного обучения в системах обнаружения сетевых вторжений **354**

Котенко И. В., Абраменко Г. Т. Использование отнологий и больших языковых моделей для интерпретаций событий SURICATA **359**

Котенко И. В., Зеличенок И. Ю. Методы обработки больших данных и их влияние на выявление многошаговых атак 364

Котенко И. В., Слётов М. А. Исследование ансамблевого метода автоматизированного пентеста на базе обучения с подкреплением 369

Красов А. В. Защиты диссертаций в России в области стеганографии 376

Красов А. В. Обнаружение сетевой стеганографии при помощи системы предотвращения вторжений Snort 382

Кушнир Д. В. Анализ возможности встраивания сообщений в структуры данных распределенных реестров 388

Лаута О. С., Васильев Н. А., Беседин М. Д., Копачев А. Ю. Сервис для генерации надежных и запоминаемых паролей 397

Левшун Д. С., Лаврентьев В. В. Архитектура системы на основе LLM-агентов для защиты умного завода 403

Левшун Д. С., Хушея К. И. Методы отравления данных на основе изображений в федеративном обучении: анализ и подходы к защите 409

Липатников В. А., Гущин И. С., Солдатенко Я. Г. Моделирование атаки типа «сканирование сети» 413

Липатников В. А., Гущин И. С., Солдатенко Я. Г. Модель атаки «доверенный объект сети» в сети передачи данных 419

Липатников В. А., Задбоев В. А. Обучение искусственного интеллекта на основе моделирования атак в сетях передачи данных 424

Макогон В. П., Негурица А. А., Трухманов И. Р. Защищенность веб-приложений: моделирование сетевых атак в структуре киберполигона 430

Перевозник Ю. Я., Гвоздков И. В., Ликарь А. И. Постквантовая криптография, не пора-ли начинать беспокоиться 436

Петрив Р. Б. Гибридные Honeypot- и Honeynet-решения для кибербезопасности на основе портативных высокопроизводительных вычислительных платформ 446

Саенко И. Б., Иванцов Д. С. Методика оптимизации плана распределения файлов в распределенном хранилище данных SIEM-систем 451

Сахаров Д. В., Борисов С. В. Анализ моделей распространения информации в социальных группах 456

Сахаров Д. В., Демидов Г. А. Современные технологии защиты от телефонного мошенничества: обзор антифрод-решений. 460

Сахаров Д. В., Шашкин В. С. Анализ фейковых аккаунтов, объединенных в ботнеты в социальных сетях 466

Свечников Д. А., Авдеев М. С., Горбачев П. Н. Защита программного обеспечения от динамического анализа 472

Свечников Д. А., Астахов М. Р., Горбачев П. Н. Повышение оперативности обнаружения уязвимостей класса слепая SQL-инъекция 476

Свечников Д. А., Горбачев П. Н., Рощупкина П. А., Смольянинов А. С. Анализ способов управления программно-конфигурируемой информационной инфраструктурой 480

Спицин О. Л., Шевченко А. А., Калиникин Н. А., Ткачёв М. А. Детализация модели атаки «Перехват сессии TCP» на основе CYBER KILL CHAIN 484

Спицин О. Л., Шевченко А. А., Калиникин Н. А., Ткачёв М. А. Ключевые особенности реализации компьютерной атаки на сеть передачи данных типа «анализ сетевого трафика» 490

Ткачев Д. Ф., Задбоев В. А. Основные концепции нейронных сетей в сетях передачи данных 495

Ушаков И. А., Скорых М. А. Обзор сетевых индикаторов компрометации для обнаружения каналов управления вредоносным программным обеспечением 500

Ушаков И. А., Черкашин А. И. Анализ методов обеспечения безопасности в сетях LTE 506

Чечулин А. А., Антонюк Е. А. Поиск следов киберпреступлений с применением матрицы MITRE ATTACK 512

Чечулин А. А., Горда М. Д. Основные проблемы обеспечения информационной безопасности в бюджетных организациях и пути их решения 516

Чечулин А. А., Кюнер А. П. Социальная инженерия. Алгоритмы противодействия атакам 521

Шариков П. И. Исследование влияния замен опкодов условных переходов JVM на работоспособность CLASS-файлов 527

Шевченко А. А., Кириков Н. Д., Кудрявцева Ю. А. Анализ методов корреляции событий безопасности в SIEM-системах 532

Шемякин С. Н. Проверки простоты числа с помощью эллиптических кривых 536

Штеренберг С. И. Гипотеза о достижении технологической сингулярности через квазибиологическую парадигму описания интеллектуальных IDS 541

СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Бояринцев А. И., Повзнер А. А., Хохлов К. О., Манько И. Д. Регулируемый цифровой генератор шума средне-высокочастотного диапазона 547

Будко П. А., Южакова А. А. Управление надежностью функционирования техники связи специального назначения в интересах внедрения стратегий прогнозного технического обслуживания 553

Васильев Н. А., Такшеев А. Д., Тарасенко С. Е. К вопросу о внедрении адаптивной системы подготовки специалистов в образовательные процессы вузов 557

Глушко А. В., Гриднев В. А., Знобищев Р. С., Стахеев И. Г. Предлагаемый способ использования учебно-тренировочной карты в совершенствовании навыков работы на первичном мультиплексоре 562

Гриднев В. А., Груздев Д. А., Стахеев И. Г. Способ контроля формирования профессионально-важных качеств у студентов военного учебного центра в условиях проведения СВО 567

Гриднев В. А., Стахеев И. Г. Предлагаемый способ подготовки специалистов в области телекоммуникаций в условиях проведения специальной военной операции 572

Груздев Д. А., Загорельский В. В., Марченков А. А. Разработка алгоритма действий ответственных за организацию ФПС в воинской части 577

Косырев А. В. Моделирование процессов с дискретным состоянием и непрерывным временем на примере модели возникновения отказов и боевых повреждений военной техники связи 581

Манаенко С. С., Сазонов В. В., Альбадр Х. Б., Луконин К. А. Вариант формирования ортогональных сигналов для системы связи специального назначения 585

Попов А. И., Семкина М. Р., Тухбатуллина Э. Ф. Автономная навигация БПЛА с функцией избегания препятствий и планирования траектории на основе машинного зрения 592

Попов А. И., Семкина М. Р., Тухбатуллина Э. Ф. Навигация дронов на основе технологии БПЛА-РПС с использованием регионов и приграничных зон 598

Сагдеев А. К., Самаркин Д. С., Алехин И. Н., Новиков Н. С. Методика оценки комплекса радиоэлектронного подавления по возможности ведения радиоразведки 603

Сагдеев А. К., Самаркин Д. С., Алехин И. Н., Новиков Н. С. Методика оценки возможностей комплекса РЭП по радиоподавлению 609

Сазонов В. В. Преобразования и передача данных в трактах и каналах системы связи специального назначения 615

АВТОРЫ СТАТЕЙ 619

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА

УДК 004.946
ГРНТИ 28.17.33

КОНЦЕПЦИЯ ФОРМИРОВАНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ КИБЕРФИЗИЧЕСКОЙ СРЕДЫ НА БАЗЕ ПРИНЦИПОВ АГЕНТНОСТИ, ИНФОРМАЦИОННОГО САМООБСЛУЖИВАНИЯ И УПРАВЛЯЕМОЙ ИНФОРМАЦИОННОЙ ОТКРЫТОСТИ

С. В. Акимов, Г. В. Верхова

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

Приведены результаты исследований в области создания концепции децентрализованной киберфизической среды, которая обеспечит преодоление многих проблем, присущих современной Всемирной паутине, среди которых ее сегментация на множество изолированных экосистем, наличия крупных монополистов, владеющих веб-сервисами, а также необходимость для пользователей регистрироваться в многочисленных информационных системах с дальнейшей поддержкой в них своих информационных профилей. В основу децентрализованной киберфизической среды положены принципы агентности, информационного самообслуживания и управляемой информационной открытости. Все информационные взаимодействия между агентами осуществляются с помощью прокси-агентов, которые представляют этих агентов в локальных киберсредах. Показано, что предложенная архитектура позволяет сформировать киберфизическую среду, объединяющую отдельных физических лиц и их группы, юридических лиц, природные и техногенные объекты.

децентрализованная среда, киберсреда, киберфизическая система, информационное самообслуживание, управляемая информационная открытость, локальные киберсреды, глобальная киберсреда, P2P, F2F

За период своего существования Всемирная паутина проделала значительный путь развития от статичных сайтов до новейших высокотехноло-

гичных иммерсивных систем, объединяющих людей и технические системы. Каждое поколение Всемирной паутины в разной степени поддерживает такие аспекты как децентрализация, коллаборативность, владение данными, киберфизичность (рис. 1). Интересно отметить, что степень децентрализации во втором поколении стал ниже, чем в первом (рис. 1). В настоящее время представлены элементы всех поколений Всемирной паутины, хотя подавляющее число сайтов и веб-сервисов все еще относятся к Web 2.0, что заставляет некоторых авторов называть современное поколение Web 2.5.

Переход к децентрализованному Web 3.0 и к иммерсивному Web 4.0 требует решения как технических, так и методологических проблем. Исходя из особенностей Web 4.0 [1-2], можно утверждать, что его внедрение требует формирования единой киберфизической среды, сформированной из локальных интероперабельных киберсред, построенных на принципах агентности, информационного самообслуживания и управляемой информационной открытости [3]. Целью данной статьи является изложение концепции формирования такой среды.

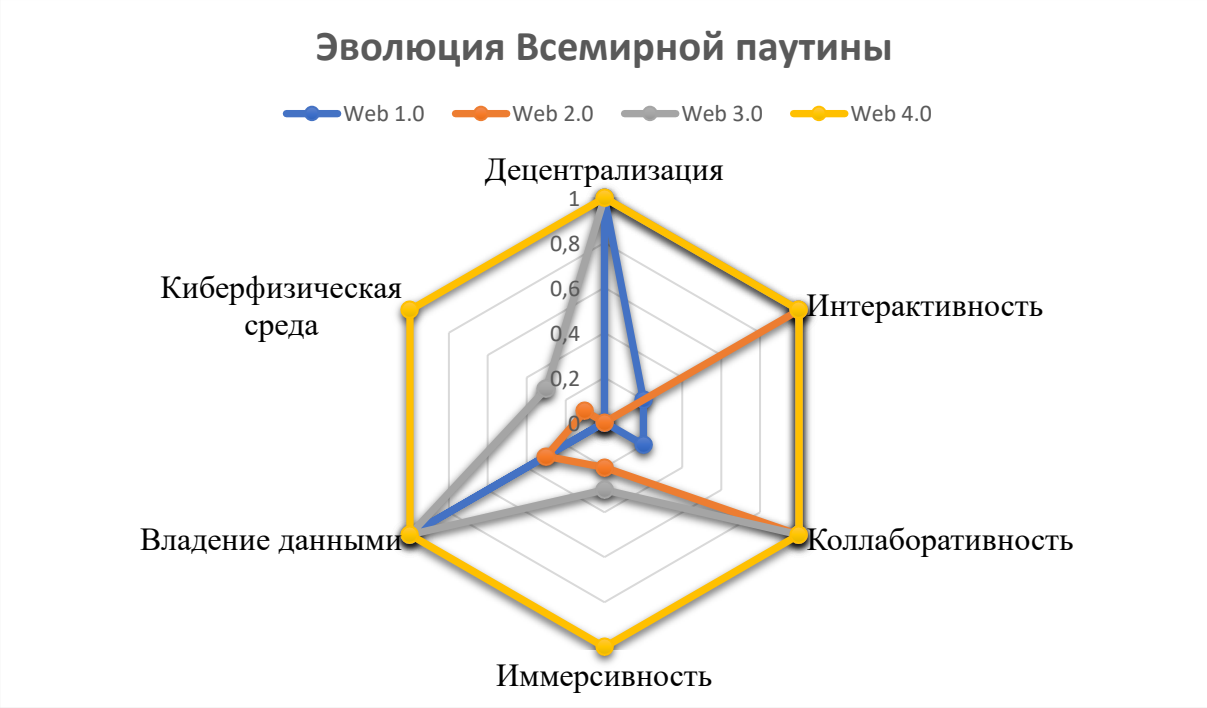


Рис. 1. Эволюция Всемирной паутины

Концепция формирования децентрализованной киберфизической среды на базе принципов агентности, информационного самообслуживания и управляемой информационной открытости предполагает формирование

единой киберфизической среды из локальных киберсред. В частном случае локальная киберсреда может включать только одного агента. Установление связей и коммуникации между агентами осуществляются единообразно, вне зависимости от того, расположены агенты в единой киберсреде или в разных киберсредах. Это достигается путем введения прокси-агентов, которые составляют окружение агента, и через которые агент коммуницирует с коагентами (friends) – агентами, с которыми у данного агента установлены связи. В случае смены агентом киберсреды или изменения URI, она распространит данную информацию всем своим коагентам, и данная миграция окажется абсолютно прозрачной для остальных участников.

Принцип агентности предполагает абсолютное равноправие агентов по отношению к киберсреде, причем агентами могут являться физические и юридические лица, а также любые другие природные и техногенные объекты. Агенты могут базироваться на серверах, в облачных сервисах, или на компьютере пользователя, имеющего свой IP и круглосуточный доступ в интернет. При этом место дислокации и способ базирования агент может сменить в любое время. Информационное самообслуживание предполагает, что информация, в распространении которой до ограниченного или неограниченного круга лиц агент заинтересован, загружается в среду самим агентом (принципалом). При этом информация заносится один раз, а дальше используется неограниченное время на основе принципа управляемой информационной открытости.

Киберсреда, построенная на базе предложенной концепции, предоставляет пользователям ряд полезных возможностей, одним из которых является возможность отчуждения сервисов (рис. 2).

Агенты, использующие отчуждаемый сервис, создают своих прокси-агентов в киберсреде, в которой данный сервис размещен, после чего осуществляется репликация сервиса в целевых средах. В рамках данной концепции модель коллективной работы над артефактом носит полностью распределенный характер. Другим важным достоинством модели отчуждения сервиса является возможность масштабирования средствами киберсреды, когда под отдельную задачу или набор задач может быть создан отдельная реплика сервиса.

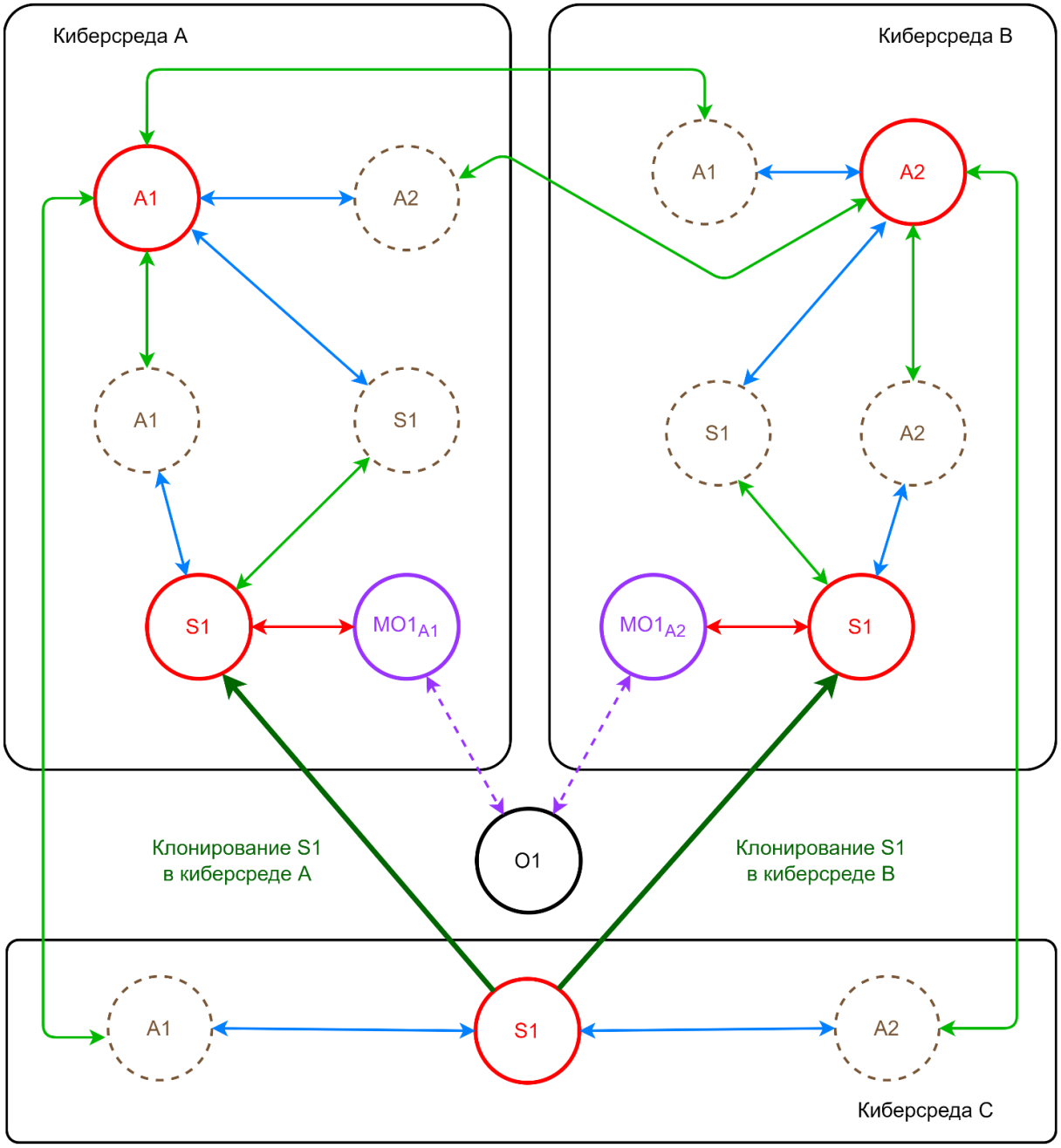


Рис. 2. Модель отчуждения сервиса

Единая киберфизическая киберсреда, сформированная из локальных интероперабельных киберсред, полностью соответствует концепциям Web 3.0 и Web 4.0, и предоставляет ее участникам следующие возможности:

– устанавливать связи между агентами, по аналогии с сетями типа F2F;
– выполнять миграцию между киберсредами, прозрачным образом для всех коагентов, с которыми была установлена связь;
– гибко управлять доступом к ресурсам, владельцам которых является пользователь;
– выполнять доставку сервиса через прокси-агента;

– выполнять отчуждение сервиса;
– работать в условиях DDIL.

На базе рассмотренной децентрализованной киберфизической среды могут быть созданы децентрализованные сервисы, предоставляющие пользователям возможности, которые не могут предоставить традиционные сервисы. Примером такого сервиса может стать децентрализованная коллаборативная геоинформационная система, позволяющая пользователям независимо создавать модели геосистем независимо друг от друга в рамках единой геоинформационной киберсреды.

Список используемых источников

1. Zhou Z., Li Z., Zhang X., Sun Y. and Xu H. A Review of Gaps between Web 4.0 and Web 3.0 Intelligent Network Infrastructure // IEEE 9th World Forum on Internet of Things (WF-IoT), Aveiro, Portugal, 2023. PP. 1-6. DOI: 10.1109/WF-IoT58464.2023.10539509.

2. Жмурко Д. Ю., Лаптев С. В. Эволюция интернета: от Web 3.0 к Web 4.0 - перспективы развития глобальной сети // В сборнике: Математические методы и информационно-технические средства. Материалы XX Международной научно-практической конференции. Краснодар, 2024. С. 79-87.

3. Верхова Г. В., Акимов С. В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества // В сборнике: Волновая электроника и инфокоммуникационные системы. Сборник статей XXIV Международной научной конференции. Санкт-Петербург, 2021. С. 34-39.

THE CONCEPT OF FORMING A DECENTRALIZED CYBER-PHYSICAL ENVIRONMENT BASED ON THE PRINCIPLES OF AGENCY, INFORMATION SELF-SERVICE AND CONTROLLED INFORMATION OPENNESS

Akimov S., Verkhova G.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the results of research in the field of creating a concept of a decentralized cyber-physical environment that will overcome many problems inherent in the modern World Wide Web, including its segmentation into many isolated ecosystems, the presence of large monopolists owning web services, and the need for users to register in numerous information systems with subsequent support of their information profiles. The decentralized cyber-physical environment is based on the principles of agency, information self-service and controlled information openness. All information interactions between agents are carried out using proxy agents that represent these agents in local cyber environments. It is shown that the proposed architecture allows for the formation of a cyber-physical environment that unites individuals and their groups, legal entities, natural and man-made objects.

Key words: *decentralized environment, cyber environment, cyber-physical system, information self-service, managed information openness, local cyber environments, global cyber environment, P2P, F2F*

УДК 681.5
ГРНТИ 71.01.85

ПРОТОКОЛЫ ДЛЯ ПОСТРОЕНИЯ СИСТЕМ МАЛОЙ АВТОМАТИЗАЦИИ

К. В. Белоус, С. М. Белов, В. Д. Михайлов, А. П. Шабанов

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

Активное развитие систем управления технологическими процессами и производствами, в том числе в области малой автоматизации, приводит к распространению систем класса «умный дом». Статья посвящена вопросам исследования различных протоколов и программно-аппаратных платформ для построения систем малой автоматизации. Приводятся различные варианты согласованной работы элементов различных производителей.

ModBus, MQTT, Zigbee, интеллектуальная система автоматизации, умный дом

В последнее время промышленные системы управления и системы малой автоматизации претерпевают значительные изменения, что связано с повышением требований к безопасности систем критической инфраструктуры, совершенствования их эффективности, а также с внедрением микроконтроллерной техники в системы управления, такие как АСУ ТП, АСУ П и системы малой автоматизации [1]. Совершенствование систем управления предприятием и средой обитания с учетом концепции Индустрии 4.0, одной из компонентов которой является промышленный Интернет вещей (IIoT), позволяет интегрировать различные разрозненные системы в единую информационную сеть, что позволяет повысить уровень автоматизации и оптимизировать производственные процессы в реальном масштабе времени. Важной частью современных систем управления промышленными предприятиями является внедрение концепции цифровых двойников, представляющих собой цифровую копию физического объекта или процесса, позволяющая повысить эффективность производства и проводить его оптимизацию. Концепция цифровых двойников является частью Индустрии 4.0 и направлена на оказание помощи предприятиям в вопросах обнаружения физических проблем, точное предсказание их результатов и повышение качества продукции.

Несмотря на то, что существующие решения позволяют строить системы практически неограниченной сложности, базовые протоколы систем управления промышленными предприятиями остаются в большинстве своем неизменными, либо совершенствуются незначительно. Связано это, в

первую очередь, с требованиями обеспечения совместимости промышленного оборудования, а также малой необходимостью внесения изменений с существующие стандарты. В качестве примера приведем стандарт ISO на языки программирования промышленных контроллеров (IEC 61131-3:2013/ГОСТ Р МЭК 61131-3-2016). В настоящее время используется 3-я версия данного стандарта, принятая в 2012 г. С момента принятия первой версии (IEC 61131-3:1993), принятой в 1993 году, прошло более 30 лет, но базовые принципы остаются неизменными, так как позволяют решать 99 % задач, которые могут возникать в области управления техническими системами и управления технологических процессов и производств.

Далее рассмотрим базовые протоколы, используемые для промышленных систем автоматизации и приведем варианты их совместного использования.

Одним из наиболее «уважаемых» протоколов промышленной автоматизации является Modbus, разработанный компанией Modicon (ныне Schneider Electric) в 1979 г. По протоколу Modbus работают счетчики электрической энергии, средства динамической индикации, контроллеры температуры, промышленные контроллеры и терминалы удаленного сбора данных. Modbus активно используется в системах управления зданиями, энергетике, водоснабжении и других областях, где требуется надежная и простая автоматизация. Преимуществами протокола Modbus являются простота реализации. Протокол Modbus легко интегрируется с различными устройствами и системами. Широкая поддержка: множество производителей оборудования поддерживают Modbus, что делает его универсальным решением. Гибкость: Modbus поддерживает как последовательные (Modbus RTU), так и сетевые (Modbus TCP/IP) соединения. При необходимости существует возможность преобразования Modbus TCP ↔ Modbus RTU. Примером таких преобразователей являются устройства компании Waveshare. На рис. 1 приведет пример преобразователя интерфейсов.



Рис. 1. Преобразователь интерфейсов

Другим популярным протоколом является протокол BACnet (Building Automation and Control Networks) – это протокол, являющийся специализированным протоколом для автоматизации зданий, поддерживающий широкий спектр устройств и систем. Преимуществами протокола является его международный статус, облегчающий внедрение в международные проекты. Масштабируемость: BACnet поддерживает системы автоматизации небольшого и крупного масштаба. Безопасность: протокол включает механизмы аутентификации и шифрования данных. Наиболее активное применение протокол находит в системах управления вентиляцией, отоплением и кондиционированием, освещением, безопасностью и другими областями автоматизации зданий и сооружений.

Протокол DALI (Digital Addressable Lighting Interface) предназначен для управления освещением, позволяющий создавать гибкие системы освещения с высокой энергоэффективностью. Преимуществами протокола являются: *гибкое управление*. Поддержка адресации отдельного осветительного прибора, что позволяет выполнить точную настройку освещения. *Энергоэффективность*. Существует возможность дистанционного управления и мониторинга потребления энергии. *Легкая интегрируемость* с существующими системами автоматизации зданий. DALI применяется для автоматизации офисных зданий, торговых центров, гостиниц и других объектах, где важным требованием является обеспечение энергоэффективности и гибкости управления освещением.

KNX представляет собой международный стандарт автоматизации зданий, объединяющий несколько протоколов, разработанных ранее (EIB, EHS, BatiBUS). KNX поддерживает широкий спектр устройств и систем. Преимуществами являются: *универсальность*. Он поддерживает управление основными системами жизнеобеспечения зданий, таких как освещение, отопление, безопасность и другие. Протокол обладает *высокой надежностью* и обеспечивает защиту данных и устойчивость к сбоям. Позволяет автоматизировать как небольшие дома, так и крупные коммерческие и промышленные объекты. KNX используется в жилых домах, офисных зданиях, гостиничных комплексах, учреждениях здравоохранения и других объектах, требующих комплексной автоматизации.

В системах управления небольшими объектами, к которым относятся и системы так называемой «малой автоматизации», активное развитие получают микроконтроллерные платы. Наиболее популярным решением в данной области являются платы семейства Arduino или ESP-32 с различной аппаратной поддержкой нескольких протоколов. Как правило, данные платы

по умолчанию поддерживают следующие протоколы: UART, I2C, SPI, Wi-Fi, Bluetooth. На базе данных плат могут быть реализованы различные системы управления, среди которых системы охраны, системы автоматического полива растений, системы контроля и управления доступом и др. Существенным недостатком микроконтроллерных плат является невозможность прямого подключения к их выводам мощной нагрузки – для этого требуется обеспечение либо опторазвязки, либо использование реле. Так же данные платы не обеспечиваются степенью защиты от внешних воздействий по стандартизации IP и долговременной (в сравнении с промышленными контроллерами) работы в жестких условиях. В связи с этим построение полноценной системы управления, которая могла бы обеспечить контроль внешнией и внутренней среды исключительно на базе микроконтроллеров является достаточно сложной задачей. Наилучшим решением в данном случае является разделение функций и обеспечение информационного обмена между подсистемами, например, на базе протокола UART или Modbus, реализация которого для микроконтроллерных плат существует.

Важным требованием при построении современных систем управления должны учитывать психофизиологические особенности пользователей и условия их работы. Например, операторы могут работать в условиях повышенного шума, сильных вибраций, низкой освещенности, что требует адаптации пользовательских интерфейсов для повышения удобства и эффективности. Кроме того, необходимо обеспечить их устойчивость к ошибкам пользователей и обеспечить быстрый доступ к критической информации [2]. Проектирование систем IIoT также связано с необходимостью обеспечения кибербезопасности, так как в условиях угрозы кибератак, системы должны защищать данные и предотвращать несанкционированный доступ к системам управления. Это требует применения современных методов обеспечения защиты информации и регулярного обновления программного обеспечения и мониторинга безопасности.

Одним из ключевых аспектов проектирования HMI является интеграция с другими компонентами системы IIoT, что включает в себя взаимодействие с датчиками, контроллерами, облачными сервисами и аналитическими платформами. Эффективная интеграция позволяет создавать комплексные системы, которые собирают и анализируют данные в режиме реального времени, предоставляя операторам исчерпывающую картину происходящего и позволяя принимать оперативные решения.

Стандарты ISO и IEC, устанавливают общие принципы и требования к проектированию HMI, что позволяет создавать совместимые и безопасные интерфейсы. Следование стандартам позволяет обеспечить высокое качество и надежность разрабатываемых систем, а также облегчает их интеграцию и эксплуатацию. Человеко-машинные интерфейсы играют ключевую роль в современных системах IIoT, обеспечивая эффективное взаимодействие операторов с промышленными устройствами и системами. Введение концепции IIoT внесло значительные изменения в традиционные подходы к автоматизации и управлению производственными процессами, создавая новые вызовы и возможности для разработчиков HMI [3].

Протоколы для построения систем малой автоматизации играют ключевую роль в повышении эффективности и удобства управления различными процессами и интеграции различных приборов устройств в единую систему управления. Рассмотренные в статье протоколы представляют собой малую часть используемых в системах автоматики, а выбор конкретного зависит от специфики задач и требований к системе автоматизации. Внедрение этих технологий позволяет малым и средним предприятиям значительно оптимизировать свои процессы и повысить конкурентоспособность на рынке.

Список используемых источников

1. Денисенко В. В., Компьютерное управление процессом, экспериментом, оборудованием. М.: Горячая линия–Телеком, 2014. 606 с., ил.

2. Демидов О. Глобальное управление Интернетом и безопасностью в сфере использования ИКТ: Ключевые вызовы для мирового сообщества. М.: Альпина Паблишер, 2016. 198 с.

3. Золкин А. Л. Проектирование человеко-машинных интерфейсов для систем индустриального интернета вещей: учебник для СПО / А. Л. Золкин, Ф. Р. Ахмадуллин. СПб.: Лань, 2025. 152 с.: ил.

PROTOCOLS FOR BUILDING SMALL AUTOMATION SYSTEMS

Belous K., Belov M., Mikhailov V., Shabanov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Active development of process and production control systems, including in the field of small automation, leads to the spread of "smart home" class systems. The article is devoted to the issues of research of various protocols and software and hardware platforms for building small automation systems. Various options for coordinated operation of elements from different manufacturers are given.

Key words: *ModBus, MQTT, Zigbee, Smart House, smart automation system, smart home*

УДК 004.891
ГРНТИ 28.23.20

АНАЛИЗ АНСАМБЛЕВЫХ И НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ ИСКУСТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМАТИЗАЦИИ ОЦЕНКИ ЗНАНИЙ ОБУЧАЮЩИХСЯ

К. В. Белоус, Д. Г. Попугаев, А. П. Шабанов

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

В статье исследуется возможность и целесообразность использования моделей искусственного интеллекта в рамках классификации знаний обучающихся, на примере случайного леса и нейронной сети. С помощью инструментов языка программирования Python реализован набор обученных моделей с последующим их тестированием. Основываясь на значениях имеющихся метрических данных, полученных в результате проведения отладочных запусков предлагаемых моделей, представлены варианты использования такого рода систем оценивания знаний обучающихся.

машинное обучение, ансамблевое обучение, глубокое обучение, искусственный интеллект

Современные технологии искусственного интеллекта активно проникают в различные сферы жизни, включая образование. Причем роль данных технологий нисколько не преувеличена и обоснована. Основной причиной подобной тенденции является способность искусственного интеллекта упрощать и оптимизировать самые разные процессы. Так как в нынешнее время поток данных крайне высок и требует анализа и принятия решений, необходимы инструменты для автоматизации подобных процессов, помимо этого данную задачу необходимо решать постоянно и достаточно быстро. Такими инструментами и является модели искусственного интеллекта. Если рассматривать именно систему образования, то можно заметить следующую перспективу: происходит внедрение технологий в различные образовательные процессы и среды. Такой подход стал популярен относительно недавно, поэтому не так просто в образовательной системе встретить какие-либо модели машинного обучения.

Указанная выше перспектива заключается на только в автоматизации основных видов образовательной деятельности, таких как отслеживание присутствия и аттестация, или рассматриваемая в данной статье систематизация оценки знаний. Иной подход использования искусственного интеллекта подразумевает адаптацию программного обеспечения образовательного пространства к интересам конкретных субъектов образования. Адап-

тивно-персонализированный формат обучения на базе ИИ-технологий способствует формированию и развитию навыков познавательной самостоятельности субъектов образования, которые подразумевают их интеллектуальные способности и умения самостоятельно вычленять существенные и второстепенные признаки предметов, явлений и процессов. Внедрение языковых моделей на базе искусственного интеллекта оказывает своевременную поддержку обратной связи и коммуникации в ходе образовательного процесса [1].

Для указанных задач растет необходимость использования эффективных моделей искусственного интеллекта, благодаря которым будет достигнут наиболее точный результат. Широкий спектр алгоритмов и подходов позволяет на тренировочных и тестовых данных провести исследование в определении наиболее подходящего варианта среди рассматриваемых моделей.

Для дальнейшего исследования необходимо поставить саму задачу классификации знаний обучающихся. Имеется тренировочный и тестовый набор данных, полученный из онлайн-сообщества специалистов по машинному обучению Kaggle [2]. Необходимо создать модель, способную качественно определять класс студента. Любого студента можно классифицировать по оценке, то есть по целевому признаку будущей модели:

1. Традиционная система оценивания подозревает следующие оценки: «Отлично», «Хорошо», «Удовлетворительно» и «Неудовлетворительно».

2. Для бинарной системы характерно разделять студентов на тех, у которых оценка «Зачтено» или «Не зачтено».

Ранее для задачи классификации и систематизации оценки знаний обучающихся, на одних и тех же данных рассматривались такие подходы как логистическая регрессия и дерево решений. Несмотря на простоту были получены весьма неплохие результаты (табл.1) [3].

ТАБЛИЦА 1. Отчет по метрикам моделей логистической регрессии и дерева решений.

	Метрики						
Метрики / Модели	precision		recall		f1-score		accuracy
	0	1	0	1	0	1	
Логистическая регрессия	0.89	1.00	1.00	0.33	0.94	0.50	0.90
Дерево решений	0.94	1.00	1.00	0.67	0.97	0.80	0.95

В данном исследовании наилучший результат показала модель, используемая алгоритм дерева решений. Ее точность составляет 95 %, что говорит о том, что в вопросе выставления рекомендованной оценки на основе данных о посещении модель будет корректно работать. Тем не менее, даже при таких высоких показателях, стоит рассмотреть возможность достижения более высокой точности за счет изменения алгоритмов модели.

Учитывая высокий показатель модели, используемой алгоритм дерева решений, принято создать новую модель на основе ансамбля исходной. Ансамблевые модели или просто ансамбли (ensembles) представляют собой методы машинного обучения, где несколько простых моделей (часто называемых «слабыми учениками») обучаются для решения одной и той же задачи и объединяются для получения лучших результатов. Существует несколько способов построения ансамблей, в данной статье рассматривается исключительно бэггинг, то есть параллельно обучается множество одинаковых моделей, а для предсказания берется среднее по предсказаниям каждой из моделей, так как именно этот подход реализует модель случайного леса, где базовой моделью является дерево решений. В основе алгоритма лежит статистический метод, который называется бутстрэпом (bootstrap), его идея заключается в том, что генерируется k выборок размера n (бутстрэп-выборок) из исходного набора данных размера m путем случайного выбора элементов с повторениями в каждом из наблюдений (рис. 1).

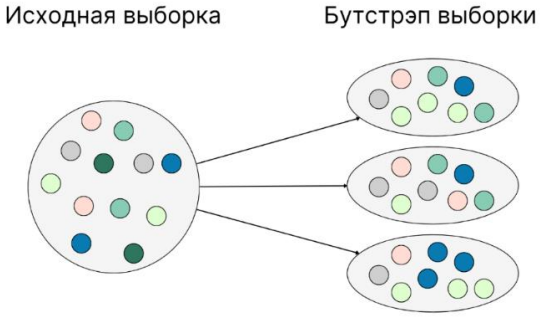


Рис. 1. Принцип разделения на bootstrap-выборки

Пусть количество объектов в наборе данных равно N, а количество признаков – M. То есть размер набора данных – (N, M). Количество деревьев в лесу равно K. Тогда для обучения случайного леса выполняются следующие шаги:

1. С помощью бутстрэпа создается K наборов данных размера (N, M).

2. Для каждого сгенерированного набора данных применяется метод случайных подпространств: выбирается $L < M$ случайных признаков и получается K новых наборов данных размером (N, L).

3. На каждом наборе данных обучается отдельное дерево решений.

Когда поступят новые данные, нам нужно будет прогнать их через каждое дерево и объединить результаты отдельных деревьев мажоритарным голосованием или путем комбинирования вероятностей.

Ниже приведена схема работы описанного алгоритма для решения задачи классификации. Для простоты лес состоит из четырех деревьев (K = 4).

На основе признаков, ранее используемых для классификации оценки знаний обучающегося с помощью дерева решений, обучена модель случайного леса. Работоспособность модели проверена на тестовых данных, оценить ее позволили метрики (табл. 2).

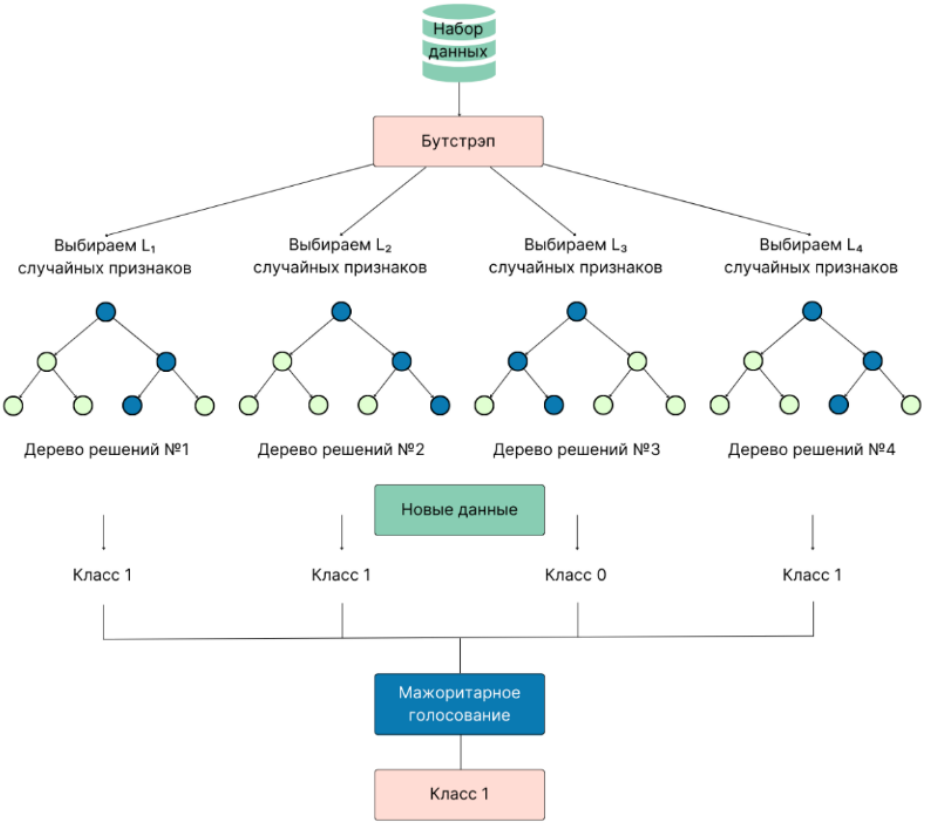


Рис. 2. Схема работы алгоритма построения случайного леса для задачи классификации

ТАБЛИЦА 2. Отчет по метрикам модели случайного леса

	Метрики						
Метрики / Модель	precision		recall		f1-score		accuracy
	0	1	0	1	0	1	
Случайный лес	1.00	1.00	1.00	1.00	1.00	1.00	1.00

Точность модели составляет 100 %. Это означает, что алгоритм безошибочно классифицирует данные, что может указывать либо на исключительно качественную обучающую выборку, либо на возможное переобучение. Для дальнейшего потенциального анализа стоит проверить модель на независимых данных, а также изменить баланс классов в выборке, так как в исходной выборке количество студентов класса 1 в разы меньше, чем студентов класса 0.

Также для сравнения рассмотрена простейшая полносвязная нейронная сеть для бинарной классификации, реализованная с помощью keras. Данная нейронная сеть имеет следующую архитектуру:

1. Входной слой, состоящий из 16 нейронов с активацией ReLU.

2. Скрытый слой, состоящий из 8 нейронов с активацией ReLU.

3. Выходной слой, состоящий из 1 нейрона с сигмоидной активацией (sigmoid).

Использование на выходном слове одного нейрона с sigmoid-активацией является стандартным, так как в результате должен быть выбран только один класс. Результаты работы сети представлены в таблице 3.

ТАБЛИЦА 3. Отчет по метрикам модели нейронной сети

	Метрики						
Метрики / Модель	precision		recall		f1-score		accuracy
	0	1	0	1	0	1	
Нейронная сеть	0.81	0.00	1.00	0.00	0.90	0.00	0.81

По полученным метрикам заметно, что модель совершенно не умеет работать с классом 1, что вероятно связано с неправильным балансом между классами, в результате чего точность данной модели достаточно низка по сравнению с ранее рассмотренными моделями.

Таким образом, была найдена наиболее оптимальная модель для поставленной задачи. Случайный лес показал высокий результат в определении класса обучающегося. Реальная ситуация может потребовать расширение списка признаков и выборки, в таком случае потребуется вносить корректировки в исходную модель.

Список используемых источников

1. Коровникова Н. А. Искусственный интеллект в образовательном пространстве: проблемы и перспективы // Социальные новации и социальные науки. М.: ИНИОН РАН, 2021. № 2. С. 98–113.
2. Student Grades Prediction Dataset [Электронный ресурс] URL: https://www.kaggle.com/datasets/sujaykapadnis/student-grades-prediction-dataset/data (дата обращения 13.12.2024).
3. Попугаев Д. Г., Шабанов А. П. Анализ моделей машинного обучения в задаче классификации оценки знаний студентов // V Всероссийская научно-техническая и научно методическая конференция магистрантов и их руководителей. Сборник лучших докладов: в 2 т. / Под ред. А. Н. Бучатского; сост. И. Е. Скалецкая. СПб.: СПбГУТ., 2025. Том 1. С. 704–708.

ANALYSIS OF MACHINE LEARNING MODELS IN THE TASK OF CLASSIFYING STUDENT KNOWLEDGE ASSESSMENT

Belous K., Popugaev D., Shabanov A.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

This article examines the feasibility of using various machine learning methods to classify students' knowledge, using the example of algorithms such as logistic regression and decision trees. Using Python programming language tools, models were trained on a training sample, and predictions made on a test sample made it possible to determine the most accurate model. Based on the values of the metrics obtained as a result of prediction, options for using such a model in the system of automated assessment of students' knowledge are proposed.

Key words: *machine learning, ensemble learning, deep learning, artificial intelligence*

УДК 654.739
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ АДАПТИВНЫХ ФИЛЬТРОВ В АНТЕННАХ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

И. А. Бойко, Н. О. Агейчик

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

В докладе представлено исследование применения адаптивных фильтров в антенных системах беспилотных авиационных комплексов. Рассмотрены основные принципы работы адаптивных фильтров, их роль в повышении помехоустойчивости и качества сигналов в условиях динамически изменяющейся электромагнитной обстановки. Проведен анализ современных алгоритмов адаптивной фильтрации, таких как LMS и RLS, и их эффективность в задачах подавления помех и улучшения характеристик антенных систем. На основе моделирования и экспериментальных данных показаны преимущества использования адаптивных фильтров для повышения точности навигации, устойчивости связи и общей производительности БАС. Результаты исследования могут быть полезны для разработчиков антенных систем и специалистов в области беспилотных технологий.

адаптивные фильтры, LMS, NLMS, RLS, БАС, эффект Доплера, среднеквадратическая ошибка

Беспилотные авиационные системы (БАС) требуют высокой помехоустойчивости антенных систем для обеспечения надежной связи и навигации. Динамические условия эксплуатации, такие как движение БАС, приводят к эффекту Доплера и изменению угла направления сигнала, что ухудшает качество принимаемых данных. Цель работы – исследование адаптивных фильтров для минимизации помех и оптимизации сигналов в антенных решетках БАС.

1. Методы исследования

1. Создание модели в MATLAB.

Разработана среда для анализа эффективности адаптивных фильтров. Исходный сигнал задан функцией:

$$d = \cos(2 * pi * f_0 * t) + j * \sin(2 * pi * f_0 * t) \quad (1)$$

где f_0=50 Гц.

В качестве помехи выступает аддитивный белый Гауссовский шум (АБГШ). Антенная система – линейная решетка из N элементов.

2. Исследуемые алгоритмы

Алгоритм LMS (Least Mean Squares). Принцип работы LMS основан на методе градиентного спуска для минимизации среднеквадратической ошибки [1].

Основные шаги на каждой итерации:

– вычисление выходного сигнала фильтра

$$y(n) = w(n) \cdot x(n), \quad (2)$$

где $w(n)$ – вектор весов фильтра, x(n) – вектор входных данных;

– расчет ошибки:

$$e(n) = d(n) - y(n), \quad (3)$$

где $d(n)$ – эталонный сигнал;

– обновление весов

$$w(n+1) = w(n) + \mu \cdot e(n) \cdot x(n), \quad (4)$$

где μ – шаг обучения (коэффициент адаптации).

NLMS (Normalized LMS) – модификация LMS с нормировкой шага обучения, что улучшает стабильность [1].

RLS (Recursive Least Squares) минимизирует взвешенную сумму квадратов ошибок с экспоненциальным забыванием старых данных [2]. Основные шаги на каждой итерации:

– вычисление коэффициента усиления Калмана[3]

$$K(n) = \frac{P(n-1) \cdot x(n)}{\lambda + x(n) \cdot P(n-1) \cdot x(n),} \quad (5)$$

где $P(n)$ – обратная корреляционная матрица, λ – коэффициент забывания ($0 < \lambda \leq 1$);

– обновление ошибки

$$e(n) = d(n) - w(n-1) \cdot x(n) \quad (6)$$

– обновление весов

$$w(n) = w(n-1) + K(n) \cdot e(n). \quad (7)$$

– обновление матрицы P:

$$P(n) = (1/\lambda) \cdot (P(n-1) - K(n) \cdot x(n) \cdot P(n-1)). \quad (8)$$

3. Исследуемые динамические параметры

– эффект Доплера (изменение частоты сигнала при движении БАС);
– изменение угла направления сигнала относительно нормали антенны.

4. Результаты

Анализ сходимости алгоритмов:

– RLS демонстрирует скорость сходимости в 2–3 раза выше, чем NLMS, при быстрых изменениях угла (рис. 1);
– NLMS сохраняет стабильность даже при ограниченных вычислительных ресурсах.

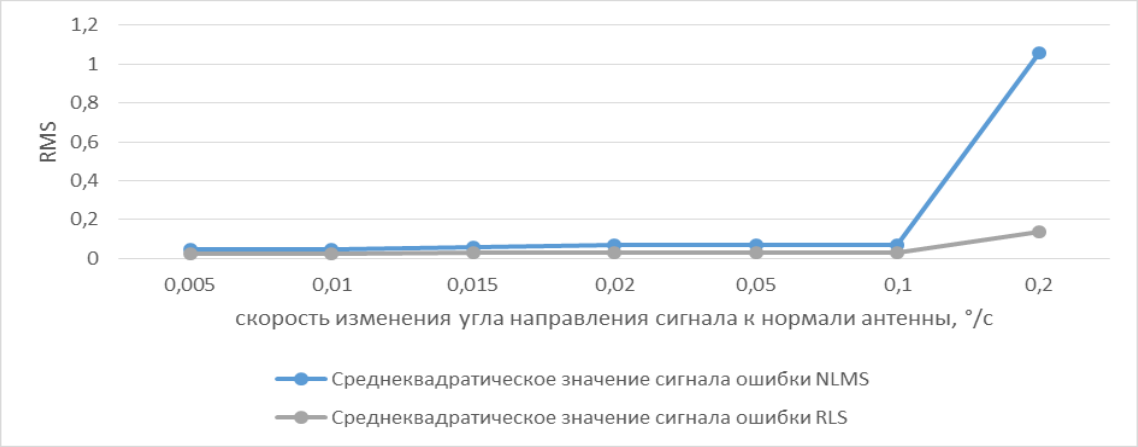


Рис. 1. Зависимость среднеквадратического значения сигнала ошибки от скорости изменения угла направления сигнала к нормали антенны.

Влияние эффекта Доплера:

При увеличении доплеровского смещения NLMS показывает на 15 % меньшее среднеквадратическое значение ошибки (RMS) по сравнению с RLS (рис. 2).

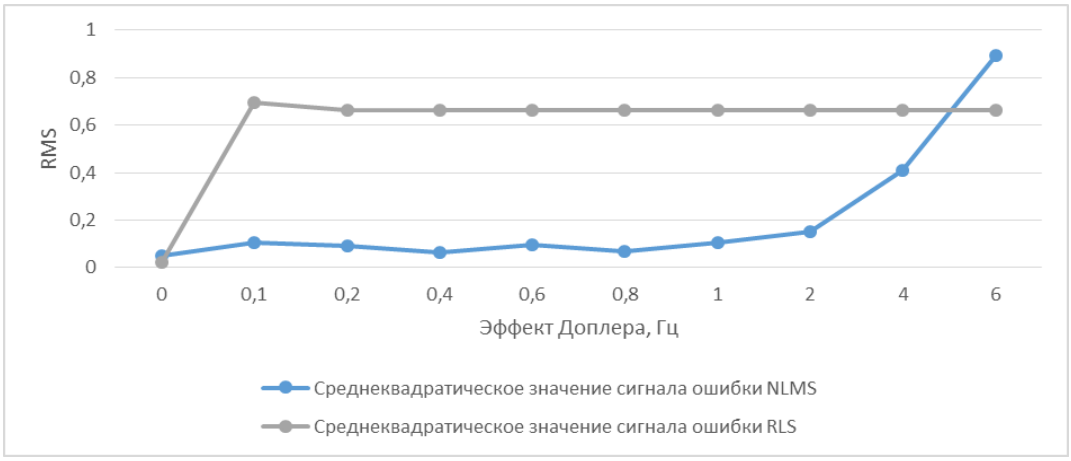


Рис. 2. Зависимость среднеквадратического значения сигнала ошибки от эффекта Доплера

5. Заключение

Алгоритм RLS демонстрирует более высокую скорость сходимости, что позволяет ему эффективнее адаптироваться к быстрым изменениям угла направления сигнала. Это приводит к меньшему среднеквадратическому значению (RMS) ошибки по сравнению с NLMS при умеренных и высоких скоростях изменения угла.

Алгоритм NLMS, несмотря на более медленную сходимость, сохраняет стабильность и требует меньше вычислительных ресурсов, что делает его предпочтительным в системах с ограниченной производительностью.

Алгоритм NLMS демонстрирует меньшие значения среднеквадратической ошибки (RMS) при увеличении эффекта Доплера.

Для работы алгоритмов RLS и NLMS в динамических системах требуется предобработка сигнала.

Проведенное исследование подтвердило эффективность адаптивных фильтров для антенных систем БАС. Алгоритм RLS рекомендован для задач с высокими динамическими требованиями, а NLMS – для энергоэффективных решений. Дальнейшая работа будет направлена на оптимизацию вычислительной сложности RLS.

Список используемых источников

1. Джиган В. Адаптивная фильтрация сигналов: теория и алгоритмы, 2022. 521 с. ISBN 978-5-94836-342-4.

2. Вечтомов В. А., Джиган В. И. Исследование характеристик алгоритмов пространственной фильтрации активных помех на основе адаптивных антенных решеток, 2022. 88 с. ISBN 978-5-7038-5838-71.

3. Солонина А.И., Цифровая обработка сигналов в зеркале MATLAB: учеб. пособие. БХВ-Петербург, 2018. 560 с. ISBN 978-5-9775-3946-3.

STUDY OF ADAPTIVE FILTERS IN ANTENNAS OF UNMANNED AERIAL SYSTEMS

Boyko I., Ageychik N.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

The report presents a study of the use of adaptive filters in antenna systems of unmanned aircraft systems (UAS). The main principles of adaptive filters, their role in increasing noise immunity and signal quality in a dynamically changing electromagnetic environment are considered. An analysis of modern adaptive filtering algorithms, such as LMS (Least Mean Squares) and RLS (Recursive Least Squares), and their effectiveness in suppressing interference and improving the characteristics of antenna systems is carried out. Based on modeling and experimental data, the advantages of using adaptive filters to improve navigation accuracy, communication stability and overall UAS performance are shown. The results of the study can be useful for developers of antenna systems and specialists in the field of unmanned technologies.

Key words: *adaptive filters, LMS, NLMS, RLS, UAS, Doppler effect, root mean square error*

УДК 654.739
ГРНТИ 49.33.29

К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ ОБУЧЕНИЯ БУДУЩИХ СПЕЦИАЛИСТОВ ФИЗИЧЕСКИМ ОСНОВАМ ЭЛЕКТРОНИКИ

С. В. Борисов[1], А. Э. Ланда[1], Ю. С. Остроумова[2], С. Д. Ханин[1], П. П. Шумаков[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Военно-медицинская академия им. С. М. Кирова

Формулируются и с дидактических и методологических позиций обосновываются рекомендации по модификации содержания и организации обучения физическим основам электроники в интересах повышения у будущих специалистов уровня обученности, обучаемости и адаптируемости. Приводятся направленные на достижение указанной цели, могущие быть использованными в практике обучения конкретные методические разработки.

обновление содержания и организации обучения, ресурсообеспечение образовательного процесса, исследовательский и проектный методы обучения

В современных условиях интенсивного изменения технологического уклада общества остро востребованными являются специалисты, способные к актуализации имеющихся знаний в целях динамичного освоения и конструктивного применения подлежащей освоению информации. Значительным потенциалом в формировании этих способностей с очевидностью обладают профессионально ориентированные физические дисциплины, такие, например, как дисциплины, посвященные физическим основам электроники в различных диапазонах частот, рассматриваемые в настоящей работе.

В этой связи возникают ставшие предметом изучения вопросы о том, насколько полно реализуется этот потенциал в практике обучения указанным дисциплинам и каковы возможности повышения его эффективности.

В научном плане проведенное в работе исследование опирается на достижения в области теории и методологии профессионального образования, в практическом плане – на опыт преподавания авторами указанных дисциплин.

В понимании выделенной в целевой установке эффективности обучения мы исходим из ее трактовки в рамках праксеологического подхода [1]

как системной совокупности обученности, обучаемости и адаптируемости в ближайшей и отдаленной перспективах.

В плане обученности основным являлся анализ в рассматриваемом аспекте содержания обучения и его информационного и материально-технического обеспечения.

Характеризуя состояние дел в части содержания обучения, нельзя не признать, что в ряде принципиально важных вопросов оно нуждается в существенном обновлении в интересах отражения передовых, имеющих перспективы дальнейшего применения достижений науки и технологий.

Учитывая имеющийся дефицит выделяемого на преподавание дисциплин учебного времени, интеграция в содержание обучения нового материала может осуществляться посредством применения развитых методических приемов расширительного анализа традиционно представляемых модельных представлений и метода аналогий [2].

Едва ли не большего внимания, чем информационный, заслуживает методологический аспект содержания обучения, необходимость его усиления в целях освоения обучающимися логико-операциональной структуры поисково-познавательной и практической деятельности.

На смену продолжающей доминировать статичной фактологии в отражении учебного материала должна прийти там, где это только возможно и оправдано, динамическая развертка содержания обучения в логике практико-ориентированного научного поиска.

Достижение указанных целей с необходимостью требует качественных изменений в учебно-информационном обеспечении образовательного процесса. Круг используемых информационных источников, наряду с традиционно рекомендуемыми учебниками и учебными пособиями, должен включать в себя авторитетные источники, отражающие наиболее значимые, имеющие потенциал дальнейшего развития достижения в изучаемой области научно-технологического развития и процесс приведшей к ней деятельности во всей ее полноте. Таковыми могут быть изданные в последнее время монографии (учебники-монографии), обзоры, базовые в решении изучаемых проблем статьи, лекции ведущих специалистов, включая Нобелевские лекции по физике, такие, например, как прекрасно адаптируемая к учебному процессу, в силу структурирования и уровня изложения, лекция Ж. И. Алферова, посвященная двойным гетероструктурам [3].

Особого внимания в плане формирования обучаемости и связанной с ней адаптируемости в результате изучения физических основ электроники

заслуживает овладение обучающимися методами получения и продуктивного применения научных знаний в конкретных их проявлениях.

Следуя дидактике и психологии образования [4, 5], в качестве средства достижения этой цели может выступать последовательное построение содержания обучения физическим дисциплинам в задачно-деятельностной форме как позволяющее придать содержанию учебного материала смысл предмета деятельности, а его освоению – ее проблемно-детерминированного, близкого к исследовательскому, осуществления, создать условия для формирования у обучающихся познавательной, имеющей тенденцию к трансформации в профессиональную, самостоятельности, проявления творческих способностей личности.

Используя разработанные в методике обучения приемы [2, 6], реализация этого подхода в практике обучения может осуществляться широкомасштабно, охватывая все виды занятий и этапы изучения подлежащей освоению информации.

Специально отметим продуктивность рассматриваемого подхода к построению содержания физического практикума, в котором могут быть востребованы и, соответственно, осваиваемы практически все выработанные в физике методы получения знаний. В качестве примера рассмотрим экспериментальное изучение концентрационного перехода «полупроводник-металл» в случайно и сильно неоднородных системах: металлодиэлектрических композитах [7, 8] и сильно легированных и компенсированных полупроводниках [9, 10]. Решение этой задачи требует применения экспериментального метода, теоретического метода, разработки физической модели, предметного и компьютерного моделирования и привлечения модельных представлений теории протекания для изыскания возможностей практических приложений.

В отношении эффективности практикума в части формирования обученности и обучаемости важно отметить необходимость оснащения учебной лаборатории современным аналитическим оборудованием, позволяющим на достаточном уровне экспериментально решать актуальные, в том числе открытые, задачи физики и технологии. Таковым является, например, сканирующий зондовый микроскоп [11]. Наряду с открываемыми возможностями приобретения умений и опыта работы на сложном оборудовании, интеграция в содержание практикума методов атомно-силовой и туннельной микроскопии целесообразна в силу наличия у обучения им значимых мотивационного и информационного ресурсов, возможности постановки и

решения ответственных задач широкого круга технологий, включая, как показывает опыт последних лет, космические технологии [12].

Принципиальное значение в плане формирования обучаемости имеет самообразование, имеющее представительный содержательный контент. В ряду прочих перед обучающимися должна ставиться задача по самостоятельному освоению на основе фундаментальных знаний содержания проблематики перспективных направлений научно-технологического развития с отвечающей приоритетам преподавания дисциплин установкой. В качестве таковой при изучении физических основ электроники должны выступать сущностное изучение физических процессов, лежащих в основе принципа действия электронных приборов, физическая картина их функционирования в рабочих режимах, связь ключевых параметров и характеристик со свойствами функциональных материалов и конструктивно-технологическими особенностями изделий.

Достижению сущностного понимания самостоятельно осваиваемого материала может способствовать применение в практике обучения технологии активного восприятия информации, предполагающей проектирование и постановку преподавателем логической цепочки вопросов, последовательные ответы на которые обеспечивают должный уровень усвоения.

Значимым, доказавшим свою продуктивность в профессиональной деятельности форматом анализа результатов самообразовательной работы является проведение семинаров. Будучи ориентированными на изучение представительной в информационном и методологическом аспектах проблематики, семинары выступают как средство критического анализа обучающимися предлагаемых ими решений. Критериями в выборе тематики семинаров должны быть широта материала, охват различных представляющих интерес физических эффектов и их применения. Пример такой тематики – физика и технология ограничителей интенсивного излучения [13], в основу принципа действия которых могут быть положены электрооптические эффекты в твердых и жидких кристаллах, акусто-, термооптические и светоиндуцированные эффекты в полупроводниках и обладающих фазовым переходом «полупроводник-металл» бистабильных материалах. Существенно, что в подготовке к такому семинару оказывается востребованными самообразование и информационно-аналитическая работа в пространстве проблем современных физики и технологии.

Важная роль в формировании обучаемости принадлежит участию обучающихся в семинарах, проводимых представителями научных и научно-

образовательных центров, выполняющих исследования и проекты на мировом уровне. Такие семинары становятся, по существу, школой освоения передовых достижений научной и инженерной мысли.

Говоря об адаптируемости, в дополнение к уже сказанному, отметим целесообразность в построении и содержании и организации процесса обучения проектного подхода, как отвечающего современной профессиональной деятельности в наукоемких областях [14].

Проектный (проектно-исследовательский) метод обучения открывает возможности выработки значимых в профессиональной деятельности способностей выявления и постановки актуальной проблемы, стратификации ее на подлежащие решению задачи, определения и ликвидации имеющегося дефицита знаний, конструктивного анализа имеющейся информации на предмет выбора (при необходимости разработки) методов и средств решения, проектирования и реализации программы исследования, критического анализа ее результатов [15, 16].

Реализация сформулированных в интересах повышения эффективности обучения физическим основам электроники рекомендаций по модификации его содержания и организации должна быть сопряжена с соответствующими изменениями в оценке качества образовательных результатов – повышением удельного веса в критериальном аппарате процессуальной характеристики, отражающей уровень мотивированности обучающихся, их погруженности в изучаемую проблематику, познавательной самостоятельности, критичности в анализе процесса получения знаний и его результатов.

Список используемых источников

1. Зуев П. В. Теоретические основы повышения эффективности обучения физике. – Дисс. … докт. пед. наук; СПб., 2000. 343 с.

2. Остроумова Ю. С. Совершенствование подготовки военно-инженерных кадров к решению наукоемких профессиональных задач: Монография. СПб.: ВАС, 2019. 240 с.

3. Алферов Ж. И. Двойные гетероструктуры: концепции и применение в физике, электронике и технологии (Нобелевские лекции по физике) // Успехи физических наук, 2002. Том 172. № 9. С. 1068-1086.

4. Сериков В. В. Педагогическая реальность и практическое знание: Монография. М.: Редакц.-изд. Дом Российского нового университета, 2018. 299 с.

5. Решетова З. А. Психологические основы профессионального образования. М.: Изд-во МГУ, 1985. 207с.

6. Ханин С. Д., Хинич И. И. Исследовательское обучение физическим основам электроники в подготовке педагогических кадров: Монография. СПб.: Изд-во РГПУ им. А. И. Герцена, 2009. 127 с.

7. Шкловский Б. И., Эфрос А. Л. Теория протекания и проводимость сильно неоднородных сред // Успехи физических наук, 1975. Т. 117. № 3. С. 401-435.

8. Харитонов Е. В. Диэлектрические материалы с неоднородной структурой. М.: Радио и связь, 1983. 128 с.

9. Бонч-Бруевич В. Л., Калашников С. Г. Физика полупроводников. М.: Наука, 1977. 672 с.

10. Шкловский Б. И., Эфрос А. Л. Электронные свойства легированных полупроводников. М.: Наука, 1979. 416 с.

11. Логинов Б. А. Новые возможности в преподавании курсов по зондовой микроскопии и нанотехнологиям // Физическое образование в вузах, 2017. Т. 23. № 4. С. 71-78.

12. Логинов Б. А., Хрипунов Ю. В., Щербина М. А., Вьюник А. О., Дмитриева В. Л., Дьякова А. А., Лебедева М. К., Макеев В. С., Первых А. Р., Шевченко Д. С., Ханин С. Д. Наблюдение изменения морфологии пленок высокотемпературных металлов в сканирующих зондовых микроскопах при прогреве в условиях открытого космоса // Наноиндустрия, 2024. Т. 17. № 2. С. 90-97.

13. Сидоров А. И. Физические основы и методы управления излучением в устройствах интегральной оптики. СПб.: Изд.-во СПбГЭТУ «ЛЭТИ», 2007. 80 с.

14. Дежина И. Г., Пономарев А. К. От науки к технологиям: новые тренды государственной политики // Инновации, 2020. Т. 40. № 1. С. 1-6.

15. Полат Е. С. Метод проектов: история и теория вопроса. Современные педагогические информационные технологии в системе образования. М.: Изд. Центр «Академия», 2010. С. 193-200.

16. Ханин С. Д., Хинич И. И. Освоение физики материалов и приборов электронной техники и проблема достижения целостности и результативности исследовательского обучения: Монография. СПб.: Изд-во РГПУ им. А.И. Герцена, 2009. 127 с.

TO THE EFFECTIVENESS INCREASING OF FUTURE SPECIALISTS TRAINING IN THE ELECTRONICS PHYSICAL BASICS

Borisov S., Landa A., Ostroumova Yu., Khanin S., Shumakov P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
Military medical academy of S. M. Kirov

Recommendations on modifying the content and organization of training in the physical basics of electronics are formulated and substantiated from didactic and methodological positions in order to increase the level of training, learnability and adaptability of future specialists. Specific methodological developments aimed at achieving this goal are presented, which can be used in the practice of teaching.

Key words: *updating the content and organization of education, resource provision of the educational process, research and project methods of teaching*

УДК 654.739
ГРНТИ 49.33.29

НАСТРОЙКА ПРЕПОДАВАНИЯ ФИЗИЧЕСКИХ ДИСЦИПЛИН НА ОБУЧЕНИЕ НАУЧНЫМ ОСНОВАМ И МЕТОДАМ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

С. В. Борисов[1], А. Э. Ланда[1], Ю. С. Остроумова[2], С. Д. Ханин[1], П. П. Шумаков[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2]Военно-медицинская академия им. С. М. Кирова

Актуализируется ориентация обучения физике на формирование способностей к получению и применению научных знаний в целях решения технологических задач. Определяются и обосновываются направления подлежащей осуществлению методической работы и реализуемые подходы к обновлению содержания и организации образовательного процесса.

образовательные ресурсы физики, задачи научно-технологического образования, ориентиры методической работы, содержание и организация обучения, методико-технологические подходы

Присущая современным условиям ориентация научных исследований и инженерных разработок на технологический прогресс [1] диктует необходимость подготовки специалистов, способных к получению и применению научных знаний в целях решения актуальных технологических задач. Особое место в такой подготовке принадлежит обучению физике как науке, являющейся ориентационной основой широкого круга современных технологий, родоначальницей методов поисково-познавательной деятельности и обладающей гигантским инженерным потенциалом.

Характеризуя в рассматриваемом аспекте существующее состояние дел, следует констатировать, что хотя в разработанной Научно-методическим советом по физике Концепции преподавания физики в качестве одной из основных его задач определяется создание базиса для освоения новых технологий [2], изучение их физических аспектов, последние до настоящего времени не получили в практике обучения должного отражения.

Сказанное предопределяет актуальность задачи настройки преподавания физики на обучение отвечающим ее компетенции научным основам и методам современных технологий, чему и посвящена настоящая работа.

Проведенный с дидактических и методологических позиций анализ состояния теории и практики обучения физике приводит к выводу о наличии в рассматриваемом аспекте ряда подлежащих разрешению противоречий, к основным из которых относятся необходимость и недостаточность: ориентации обучения физике на решение задач научно-технологического образования, соответствия его целевым установкам содержания и организации обучения, внимания к уровню сформированности у обучающихся требуемых в научно-технологической деятельности знаний и умений.

Отсюда следует, что настройка преподавания физических дисциплин на обучение научным основам и методам современных технологий с необходимостью требует изменений во всех звеньях осуществляемой педагогической системы: целеполагании, содержательном наполнении обучения, его организации, деятельности субъектов образовательного процесса, контроле его результатов.

Основными задачами подлежащей осуществлению методической работы должны служить следующие.

1. Взаимосогласованное усиление фундаментальности и практикоориентированности содержания обучения как средство преодоления его неоправданно сильного отставания от современного состояния науки и технологии и излишней академичности.

2. Целостное и системное отражение в построении и развертывании содержания процесса научно-технологической деятельности, как средство предметного обучения ее логике и методологии.

3. Создание условий для продуктивного обучения через действие как средство реализации развивающего образовательного ресурса.

4. Полномасштабное моделирование в практике обучения процесса научно-технологического решения проблемных задач как средство формирования у обучающихся умений и опыта осуществления востребованных в нем видов деятельности.

5. Актуализация в критериально-оценочной базе контроля качества образовательного процесса показателей, отражающих уровень сформированности требуемых знаний, умений и опыта.

Базируясь на достижениях теории и методике обучения физике, результатах собственных исследований в рассматриваемом проблемном поле и опыте преподавания физических дисциплин в вузах различной направленности, в работе предлагаются способствующие достижению указанных ориентиров методико-технологические подходы.

Решение первой задачи предполагает, прежде всего, обогащение информационного поля обучения физике фундаментальными знаниями, необходимыми для сущностного понимания содержания проблематики перспективных направлений научно-технологического развития. В этой связи предлагается использовать методические приемы, позволяющие осуществить органичную интеграцию нового материала в образовательный процесс с опорой на традиционно изучаемый в курсе физики материал без существенного увеличения ресурса учебного времени [3].

Выразительным примером, демонстрирующим эффективность указанных подходов, является изучение составляющих ориентировочную основу современных технологий электроники и фотоники квантовых эффектов в функциональных системах пониженной размерности, передачи электромагнитного излучения в фотонных кристаллах и элементах наноплазмоники [3, 4].

Целесообразным в плане решения второй из указанных задач методическим приемом является динамическая развертка в построении подлежащего изучению материала, осуществляемая сообразно логике и методологии научно-технологической деятельности. В процессе такой развертки должны последовательно представляться: контекст постановки и содержание изучаемой проблемы, подлежащие решению задачи, его концепция, методы и средства, достигнутые результаты, их применение и перспективы будущего развития.

В реализации указанного подхода в практике обучения следует опираться на авторитетные, раскрывающие действительный ход, приведший к значимым достижениям научно-технологической деятельности источники, такие, например, как Нобелевские лекции по физике XXI века.

Решению третьей из сформулированных задач может способствовать широкомасштабное, дидактически оправданное [5] представление содержания обучения в задачно-деятельностной форме. Будучи реализуемой в обучении, проблемность задач выступает как средство раскрытия, развития и реализации интеллектуальных и творческих способностей обучающихся.

В общем плане, использование данного методического подхода способствует достижению рекомендуемого психологией профессионального образования [6] придания учебному материалу смысла предмета деятельности, а его освоению – ее осуществления.

Сопряженным с задачно-деятельностной формой представления учебного материала является обучение методам решения проблемных задач. Та-

кое обучение может и должно охватывать методы всех ветвей современной физики: экспериментальной, теоретической и компьютерной (вычислительной). Важное место в указанном аспекте должны играть практические занятия по решению задач и лабораторный практикум при оснащении последнего современным аналитическим и технологическим оборудованием.

Особого внимания заслуживает обучение моделированию как базовому методу в объяснении, описании и прогнозировании представляющих интерес физических явлений, связующему звену между экспериментом, теорией и практикой [7-9]. Выбор опорного предметного материала должен осуществляться с учетом познавательных возможностей обучающихся. Так, для формирования способностей к построению физической картины явлений в курсе общей физики должны выбираться явления, допускающие в объяснении и описании возможность ограничиться макроскопическим подходом, а в профессионально-ориентированных физических дисциплинах главенствующая роль должна отдаваться микроскопическому подходу как позволяющему анализировать механизм явления во всей требуемой для практических приложений полноте [8, 10].

Решение четвертой из сформулированных задач предписывает необходимость опоры в организации процесса обучения на соответствующие педагогические технологии [11]. Возможности наиболее полного моделирования процесса научно-технологического решения проблемных задач открывает технология проектно-исследовательского обучения [12].

Принципиально важно, что в организованном на основе проектно-исследовательского метода обучении востребованы и, соответственно, формируются способности к основным в научно-технологическом решении задач видам деятельности: самообразованию, поиску и конструктивному анализу имеющейся по проблеме информации, проектированию и реализации программы практико-ориентированных исследований, принятию и реализации основанных на полученных знаниях практических решений, критического анализа достигнутого и приведшего к нему процесса, приобретенных знаний и опыта. Тем самым проектно-исследовательский метод организации процесса обучения выступает как средство формирования у обучающихся требуемой методологической культуры [13].

Существенную роль играет при этом использование в образовательных целях информационных технологий как средства интенсификации и интеллектуализации деятельности обучающихся [14], расширения предоставляемого информационного ресурса, обеспечения возможности решения про-

блемных задач посредством вычислительного эксперимента и компьютерного моделирования изучаемых объектов и процессов.

Необходимым условием полноценной реализации проектно-исследовательского обучения во всей ее полноте и логической завершенности является тематическое и организационное единение в образовательном процессе учебной, научной и проектной деятельности в пространстве актуальных проблем научно-технологического развития.

Наконец, в плане решения пятой из выделенных задач, требуются существенные изменения в оценочном аппарате качества результатов обучения физике, выдвижение на первый план показателей, отражающих сформированность умений получения и практического применения знаний, осуществления востребованных в научно-технологическом решении проблемных задач видов деятельности, обоснованность выбора методов и средств решения этих задач, деятельностную в нем активность.

Список используемых источников

1. Дежина И. Г., Пономарев А. К. От науки к технологиям: новые тренды государственной политики // Инновации, 2020. Т. 40. № 1. С. 1-6.

2. Бюллетень Научно-методического совета по физике. СПб.: Изд-во Политехнического Университета, 2012. № 4. С. 27-59.

3. Остроумова Ю. С., Соловьев В. Г., Ханин С. Д., Яников М. В. Формирование опыта освоения современных перспективных направлений научно-технического развития на основе фундаментальных знаний в обучении физике. Псков: Псковский государственный университет, 2015. 96 с.

4. Костарев С. В., Остроумова Ю. С., Соловьев В. Г., Ханин С. Д. Изучение перспективных направлений развития физики и технологии материалов и компонентов электроники в курсе «Специальные разделы физики» военного вуза // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник статей XIII-й Международной научно-технической и научно-методической конференции / Под ред. Р. В. Киричка. СПБ.: СПбГУТ, 2024. С. 732-735.

5. Сериков В. В. Педагогическая реальность и практическое знание: Монография. М.: Редакц.-изд. Дом Российского нового университета, 2018. 299 с.

6. Решетова З. А. Психологические основы профессионального образования. М.: Изд-во МГУ, 1985. 207с.

7. Костарев С. В., Остроумова Ю. С., Ханин С. Д. К вопросу о реализации потенциала обучения физике в интересах развития научно-технологического направления в военно-инженерном образовании // Актуальные проблемы преподавания физике в медицинских и военных вузах («Петровские чтения»). СПб.: ВМА, 2023. С.51-57.

8. Ханин С. Д., Хинич И. И. Освоение физики материалов и приборов электронной техники и проблема достижения целостности и результативности исследовательского обучения: Монография. СПб.: Изд-во РГПУ им. А.И. Герцена, 2009. 127 с.

9. Ханин С. Д., Хинич И. И. Развитие исследовательских умений соотнесения эксперимента, теории и практики в обучении физическим основам твердотельной электро-

ники // Известия Российского государственного педагогического университета. Естественные и точные науки, 2008. № 9 (48). С. 146-158.

10. Ханин С. Д., Хинич И. И. Исследовательское обучение физическим основам электроники в подготовке педагогических кадров: Монография. СПб.: Изд-во РГПУ им. А. И. Герцена, 2009. 127 с.

11. Костарев С. В., Остроумова Ю. С., Ханин С. Д. Педагогико-технологическое обеспечение профессиональной подготовки военных специалистов в контексте реализации Стратегии научно-технологического развития // Развитие военной педагогики в XXI веке: Материалы IV Международной научно-практической конференции. СПб.: ВАС, 2017. С. 128-135.

12. Костарев С. В., Остроумова Ю. С., Ханин С. Д. Практико-ориентированная проектирование педагогической системы научно-технологического образования в военно-инженерном вузе // Военная безопасность России: взгляд в будущее. Материалы 7-ой Международной межведомственной научно-практической конференции Научного отделения №10 Российской академии ракетных и артиллерийских войск. М.: 2022. Т. 1. С. 92-102.

13. Костарев С. В., Остроумова Ю. С., Ханин С. Д., Жуков В. А. Проблемно-деятельностный подход к организации учебного процесса в военном вузе как средство формирования у курсантов методологической культуры // Развитие военной педагогики в XXI веке: Материалы V Международной научно-практической конференции. СПб.: ВАС, 2018. С. 39-46.

14. Роберт И. В. Стратегические направления в развитии информационного образования в эпоху цифровых информационных технологий // Развитие военной педагогики в XXI веке: Материалы VI Международной научно-практической конференции. СПб.: ВАС, 2019. С. 31-41.

SETTING UP THE TEACHING OF PHYSICAL DISCIPLINES TO TEACH THE SCIENTIFIC FOUNDATIONS AND METHODS OF MODERN TECHNOLOGY

Borisov S., Landa A., Ostroumova Yu., Khanin S., Shumakov P.
Military medical academy of S. M. Kirov
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The orientation of physics education towards the formation of abilities to obtain and apply scientific knowledge in order to solve technological problems is being updated. The directions of the methodological work to be carried out and the approaches required for implementation in the practice of teaching to update the content and organization of the educational process are determined and justified.

Key words: *educational resources of physics, tasks of scientific and technological education, guidelines for methodological work, content and organization of training, methodological and technological approaches caching*

УДК: 538.9
ГРНТИ: 29.19.17

РАЗРАБОТКА СИСТЕМЫ РЕЦИРКУЛЯЦИИ ИЗОТОПОВ ВОДОРОДА, ОСНОВАННОЙ НА ЯВЛЕНИИ СВЕРХПРОНИЦАЕМОСТИ МЕТАЛЛИЧЕСКИХ МЕМБРАН ПО НАДТЕПЛОВЫМ ВОДОРОДНЫМ ЧАСТИЦАМ

А. О. Буснюк, С. Р. Кузенов, А. И. Лившиц, Е. Ю. Передистов, Д. А. Зайцев

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

В данной работе описана модернизация установки и приведены результаты проведенных исследований по явлению сверхпроницаемости ниобиевой мембраны по атомарному водороду в вязкостном режиме течения изотопов водорода (протий, дейтерий). Работа направлена на решение проблем топливного цикла термоядерного реактора. Модернизация установки произведена для работы в диапазоне давлений газа в придиверторной области пост-ИТЭРовских установок управляемого термоядерного синтеза. В результате исследований была определены скорости откачки сверхпроницаемой мембраны (СПМ) в различных условиях: величины потока, температуры мембраны и коэффициента атомизации.

переработка, водород, сверхпроницаемость, мембрана

Введение

Исследования управляемого термоядерного синтеза за последние годы достигли значительного прогресса. Множество научных центров и институтов по всему миру решают технологические и инженерные задачи, связанные с контролем и поддержанием термоядерной реакции. Одна из многих задач, стоящих перед учеными, является необходимость избегать чрезмерных запасов трития [1]. В термоядерном синтезе только небольшая часть дейтерия (D) и трития (T) подвергается синтезу, что требует извлечения несгоревшей DT смеси из плазмы [2]. Считается, что обработка топлива и необходимая установка по производству трития вносят наибольший вклад в капитальные затраты в термоядерном синтезе [3]. Концепция короткоциклового рециклинга может решить проблему, обойдя тритиевую установку. Короткоцикловой рециклинг – это концепция извлечения дейтерия и трития вблизи выхлопа тора и непосредственный возврат очищенных изотопов во-

дорода обратно в тор, минуя тритиевый завод, тем самым значительно сократив запасы трития. Данный процесс возможен с применением насоса, основанного на сверхпроницаемой мембране [4]. Этот насос использует эффект сверхпроводимости для отделения большого количества дейтерия и трития. Сверхпроницаемость достигается за счет образования надтепловых частиц водорода, которые проходят через тонкую металлическую мембрану. Надтепловые частицы водорода напрямую поглощаются фольгой, минуя процессы адсорбции и десорбции, приводя к существенному увеличению растворимости относительно ожиданий закона Сивертса [4, 5]. Из этого следует, насосы СПМ могут функционировать в условиях давлений, адаптированном к условиям дивертора, с расчетным значением ~ 10Па [6, 7]. Важный фактор в механизме сверхпроницаемости заключается в поверхностном ограничении проникновения водорода через металлическую фольгу и подаче надтеплового водорода вверх по потоку (рис. 1).

Надтепловой означает возбужденный выше тепловой энергии частицы в газовой фазе. Данное состояние обозначено цифрой 1, может быть задано внешним источником энергии. Надтепловые частицы водорода с градиентом энергий могут сталкиваться с фольгой, обозначено цифрой 2. Этап 3 представляет собой процессы поверхностного взаимодействия надтепловых частиц. Данные процессы зависят от качества поверхности СПМ. Как только водород проникает в объем СПМ, он диффундирует вперед и назад через кристаллическую решетку из-за процесса случайного блуждания, этап 4. В итоге, он высвобождается в газовую фазу, после нахождения пути к поверхности и рекомбинирует с другими атомами водорода на этапе 5 [0].

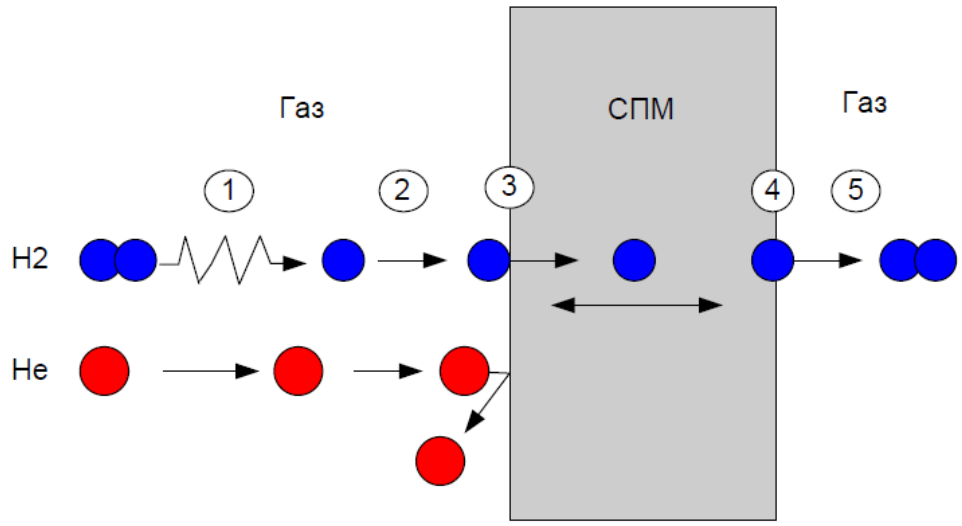


Рис. 1. Этапы частицы водорода и гелия в процессе сверхпроницаемости

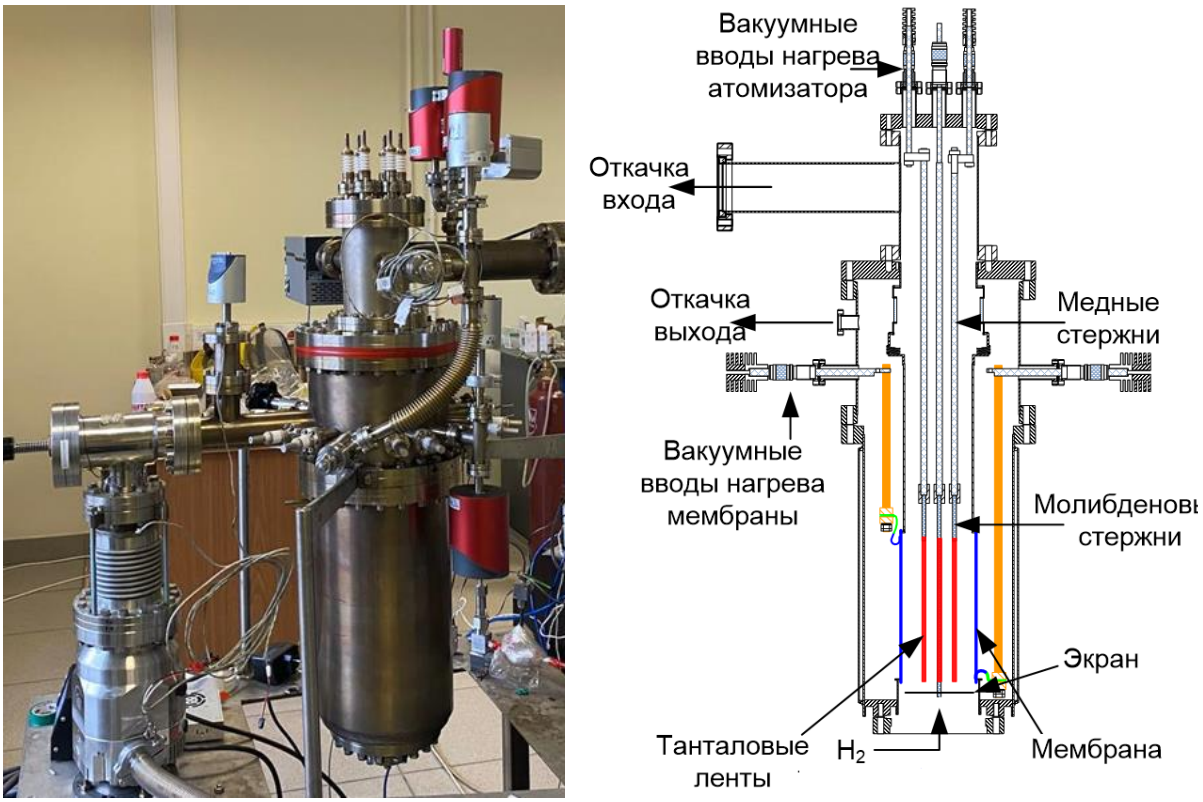
Рекомбинация может произойти по обе стороны СПМ. Вероятность зависит от соотношения энергетических барьеров с обеих сторон. Эта вероятность всегда больше вероятности диффузионного проникновения. После того, как молекула водорода высвобождается на стороне нисходящего потока в виде тепловой молекулы, ее вероятность снова адсорбироваться решеткой на несколько порядков меньше по сравнению с исходным надтепловым водородом [5, 7]. Это обеспечивает эффективную откачку. СПМ пропускают только водород и его изотопы, что делает их прекрасным инструментом для отделения примесей из потока газовой смеси.

Эксперимент

Экспериментальная установка

Испытания по исследованию СПМ проводились на экспериментальной установке СУПМЕМ-1М. Данная установка позволяет проводить исследования СПМ при вязкостном режиме течения газов. Общая фотография и схема установки приведены на рисунках 2а и 2б соответственно. Мембрана с эффективной площадью проницаемости ~ 600 см^2, герметично разделяет установку на два объема, входной и выходной. Мембрана сделана из 100 мкм листа Nb [7]. Для эффективной атомизации водорода и его изотопов были предусмотрены три пары атомизаторов, изготовленных из танталовых лент, толщиной 200 мкм. Каждая из пар атомизаторов нагревается независимо, что дает возможность исследовать производительность и скорость откачки СПМ как от температуры атомизаторов, так и от площади. Давление во входной и выходной камере измерялось мембранно-емкостными датчиками, покрывающими диапазон измерений от 10^{-5} Торр до 10 Торр. Поток газа задавался двумя электронными регуляторами массового расхода газа, с диапазоном изменения потока 0 – 100 см^3/м.

Произведена модернизация установки для проведения исследований в диапазоне давлений газа в придиверторной области пост-ИТЭРовских установок управляемого термоядерного синтеза. Установлено оборудование для проведения исследований при высоких давлениях и регистрации состава газа по средству анализатора остаточных газов.



а) б)

Рис. 2. а) общий вид установки; б) схема установки

Методика эксперимента

В ходе эксперимента СПМ непрерывно подогревается током 500 А. В процессе напуска во входной объем чистого H2, устанавливается давление 0.00177 Торр (рис. 3). После установления равновесия, в 16:41 уменьшилась скорость откачки насоса, в следствии чего давление на входе увеличилось до 0.006 Торр. В 16:45 на две пары атомизаторов подается ток по 60 А, в этот же момент ток на мембране снижается до 0 А. Давление на входе в данный момент составляет $3*10^{-4}$ Торр, а на входе давление увеличивается с 0 до 0.0042 Торр. После установления равновесия, с 16:57 на вход ступенчато напускается поток Не. Начальный поток составляет 1 $см^3$/мин, конечный поток составляет 100 $см^3$/мин. Далее поток не прекращался, для установления повторного уровня скорости откачки СПМ.

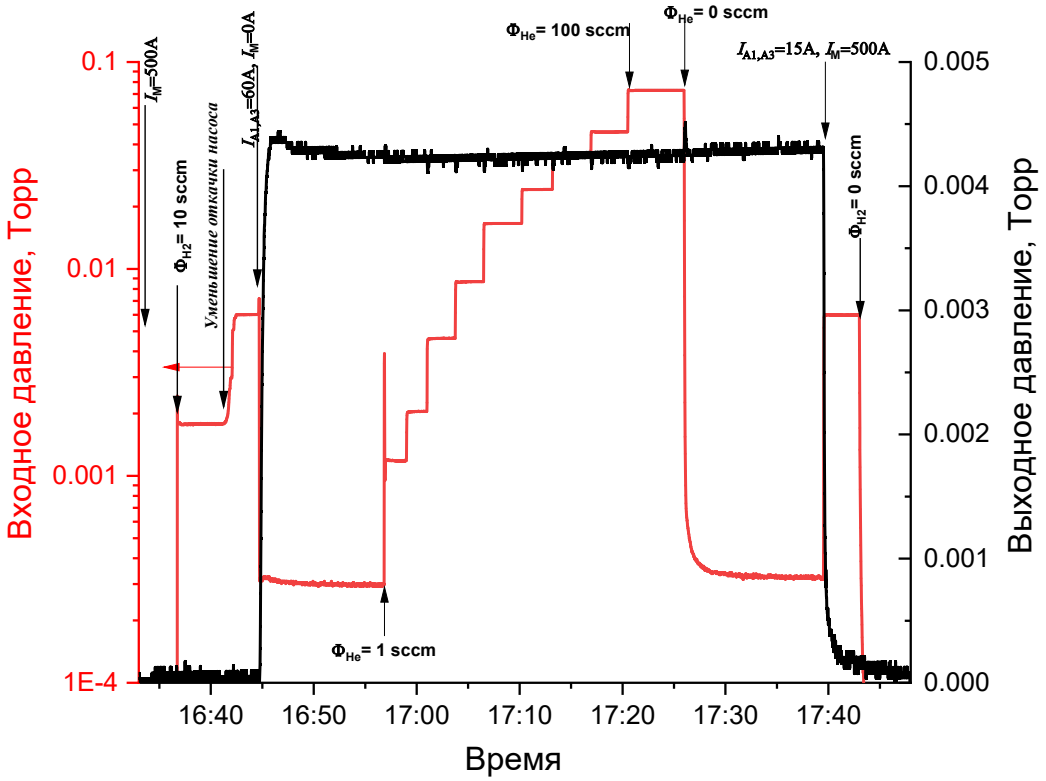


Рис. 3. Изменение входного и выходного давлений

Результаты

Стоит обратить внимание на высокую эффективность откачки водорода СПМ, которая при указанных выше условиях составила ~ 500 л\с. Выбранная Nb мембрана обладает 100 % селективность по водороду. Установлено отсутствует влияние гелия на работу системы мембранной откачки. Данный эффект можно заметить по стабильному выходному давлению при изменяющиеся потоке He. СПМ может использоваться, как высокоэффективное средство откачки и разделения смеси газов в пост-ИТЭРовских установках управляемого термоядерного синтеза (УТС). Проведенные эксперименты доказывают возможное использование насосов, основанных на СПМ в придиверторной области, например в токамаке с реакторными технологиями, для откачки и разделения смеси D/T+He из зоны реактора.

Список используемых источников

1. Peters B. J., Hanke S., C Day., Metal foil pump performance aspects in view of the implementation of direct internal recycling for future fusion fuel cycles // Fusion Eng. Des. 136 (2018) 1467–1471.

2. Chao Li, J. Douglas Way, Thomas F. Fuerst and Colin A. Wolden, The impact of helium on plasma-driven hydrogen permeation and implications for direct internal recycling in the fusion fuel cycle // Nuclear Fusion 65-016039, 2024.

3. Woodruff S., Miller R., Chan D., Routh S., Basu S. and Rao S. // Conceptual cost study for a fusion power plant based on four technologies from the DOE ARPA-E ALPHA Program, 2017.

4. Livshits A. I., Notkin M. E., Samartsev A. A., Physico-chemical origin of superpermeability – large-scale effects of surface chemistry on “hot” hydrogen permeation and absorption in metals // J. Nucl. Mater. 170 (1990) 79–94.

5. Livshits A. I., Notkin M. E., Pistunovich V. I., Bacal M. and Busnyuk A. O. Superpermeability: critical points for applications in fusion // J. Nucl. Mater. 220–2 259–63.

6. Peters B.J. Development of a hydrogen-selective vacuum pump on the basis of superpermeation // Entwicklung einer auf Superpermeation basierenden, wasserstoffselektiven Vakuumpumpe PhD, Thesis Karlsruher Institut für Technologie, 2020.

4. Передистов Е. Ю., Буснюк А. О., Алимов В. Н., Кузенов С. Р., Лившиц А. И., Демонстрация возможности селективной откачки D/T-смеси в установках управляемого термоядерного синтеза с помощью сверхпроницаемых мембран // Письма в Журнал технической физики. 2024. Т. 50. № 2. С. 44-46.

DEVELOPMENT OF A HYDROGEN RECYCLING SYSTEM BASED ON THE PHENOMENON OF SUPERPERMEABILITY OF METAL MEMBRANES FOR SUPRATHERMAL HYDROGEN PARTICLES

Livshits A., Busnyuk A., Kuzenov S., Peredistov E., Zaitsev D.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

This article describes the modernization of the installation and presents the results of the studies on the phenomenon of superpermeability of the niobium membrane for atomic hydrogen in the viscous flow mode of hydrogen isotopes (protium, deuterium). The work is aimed at solving the problems of the fuel cycle of a thermonuclear reactor. The installation was modernized for operation in the range of gas pressures in the near-diverter region of post-ITER controlled thermonuclear fusion installations. As a result of the studies, the pumping rates of the superpermeable membrane were determined under various conditions: flow rates, membrane temperatures and atomization coefficients.

Key worlds*: recycling, hydrogen, superpermeability, the membrane*

УДК 621.317.799 + 004.421
ГРНТИ 59.14.21

УСТРОЙСТВО ДЛЯ АВТОМАТИЗИРОВАННОГО КОНТРОЛЯ ТОКСИЧНОСТИ БИОЛОГИЧЕСКИХ ЖИДКИХ ДИСПЕРСНЫХ СРЕД

А. В. Ваганов

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

Рассматривается устройство для автоматизированного контроля токсичности внутренних сред организма. Данная система может найти применение как в составе комплексного стационарного обследования человека, так и для оперативной оценки его состояния в полевых условиях. Устройство реализовано в виде аппаратно-программной системы с использованием динамически программируемых дискретно-аналоговых сигнальных процессоров и программируемой логики.

токсичность, тест-объект, автоматизированный контроль, аппаратно-программная система.

Стремительное развитие прогресса во всем мире предполагает появление различных новых веществ и их соединений, многие из которых могут обладать токсичностью. Под токсичностью следует понимать возможность того или иного агента оказывать негативное действие на живое, в том числе организм человека. В связи с этим современная токсикология получила активное развитие. Область ее исследований весьма разнообразна: промышленность (новые материалы и вещества с целью экспертизы технологий их получения или очистки), пищевой индустрии (молочные продукты, соки, масла, детское питание и т. п.), экологии (почвы, сточные воды предприятий), косметологии (гели, мази, крема) [1, 2].

Отдельной областью науки, изучающей токсические свойства химических веществ, выступает медицинская токсикология. Предметом ее исследований являются: цельная кровь, ее плазма или сыворотка, а также лимфа и ликвор и т. п. Данные исследования связаны с контролем эндогенной интоксикации (ЭИ) – патологического процесса, способствующего накоплению в опасных концентрациях веществ, оказывающих весьма негативное влияние на общее состояние живого организма.

ЭИ присутствует при очень разнообразных заболеваниях человека, а ее результаты воздействия на организм могут быть очень опасными и даже фа-

тальными, поэтому изучение появления и развития ЭИ путем контроля токсичности биологических жидких дисперсных сред (БЖДС) является важной задачей для современного общества.

Для анализа различных веществ и соединений используют передовые методы аналитической химии, однако их применение для контроля эндотоксикоза имеет определенные ограничения, которые заключаются в невозможности формирования интегральной оценки воздействия на организм сразу нескольких вредных веществ одновременно.

Для устранения указанного недостатка применяют биотестирование, где в роли чувствительного «сенсора» выступают живые микроорганизмы (тест-объекты), например, инфузории. В качестве тест-реакции обычно рассматривают либо сокращение прироста клеток инфузорий в тестируемой пробе по отношению к контрольной (нетоксичной) за определенный временной интервал, либо время их полной гибели – LE_{100}. Последний вид тест-реакции наиболее экспрессным.

К настоящему моменту существует множество различных методов определения концентрации живых (подвижных) микроорганизмов в исследуемой пробе, однако все они имеют определенные недостатки: высокая трудоемкость и низкая точность (микроскопный счет), невозможность дифференцирования живых и неживых клеток (кондуктометрия), сложность методики пробоподготовки (биохемолюминесценция) и проведения исследования (лазерная корреляционная спектроскопия), дороговизна оборудования и избыточность получаемой информации (телевизионные методы).

Для исследования токсичности водных сред с применением в качестве тест-объекта инфузорий был разработан прибор «Биотестер-2М», однако его использование для контроля токсичности БЖДС имело существенные ограничения: сравнительно большой объем исследуемой пробы, неприспособленность к работе с мутными средами и т. п.

В работе [3] описан концентратомер подвижных инфузорий, предназначенный для реализации метода автоматизированного контроля токсичности БЖДС, основанный на тест-реакции «гибель инфузорий». Формула изобретения рассматриваемого концетратомера описана в патенте [4].

Из рис. 1 показан возможный вариант реализации устройства автоматизированного контроля токсичности (УАКТ) биосред.

Устройство реализовано в виде аппаратно-программной системы, состоящей из импульсного фотометра-турбидиметра высокого амплитудного разрешения и блока, реализующего выявление тест-реакции простейших на

основе двухстороннего непараметрического двухступенчатого контрастного метода обнаружения сигналов, обеспечивающего постоянство уровня вероятности ложных тревог, даже если вид распределения сигнала от тест-объекта на выходе ОП отличен от нормального [5].

Работает устройство следующим образом: сфокусированный световой поток от матричного источника излучения (ИИ), одновременно проходя через каждую ячейку 96-луночного планшета, поступает на соответствующий оптоэлектронный преобразователь (ОП), формируя на его выходе электрический сигнал в диапазоне частот Δf с амплитудой $U(t)$, поступающий в центральный блок обработки (ЦБО).

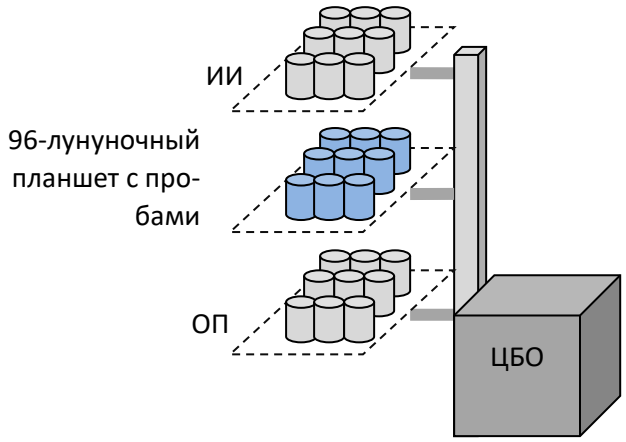


Рис. 1. Устройство автоматизированного контроля токсичности БЖДС

Обобщенная структурная схема ЦБО показана на рис. 2. Она включает в себя: ИИ – матричный источник излучения, Кв – термостатируемые кюветы (ячейки 96-луночного планшета), ОП – матричный оптоэлектронный преобразователь, БСТ – блок стабилизатора температуры кюветы (термостата), БФ – блок частотных фильтров, АРУ – автоматический регулируемый усилитель, БСО – блок статистической обработки, МК – микроконтроллер и индикатор.

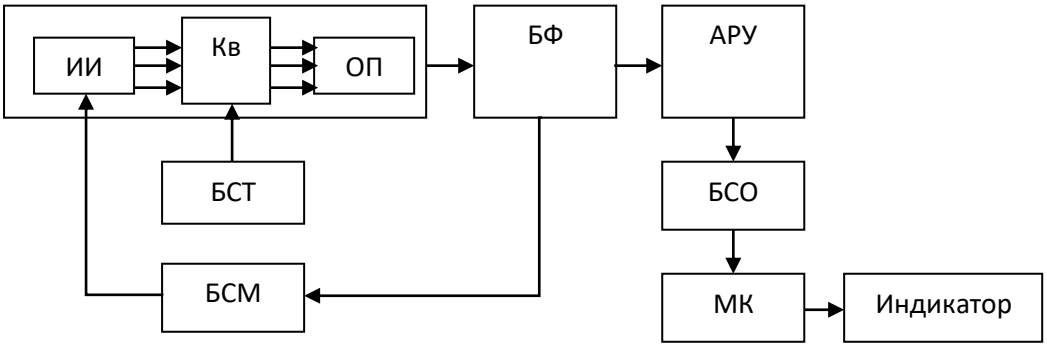


Рис. 2. Структурная схема ЦБО

Сформированный в ОП сигнал после прохождения полосовых фильтров и шумового АРУ поступает в БСО, в котором производится выявление совокупной тест-реакции популяции инфузорий путем проверки выполнения решающего правила «не менее k из n» :

$$U_{бco} = \begin{cases} 0, \; H_0^*: \left(\frac{k_{фл}}{n_{фл}}\right)_{мин} < \left(\frac{k_{фл}}{n_{фл}}\right)_{изм} \\ 1, \; H_1^*: \left(\frac{k_{фл}}{n_{фл}}\right)_{мин} \geq \left(\frac{k_{фл}}{n_{фл}}\right)_{изм} \end{cases}, (1)$$

где $(k_{фл} / n_{фл})_{мин}$ и $(k_{фл} / n_{фл})_{изм}$ – минимальное (пороговое) и измеряемое отношения текущего к максимально возможному количеству флуктуаций сигнала на выходе ОП за время наблюдения от перемещения нормально подвижных (живых) инфузорий в каждой измерительной кювете 96-луночного планшета, определяемое вероятностью ложного обнаружения данных флуктуаций F.

Алгоритм работы ЦБО для каждой i-ой ячейки 69-луночного планшета устройства автоматизированного контроля токсичности БЖДС показан на рис. 3.

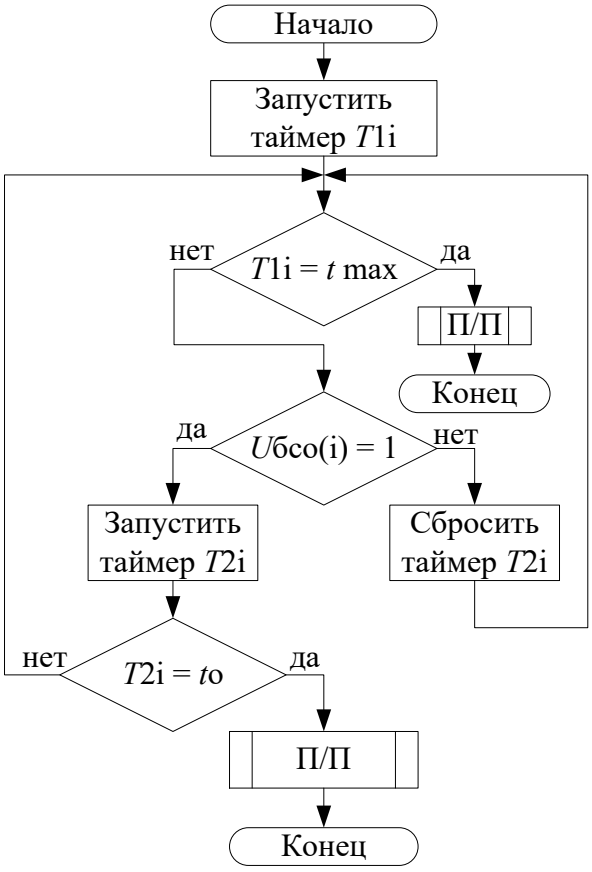


Рис. 3. Алгоритм работы i-ой кюветы устройства для автоматизированного контроля токсичности БЖДС

В ходе выполнения данного алгоритма производится отсчет общего времени исследования ($T1_i$) и времени ($T2_i$), прошедшего с момента фиксации альтернативной гипотезы согласно зависимости 1. В случае выполнения условий: $T1_i = t_{\max}$ и(или) $T2_i = 3 \cdot (n_{фл}/\Delta f) = t$о происходит переход в подпрограмму, которая фиксирует время ($T1_i$), прошедшее с начала исследования, и инициирует зажигание соответствующего светодиода на индикаторе устройства согласно следующим условиям (время в минутах): $T1_i \leq 10{,}5$ (I ст. ЭИ); $10{,}5 < T1_i \leq 13$ (II ст. ЭИ); $13 < T1_i \leq 17$ (III ст. ЭИ); 18-20 $< T1_i$ (ЭИ отсутствует) [6]. Таким образом, максимальное время исследования ($t_{\max}$) не превышает 18-20 минут.

Реализация ЦБО рассматриваемого УАКТ возможна различными способами, однако его построение с использованием динамически программируемых аналоговых сигнальных процессоров (*dpASP*) имеет неоспоримые преимущества: во-первых, указанные микросхемы позволяют упростить разработку и отладку устройства в целом, а во-вторых, повысить точность и стабильность проводимых исследований [7].

Предложенное устройство автоматизированного контроля токсичности БЖДС может быть использовано как в стационарных медицинских учреждениях, так и стать частью мобильной (выездной) лаборатории.

Список используемых источников

1. Смирнова В. М. Токсикология: промышленные и экологические аспекты: учеб. пособие / В.М. Смирнова [и др.]; Нижегород. гос. техн. ун-т им. Р. Е. Алексеева. Нижний Новгород, 2019. 240 с.

2. Папий Н. А., Папий Т. Н. Медицинская косметология: Руководство для врачей – 2-е изд., испр. и доп. М.: ООО «Издательство «Медицинское информационное агентство», 2013. 600 с.

3. Ваганов А. В. Автоматизированная система контроля токсичности биологических жидких дисперсных сред на основе динамически программируемого аналогового сигнального процессора // Известия СПбГЭТУ «ЛЭТИ» СПб.: СПбГЭТУ «ЛЭТИ», 2017. № 7. С. 74-79.

4. Ваганов А. В. Концентратомер подвижных инфузорий в жидких средах. Пат. 2650424 Российская Федерация; заявитель и патентообладатель СПб., АО «Концерн «Океанприбор» – № 2017106399; заявл. 13.04.2018; опубл. 27.02.2017.

5. Ваганов А. В. Непараметрический обнаружитель двигательной активности инфузорий в биологических жидких дисперсных средах на основе dpASP // Известия СПбГЭТУ «ЛЭТИ» СПб.: СПбГЭТУ «ЛЭТИ», 2017. № 9. С. 78-83.

6. Мельников В. Л., Матросов М. Г. Острая почечная и печеночная недостаточность. Синдром эндогенной интоксикации: учеб. пособие / Пензенский государственный университет медицинский институт кафедра ТО и ВЭМ курс "Экстремальная и военная медицина". Пенза, 2003. 32 с.

7. Полищук А. Программируемые аналоговые интегральные схемы Anadigm. Часть 1. Структура и характеристики. СПб.: Компоненты и технологии, 2005. № 1. С. 29-35.

DEVICE FOR AUTOMATED TOXICITY CONTROL OF BIOLOGICAL LIQUID DISPERSED MEDIA

Vaganov A.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

A device for automated control of the toxicity of the body's internal environment is being considered. This system can be used both as part of a comprehensive inpatient examination of a person and for an operational assessment of his condition in the field. The device is implemented as a hardware and software system using dynamically programmable digital-analog signal processors and programmable logic.

Key words: *toxicity, test object, automated control, hardware and software system*

УДК 004.946
ГРНТИ 28.17.33

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С МИКРОСЕРВИСНОЙ АРХИТЕКТУРОЙ ДЛЯ ОПРЕДЕЛЕНИЯ ДОПУСТИМЫХ ОБЛАСТЕЙ РАЗМЕЩЕНИЯ ТЕХНИЧЕСКИХ ОБЪЕКТОВ НА ОСНОВЕ АНАЛИЗА ГЕОДАННЫХ

Г. В. Верхова, А. А. Пермяков

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

Представлены результаты разработки и программной реализации алгоритма определения допустимых зон размещения мобильных узлов связи. В роли источника данных выступил некоммерческий картографический веб-сервис OpenStreetMap. Используя геоинформацию, представленную в формате GeoJSON, разработанный алгоритм определяет допустимые зоны размещения с учетом рельефа местности, грунта и возможности подъезда мобильного узла связи, размещенного на шасси грузового автомобиля повышенной проходимости. Помимо рассмотренного алгоритма было разработано программно-алгоритмическое обеспечение для импорта геоданных из OpenStreetMap по заданному ограничивающему прямоугольнику. Приведены результаты анализа разработанного алгоритма. Рассмотрены дальнейшие пути исследований.

геоданные, оптимизация, технический объект, микросервисная архитектура, масштабируемость, полигон, мультиполигон, геопространственный анализ

В современных условиях, когда требования к размещению технических объектов становятся все более жесткими и зависят от множества факторов, включая географические и инфраструктурные ограничения, задача определения допустимых зон для размещения таких объектов становится особенно актуальной. При размещении мобильных узлов связи, а также других технических установок необходимо учитывать как характеристики площадки, на которых будут размещены объекты, так и доступность этих участков, включая наличие дорог, топографические особенности и плотность застройки. При решении таких задач обычно используются поисковые алгоритмы, которые требуют жесткого задания допустимых областей размещения технических объектов. Целью данной статьи является изложение результатов разработки программно-алгоритмического обеспечения для определения допустимых зон размещения технических объектов на основе анализа геоданных, полученных из геоинформационной системы OpenStreetMap.

Разработанная система написана на языке программирования C#, который предоставляет широкий функционал для работы с многозадачностью, сетевыми протоколами и обработкой данных. Работа с географическими данными реализована на базе библиотеки NetTopologySuite, которая представляет собой мощный инструмент для анализа и обработки пространственных данных, представленных полигонами, линиями и точками. NetTopologySuite предоставляет удобные средства для выполнения операций с метрическими данными, включая пересечения, объединение, проверку на принадлежность точек к многоугольникам, а также других операций клипирования, которые необходимы для решения задачи выделения доступных для размещения технических объектов территорий.

Newtonsoft.Json используется для работы с форматом JSON, что позволяет удобно сериализовать и десериализовать данные при информационном обмене между микросервисами. Одной из важных особенностей системы является использование Overpass API для получения данных из открытого картографического веб-ресурса OpenStreetMap, что позволяет получить актуальные и детализированные географические объекты, такие как дороги, здания, леса и другие элементы, учет которых необходим при пространственном анализе и определении допустимых зон для размещения технических объектов.

Процесс определения допустимых зон размещения технических объектов состоит из нескольких шагов.

Шаг 1. Из OpenStreetMap импортируем данные о зонах, на которых могут быть размещены технические объекты (рис. 1).



Рис. 1. Начальные данные, полученные из OpenStreetMap с помощью модуля импорта

Шаг 2. Определяем зоны, которые пересекаются с основными магистралями (рис. 2), что необходимо для обеспечения к ним подъезда.



Рис. 2. Результаты определение исходной допустимой зоны после первой итерации

Шаг 3. Расширяем допустимые зоны, путем нахождения второстепенных дорог, пересекающих зоны, полученные на шаге 2, и нахождение зон, которые могут быть доступны с помощью этих второстепенных дорог (рис. 3). Данный процесс повторяется до тех пор, пока не будут определены все доступные зоны.



Рис. 3. Результаты определение исходной допустимой зоны после первой итерации

Разработанное программное обеспечение является первым шагом на пути решения задачи размещения мобильных узлов связи с помощью поисковых методов. Для этих целей могут быть использованы генетические алгоритмы [1-2], которые совместно с задачами выделения допустимых зон размещения узлов связи и расчета радиотрасс, могут быть инкапсулированы в рамках интегративной геоинформационной модели [3].

Список используемых источников

1. Algorithm I. U. E., Neretina K. A., Pechurin V. V. The spatial configuration optimization of real-time positioning systems using a genetic algorithm // В сборнике: Радиолокация, навигация, связь. Сборник трудов XXX Международной научно-технической конференции. В 5-ти томах. Воронеж, 2024. С. 205-212.
2. Горбийчук М. И., Пашковский Б. В. Оптимизация параллельного алгоритма синтеза модели оптимальной сложности на принципах генетических алгоритмов // Компьютерные науки и телекоммуникации. 2016. № 1 (47). С. 23-34.
3. Akimov S. V., Verkhova G. V. The four-level integrative model methodology of structural and parametric synthesis of system objects // В сборнике: Proceedings of the 19th International Conference on Soft Computing and Measurements, SCM 2016. 2016. С. 321-323.

DEVELOPMENT OF SOFTWARE WITH MICROSERVICE ARCHITECTURE FOR DETERMINING ACCEPTABLE AREAS FOR PLACEMENT OF TECHNICAL OBJECTS BASED ON GEODATA ANALYSIS

Verkhova G., Permiakov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the results of development and software implementation of the algorithm for determining the permissible zones for placement of mobile communication nodes. The non-commercial cartographic web service OpenStreetMap served as a data source. Using geoinformation presented in GeoJSON format, the developed algorithm determines the permissible zones for placement taking into account the terrain, soil and the possibility of access of a mobile communication node placed on the chassis of a cross-country truck. In addition to the considered algorithm, software and algorithmic support was developed for importing geodata from OpenStreetMap using a specified bounding rectangle. The results of the analysis of the developed algorithm are presented. Further research directions are considered.

Key words: *geodata, optimization, technical object, microservice architecture, scalability, polygon, multipolygon, geospatial analysis*

УДК 004.891
ГРНТИ 28.23.35

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ БОЛЬШОЙ ЯЗЫКОВОЙ МОДЕЛИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ПРОСТРАНСТВЕННОГО АНАЛИЗА

Верхова Г. В., Чернышов А. С.

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

Одной из проблем, возникающих при создании инфраструктуры пространственных данных, является формирование многоаспектных моделей геосистем, включая учет отношений между отдельными геосистемами, на основании информации, полученной из разных источников. Решение данной проблемы не является тривиальным, так как информация о разных аспектах геосистем представлена в различных источниках, часто слабо структурированных, и не позволяющих выполнить идентификацию объектов классическими методами информационных технологий. В статье приведены результаты исследований в области возможностей и сценариев применения большой языковой модели для решения задач пространственного анализа, включая формирование пространственных баз знаний на базе многоаспектных геоинформационных моделей.

геосистемы, многоаспектные модели, искусственный интеллект, языковые модели

В настоящее время большие языковые модели (Large Language Models или LLM), основанные на нейронных сетях, стали ключевым направлением развития искусственного интеллекта [1]. Изначально целью создания больших языковых моделей было формирование базы знаний с последующей генерация на ее основе осмысленных ответов в процессе взаимодействии с пользователем. Недавние исследования показали, что большие языковые модели способны не только обрабатывать информацию, но и генерировать управляющие воздействия, что позволяет им функционировать в роли автономных агентов, которые могут воспринимать окружающую среду, принимать решения и выполнять действия в различных контекстах.

Одной из наиболее перспективных областей применения LLM является пространственный анализ, который включает обработку и интерпретацию географической информации. Такие модели обучались на огромных массивах данных [2], например, ChatGPT-3 использует 570 гигабайт текстовой информации [3], что позволяет хранить знания о множестве географических объектов и их характеристиках. Следует учитывать, что такие модели формируют свои выводы на основе текстовых данных, а не на основе строгих

географических принципов и взаимосвязей между географическими объектами, но тем не менее, LLM могут использоваться при заполнении геоинформационных систем данными, используя информации о местоположении объектов, их размерах, координатах и взаимосвязях.

Эффективное использование LLM в геоинформационных системах подразумевает решение трех ключевых задач: 1) идентификации геообъектов, 2) определения отношений между ними и 3) идентификации их геометрии. Отсутствие точной идентификации геообъектов затрудняет классификацию объектов на местности, что негативно сказывается на качестве анализа и принятия решений. Такая ситуация приводит к созданию устаревших или неточных карт и баз данных, что может иметь серьезные последствия в таких областях, как экология, градостроительство и управление ресурсами. Недостаток информации о взаимосвязях и зависимостях между различными геообъектами усложняет анализ пространственных взаимодействий, без учета которых невозможно эффективное планирование и управление ресурсами, особенно в ситуациях, связанных с природными катастрофами или развитием инфраструктуры природно-техногенных геосистем. Отсутствие точной идентификации геометрии объектов ограничивает возможности моделирования, что создает трудности при выполнении пространственного анализа.

Извлечение информации из языковой модели осуществляется с помощью специальных запросов (промптов) [4], позволяющих точно идентифицировать геоинформационный объект. Корректировка результата может осуществляться через изменение промпта или настройку параметров модели, таких как temperature, sampling (Top-p и Top-k), а также штрафы за частоту и присутствие [5]. Промпт реализуется в виде шаблона в программном коде, который подставляет нужный контекст для получения желаемого результата. Использование контекстной информации помогает модели различать географические объекты, имеющие одинаковое имя, но при этом являющиеся различными объектами (например, Ленинский проспект в Санкт-Петербурге и в Москве).

Рассмотрим функциональные возможности LLM на примере анализа административно-территориального деления Санкт-Петербурга. В качестве интерфейса для взаимодействия с языковой моделью используется библиотека transformers [6] для языка Python. С целью получения результатов используется запрос на естественном языке к модели Phi-4-bnb-4bit [7] с дополнительным системным промптом, позволяющим корректировать вывод:

```
sys_prompt = f"""Это системный промпт. Ответ всегда должен выводиться как список
объектов через запятую: обеъект1, объект2, объект3. Кроме объектов ответ не должен
содержать никакой информации. Вопрос пользователя: """
print(pipe([{"role": "user", "content": f"{sys_prompt} Выведи административно-тер-
риториальное устройство Санкт-Петербурга"}]))
```

В результате было получено то, что Санкт-Петербург делится на 27 районов, что не соответствует действительности. Некорректная кластеризация географических объектов, наблюдаемая в случае ошибочного разделения Санкт-Петербурга, демонстрирует фундаментальное ограничение квантованных нейронных сетей [8] в задачах семантического анализа пространственных данных. Данная проблема возникает из-за необратимой потери высокоуровневых признаков при квантовании весов модели до 4 бит, что повышает вычислительную эффективность, но критически снижает способность сети к генерализации в условиях неполноты обучающей выборки. Для устранения артефактов классификации предложены два комплементарных подхода: 1) обучение языковых моделей и 2) использование гибридных RAG-архитектур. В случае обучения LLM интеграция онтологически структурированных географических справочников и семантически размеченных текстовых корпусов позволяет реконструировать потерянные при квантизации паттерны. В случае использование гибридных RAG-архитектур [9] системы преодолевают ограничения фиксированных параметров модели за счет динамического доступа к внешним базам знаний. Ключевым преимуществом такого подхода является возможность корректировки пространственных данных без переобучения ядра сети, что критически важно для систем реального времени.

В случае с административным делением Санкт-Петербурга, мы можем дать возможность модели обращаться к закону Санкт-Петербурга от 25 июля 2005 года N 411-68 «О территориальном устройстве Санкт-Петербурга» [10]. Повторив обращение к модели, мы можем получить корректный список районов, что было подтверждено в ходе эксперимента.

Успешная идентификация геообъектов также продемонстрировала определение отношений между ними, поскольку учитывается административно-территориальное деление. Однако эта задача требует от модели не только понимания контекста, но и способности к логическому выводу, для чего модель должна обучена на корпусе данных, содержащем описания городской инфраструктуры и административного деления. Так, при анализе текста «Улица С проходит через район А и соединяет его с районом В» мо-

дель должна уметь выделить взаимосвязи между этими объектами. Важной особенностью является возможность выявления не только логических (например, административные границы), но и топологических отношений (например, соседство объектов).

Идентификация геометрии объектов, позволяет визуализировать данные и проводить пространственные вычисления. LLM могут быть интегрированы с внешними источниками данных, такими как OpenStreetMap (OSM) [11], для получения необходимой геометрической информации. В данном случае для извлечения геометрической информации о конкретных географических объектах модель обрабатывает запросы, обращаясь к API OSM для получения данных о границах районов. Этот процесс требует от модели не только понимания запроса, но и способности сопоставлять полученную информацию с ранее идентифицированными объектами.

Важно учитывать, что модель должна обрабатывать различные форматы данных, включая простые координаты и сложные полигоны. Она должна уметь интерпретировать эти данные и представлять их в удобном виде для дальнейшего анализа. Использование методов проверки качества данных осуществляется с помощью аналитических инструментов ГИС, что обеспечивает надежность и точность извлеченной информации.

Применение больших языковых моделей для решения задач пространственного анализа представляет собой перспективное направление исследований. Использование больших языковых моделей для идентификации геообъектов, определения отношений между ними и работы с геометрией открывает новые возможности для обработки и интерпретации географической информации. Интеграция технологий искусственного интеллекта в системы пространственного анализа способствует повышению точности и эффективности работы с данными. Особенно перспективным направлением исследований является объединение LMS и многоаспектных геоинформационных моделей [12].

Список используемых источников

1. IBM. What are large language models (LLMs)? [Электронный ресурс] // IBM : сайт. 2023. URL: https://www.ibm.com/think/topics/large-language-models (дата обращения 13.01.2025).

2. OpenAI. Introducing ChatGPT [Электронный ресурс] // OpenAI : сайт. 2022. URL: https://openai.com/index/chatgpt/ (дата обращения 13.01.2025).

3. Sabzalieva E., Valentini A. ChatGPT и искусственный интеллект в высшем образовании. Краткое руководство [Электронный ресурс] / Международный институт ЮНЕСКО по высшему образованию в Латинской Америке и Карибском бассейне.

UNESCO, 2023. URL: https://unesdoc.unesco.org/ark:/48223/pf0000385146_rus (дата обращения 13.01.2025).

4. Яндекс Практикум. Что такое промпт для нейросети и как его составлять [Электронный ресурс] // Яндекс Практикум: блог. 2023. URL: https://practicum.yandex.ru/blog/chto-takoe-prompt-dlya-neyroseti-kak-sozdat/ (дата обращения 17.01.2025).

5. Renze, Matthew; Guven, Erhan. The Effect of Sampling Temperature on Problem Solving in Large Language Models [Электронный ресурс] // arXiv: репозиторий электронных препринтов. 2024. URL: https://arxiv.org/html/2402.05201v1 (дата обращения 17.01.2025). Лицензия: CC BY 4.0.

6. Hugging Face. Transformers documentation [Электронный ресурс] // Hugging Face: сайт. 2024. URL: https://huggingface.co/docs/transformers/index (дата обращения 17.01.2025).

7. Unsloth AI. unsloth/phi-4-bnb-4bit [Электронный ресурс] // Hugging Face: сайт. 2024. URL: https://huggingface.co/unsloth/phi-4-bnb-4bit (дата обращения 20.01.2025).

8. Motoroller_love. Сравнение различных схем квантования для LLM [Электронный ресурс] // Habr: сайт. 2024. URL: https://habr.com/ru/articles/797443/ (дата обращения 20.01.2025).

9. dimasklyarov. RAG (Retrieval Augmented Generation) – простое и понятное объяснение [Электронный ресурс] // Habr : сайт. 2023. URL: https://habr.com/ru/articles/779526/ (дата обращения 23.01.2025).

10. Закон Санкт-Петербурга от 25 июля 2005 года N 411-68 "О территориальном устройстве Санкт-Петербурга" (с изменениями, внесенными Законом Санкт-Петербурга от 3 апреля 2024 года N 208-50).

11. OpenStreetMap. OpenStreetMap [Электронный ресурс] // OpenStreetMap: сайт. 2025. URL: https://www.openstreetmap.org/ (дата обращения 23.01.2025).

12. Верхова Г. В., Акимов С. В. Метод объединения гетерогенных геопространственных данных на основе многоаспектных моделей // Телекоммуникации. 2021. № 3. С. 34-40.

LARGE LANGUAGE MODEL APPLICATIONS FOR SPATIAL ANALYSIS TASKS

Verkhova G., Chernyshov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

One of the challenges in creating spatial data infrastructure is the development of multi-faceted geosystem models, including the consideration of relationships between individual geosystems based on information derived from various sources. Addressing this issue is non-trivial because information about different aspects of geosystems is often presented in diverse, poorly structured sources, making it difficult to identify objects using classical information technology methods.

This paper presents research results on the possibilities and scenarios for applying large language models to solve spatial analysis tasks, including the creation of spatial knowledge bases based on multi-faceted geoinformation models.

Key words: *geosystems, multi-faceted models, artificial intelligence, language models*

УДК 550.385.4
ГРНТИ 10.19.61

АНАЛИЗ ХАРАКТЕРИСТИК ГЕОМАГНИТНЫХ ВОЗМУЩЕНИЙ

В. А. Волостных, П. В. Воробьев

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

В статье рассмотрены характеристики геомагнитных возмущений природного характера, влияющие на функционирование магистральных коротковолновых радиолиний. Предложены показатели характеристик геомагнитных возмущений, которые могут быть использованы при планировании магистральной коротковолновой радиосвязи и прогнозировании состояния радиосвязи. По предложенными показателям по сезонам 2024-2025 радиогода, проведен анализ геомагнитных возмущений.

анализ ионосферных возмущений, геомагнитные возмущения, магистральная коротковолновая радиосвязь магнитная буря, радиогод

Из средств массовой информации известно, что 2024 год характеризовался систематическими магнитными бурями, вызванными повышенной солнечной активностью. Данные природные явления безусловно влияют на состояние людей и в первую очередь на людей пожилого возраста. Кроме того, широко известно, что геомагнитные возмущения (ГМВ) или магнитные бури (МБ) оказывают влияние на состояние ионосферы и следовательно, на возможность обеспечения радиосвязи ионосферной волной в коротковолновом (КВ) диапазоне [1-5]. В целях оценки возможного воздействия ГМВ на магистральную коротковолновую радиосвязь проведен анализ характеристик геомагнитных возмущений. Анализ проводился по прогнозам МБ публикуемым на каждый месяц года. Данные об уровне МБ по 10 бальной шкале приводятся на каждые сутки в дискретном виде на каждый трехчасовой интервал.

Полагается целесообразным проводить оценки ГМВ по сезонам радиогода и за каждый радиогод в целом.

В качестве показателей, характеризующих ГМВ предлагаются следующие:

$N^{jc}_{(y \geq y_{зад})}$ – количество ГМВ в j-ом сезоне радиогода, уровня не ниже заданного, ед;

$\bar{t}^{\,jc}_{(y \geq y_{зад})}$ – среднее значение продолжительности ГМВ в j-ом сезоне радиогода, уровня не ниже заданного, в часах;

$K^{jc}_{\text{в }(y \geq y_{\text{зад}})}$ – коэффициент воздействия ГМВ уровня не ниже заданного, на обеспечение радиосвязи ионосферной волной в j-ом сезоне радиогода, в %.

Коэффициент воздействия ГМВ на состояние радиосвязи рассчитывается по формуле ниже:

$$K^{jc}_{\text{в }(y \geq y_{\text{зад}})} = \frac{t(y \geq y_{\text{зад}})}{T_{jc}} \cdot 100\ \%, \quad (1)$$

где T_{jc} – продолжительность сезона радиогода, часы.

В соответствии с установленными правилами анализ воздействия ГМВ проведен: для 1 сезона радиогода за период с 1 марта по 6 мая;

для 2 сезона радиогода за период с 7 мая по 31 августа;

для 3 сезона радиогода за период с 1 сентября по 31 октября;

для 4 сезона радиогода за период с 1 ноября по 28 февраля.

для 2024 – 2025 радиогода в целом за период с 1 марта 2024 г. по 28 февраля 2025 г.

Поскольку на обеспечение коротковолновой магистральной радиосвязи ГМВ оказывают заметное влияние начиная с уровня 5 ($y \geq y_5$), то анализ проведен для ГМВ, начиная с 5 уровня.

С целью обеспечения удобства анализа и большей наглядности табличные данные прогнозов представлялись в графическом виде в соответствии с рисунком 1 для уровней 5 и 6.

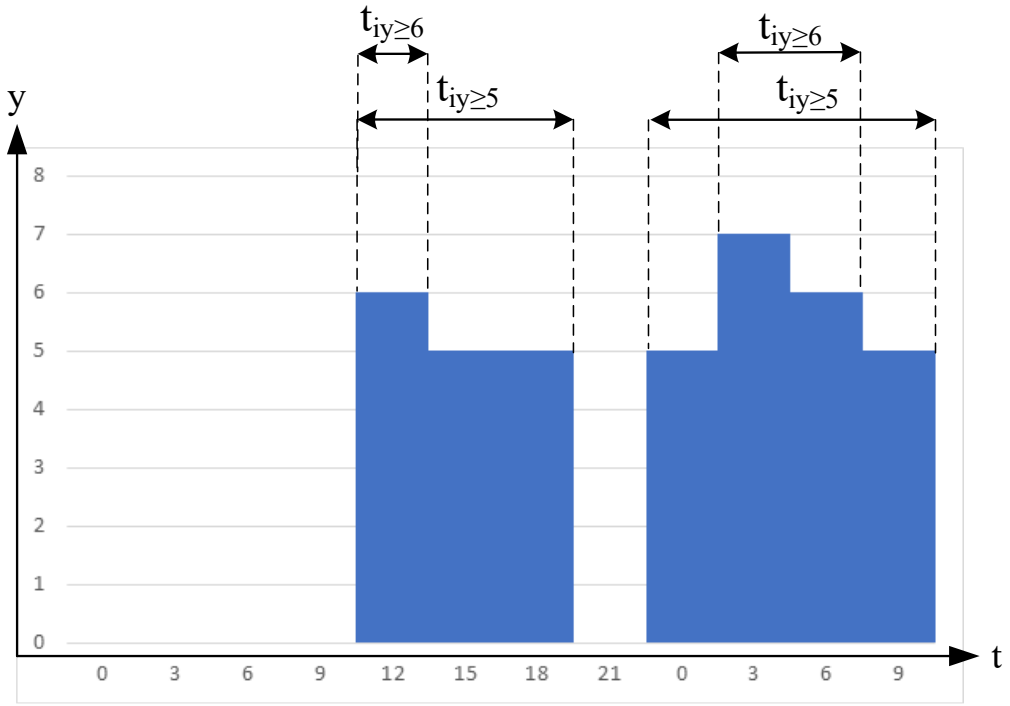


Рис. 1. Графическое представление уровней ГМВ

На основе ежемесячных прогнозов [6] по предложенным показателям проведены расчеты и оценки данных об уровне ГМВ, которые представлены в таблице 1.

Таблица 1. Оценка геомагнитных возмущений за 2024 – 2025 радиогод.

Сезон РГ	Показатель характеристик ГМВ	Значение характеристик ГМВ для уровней				
		$У_5$	$У_6$	$У_7$	$У_8$	$У_9$
1	Кол-во ГМВ, ед	9	1	-	-	-
	$Т_{средн}$, час	6	9	-	-	-
	$К_{возд}$, %	3	0,6			
2	Кол-во ГМВ, ед	21	7	3	2	1
	$Т_{средн}$, час	8,14	9,9	12	7,5	3
	$К_{возд}$, %	6	2,5	1,3	0,5	0,1
3	Кол-во ГМВ, ед	13	6	3	3	-
	$Т_{средн}$, час	12	13	11	4	-
	$К_{возд}$, %	1 11	5,3	2,2	0,8	
4	Кол-во ГМВ, ед	8	-	-	-	-
	$Т_{средн}$, час	16,9				
	$К_{возд}$, %	0,4				
За радиогод	Кол-во ГМВ, ед	51	14	6	5	1
	$Т_{средн}$, час	10,8	10,6	11,5	5,7	3
	$К_{возд}$, %	5,88	1,78	0,79	0,3	0,034

Примечание: уровень 5 – умеренная геомагнитная буря; уровень 6 – сильная геомагнитная буря; уровень 7 – жесткий геомагнитный шторм; уровень 8 – экстремальный шторм.

Анализ данных о геомагнитных возмущениях показал, что в год максимальной солнечной активности (Рис. 2) число возмущений уровня не ниже 5 ($У \geq У_5$) может быть равно 51 при средней продолжительности 10,8 часов; из них число возмущений уровня не ниже 6 ($У \geq У_6$) может быть равно 14 при средней продолжительности 10,6 часов, из них число возмущений уровня не ниже 7 ($У \geq У_7$) может быть равно 6 при средней продолжительности 11,5 часов, из них число возмущений уровня не ниже 8 ($У \geq У_8$) может быть равно 5 при средней продолжительности 5,7 часов.

Геомагнитное возмущение 9 уровня произошло в мае месяце 2024 года. Это явление продолжалось в течение 3-х часов и оказало существенное влияние на распространение радиоволн в КВ диапазоне.

При этом, коэффициент воздействия ГМВ на КВ радиосвязь за анализируемый радиогод для уровней У5, У6, У7, У8, У9, составляет: 5,88 %, 1,78 %, 0,79 %, 0,3 %, 0,034 % соответственно.

Полученные характеристики ГМВ могут быть использованы для прогнозирования и расчета показателей обеспечения магистральной коротковолновой связи.

Можно полагать целесообразным в целях планирования радиосвязи набрать статистические данные ГМВ для всего 11-летнего периода солнечной активности, провести анализ характеристик ГМВ по предложенным показателям. На основе анализа ГМВ за 11-летний период солнечной активности предполагается возможным определение закономерностей ГМВ и прогнозирование условий распространения радиоволн. Полученные прогнозы ГМВ могут быть также полезны разработчикам систем магистральной радиосвязи.

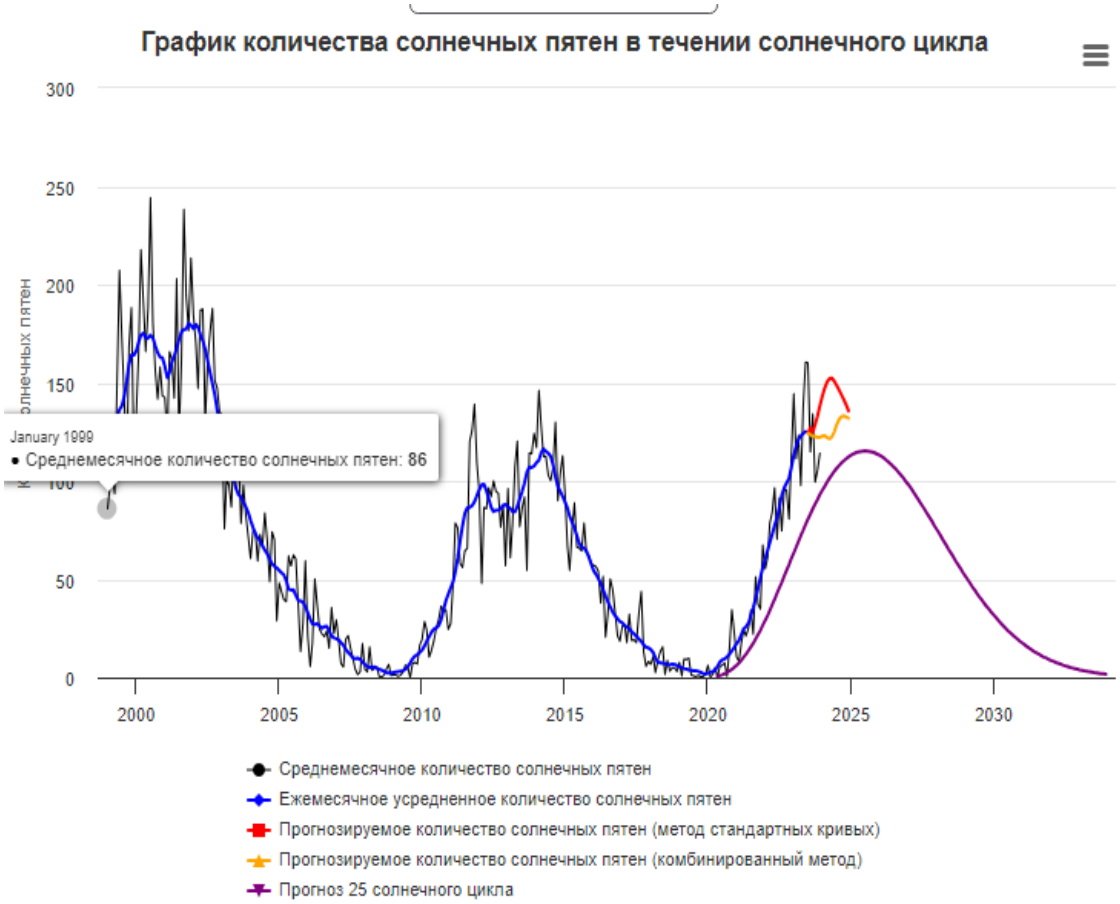


Рис. 2. График циклов солнечной активности

Несмотря на значительное количество материалов, посвященных исследованию влияния магнитных бурь на распространение радиоволн КВ

диапазона, в связи с мало предсказуемостью солнечной активности, можно считать целесообразным продолжение исследований в данном направлении [6]. Представляется целесообразным проведение исследований влияния ГМВ на обеспечение магистральной КВ радиосвязи для каждого уровня ГМВ.

Список используемых источников

1. Ротхаммель К., Кришке А. Антенны. Том 1.: Пер. с нем. Мн: ОМО «Наш город», 2001. 416 с.: ил.

2. Котова Д. С., Клименко В. В., Клименко М. В., Захаров В. Е. Численное моделирование влияния геомагнитной бури 2 – 3 мая 2010 года на распространение коротких радиоволн в ионосфере. / Известия вузов. Радиофизика №7, 2014, 520 530 стр.

3. Благовещенский Д. В., Сергеева М. А., Воздействие магнитных бурь на нижнюю ионосферу в авроральной зоне. / Солнечно-земная физика. 2015. Том 1 № 3. 3-10 стр.

4. Куркин В. И., Полех Е. М., Золотухина Н. А. Влияние слабых магнитных бурь на характеристики распространения КВ-радиоволн. / Геомагнитизм и аэронамия, 2022. Т. 62. № 2. С. 245-256.

5. Волостных В. А., Стародубцев Ю. И., Ткачев Д. Ф. Влияние магнитных бурь на распространение радиоволн коротковолнового диапазона. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах. СПб.: СПбГУТ, 2024. С 36-42.

6. Волостных В. А., Воробьев П. В., Ткачев Д. Ф. Мониторинг декаметрового диапазона радиоволн // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах. СПб.: СПбГУТ, 2024. С. 104-108.

ANALYSIS OF THE CHARACTERISTICS OF GEOMAGNETIC DISTURBANCES

Volostnyh V. Vorobyev P.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article discusses the characteristics of geomagnetic disturbances of a natural nature that affect the functioning of long-range shortwave radio lines. Indicators of the characteristics of geomagnetic disturbances are proposed, which can be used in planning shortwave backbone radio communications and forecasting the state of radio communications. According to the proposed indicators for the 2024-2025 radio weather seasons, an analysis of geomagnetic disturbances was carried out.

Key words: *analysis of ionospheric disturbances, geomagnetic disturbances, mainline shortwave radio communication, magnetic storm, radioyear*

УДК 681.5:681.586
ГРНТИ 55.30.31

АППАРАТНО-ПРОГРАММНЫЕ РЕШЕНИЯ РАСШИРЕНИЯ МОБИЛЬНОГО РОБОТОТЕХНИЧЕСКОГО КОМПЛЕКСА ROBO-PICA СРЕДСТВАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

П. А. Волынкин

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

Робототехнический комплекс ROBO-PICA, построенный на базе контроллера RBX-877 V2.0 с микроконтроллером PIC16F887, принадлежит к роботам 2-го поколения и не обладает элементами искусственного интеллекта. Сильно ограниченный объем памяти для программы (8 Кслов) не позволяет реализовать функции искусственного интеллекта без существенных изменений в аппаратной и программной области. В работе рассматриваются варианты расширения возможностей робототехнического комплекса ROBO-PICA до уровня роботов 3-го поколения, в частности, с возможностями технического зрения.

робототехнический комплекс, искусственный интеллект, техническое зрение

Мобильный робототехнический комплекс ROBO-PICA (рис. 1) построен на базе контроллера RBX-877 V2.0, центральное место которого занимает микроконтроллер PIC16F887 [1].

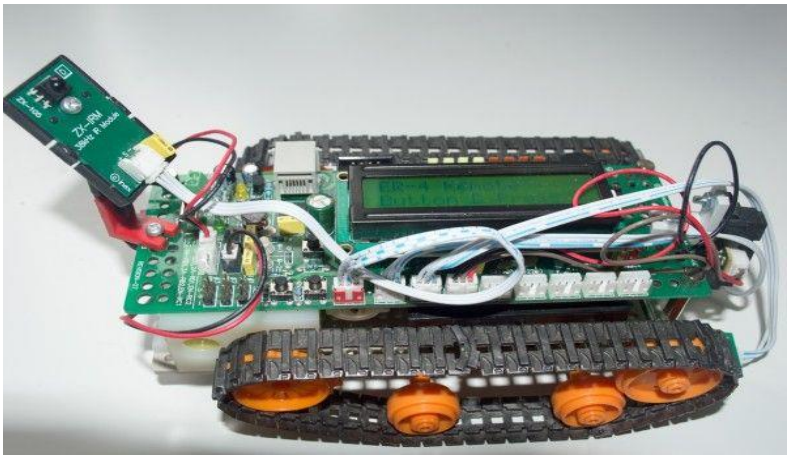


Рис. 1. Мобильный робототехнический комплекс ROBO-PICA

Этот комплекс можно отнести к роботам 2-го поколения с адаптивным управлением. Однако возможности вышеупомянутого микропроцессора весьма ограничены в плане памяти как для данных (256 байт), так и для кода (8 КСлов). Данные ограничения не позволяют реализовывать в рамках этого комплекса элементы искусственного интеллекта, в частности, машинное

зрение. В связи с этим ставится задача расширить возможности робота с использованием дополнительных аппаратных и программных средств.

Микроконтроллер PIC16F887 построен по Гарвардской RISC 8-разрядной архитектуре и имеет в распоряжении 35 простых инструкций, работая на частоте 20 МГц. Для программирования этого микроконтроллера имеется в наличии специальная версия языка С для микроконтроллеров – microC компании microElektronika.

Микроконтроллер PIC16F887 и соответственно контроллер RBX-877 V2.0 поддерживают следующие интерфейсы:

– 9 программируемых одноразрядных портов ввода-вывода;
– UART;
– I^2C.

Для решения поставленной задачи можно рассмотреть несколько вариантов:

1. Расширение памяти как для кода, так и для данных.

Однако данный вариант потребует дополнительных существенных аппаратных и программных решений по интерфейсам расширения. При этом не решается проблема реализации элементов искусственного интеллекта в части компьютерного зрения. У контроллера RBX-877 V2.0 нет адекватных интерфейсов для организации взаимодействия микроконтроллера с видеокамерой.

2. Организация пары: «Контроллер робота RBX-877 V2.0 – Микрокомпьютер».

При этом варианте выдвигаются следующие требования к микрокомпьютеру:

– достаточный объем памяти как для кода, так и для данных. RAM>=256 Mb, Flash >= 8 Gb;
– наличие интерфейса для элементов искусственного интеллекта (для начала – видеокамеры для реализации машинного зрения);
– наличие интерфейса для организации взаимодействия контроллера робота RBX-877 V2.0 с микрокомпьютером;
– конструктивная возможность размещения микрокомпьютера на комплексе ROBO-PICA.

В настоящее время имеется довольно обширный выбор одноплатных микрокомпьютеров. Из них наиболее приемлемыми становится список из 10 предложений (таблица 1).

По совокупности удовлетворяющих выдвинутым требованиям выбор останавливается на микрокомпьютере Raspberry Pi 3(4) B. Данный микро-

компьютер построен на гарвардской RISC архитектуре ARM11 на чипсете Broadcom BCM2835, имеет центральный 4-ядерный 64-битный процессор на частоте 700(1500) МГц [2]. В качестве интерфейсов у данного микрокомпьютера присутствуют: HDMI, USB 2.0 (3.0), 15-pin MIPI Camera interface – для подключения видеокамеры, 15-pin Display interface – для подключения монитора, MicroSD card slot: до 32 Гб, а также низкоуровневые интерфейсы: 40 портов ввода-вывода общего назначения, UART, I²C, SPI.

ТАБЛИЦА 1. Современные одноплатные микрокомпьютеры

Микрокомпьютер	Частота, ГГц	RAM, Mb	Flash, Mb	USB	WiFi	UART	I2C	CSI-camera	HDMI	Карта памяти
Onion Omega2S	0.568	64	16	2.0	+	+	+	нет	нет	
Orange Pi Zero	1.2	512	64	2.0	+	нет	нет	нет	нет	
FriendlyElec NanoPi NEO3	1.4	1000	8000	3.0	нет	нет	нет	нет	нет	
Arduino mega 2560 r3	0.016	0.008	256	2.0	нет	нет	нет	нет	+	
Raspberry Pi 4 B	1.5	512	8000	3.0	+	+	+	+	2	microSD
ASUS Tinker Board S	1.8	2000		2.0	+		+	+	+	microSD
Odroid-XU4	2		64	3.0	+	нет	нет	+	+	microSD
NVIDIA Jetson Nano Developer Kit	1.4	4000		3.0	нет				+	
Khadas VIM2	1.5	3000		2.0	+	нет	нет	нет	+	microSD
Udoo x86	2.5		8000	3.0	нет	+	+	нет	+	microSD

В качестве программного обеспечения этот микрокомпьютер поддерживает: штатную операционную систему Debian Linux Raspberry Pi OS, устанавливаемую на micro-SD карту. В рамках этой операционной системы имеется средство разработки ПО – Python в среде Thonny.

Для обеспечения взаимодействия микрокомпьютера Raspberry Pi с контроллером робота RBX-877 V2.0 возможно два интерфейса, которые присутствуют на обеих сторонах: UART или I²C.

С учетом того, что интерфейс I²C по сравнению с UART более стабилен и имеет возможность подключать к ведущему устройству не одно, а несколько ведомых устройств (что может потребоваться при дальнейшей модернизации данного робототехнического комплекса), выбор останавливается на интерфейсе I²C.

В таком случает структурная схема модернизированного комплекса выглядит согласно рисунку 2.

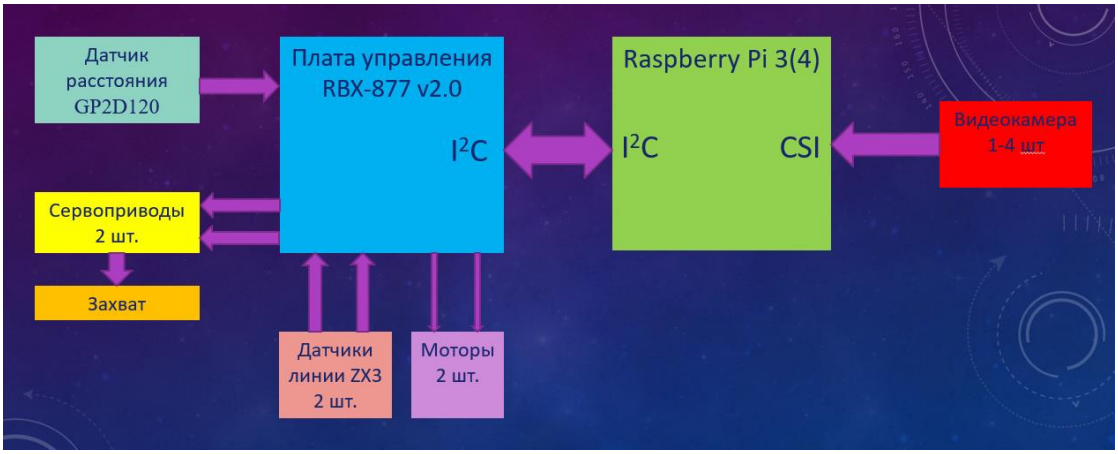


Рис. 2. Структурная схема модернизированного робототехнического комплекса с машинным зрением

Конструктивно модернизированный комплекс представлен на рисунке 3.

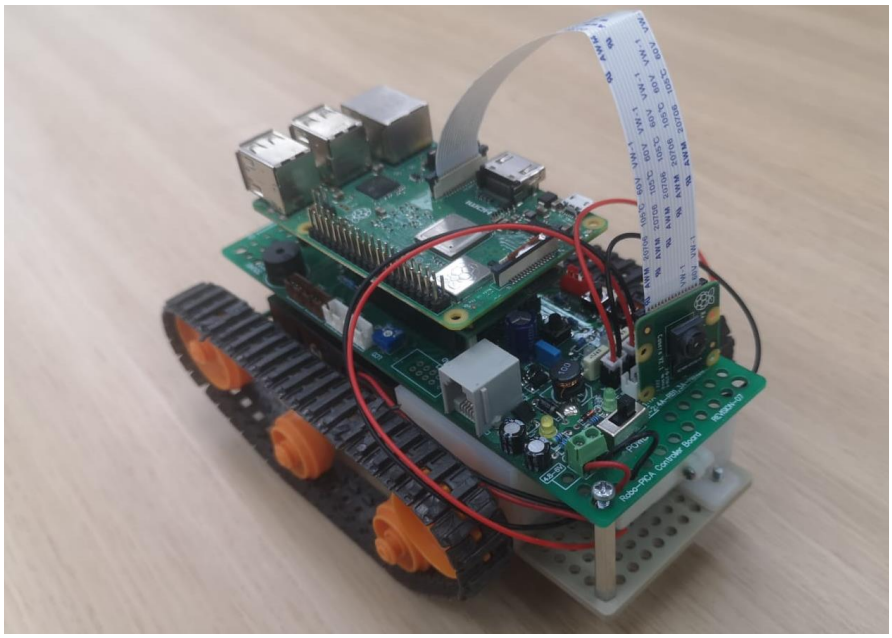


Рис. 3. Роботехнический комплекс ROBO-PICA с блоком компьютерного зрения

На данном этапе работы над поставленной задачей программно реализовано взаимодействие и обмен данными между контроллером RBX-877 V2.0 и микрокомпьютером Raspberry Pi. При этом контроллеру робота переданы исключительно функции управления моторами (движение вперед, назад, повороты), а микрокомпьютер с подключенной видеокамерой получает, обрабатывает изображение (рис. 4) и в зависимости от поставленной перед роботом задачей по интерфейсу передает контроллеру управляющие сигналы.

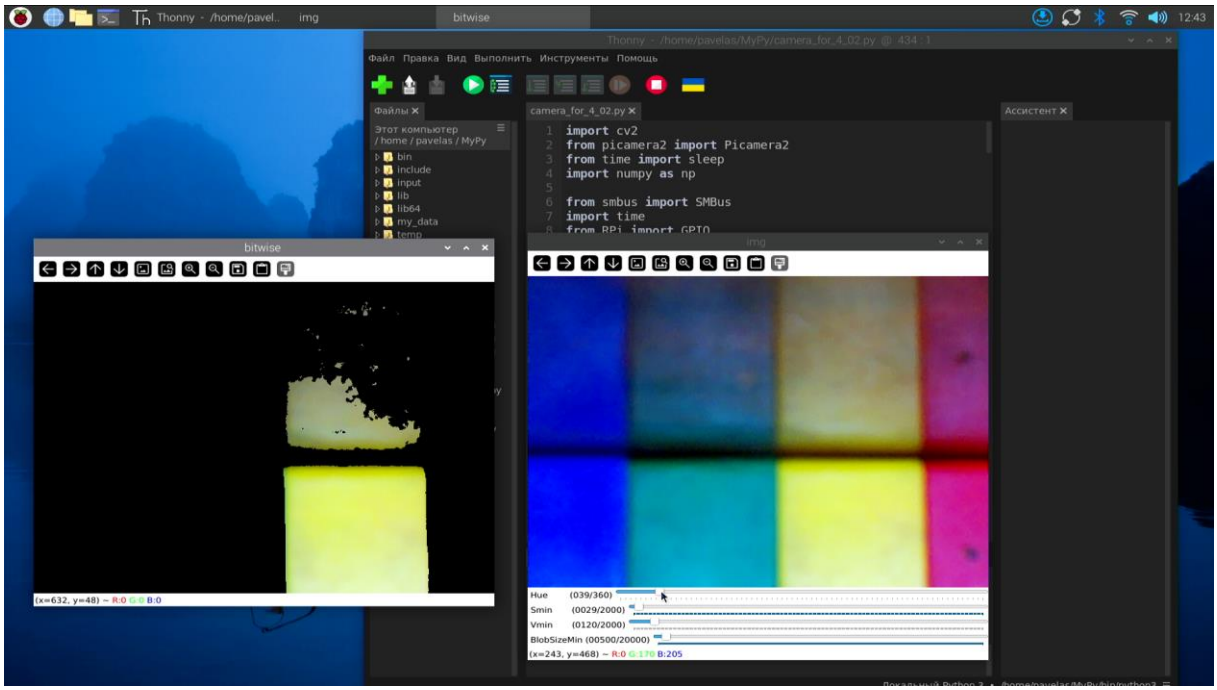


Рис. 4. Получение и обработка фильтрацией изображения микрокомпьютером Raspberry Pi

Список используемых источников

1. Robot experiment with PIC microcontroller based-on Robo-PICA robot kit // Innovative Experiment Co. Ltd., 2006.

2. Магда Ю. С. Raspberry Pi. Руководство по настройке и применению, ДМК Пресс, 2015, 188 с., ISBN: 978-5-97060-412-0

HARDWARE AND SOFTWARE SOLUTIONS FOR EXPANDING THE ROBO-PICA MOBILE ROBOTIC COMPLEX BY MEANS OF ARTIFICIAL INTELLIGENCE

Volynkin P. A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The ROBO-PICA robotic complex, built on the basis of the RBX-877 V2.0 controller with a PIC16F887 microcontroller, belongs to the 2nd generation robots and does not have elements of artificial intelligence. The very limited memory capacity for the program (8 Kwords) does not allow the implementation of artificial intelligence functions without significant changes in the hardware and software. The paper considers options for expanding the capabilities of the ROBO-PICA robotic complex to the level of 3rd generation robots, in particular, with the capabilities of technical vision.

Key words: *robotic complex, artificial intelligence, technical vision*

УДК 681.391
ГРНТИ 47.05.09

ИССЛЕДОВАНИЕ ПРОСТЫХ И КОМБИНИРОВАННЫХ СВЕРТОЧНЫХ КОДОВ В РАДИОТЕХНИЧЕСКИХ СИСТЕМАХ

Е. И. Глушанков, Т. З. Ву

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

Сверточные коды (СК) находят широкое применение в системах передачи цифровой информации, они способны эффективно исправлять ошибки в условиях сложной помеховой обстановки. СК используются в системах мобильной связи, спутниковой связи, системах хранения данных, подводной связи и в других радиотехнических системах. В современных условиях развития радиотехнических систем широкое распространение находят комбинированные методы кодирования, в которых происходит объединение сверточных кодов с другими способами для достижения более высокой помехоустойчивости в процессе передачи информации. В данной статье исследуется эффективность простых и комбинированных сверточных кодов в радиотехнических системах. Моделирование выполняется в среде MATLAB.

простые сверточные коды, комбинированные сверточные коды, помехоустойчивость, декодер Витерби, вероятность ошибки

В современных условиях функционирования различных радиотехнических систем одной из наиболее актуальных остается проблема обеспечения их помехоустойчивости в условиях воздействия различных помех. Для решения этой проблемы широкое распространение получают различные методы кодирования с коррекцией ошибок. Среди них широко используемыми методами кодирования считаются сверточные коды, каскадные коды и турбокоды. Каждый метод кодирования имеет свои уникальные преимущества, обеспечивая оптимальные решения для современных систем передачи данных.

Для описания сверточного кодера необходимо задать три числа [1] (*k, n, K)*, где *k* показывает количество информационных входов, то есть информационных символов, поступающих за один такт на вход сверточного кодера; *n* представляет количество кодовых выходов; *K* – длина кодового ограничения, которая показывает число моментов времени, в которые входные информационные символы участвуют в формировании выходных кодовых символов.

Алгоритм декодирования Витерби используется для декодирования сверточных кодов. Принцип работы алгоритма декодирования основан на нахождении путей (кодовых символов) по входным информационным символам на решетчатой диаграмме. Алгоритм рассчитает и сравнит метрики всех путей к каждому состоянию, чтобы найти оптимальный путь декодирования [2]. Если есть два пути входят в одно и то же состояние, то выбирается выживающий путь с наименьшей метрикой.

Основным недостатком алгоритма Витерби является увеличение количества рассматриваемых путей с увеличением конструктивной длины *K*. Вероятность ошибки с увеличением конструктивной длины представлена в случае работы с каналом АБГШ показана на рис. 1. Из данного графика видно, что при использовании алгоритма декодирования Витерби с кодовой скоростью 1/2, чем больше конструктивной длины *K*, тем выше способность правильного декодирования. С увеличением конструктивной длины кода на единицу выигрыш кодирования [ISBN 978-5-9775-0878-0.

2] увеличивается на 0.5–1 дБ.

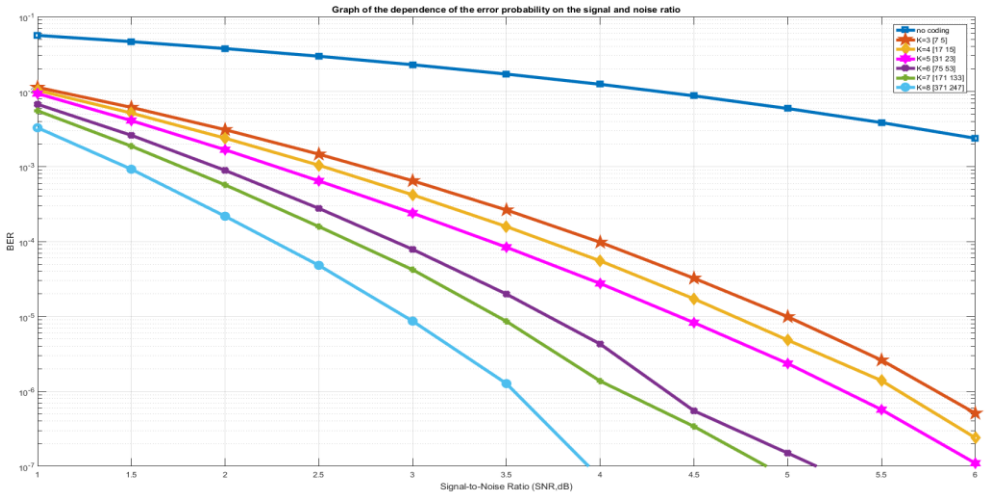


Рис. 1. Оценка характеристик декодера Витерби для кодовой скорости *r* = 1/2 в канале АБГШ

В рамках статья исследуется каскадный код, который представляет собой код, построенный на основе использования нескольких составляющих кодов, в частности из двух составляющих кодов, как рассмотрено далее. На рис. 2 [2] показано, что сначала информационные символы кодируются внешним кодом (n_1, k_1). В качестве внешнего кода выберем недвоичный код Рида-Соломона. После этого символы, закодированные во внешнем коде, кодируются внутренним кодом (n_2, k_2), здесь будет применяться свер-

точный код. Длина кодового слова каскадного кода будет равной $N = n_1\, n_2$, причем $K = k_1\, k_2$ из них являются информационными. Кодовая скорость передачи сообщений составляет:

$$R = \frac{K}{N} = \frac{k_1\, k_2}{n_1 n_2} = r_1\, r_2$$

где r_1 , r_2 - кодовые скорости внешнего и внутреннего кодов.

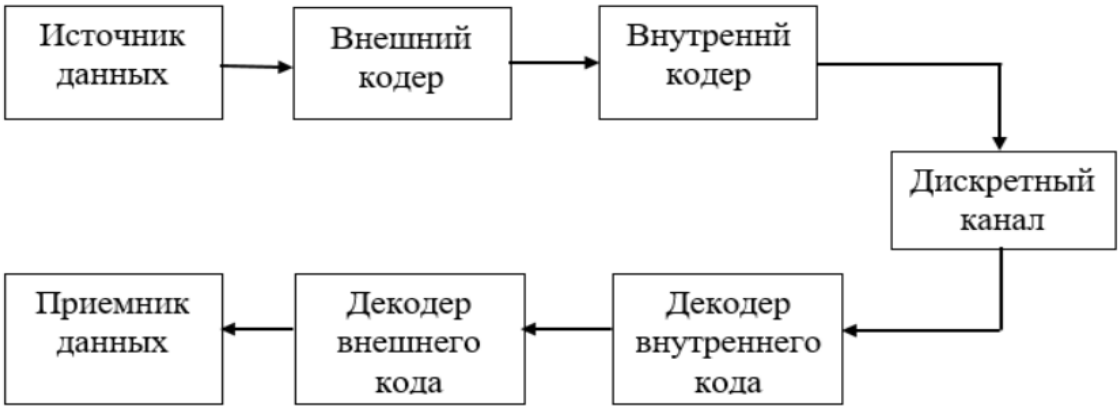


Рис. 2. Схема системы связи, в которой используется каскадный код

Декодирование каскадного кода производится в обратном порядке [3]. В дополнение к мощной способности исправления ошибок, особенно пакетных ошибок, использование каскадного кода открыло новые перспективы для систем надежной связи в условиях помех.

Турбокоды строятся на основе комбинации двух или более простых сверточных кодов, связанных между собой посредством перемежителя. На рис. 3 [4] представлена структурная схема турбокодирования.

Такая структура создает код с хорошими свойствами по дисперсии ошибок, что значительно улучшает эффективность исправления ошибок по сравнению с традиционными канальными кодами.

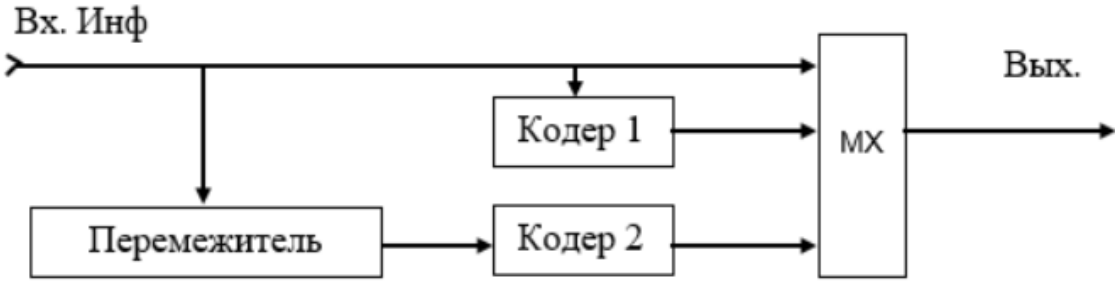


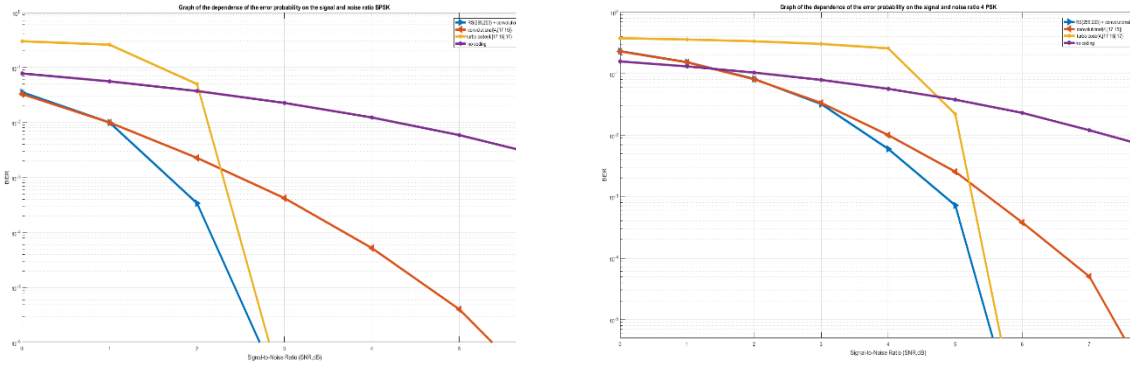
Рис. 3. Структурная схема канального кодер турбокода

Одной из важных особенностей турбодекодирования является итеративный алгоритм декодирования, в качестве которого используются:

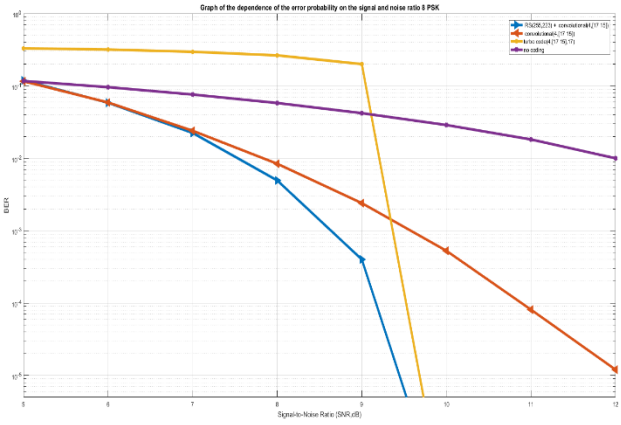
– MAP (Maximum of A-posteriori Probability) – максимум апостериорной вероятности;
– Log-MAP – логарифмический максимум апостериорной вероятности;
– Max-Log-MAP – максимальный логарифмический максимум апостериорной вероятности;
– SOVA(SoftOutputViterbiAlgorithm) – алгоритм декодирования Витерби [4, 5].

Итеративный процесс декодирования помогает более точно воспроизводить информацию на каждой итерации благодаря обмену информацией между субдекодерами.

Сравнение эффективности исправления ошибок между сверточными кодами, каскадными кодами и турбокодами с различными типами каналов модуляции, представленными на рис. 4 и рис. 5.

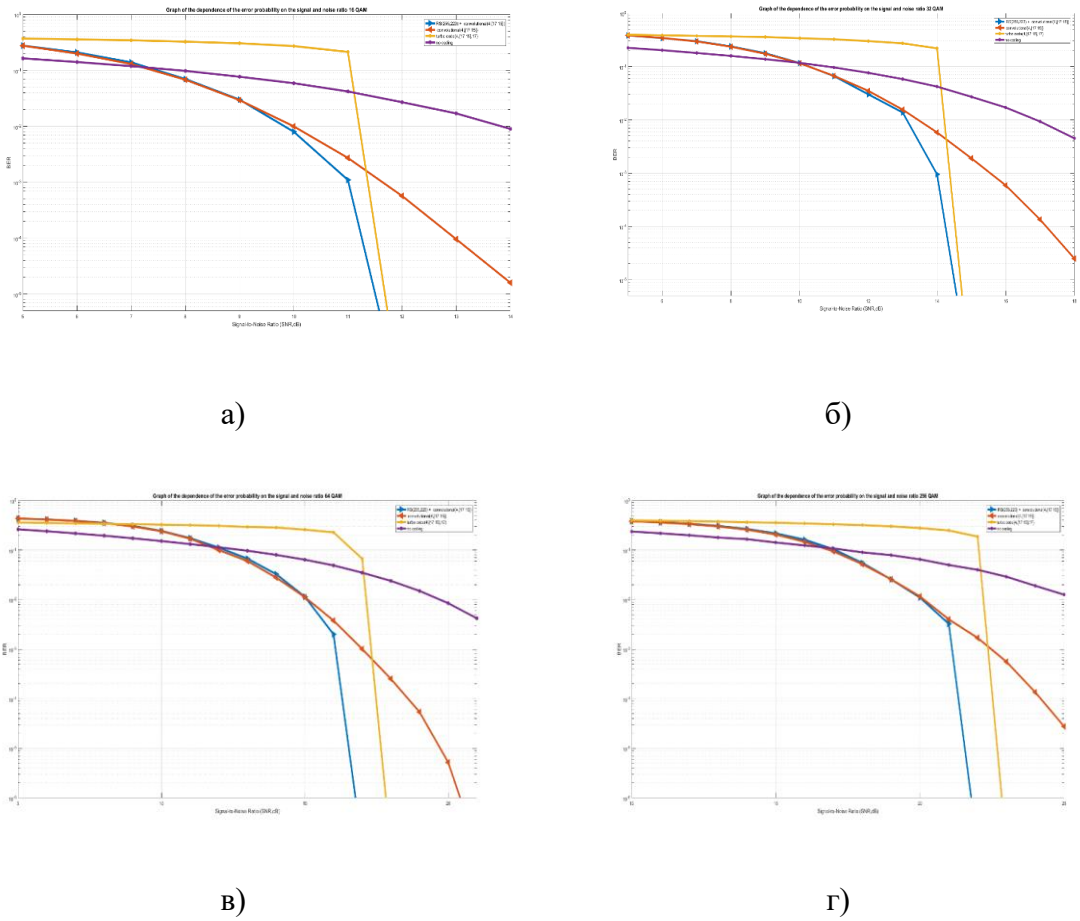


а) б)



в)

Рис. 4. Результаты моделирования сверточного кода, каскадного кода, турбокода, в канале с АБГШ для PSK: а) для BPSK; б) для 4-PSK; в) для 8-PSK



а) б)

в) г)

Рис.5. Результаты моделирования сверточного кода, каскадного кода, турбокода, в канале с АБГШ для QAM: а) для 16-QAM; б) для 32-QAM; в) для 64-QAM; г) 256-QAM

Из результатов моделирования видно, что при отсутствии кодирования эффективность исправления ошибок наихудшая. Турбокод обладает пороговым эффектом, в работе определены значения этого порога и при средних и высоких уровнях отношений сигнал/шум турбокод начинает демонстрировать заметное улучшение. Каскадный код продолжает сохранять лучшую эффективность, чем другие рассмотренные коды на основе сверхточных.

Список используемых источников

1. Варгаузин В. А., Цикин И. А., Методы повышения энергетической и спектральной эффективности цифровой радиосвязи: учебное пособие. СПб.: БХВ-Петербург, 2013. 352 с.: ил. (Учебная литература для вузов). ISBN 978-5-9775-0878-0.

2. Золотарев В. В., Овечкин Г. В., Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под. ред. чл.-кор. РАН Ю. Б. Зубарева. М.: Горячая линия–Телеком, 2004. 126 с.: ил. ISBN 5-93517-169-4.

3. Быховский М. А., Гиперфазовая модуляция–оптимальный метод передачи сообщений в гауссовских каналах связи., Москва: ТЕХНОСФЕРА, 2018. 310с. ISBN 978-5-94836-478-0.

4. Королев А. И., Турбокоды и итеративное декодирование: учеб. –метод. пособие/ А. И. Королев, В. К. Конопелько. Минск: БГУИР, 2015. 74 с.: ил. ISBN 978-985-543-133-7.

5. Голиков А. М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: учебное пособие для вузов / А. М. Голиков. 2-е изд., стер. СПб.: Лань, 2021. 452 с.: ил. Текст: непосредственный. ISBN 978-5-8114-7828-6.

RESEARCH OF SIMPLE AND COMBINED CONVOLUTIONAL CODES IN RADIO ENGINEERING SYSTEMS

Glushankov E., Vu T. D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Convolutional codes (CC) are widely used in digital information transmission systems; they are able to effectively correct errors in complex interference conditions. CC are used in mobile communication systems, satellite communications, data storage systems, underwater communications and other radio engineering systems. In modern conditions of development of radio engineering systems, combined coding methods are widely used, in which convolutional codes are combined with other methods to achieve higher noise immunity in the process of information transmission. This article examines the effectiveness of simple and combined convolutional codes in radio engineering systems. Modeling is performed in the MATLAB environment.

Key words: *simple convolutional codes, combined convolutional codes, noise immunity, Viterbi decoder, error probability*

УДК 621.391:621.396
ГРНТИ 47.05.17

СИНТЕЗ СТОХАСТИЧЕСКИХ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ ДЛЯ МОДЕЛИРОВАНИЯ СЛУЧАЙНЫХ ПРОЦЕССОВ В КОРРЕЛЯЦИОННОМ ПРИБЛИЖЕНИИ

Е. И. Глушанков[1], З. К. Кондрашов[2], А. В. Суденкова[1]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
[2]НИИМА «Прогресс»

При моделировании сигналов в каналах пространственно-временной обработки, как правило, рассматриваются случаи полной или частичной пространственной когерентности сигналов в приемных антенных решетках. Частичная когерентность характерна для трасс с многолучевостью, сетей мобильной связи, тропосферных и прочих каналов радиосвязи, а также при использовании широкополосных в пространственно-временном смысле сигналов. В данной работе на основе корреляционных матриц синтезированы многомерные стохастические дифференциальные уравнения для гауссовских случайных процессов, разработаны модели для стационарного случая.

пространственно-временная обработка, частично-когерентные сигналы, синтез стохастических дифференциальных уравнений, корреляционная матрица

Условие частичной пространственной когерентности сигналов на входе приемных антенных решеток (АР) справедливо для случая, когда источники излучений располагаются в ближней зоне приемной АР, что обуславливает искажение фазового фронта приходящих волн и требует учета коэффициентов корреляции между фазами сигналов на входе антенных элементов. Такие сигналы могут быть описаны случайными полями [1, 2] или многомерными случайными процессами (СП). Для АР с случайные параметры сигналов удобно представлять в виде векторов, каждый элемент которых соответствуют одному из L пространственно-распределенных антенных элементов (каналов обработки).

В литературе [3, 4] изложены методы синтеза стохастических дифференциальных уравнений (СДУ) для когерентных и некогерентных сигналов, базирующиеся на теории диффузионных марковских процессов. При рассмотрении многомерных частично-когерентных сигналов воспользуемся методами синтеза коэффициентов линейных СДУ по корреляционным матрицам входных сигналов [5]. При этом рассматриваемый процесс будем полагать гауссовским, имея в виду, что результаты синтеза можно распростра-

нить и на негауссовские СП. В этом случае необходимо воспользоваться методами линеаризации, например, разложением Карунена-Лоэва, при котором коэффициенты разложения гауссовы.

Представим многомерный процесс $X(t)$ в виде линейного СДУ следующего вида:

$$\frac{dX(t)}{dt} = F(t)X(t) + G(t)V(t), \quad (1)$$

где $F^{(j)}(t) = \mathrm{diag}[f_1^{(j)}(t), f_2^{(j)}(t), \dots, f_L^{(j)}(t)]$ и $G^{(j)}(t) = \mathrm{diag}[g_1^{(j)}(t), g_2^{(j)}(t), \dots, g_L^{(j)}(t)]$ – $L \times L$-мерные матричные коэффициенты СДУ, в которых j – число сигнально-помеховых излучений, воздействующих на вход АР, в случае многолучевого распространения (в дальнейшем считаем, что $j = 1$), L – количество каналов обработки (антенных элементов); $V(t) = [v_1^{(j)}(t), v_2^{(j)}(t), \dots, v_L^{(j)}(t)]$ – вектор формирующих гауссовских шумов.

В зависимости от способа представления корреляционной матрицы $R_{XX}(t,\tau) =< X(t)X^T(\tau) >$ можно выделить несколько случаев.

Стационарный случай:

$$R_{XX}(\tau) = lim_{t\to\infty} R_{XX}(t,\tau);\ F(t),\ G(t) = const - \text{неизвестны}. \quad (2)$$

Случай $t = \tau$:

$$R_{XX}(t,\tau) = R_{XX}(t,t);\ F(t),\ G(t)\ - \text{неизвестны}.$$

Общий случай (любые t, τ):

$$R_{XX}(t,\tau)\ \textit{или}\ R_{XX}(t-\tau);\ F(t),\ G(t) - \text{неизвестны}.$$

В качестве примера будем рассматривать стационарный вариант корреляционной матрицы $R_{XX}(\tau)$ (2). Коэффициенты уравнения (1) ищутся в соответствии со следующими равенствами:

$$F(t) = -\Phi^{-1}(t)\frac{d\Phi(t)}{dt}, \quad (3)$$

$$P_0 = \Phi^{-1}(0)\Phi R_{XX}(0), \quad (4)$$

$$G(\tau)G^T(\tau) = \Phi^{-1}(\tau)\frac{d\Phi(t)}{dt}\left[\frac{dR_{XX}(\tau)}{dt} - R_{XX}(\tau)F^T(\tau)\right], \quad (5)$$

где $\Phi(t,\tau) = R_{XX}(t,\tau)R_{XX}^{-1}(\tau,\tau)$ – переходная матрица при граничном условии $\Phi(\tau,\tau) = I$, I – единичная матрица; P_0 – начальное условие для корреляционной матрицы $R_{XX}(t,\tau)$.

На основе приведенных соотношений можно построить различные модели СДУ.

Модель СДУ № 1:

Пусть элементы переходной матрицы не зависят от времени: $\Phi(t) = \Phi = const$. Подставляя Φ в (3), (4) и (5), получаем соответственно:

$$F(t) = 0,\ P_0 = R_{XX}(0),\ G(\tau)G^T(\tau) = dR_{XX}(\tau)/dt,$$

Коэффициенты корреляционной матрицы:

$$r_{ji}(\tau) = \frac{1}{B} I_0^2\, exp(\, j_0 \omega \frac{r_0}{c} - r_i' + r_{ij}'), j \neq i, \quad (6)$$

$$r_{ii}(\tau) = \sigma_X^2 \exp(-\frac{\tau}{\tau_{corr}}), \quad (7)$$

где B – константа, I_0 – интенсивность шума, r_0 – расстояние между источником и приемной антенной; r_i', r_{ij}' – коэффициенты соответственно временной и пространственной корреляции, σ_X – среднеквадратическое отклонение $X(t)$, τ_{corr} – интервал корреляции.

Представление коэффициентов (6) формирует нули на всех позициях матрицы $G(t)$, кроме ее диагонали, поскольку $r_{ji}(\tau) = r_{ji}$ (не зависят от τ). Тогда коэффициент СДУ $G(t)$ определяется как квадратный корень производной от $R_{XX}(\tau)$ (7) по τ, помноженный на единичную матрицу:

$$G(t) = j_0 \frac{\sigma_X}{\sqrt{\tau_{corr}}} exp(\, -\frac{t}{2\tau_{corr}}) I.$$

где j_0 – мнимая единица.

СДУ будет выглядеть так:

$$\frac{dX(t)}{dt} = j_0 \frac{\sigma_X}{\sqrt{\tau_{corr}}} exp(\, -\frac{t}{2\tau_{corr}}) I \cdot V(t). \quad (8)$$

Модель СДУ № 2:

Пусть переходная матрица меняется пропорционально некоторому ненулевому коэффициенту $m(t)$: $\Phi(t) = m(t)\Phi$, при условии $\lim\limits_{t\to\infty} m(t) = 1$. Из формул (3) - (5) можно записать:

$$F(t) = -\frac{m(t)}{dt}\frac{I}{m(t)},\ P_0 = \frac{1}{m(0)} R_{XX}(0),$$
$$G(t)G^T(t) = \frac{1}{m(t)}\frac{dR_{XX}(t)}{dt} + \frac{dm(t)}{dt} R_{XX}(t).$$

Положим $m(t) = 1 + \exp(-\omega t)$, $\omega > 0$. Тогда

$$F(t) = \frac{\omega\, exp(-\omega t)}{1 - exp(-\omega t)} I,\ P_0 = \frac{1}{2} R_{XX}(0),\ G(t)G^T(t) = \{m_{ij}(t)\}.$$

Если определить корреляционную матрицу через коэффициенты (6), (7), то

$$m_{ii}(t) = -\frac{\sigma_X^2\, exp(-t/\tau_{corr})[1 + (1 + \omega\tau_{corr})\, exp(-\omega t)]}{\tau_{corr}[1 + exp(-\omega t)]^2},$$
$$m_{ij}(t) = -\frac{\omega\, exp(-\omega t)}{1 + exp(-\omega t)} r_{ij},\ i \neq j.$$

СДУ будет выглядеть так:

$$\frac{dX(t)}{dt} = \frac{\omega\, exp(-\omega t)}{1 - exp(-\omega t)} I \cdot X(t) + G(t) \cdot V(t) \qquad (9)$$

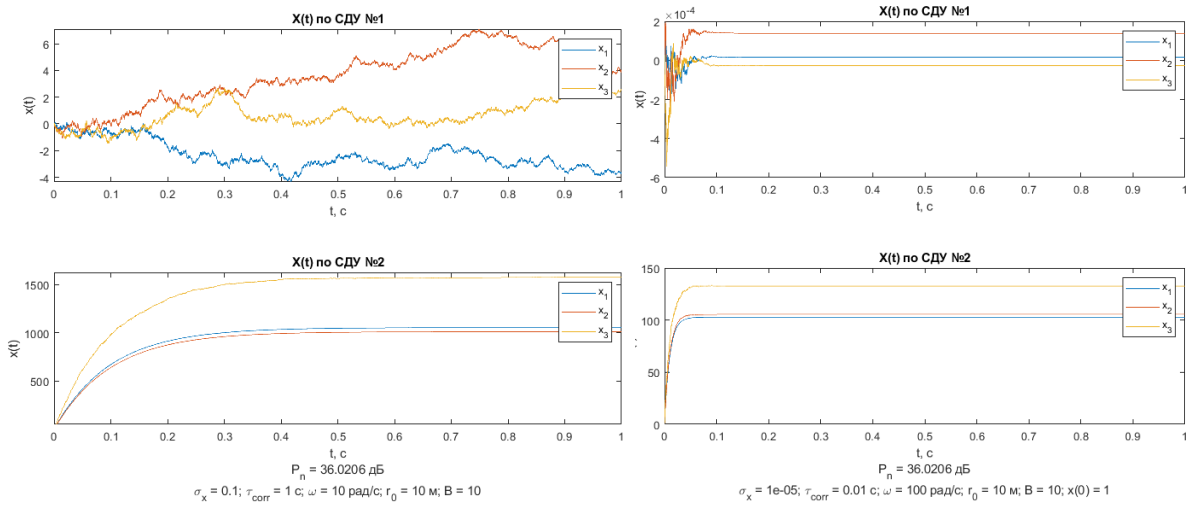
Следует помнить, что, в отличие от модели (8), теперь выражение $G(t)G^T(t)$ приравнивается не отмасштабированной единичной матрице $r_{ii} \cdot I$, а матрице $M(t) = \{m_{ij}(t)\}$, поэтому поиск g_{ij} сводится к решению более сложной системы уравнений вида:

$$GG^T(t) = \begin{bmatrix} g_{11}^2 + g_{12}^2 + \ldots + g_{1L}^2 & \ldots & g_{11}g_{L1} + g_{12}g_{L2} + \ldots + g_{1L}g_{LL} \\ \ldots & \ldots & \ldots \\ g_{11}g_{L1} + g_{12}g_{L2} + \ldots + g_{1L}g_{LL} & \ldots & g_{L1}^2 + g_{L2}^2 + \ldots + g_{LL}^2 \end{bmatrix} = \begin{bmatrix} m_{11} & \ldots & m_{1L} \\ \ldots & \ldots & \ldots \\ m_{L1} & \ldots & m_{LL} \end{bmatrix}.$$

Таким образом, нахождение элементов матрицы $\boldsymbol{G}(t)$ при данной постановке задачи встречает некоторые вычислительные сложности, которые определяются размерностью L.

На рис. 1-3 представлены графики, полученные при моделировании СДУ для различных сочетаний параметров. Введено обозначение P_n – мощность шума.

Для СДУ №1 (8) на рис. 1 изображена мнимая часть $\boldsymbol{X}$, а реальная часть постоянна и равна начальному значению $\boldsymbol{X}(0)$. Для СДУ №2 (9) изображен модуль $\boldsymbol{X}$. Выбранные расстояние между корреспондентами r_0 и частота ω задают условия работы в ближней зоне ($kr_0 < 1, k = \frac{2\pi}{\lambda}$).

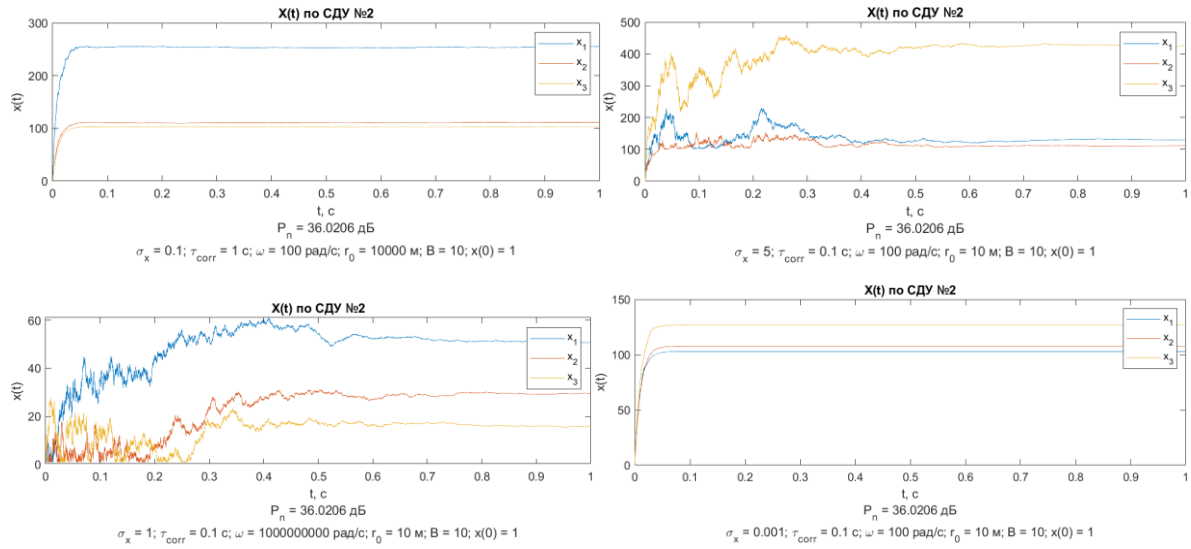


а) б)

Рис. 1. График зависимости $X(t)$ для 3 каналов обработки ($L = 3$) по СДУ №1 и №2 для а) дисперсии $\sigma_X^2 = 0.01$ и $\tau_{corr} = 1$ с; б) дисперсии $\sigma_X^2 = 10^{-10}$ и $\tau_{corr} = 0.01$ с

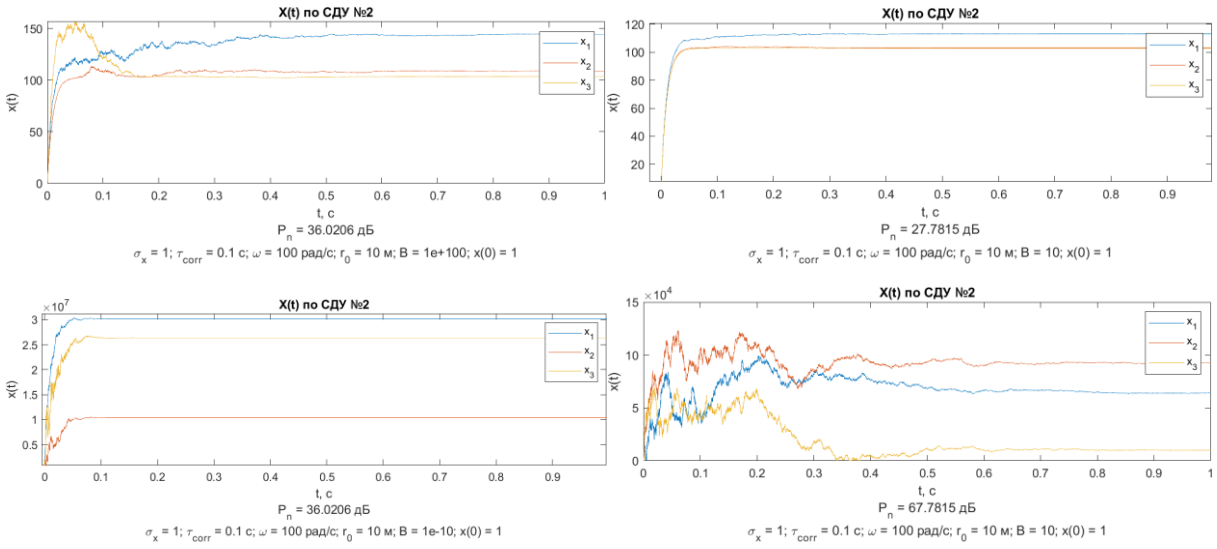
Для СДУ 1 СКО и интервал корреляции – единственные параметры, которые можно поменять. При уменьшении интервала корреляции (начиная с $\tau_{corr} \cong 0.1$ с) сигналы от разных антенн сходятся каждый к своему значению. СКО регулирует размах колебаний.

По рис. 2-3 можно наблюдать разницу в поведении сигналов при изменении расстояния между корреспондентами r_0 и круговой частоты ω, СКО σ_{XX}, коэффициента B, мощности шума P_n.



а) б)

Рис. 2. Графики зависимости $X(t)$ по СДУ №2 при изменении а) r_0 и ω, б) σ_{XX}



а) б)

Рис. 3. Графики зависимости $X(t)$ по СДУ №2 при изменении а) B и б) P_n

Список используемых источников

1. Шмелев А. Б. Основы марковской теории нелинейной обработки случайных полей //М.: Изд-во МФТИ. 1998.

2. Розанов Ю. А. Случайные поля и стохастические уравнения с частными производными //М.: Физматлит. 1995.

3. Кловский Д. Д., Конторович В. Я., Широков С. М. Модели непрерывных каналов связи на основе стохастических дифференциальных уравнений/ Под ред. Д. Д. Кловского. М.: Радио и связь, 1984. 248 с.

4. Глушанков Е. И., Конторович В. Я., Караваев Д. А. Математическое моделирование сигналов в непрерывных каналах связи в форме стохастических дифференциальных уравнений // Системы управления, связи и безопасности, 2023, № 4. С. 1-35.

5. Журавлев А. К. и др. Адаптивные радиотехнические системы с антенными решетками //Л.: Изд. Ленинградского университета. 1991.

SYNTHESIS OF STOCHASTIC DIFFERENTIAL EQUATIONS FOR MODELING RANDOM PROCESSES IN THE CORRELATION APPROXIMATION

Glushankov E., Kondrashov Z., Sudenkova A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
Research Institute of Microelectronic Equipment "Progress"

When modeling signals in space-time processing channels, as a rule, the cases of full or partial spatial coherence of signals in receiving antenna arrays are considered. Partial coherence is typical for traces with multipath, mobile networks, tropospheric and other radio communication channels, as well as when using broadband in the spatio-temporal sense of signals. In this paper, we synthesize multivariate stochastic differential equations for Gaussian random processes on the basis of correlation matrices and develop models for the stationary case.

Key words: *spatio-temporal processing, partially coherent signals, synthesis of stochastic differential equations, correlation matrix*

УДК 621.391.1
ГРНТИ 49.43.29

ИССЛЕДОВАНИЯ МЕТОДОВ КОДИРОВАНИЯ И МНОГОПОЗИЦИОННОЙ МОДУЛЯЦИи В КАНАЛАХ С ЗАМИРАНИЯМИ И ЭФФЕКТОМ ДОПЛЕРА

Е. И. Глушанков, К. К. Фам

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

Целью данной работы являлось исследование некоторых методов кодирования и многопозиционной модуляции в канале с замираниями. Предложен подход, основанный на моделировании воздействия канала с замираниями и эффектом Доплера на качества переданного сигнала. В результате представлены характеристики некоторых простых и комбинированных методов кодирования в канале передачи с некоторыми методами многопозиционной модуляции. Моделирование выполнялось в среде MATLAB.

помехоустойчивое кодирование, многопозиционная модуляция, канал Райса, эффект Доплера, MATLAB

Современные системы связи сталкиваются с множеством факторов, связанных с ухудшением качества передачи сигнала в реальных условиях. Одними из них являются влияние замираний и эффекта Доплера. Нахождение метода минимизации воздействия такого канала представляет собой важную задачу. В данной работе исследуется вероятность возникновения ошибок для различных методов кодирования и модуляции в условиях замирания и эффекта Доплера.

Предположим, что математическая модель канала связи с замираниями представлена следующим выражением:

$$s(t) = b(t)A(t-\tau)\cos[\omega_0 t + \Psi(t-\tau) - \varphi(t)] \quad (1)$$

где $b(t)$ – характеризует амплитудные замирания, $\varphi(t)$ – фазовый сдвиг по несущей частоте.

В данной работе рассматривается случай, при котором принимаемый сигнал формируется в условиях многолучевости и наличия прямой видимости между передатчиком и приемником. Данный тип канала известен как райсовский канал. Распределение плотности вероятности амплитуды сигнала в таком канале описывается вторым выражением [1, 2]:

$$p(b) = \frac{2bK}{b_0^2} exp\left(-\frac{Kb^2}{b_0^2} - K\right) I_0\left(\frac{2bK}{b_0^2}\right), b \geq 0 \quad (2)$$

$$S(f) = \frac{1}{\pi f_d \sqrt{1-(\frac{f-f_0}{f_d})^2}} \quad (3)$$

где b_0 – амплитуда прямой сигнала, $K = \frac{{b_o}^2}{2\sigma^2}$ – отношение мощности прямого сигнала к мощности многолучевого сигнала, $I_0(x)$ – модифицированная функция Бесселя первого рода нулевого порядка, f_d – частота Доплера.

Выражение (3) и рис. 1 иллюстрируют сдвиг частоты принимаемого сигнала относительно несущей частоты, обусловленный эффектом Доплера [3].

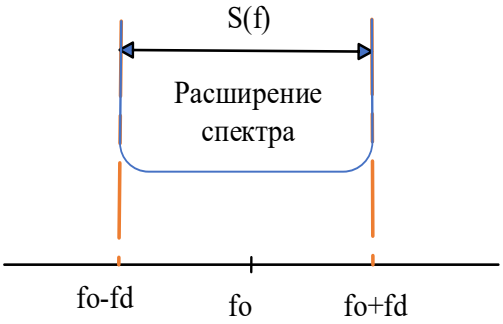


Рис. 1. Доплеровский спектр

Для уменьшения влияния замираний можно использовать методы помехоустойчивое кодирование со скоростью $R_c < 1$. Отметим, что при применении помехоустойчивых кодов удельная скорость передачи сообщений R_0, характеризующая спектральную эффективность системы связи, уменьшается по сравнению со случаем, когда кодирование отсутствует и она равна R_f. При использовании кодов она становится равной $R_0 = R_c R_f$ [4].

Важное направление повышения спектральной эффективности (увеличения R_0 при сохранении значения R_c) является применение методов модуляции различных уровней, таких как M-ФМ, M-КАМ и других. При этом, объединяя символы двоичного алфавита исходного сообщения в общем случае в блоки по K символов, то есть переходя к канальному алфавиту объемом $M = 2^K$. В этом случае удельная скорость передачи информации оказывается равной $R_0 = R_c R_f \, log_2 M$. Однако минимальное евклидово расстояние d_E между сигналами существенно уменьшается с увеличением их позиционности. Из-за этого снижается эффективность использования помехоустойчивого кодирования, что приводит к уменьшению энергетической эффективности [5, 6].

Таким образом, процессы многопозиционной модуляции и помехоустойчивого кодирования уже нельзя рассматривать в отрыве друг от друга. Они являются частями единого процесса, результатом которого становится формирование так называемых сигнально-кодовых конструкций (СКК) [7].

С целью разработки методов создания СКК, которые обеспечивают как высокую спектральную эффективность системы связи, так и высокую помехоустойчивость, в данной работе были применены методы помехоустойчивого кодирования в сочетании с методами многопозиционной модуляции (таблица 1) [8-12].

ТАБЛИЦА 1. Параметры помехоустойчивого кодирования

Типы кодов	Параметры кодов
Хэмминга	n = 63; k = 57; R_c = 57/63
БЧХ	n = 15; k = 7; R_c = 7/15
Рида-Соломона	n = 15; k = 9; R_c = 9/15
НСК	ν = 3; k = 1; n = 2; R_c = 1/2
Каскадный код	РС (15;9) + БЧХ (15;7)
Турбокод	ν = 3; L = 65536; R_c = 1/2

Предположим, что в канале с замираниями принятый сигнал состоит из основного сигнала и отраженных сигналов с временем задержки от 10^{-6} до 10^{-9} секунд. На рис. 2 представлены результаты анализа значений вероятности ошибки Рош при сочетании методов кодирования с М-ФМ и М-КАМ для разных значения М. Первый график демонстрирует передачи сигнала через канал с адаптивным белым гауссовым шумом, в то время как второй и третий графики отражают передачу сигнала через райсовский канал с частотой Доплера, равной нулю и ста Гц соответственно.

Из приведенных графиков можно сделать следующие выводы:

1. Каскадные коды и турбокоды демонстрируют хорошую способность к исправлению ошибок по сравнению с другими методами, несмотря на их более высокую вычислительную сложность;

2. Для достижения одинакового значения вероятности ошибки при использовании методов модуляции более высокого порядка требуется более высокое отношение сигнала к шуму;

3. С увеличением частоты Доплера влияние райсовского канала на качество принимаемого сигнала становится особенно значительным при использовании методов модуляции высокого порядка;

4. В условиях низкого ОСШ и сильного затухания рекомендуется использовать методы модуляции с высокой надежностью, такие как ФМ2 и ФМ4.

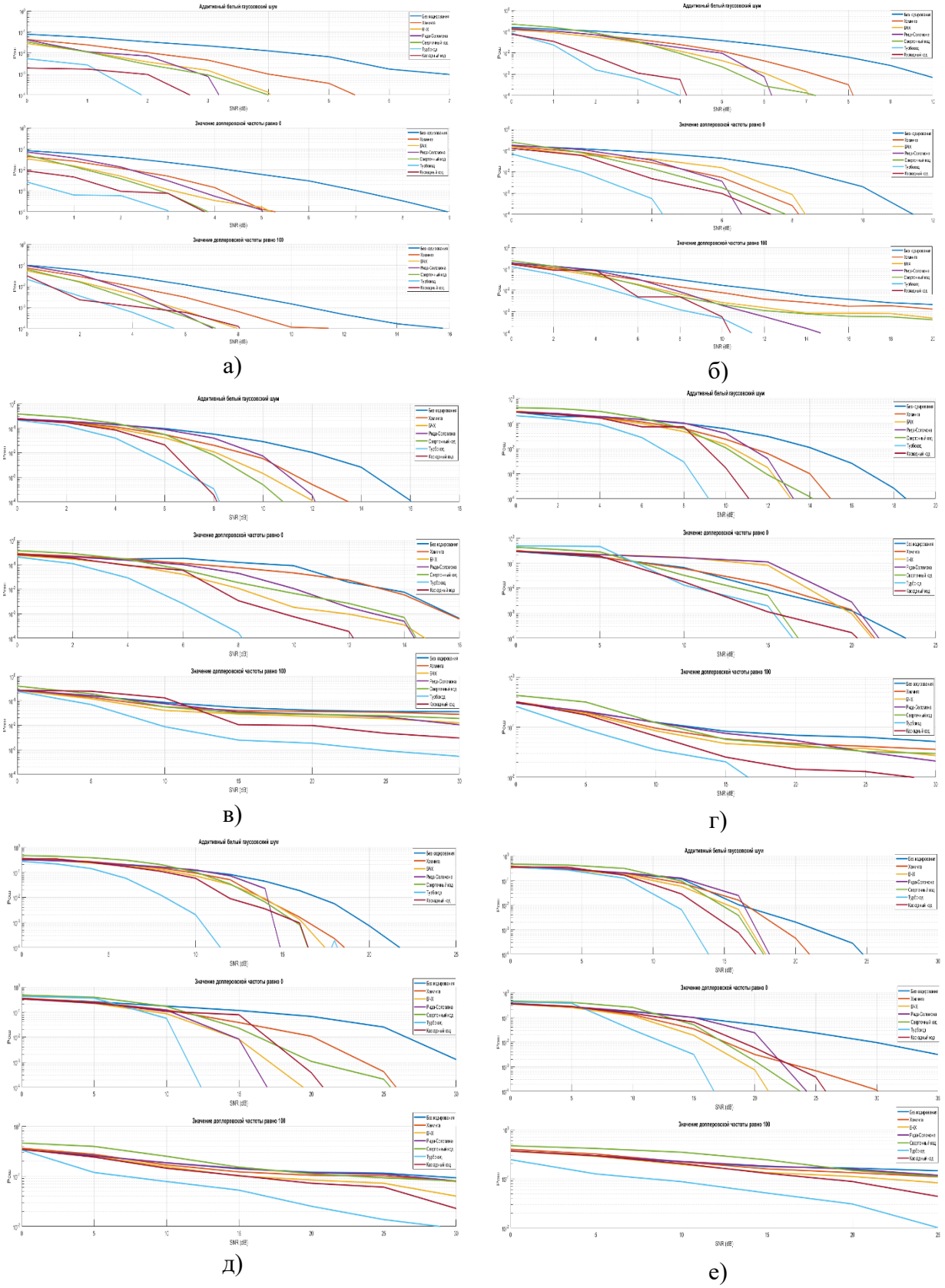


Рис. 2. Характеристики некоторых методов кодирования и модуляция: а) ФМ2; б) ФМ4; в) ФМ8; г) КАМ16; д) КАМ32; е) КАМ64 (K=5; $\tau_0 = 10^{-6} - 10^{-9}$)

В данной работе проведена оценка эффективности исправления ошибок некоторых простых и комбинированных методов кодирования в каналах с замираниями. Полученные результаты могут быть использованы для разработки методов создания сигнально-кодовых конструкций, обеспечивающих оптимальные значения спектральной и энергетической эффективности.

Список используемых источников

1. Дырин В. И., Исса А., Ишимов А. С. Математическая модель замираний для каналов беспроводной связи //Актуальные проблемы прикладной математики, информатики и механики. 2023. С. 402–410.

2. Чердынцев В. А. Прием сигналов на фоне помех. Учебное пособие для студентов радиотехнических специальностей. Минск 2007. 175 с.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / пер. с англ. Изд. 2-е, исп. М.: Вильямс, 2003. 1104 с.

4. Быховский М. А. Гиперфазовая модуляция оптимальный метод передачи сообщений в гауссовских каналах связи. Москва: ТЕХНОСФЕРА, 2018. 310 с. ISBN 978-5-94836-478-0.

5. Васильев К. К., Глушков В. А., Дормидонтов А. В., Нестеренко А. Г. Теория электрической связи: учебное пособие / под общ. ред. К. К. Васильева. Ульяновск: УлГТУ, 2008, 452 с.

6. Брычков Ю. А., Савищенко Н. В. Пропускная способность канала связи с квадратурной фазовой модуляцией и фазовым квантователем // Ученые записки Казанского университета. Серия Физико-математические науки. 2024. Т. 166. № 3. С. 306–319.

7. Варгаузин В. А. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи: учеб. пособие СПб.: БХВ-Петербург, 2013, 352 с. ISBN 978-5-9775-0878-0.

8. Золотарев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под. ред. чл.-кор. РАН Ю. Б. Зубарева, 2004, 126 с. ISBN 978-5-9775-0878-0.

9. Голиков А. М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: учебное пособие Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2016. 516 с.

10. Ершов А. Н. и др. Эффективность применения обобщенного каскадного кода в высокоскоростной радиолинии // Ракетно-космическое приборостроение и информационные системы. 2019. Т. 6. № 4. С. 32–36.

11. Дубовцева Д. А., Фрейман В. И. Исследование методов и алгоритмов турбокодирования в инфокоммуникационных системах // Автоматизированные системы управления и информационные технологии. 2019. С. 221–227.

12. Фрейман В. И., Дубовцева Д. А. Исследование алгоритмов мягкого декодирования в приемных устройствах элементов распределенных систем управления // Управление большими системами. УБС-2017. 2017. С. 267–277.

RESEARCH ON CODING METHODS AND MULTIPOSITION MODULATION IN CHANNELS WITH FADING AND THE DOPPLER EFFECT

Glushankov E., Fam C.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

The objective of this study was to investigate specific coding methods and multiposition modulation techniques in a fading channel. A proposed approach is based on modeling the impact of the fading channel and the Doppler effect on the quality of the transmitted signal. As a result, the study presents the characteristics of several simple and combined coding methods in a transmission channel using certain multiposition modulation techniques. The modeling was conducted in the MATLAB environment.

Key words: *Error-resilient coding, multiposition modulation, Rician channel, Doppler effect, MATLAB*

УДК 378.147
ГРНТИ 14.35.09

ИНТЕГРАЦИЯ ИНЖЕНЕРНЫХ ЗАДАЧ В КУРС ОБЩЕЙ ФИЗИКИ: ПОВЫШЕНИЕ МОТИВАЦИИ СТУДЕНТОВ ТЕХНИЧЕСКИХ ВУЗОВ

В. М. Деткова, О. А. Долматова

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

Статья посвящена проблемам преподавания физики в технических вузах с учетом современных требований к подготовке инженеров. Рассматриваются основные трудности, такие как снижение мотивации студентов, недостаточная связь физики с будущей инженерной деятельностью и слабая интеграция предмета с другими дисциплинами. Предложены методы активного обучения, включая использование инженерно-ориентированных задач, лабораторных работ с применением симуляционных программ. Особое внимание уделено внедрению междисциплинарного подхода, который способствует формированию у студентов комплексного понимания физики как основы для решения реальных инженерных задач. Приведены примеры практической реализации данных подходов и их влияние на успеваемость, вовлеченность студентов и качество их подготовки. Статья подчеркивает важность обновления методики преподавания физики для соответствия требованиям современного инженерного образования и рынка труда.

преподавание физики, технический вуз, цифровые технологии, междисциплинарный подход

Введение

Преподавание физики в техническом вузе играет ключевую роль в формировании у студентов фундаментальных знаний, необходимых для их будущей профессиональной деятельности. Однако традиционные методы обучения, ориентированные на изолированное изучение теоретических концепций, зачастую не позволяют студентам увидеть связь между физикой и реальными инженерными задачами. Это снижает интерес к предмету, ограничивает практическую направленность обучения и создает разрыв между образовательным процессом и потребностями инженерной практики [1].

В условиях стремительного развития технологий и растущего спроса на квалифицированных инженеров возникает необходимость пересмотра подходов к преподаванию физики. Современные образовательные методики должны ориентироваться на создание тесной взаимосвязи между тео-

рией и практикой, развитие междисциплинарного мышления и активное использование инженерно-ориентированных задач.

В данной статье рассматриваются основные проблемы и перспективы преподавания физики в технических вузах. Обсуждаются методы повышения мотивации студентов, примеры интеграции инженерных задач в учебный процесс, преимущества активных форм обучения, а также результаты их внедрения. Особое внимание уделяется перспективам междисциплинарного подхода, который позволяет более эффективно готовить студентов к решению сложных инженерных задач.

Проблема мотивации студентов: как связать базовый курс физики с будущей инженерной специальностью

Одной из ключевых задач преподавания физики в техническом вузе является формирование у студентов осознания значимости изучаемой дисциплины в контексте их будущей профессии. Однако на первых курсах, когда студенты только начинают осваивать основы электростатики, электромагнетизма и других разделов физики, связь между теоретическими знаниями и практическими инженерными задачами часто остается для них неочевидной.

Основная сложность заключается в том, что базовый курс физики нередко воспринимается студентами как отвлеченная теоретическая дисциплина, не имеющая прямого отношения к реальным инженерным задачам. Это снижает их мотивацию к глубокому изучению материала и приводит к пассивному восприятию знаний. Особенно остро эта проблема проявляется у студентов, которые изначально ориентированы на практическую деятельность, например, на разработку электроники, проектирование устройств или анализ сложных технических систем.

Чтобы преодолеть этот разрыв, важно показать студентам, что физика лежит в основе многих процессов, с которыми они будут работать в профессиональной деятельности. Например, понимание принципов работы полупроводников, методов анализа электрических цепей и основ термодинамики является критически важным для будущих инженеров-электронщиков. В этом контексте ключевым педагогическим приемом становится включение в курс физики примеров и задач, отражающих реальные инженерные приложения.

Таким образом, проблема мотивации студентов требует пересмотра традиционного подхода к преподаванию физики: теоретические темы

должны быть обогащены прикладным контекстом, который поможет студентам увидеть непосредственную пользу от изучаемого материала в их профессиональной деятельности.

Примеры интеграции: включение инженерных задач в курс физики

Интеграция инженерных задач в курс общей физики позволяет сделать изучаемый материал более прикладным и показать его практическую значимость. Такой подход особенно важен в техническом вузе, где от студентов требуется не только понимание теоретических основ, но и умение применять их для решения инженерных проблем.

Одним из удачных примеров является использование задач, связанных с анализом электрических цепей. Например, при изучении электростатики можно предложить студентам рассчитать емкость системы конденсаторов в сложной схеме, которую они могли бы встретить при разработке реальных электронных устройств. В теме электромагнитной индукции можно рассмотреть проектирование катушек индуктивности для использования в силовых трансформаторах. Такие задания не только помогают лучше усвоить теоретические концепции, но и формируют у студентов понимание их инженерного применения.

Интеграция инженерных задач в курс физики помогает создать образовательную среду, в которой студенты видят практическую ценность изучаемого материала, развивают навыки проектирования и получают опыт, связанный с реальными инженерными проблемами. Это не только способствует повышению мотивации, но и обеспечивает более качественную подготовку выпускников к профессиональной деятельности.

Методы активного обучения: лабораторные работы на основе инженерной практики

Методы активного обучения становятся ключевым инструментом для вовлечения студентов в процесс изучения физики и подготовки их к решению инженерных задач. В технических вузах особое внимание уделяется разработке таких форм обучения, которые позволяют студентам не только усвоить теоретические знания, но и применить их на практике.

Одним из наиболее эффективных подходов является использование инженерно-ориентированных лабораторных работ. В отличие от традиционных экспериментов, направленных на подтверждение теоретических законов, такие работы моделируют реальные технические задачи. Например, в

рамках курса электричества и магнетизма можно предложить студентам спроектировать и собрать схему, имитирующую реальный прибор, – например, зарядное устройство для аккумуляторов. При этом студенты работают с реальными компонентами, анализируют погрешности измерений и исследуют способы оптимизации схемы.

В дополнение к физическим экспериментам активно применяются компьютерные симуляции. Современные программные среды, такие как MATHCAD, MATLAB или LABVIEW, позволяют создавать цифровые модели физических процессов и изучать их поведение в различных условиях. Например, в разделе «Магнитостатика» студенты могут моделировать поведение электронов под действием внешнего магнитного поля. Такие симуляции не только экономят время, но и предоставляют доступ к анализу сложных процессов, которые трудно воспроизвести в лаборатории.

Комбинирование лабораторных работ и компьютерных симуляций создает учебную среду, приближенную к реальной инженерной деятельности. В результате они не только лучше усваивают физику, но и получают необходимую базу для успешного выполнения профессиональных обязанностей.

Примеры реализации инженерно-ориентированных подходов на успеваемость и вовлеченность студентов

Один из главных эффектов внедрения таких подходов – увеличение уровня вовлеченности студентов. Когда изучение физики связано с их будущей профессией, студенты начинают воспринимать материал как полезный инструмент, а не как абстрактную теорию.

Кроме того, использование инженерно-ориентированных заданий позволяет улучшить успеваемость. Исследования показывают, что применение прикладных задач и проектной деятельности помогает студентам легче усваивать сложные концепции, такие как электромагнитные поля или принципы работы полупроводниковых приборов. Это связано с тем, что студенты воспринимают теорию через призму ее практического применения, что значительно ускоряет процесс понимания [2].

Дополнительным показателем эффективности является рост числа студентов, которые начинают интересоваться научной и инженерной деятельностью за пределами обязательной программы. Многие из них вовлекаются в студенческие проекты, связанные с проектированием устройств или созданием инженерных решений, что подтверждает их осознанное отношение к изучению физики.

Преподаватели также отмечают, что применение таких подходов способствует развитию у студентов ключевых профессиональных компетенций, таких как анализировать данные и применять математический аппарат для решения инженерных задач. Эти навыки особенно ценны для их дальнейшей карьеры.

Таким образом, внедрение инженерно-ориентированных методов обучения не только повышает успеваемость и заинтересованность студентов, но и делает учебный процесс более эффективным, закладывая прочную основу для их профессионального становления.

Перспективы: возможности междисциплинарного подхода в подготовке инженеров

Современная инженерная подготовка требует не только глубокого понимания фундаментальных наук, но и способности интегрировать знания из разных областей для решения сложных задач. В этом контексте междисциплинарный подход становится важным элементом учебного процесса, а курс физики может играть в этом ключевую роль.

Одним из перспективных направлений является разработка совместных проектов на стыке физики, математики, информатики и инженерных дисциплин. Например, студенты могут моделировать поведение физических систем, таких как электромагнитные поля или теплообменные процессы, с использованием вычислительных методов и языков программирования. Такие проекты позволяют не только глубже понять физические принципы, но и освоить современные инструменты, востребованные в инженерной практике, такие как Python или MATLAB.

Еще одна важная перспектива – интеграция курса физики с профессионально-ориентированными дисциплинами. Например, изучение физики полупроводников можно связать с курсами электроники, где студенты рассматривают реальные примеры применения транзисторов и других элементов в схемотехнике. Подобная синергия облегчает восприятие сложных тем и помогает студентам видеть физику не как изолированную дисциплину, а как часть общей инженерной подготовки.

Междисциплинарный подход способствует формированию у студентов системного мышления – ключевого навыка современного инженера. Осознание взаимосвязи между различными науками позволяет им не только решать узкие задачи, но и находить инновационные подходы к сложным техническим проблемам.

Заключение

Преподавание физики в технических вузах нуждается в трансформации, направленной на повышение ее прикладного значения и интеграции с инженерной практикой. Современные методы обучения, ориентированные на связь теоретических знаний с реальными задачами, помогают студентам осознать важность физики для их профессионального развития, а также формируют необходимые навыки для успешной инженерной карьеры.

Инженерно-ориентированные задачи, активные методы обучения и междисциплинарный подход позволяют создать учебную среду, которая стимулирует студентов к самостоятельному поиску решений, развитию критического мышления и командной работы. Результаты внедрения таких подходов показывают их высокую эффективность: увеличивается вовлеченность студентов, растет их успеваемость, а также формируется целостное понимание взаимосвязей между физикой и другими дисциплинами.

Список используемых источников

1. Пономаренко Е. В. Анализ современного состояния методики преподавания физики в высшей школе: компетентностный подход // Международный журнал экспериментального образования. 2013. № 10-2. С. 207-210.

2. Лидер А. М., Склярова Е. А., Семкина Л. И. Вопросы методики преподавания курса физики в техническом университете // Фундаментальные исследования. 2015. № 2-4. С. 787-790.

INTEGRATION OF ENGINEERING PROBLEMS INTO THE COURSE OF GENERAL PHYSICS: INCREASING MOTIVATION OF STUDENTS OF TECHNICAL UNIVERSITIES

Detkova V., Dolmatova O.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the problems of physics teaching in technical universities taking into account modern requirements for engineering training. We considered the main difficulties, such as lack of student motivation, insufficient connection of physics with future engineering profession and weak integration of the subject with other disciplines. We proposed active learning methods, including the use of engineering-oriented tasks, laboratory work with the use of simulation programs. Particular attention is paid to the introduction of an interdisciplinary approach that helps students develop a comprehensive understanding of physics as a basis for solving real engineering problems. Examples of the practical implementation of these approaches and their impact on academic performance, student involvement and the quality of their training are given. The article emphasizes the importance of updating the methodology of physics teaching to meet the requirements of modern engineering education and the labor market.

***Key words**: physics education, teaching physics, technical university, digital technologies, interdisciplinary approach*

УДК 378.146
ГРНТИ 14.35.09

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРЕПОДАВАНИЯ ФИЗИКИ: КРИТЕРИИ, МЕТОДЫ И ИНСТРУМЕНТЫ ОБРАТНОЙ СВЯЗИ

В. М. Деткова, О. А. Долматова

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

Статья посвящена проблемам оценки эффективности преподавания физики в технических вузах в условиях современных вызовов образования. Рассмотрены ключевые аспекты, включая критерии оценки, методы и инструменты обратной связи. Особое внимание уделено интеграции цифровых технологий, проектному обучению и формирующему оцениванию, которые позволяют сделать образовательный процесс более гибким и ориентированным на результат. Статья подчеркивает, что оценка эффективности преподавания является не только инструментом контроля, но и важным элементом стратегии развития образовательных программ, способствующим повышению качества подготовки будущих инженеров. Перспективы дальнейшего развития связаны с углублением интеграции цифровых технологий и усилением междисциплинарного подхода.

преподавание физики, технический вуз, оценка эффективности, цифровые технологии, проектное обучение, обратная связь, формирующее оценивание.

Введение

Преподавание физики в техническом вузе – не просто передача фундаментальных знаний. В первую очередь это формирование инженерного типа мышления. Как дисциплина, физика учит анализировать, моделировать и объяснять процессы, лежащие в основе современных технологий. Эффективность преподавания физики напрямую влияет на качество профессиональной подготовки любого технического специалиста.

Оценка эффективности преподавания должна выполнять не контролирующую, а регулятивную функцию. Оценка должна быть встроена в образовательный процесс и непрерывно корректировать его. Речь не только о результатах студентов. Важнее оперативно понимать, какие методики работают, где теряется мотивация, какие формы подачи учебного материала обеспечивают вовлечение в процесс.

Также проблемой является зазор между тем, что изучается на занятиях, и тем, что реально востребовано в инженерной практике. В реальной работе

инженер сталкивается с неопределенными условиями – с задачами, в которых нет заранее известного алгоритма. Поэтому актуальным стало внедрение методов анализа, моделирования, поиск решения. Например, физические расчеты, встроенные в проект устройства связи, или анализ работы реальных технических систем, помогают увидеть, зачем студенту физика.

Оценка знаний в вузах по-прежнему часто строится на финальных экзаменах и контрольных. Но такой подход не дает понимания и не помогает двигаться вперед. Здесь могут помочь простые форматы обратной связи по ходу курса: короткие тесты, разбор типичных ошибок, обсуждение промежуточных результатов. Это позволяет понять, над чем еще стоит поработать, а преподаватель может вовремя скорректировать подачу материала.

Цель статьи – определить ключевые критерии, методы и инструменты оценки, позволяющие сделать преподавание физики в техническом вузе гибким, встроенным в формирование профессионально значимых умений.

Критерии оценки эффективности преподавания

Оценить качество преподавания – задача непростая. Сам по себе результат экзамена или средний балл мало что говорит о том, насколько успешно обучение. Так что важно подходить к оценке комплексно, учитывая не только объем усвоенного, но и то, как он используется, насколько он становится частью профессионального мышления. Рассмотрим ключевые направления, по которым можно судить об эффективности преподавания (с упором на реальные цели инженерного образования).

1. Достижения студентов с позиции компетенций

Способность применять знания в задачах, приближенных к профессиональной практике означает, что кроме тестов, задач, контрольных требуется включать задания на моделирование физических процессов в технических системах.

Еще важнее дифференцировать виды достижений. С одной стороны, учитывать академические успехи: знание формул, понимание теории, умение решать стандартные задачи. С другой – практические: способность сформулировать физическую модель реальной задачи, выбрать подходящий метод расчета, обосновать допущения. Такая дифференциация дает более аккуратную картину прогресса каждого студента и помогает корректировать курс в нужную сторону.

2. Устойчивый интерес к дисциплине и ожидания профессионального сообщества

Высокая мотивация студентов – лучший признак того, что преподавание работает. Однако оценить мотивацию еще сложнее, чем оценить знания.

Сделать это можно не только через анкетирование, но и по косвенным признакам: участие в дополнительных мероприятиях, активность на занятиях, интересные вопросы, которые задают студенты. Большую роль здесь играет личность преподавателя, его умение заражать интересом, находить примеры из жизни, поддерживать инициативу.

Кроме того, хороший курс должен быть тесно связан с тем, что происходит в профессии. Значит, важный критерий эффективности – насколько содержание и формат преподавания соответствуют запросам индустрии.

Здесь важна обратная связь работодателей, материалов, ориентация на профстандарты, отраслевые рекомендации. Если физика подана как инструмент решения реальных задач, а не как набор отвлеченных формул, она воспринимается иначе.

Методы оценки эффективности преподавания

Оценка преподавания не может и не должна сводиться к единому показателю. Необходим целый комплекс методов, которые будут фиксировать уровень освоения теоретического материала, способность применять знания. Это требует сбалансированного сочетания различных подходов.

1. Комбинирование традиционного и формирующего оценивания

Традиционные инструменты – экзамены, зачеты, контрольные работы – обеспечивают базовую проверку качества знаний. Они привычны и необходимы, но обладают ограниченной диагностической ценностью: фокусируются лишь на воспроизведении информации. Глубина понимания или способность к переносу знаний в новые контексты остается за кадром.

Другой метод – формирующее оценивание – позволяет отслеживать динамику обучения и оперативно реагировать на возникающие затруднения. Здесь важны регулярные мини-тесты, парная и групповая оценка, а также письменные или устные опросы.

В любом случае оценивание должно быть встроено в образовательный процесс, то есть выступать не финальным актом профпригодности, а частью обучения. Это способ развития, а не только контроля.

2. Проектно-ориентированные методы и цифровые инструменты

Проектные форматы позволяют студенту индивидуально воспринимать условия задачи, выбирать методы, аргументировать решения. Проекты – прекрасная форма комплексной оценки метапредметных и профессиональных компетенций: самостоятельности, командной работы, критичности мышления.

Критерии оценивания здесь включают оригинальность решений, обоснованность методов, полноту анализа и качество представления результатов.

Современная цифровая среда предоставляет широкие возможности для точного, своевременного оценивания. Образовательные платформы позволяют отслеживать активность, темп и глубину усвоения учебного материала каждым студентов по отдельности [1].

Виртуальные лаборатории поднимают уровень исследовательских и практических навыков – планирование экспериментов, интерпретацию данных, обоснование выводов.

Цифровые инструменты не подменяют преподавателя, но усиливают его возможности: они делают оценку глубже, а корректировку образовательного процесса – быстрее.

3. Междисциплинарный проектный подход

Междисциплинарные формы обучения особенно актуальны в нынешних условиях, когда широта проблем так контрастирует с узостью специализации. Физика, будучи фундаментальной наукой, обладает высоким потенциалом для интеграции ее с прикладными дисциплинами. В первую очередть это телекоммуникации, электроника, программирование, мехатроника.

Оценка междисциплинарных проектов требует гибкой системы критериев: корректность физического моделирования, инженерную реализуемость, оригинальность, обоснованность, ясность представления результата. Участие преподавателей-специалистов из разных областей позволяет сделать оценку объективной, многомерной.

Внедрение междисциплинарных форматов не требует полной перестройки курса, и это очень важно в ситуации. когда модернизация образования не может быть выстроена одномоментно. Однако, система нуждается в четкой координации и поддержке со стороны кафедр. Оптимально начинать с пилотных элементов: одного-двух модулей в семестре – с последующим расширением, по мере накопления опыта.

В конечном счете, реализация данного пункта позволяет развивать системное инженерное мышление, формировать навыки, максимально приближенные к практике.

Инструменты обратной связи

Эффективная система обратной связи – ключевой элемент оценки преподавания физики в техническом вузе. Она позволяет преподавателю не только своевременно выявлять пробелы в обучении, но и гибко адаптировать методику под реальные запросы студентов и профессиональной среды [2].

Обратная связь должна встраиваться как в структуру курса, так и в повседневную практику преподавания. Один уровень – это регулярные итоговые опросы после тем и модулей, позволяющие оценить целостное восприятие курса. Другой – краткие онлайн-опросы и мини-рефлексии, выявляющие локальные трудности и снижение интереса. Это дает преподавателю возможность быстро корректировать содержание, темп и формат подачи образовательного материала.

При анкетировании важно использовать как структурированные шкалы, так и открытые вопросы, позволяющие получить содержательную обратную связь. Собранные данные анализируются и обобщаются в виде кратких отчетов. Это позволяет преподавателям видеть сигналы о необходимости корректировки.

Анонимное анкетирование позволяет зафиксировать 1) уровень удовлетворенности, 2) глубину вовлеченности обучающихся. Важно использовать различные шкалы, например, оценивать с одной стороны такие аспекты как ясность, полезность, а с другой – эмоциональные (мотивация, уверенность в себе).

Рефлексия преподавателя о процессе обучения также должна быть не эпизодической, а системной. Анализ причин неуспешного восприятия тем, учет повторяющихся ошибок на промежуточных аттестациях – все это формирует вузовскую культуру педагогики. Горизонтальная оценка профессионального роста – совместная экспертиза с коллегами – помогает избежать методических замыканий. Взаимопосещение занятий, анализ материалов, совместное создание проектов позволяют выработать общие принципы преподавания и создать дружественную и эффективную рабочую обстановку.

Заключение

Оценка эффективности преподавания физики в техническом вузе – это важнейшая часть образовательного процесса. Эффективное преподавание – это не только усвоение теоретического материала, но и формирование профессионального мышления, тренировки решать инженерные задачи, работать в команде, применять знания в контексте будущей профессии.

Такая стратегия позволяет грамотно выстраивать инженерное образование, цель которого не только передавать знания, но и формировать компетентных специалистов, быстро адаптирующихся в современных реалиях.

Список используемых источников

1. Герасимова Е. К. Цифровизация образования: от теории к практике сети: учеб. пособие. М.: Знание-М, 2022. 155 с.

2. Липатова Н. Г., Никитченко И. И., Сомов Ю. И. Информационные технологии в науке и образовании / под общ. ред. канд. техн. наук, ст. науч. сотр. Н.°Г.°Липатовой. М.: РИО Российской таможенной академии, 2023. 381 с.

ASSESSMENT OF EFFECTIVENESS OF PHYSICS TEACHING: CRITERIA, METHODS AND FEEDBACK TOOLS

Detkova V., Dolmatova O.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the problems of effectiveness assessment of physics teaching in technical universities in the context of modern educational challenges. We considered key aspects, including assessment criteria, methods and feedback tools. We paid particular attention to the integration of digital technologies, project-based learning and formative assessment, which make the educational process more flexible and results-oriented. The article emphasizes that the assessment of teaching effectiveness is not only a control tool, but also an important element of the strategy for developing educational programs that contributes to improving the quality of future engineering training. Prospects for further development are associated with the deepening integration of digital technologies and strengthening of the interdisciplinary approach.

***Key words**: teaching physics, technical university, digital technologies, performance assessment, project-based learning, feedback, formative assessment*

УДК 378.147.88
ГРНТИ 14.35.09

АПРОБАЦИЯ МЕТОДИЧЕСКИХ УКАЗАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ «ИЗУЧЕНИЕ ЯВЛЕНИЙ И ЗАКОНОВ ВОЛНОВОЙ ОПТИКИ. ДВУЛУЧЕПРЕЛОМЛЕНИЕ. ЧЕТВЕРТЬВОЛНОВАЯ ФАЗОВАЯ ПЛАСТИНКА»

В. М. Деткова, Н. Л. Урванцева, Ю. В. Шарихина

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

Санкт-Петербургским государственным университетом телекоммуникаций им. проф. М. А. Бонч-Бруевича был приобретен комплект учебно-лабораторного оборудования «Квантовая оптика», переданного на кафедру физики. Работа посвящена апробации в учебном процессе методических указаний для выполнения лабораторной работы «Изучение явлений и законов волновой оптики. Двулучепреломление. Четвертьволновая фазовая пластинка», входящей в состав данного комплекса. Лабораторная установка позволяет получить эллиптически поляризованный свет из линейно поляризованного с помощью четвертьволновой пластинки и проанализировать результаты. Лабораторная работа будет введена в учебный процесс в рамках дисциплин «Физика (спецглавы)» и «Физика конденсированного состояния» в СПбГУТ им. проф. М. А. Бонч-Бруевича.

волновая оптика, двулучепреломление, поляризованный свет, четвертьволновая фазовая пластинка

Свет имеет волновую природу. Рассмотрим электромагнитную волну, которая состоит из двух взаимно перпендикулярных компонент: вектора напряженности электрического поля $\vec{E}$ и вектора напряженности магнитного поля $\vec{H}$. Эти вектора образуют с вектором скорости $\vec{V}$ правую тройку векторов [1, 2].

Рассмотрим световую волну, распространяющуюся вдоль оси z [1, 2]. Вектор $\vec{E}$ совершает колебания в плоскости XY. Его можно разложить на две компоненты если нет поглощения в среде:

$$\vec{E} = \vec{E}_x + \vec{E}_y, \vec{E}_x = \vec{\imath}E_{x0}\cos\omega t, \vec{E}_y = \vec{\jmath}E_{y0}\cos(\omega t + \delta),$$

где ω – частота колебаний, δ – разность фаз между компонентами светового вектора $\vec{E}_x$ и $\vec{E}_y$.

Тангенс угла между вектором $\vec{E}$ и осью OX

$$tg\varphi = \frac{E_{y0}\cos(\omega t+\delta)}{E_{x0}\cos\omega t}. \quad (1)$$

Для естественного света при случайных хаотических изменениях разности фаз δ угол φ меняется случайным образом. Такой свет можно представить в виде суммы двух взимноперпендикулярных некогерентных составляющих. Свет называется поляризованным в случае, когда колебания $\vec{E}$ подчиняются определенному закону.

Выделяют несколько видов поляризации. Из (1) следует, что:

1. $\delta = 0 \pm \pi \Rightarrow \mathrm{tg}\varphi = const$

Результирующий вектор $\vec{E}$ совершает колебание вдоль прямой, лежащей в плоскости XY. Это случай линейно поляризованного света.

2. $\delta = 0 \pm {}^{\pi}/_{2}$ и $E_{x0} = E_{y0} \Rightarrow tg\varphi = \pm \mathrm{tg}(\omega t)$

В случае круговой поляризации конец светового вектора $\vec{E}$ описывает окружность в плоскости XY с угловой скоростью ω.

3. $\delta = 0 \pm {}^{\pi}/_{2}$, $E_{x0} \neq E_{y0}$

Конец вектора $\vec{E}$ будет описывать эллипс, полуоси которого равны соответствующим амплитудам E_{x0} и E_{y0}. Это эллиптически поляризованная волна.

Для изотропных сред вектор напряженности электрического поля $\vec{E}$ связан с вектором электрического смещения $\vec{D}$ соотношением: $\vec{D} = \varepsilon\varepsilon_0\vec{E}$.

Относительная диэлектрическая проницаемость среды ε в этом случае – скалярная величина. Для анизотропной среды, свойства которой разные в различных направлениях вектора $\vec{E}$ и $\vec{D}$ не параллельны друг другу, для характеристики оптических свойств среды требуется 9 величин (тензор диэлектрической проницаемости).

Используя оптически анизотропные среды, можно получить циркулярно и эллиптически поляризованный свет. Отличительной особенностью таких сред является зависимость относительной диэлектрической проницаемости ε от направления. Следовательно, волны, распространяющиеся в разных направлениях, будут иметь разные скорости $V = c/n$, где c – скорость света в вакууме, $n = \sqrt{\mu\varepsilon} \approx \sqrt{\varepsilon}$ при μ≈1.

В случае падения линейно поляризованного света на анизотропное вещество в среде будут распространяться с разными скоростями две волны, линейно поляризованные во взаимно перпендикулярных направлениях. Оптической осью кристалла называется направление, вдоль которого волны распространяются с одинаковой скоростью. В одноосных кристаллах одна оптическая ось, в двуосных – две.

Пусть линейно поляризованный свет падает на одноосный кристалл, представляющий собой плоскопараллельную пластинку толщиной *d,* вырезанную параллельно оптической оси *OO`* (рис. 1).

Направим ось *OX* вдоль главной оси кристалла (рис. 1) и обозначим угол между напряженностью электрического поля падающей линейно поляризованной световой волны и оптической осью через φ, а амплитуду светового вектора через E_0. Разложим вектор напряженности электрического поля $\vec{E}$ на две составляющие: $\vec{E} = \vec{E}_{\parallel} + \vec{E}_{\perp}$. $\vec{E}_{\perp}$ соответствует обыкновенной волне с показателем преломления n_o, $\vec{E}_{\parallel}$ – необыкновенной с показателем преломления n_e. Направление колебаний $\vec{E}$ обыкновенной волны перпендикулярно главной плоскости, которая проходит через направление распространения света и оптическую ось. У второй волны вектор напряженности электрического поля колеблется вдоль оптической оси в главной плоскости кристалла.

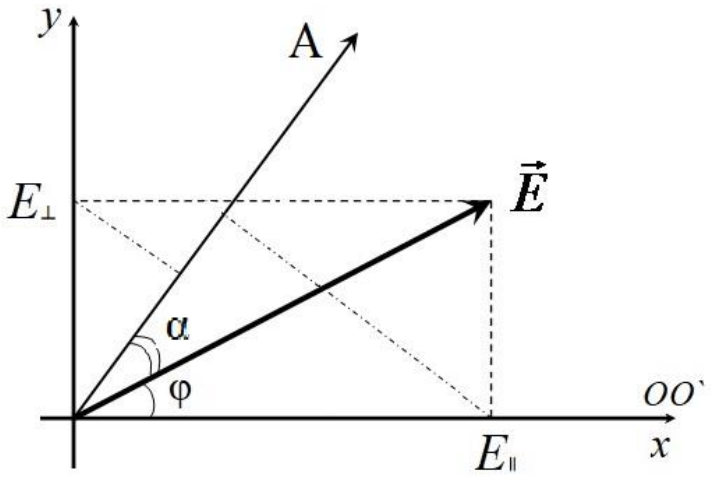


Рис. 1. Вектор напряженности электрического поля $\vec{E}$ и его составляющие

Амплитудные значения векторов напряженности электрического поля на входе анизотропной пластинки:

$$E_{\parallel} = E_0 \cos\varphi,\ E_{\perp} = E_0 \sin\varphi$$

Оптическая разность хода между обыкновенной и необыкновенной волнами равна:

$$\Delta = (n_e - n_0)d,\ (2)$$

где *d* – толщина пластинки.

При этом разность фаз на выходе из пластинки: $\delta = 2\pi\Delta/\lambda_0$,
где λ_0 – длина волны света в вакууме.

Компоненты светового вектора на выходе кристаллической пластинки взаимно перпендикулярны:

$$E_{\parallel} = E_0 \cos\varphi \cos(\omega t + \delta),\ E_{\perp} = E_0 \sin\varphi \cos\omega t$$

Для наблюдения интерференционной картины на пути света располагают еще один поляризатор (анализатор) А. Обозначим α угол между вектором $\vec{E}$ и направлением пропускания анализатора. Амплитуды составляющих вектора $\vec{E}$ обыкновенной и необыкновенной волн на выходе анализатора:

$$E_{\parallel A} = E_0 \cos\varphi \cos(\alpha + \varphi),\ E_{\perp A} = E_0 \sin\varphi \sin(\alpha + \varphi)$$

Лучи, вышедшие из анализатора, интерферируют, так как обыкновенная и необыкновенная волны в пластинке когерентны. Интенсивность на выходе анализатора:

$$I = I_0 \left[\sin^2\varphi \sin^2(\alpha + \varphi) + \cos^2\varphi \cos^2(\alpha + \varphi) + \frac{1}{2}\sin 2\varphi \sin 2(\alpha + \varphi) \cos\delta\right].$$

Формула справедлива для любого взаимного расположения анализатора и поляризатора.

Явление двулучепреломления (ДЛП) используют для получения поляризованного света. Существует два класса приборов: для его изучения поляризационные приборы и дихроичные пластинки.

На рис.º2 представлен лабораторный стенд «Волновая оптика».

Установка позволяет получить эллиптически поляризованный свет из линейно поляризованного и проанализировать результаты. В данной лабораторной работе используют кварцевую пластинку λ/4, склеенную из двух пластинок толщиной d_1 и d_2 ($d = d_1 + d_2$), оптические оси которых взаимно перпендикулярны. Показатели преломления кварца для λ = 0,635 мкм равны n_o = 1,5423 и n_e = 1,5513. Обыкновенная волна в первой пластинке становится необыкновенной во второй и наоборот. Вследствие неравенства толщины пластинок появляется разность фаз. Установка дает возможность проанализировать вид поляризации прошедшего света. При этом оптическая разность хода волн будет равна:

$$\Delta = (n_o d_1 + n_e d_2) - (n_e d_1 + n_o d_2) = (d_2 - d_1)(n_e - n_o),\ \Delta = m\lambda_0/4,$$

где m = 1, 3, 5…

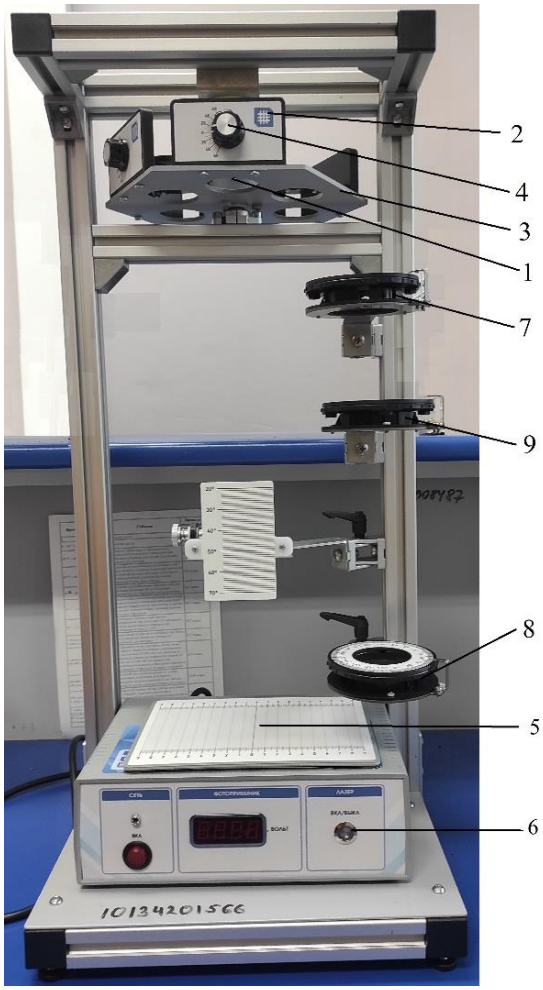


Рис. 2. Внешний вид лабораторного стенда «Волновая оптика»

1 – источник излучения, 2 – пиктограммы элементов, 3 – турель, 4 – поворотное устройство, 5 – экран, 6 – блок питания, 7, 8 – поляроиды, 9 – пластинка λ/4.

При использовании четвертьволновой пластинки в качестве двулучепреломляющего образца результирующая интенсивность равна:

$$I = I_0[sin^2\,\varphi\, sin^2(\alpha+\varphi) + cos^2\,\varphi\, cos^2(\alpha+\varphi)].$$

На выходе из пластины получим эллиптически поляризованный свет. При этом направление осей эллипса совпадает с направлением координатных осей.

Если оптическая ось составляет с направлением светового вектора $\vec{E}$ угол $\varphi = 45^{\circ}$, то на выходе из пластины свет будет обладать круговой поляризацией:

$$I = \frac{I_0}{2}\left(sin^2\left(\alpha+\frac{\pi}{4}\right) + cos^2\left(\alpha+\frac{\pi}{4}\right)\right) = \frac{I_0}{2}.$$

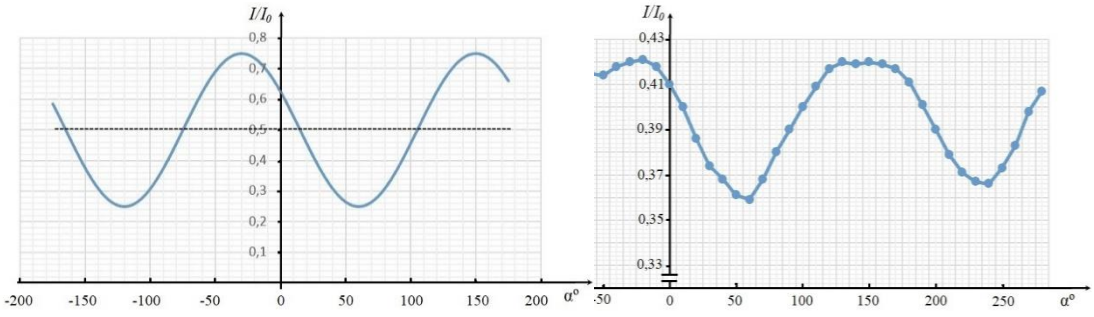
Интенсивность света на выходе из анализатора не зависит от угла между анализатором и поляризатором.

При установке главного направления поляризатора под углом 45° с оптической осью пластинки можно снять зависимость тока фотоприемника от углового положения анализатора α. Эллиптичность выходного излучения света зависит от точности установки угла φ.

Для оценки вида поляризации излучения необходимо снять зависимость выходного сигнала от угла поворота анализатора при различных положениях поляризатора на входе $\varphi = 0^{\circ}, 30^{\circ}, 45^{\circ}, 60^{\circ}$.

На рис. 3 для примера приведены теоретическая (а) и экспериментальная (б) зависимости относительной интенсивности I/I_0 от угла α для $\varphi = 30^{\circ}$. Интенсивность на выходе из пластины:

$$I = I_0\left(\frac{1}{4}sin^2\left(\alpha+\frac{\pi}{6}\right)+\frac{3}{4}cos^2\left(\alpha+\frac{\pi}{6}\right)\right) = \frac{I_0}{4}\left(2+cos\left(2\alpha+\frac{\pi}{3}\right)\right).$$



а) б)

Рис. 3. Теоретическая (а) и экспериментальная (б) зависимости относительной интенсивности от угла поворота анализатора α для $\varphi = 30^{\circ}$. Пунктиром приведена теоретическая зависимость для случая круговой поляризации

Как видно из представленных графиков, вид зависимостей совпадает, с учетом поправки на потери интенсивности в оптических элементах схемы.

Представленный лабораторный стенд позволяет получить свет эллиптической и круговой поляризации из линейно поляризованного с помощью четвертьволновой пластинки, а также провести анализ зависимости относительной интенсивности от угла поворота анализатора.

Список используемых источников

1. Борн М., Вольф Э. Основы оптики: пер. с англ. М.: Наука, 1973. 720 с.

2.Сивухин Д. В. Общий курс физики. Оптика: М.: Наука, 1980. 752 с.

3. Урванцева Н. Л. Оптическая физика: учебное пособие / Н. Л. Урванцева. СПб.: СПбГУТ, 2019. 100 с.

TESTING THE METHODOLOGICAL INSTRUCTIONS FOR EXECUTING THE LABORATORY WORK "STUDY OF THE PHENOMENA AND LAWS OF WAVE OPTICS. BIREFRINGENCE. QUARTER-WAVE PHASE PLATE"

Detkova V., Urvantseva N., Sharikhina Yu.
The Bonch-Bruevich St Petersburg State University of Telecommunications

The Bonch-Bruevich St Petersburg State University of Telecommunications purchased a set of educational and laboratory equipment "Wave Optics", transferred to the Department of Physics. The report is devoted to the testing in the educational process of methodological instructions for performing the laboratory work "Study of the phenomena and laws of wave optics. Birefringence. Quarter-wave phase plate", which is part of this complex. The laboratory setup allows to obtain elliptically polarized light from linearly polarized light using a quarter-wave plate and analyze the results. Laboratory work will be introduced into the educational process within the framework of the disciplines "Physics (special chapters)" and "Physics of Condensed Matter" at The Bonch-Bruevich St Petersburg State University of Telecommunications.

***Key words**: wave optics, birefringence, polarized light, quarter-wave phase plate*

УДК.681.51
ГРНТИ 47.05.05

РАЗРАБОТКА И СОЗДАНИЕ ВИРТУАЛЬНОГО ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ИССЛЕДОВАНИЮ УСТОЙЧИВОСТИ АКТИВНЫХ ЧЕТЫРЕХПОЛЮСНИКОВ

З. В. Зайцева

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

Рассматриваются вопросы разработки и создания виртуального лабораторного практикума по исследованию вопросов устойчивости ARC-цепей на основе использования интегрированной программной среды Mathcad и Fastmean. Показано, как использование компьютерных технологий, позволяющих проводить моделирование при выполнении лабораторных работ, повышает наглядность и эффективность освоения материала при изучении различных критериев устойчивости

лабораторный практикум, ARC-цепи, критерии устойчивости, интегрированная программная среда, моделирование процессов

Одной из важнейших задач, возникающих при проектировании самых разнообразных цепей, является задача исследования проектируемой цепи на устойчивость [1, 2]. Важной задачей при анализе работы активного четырехполюсника является задача определения параметров, при которых он является устойчивым, поскольку изменение параметров ARC-цепи, приводящее к нарушению устойчивости, приводит к недопустимым режимам работы системы в целом. Происходит неконтролируемый рост сигналов, что вызывает искажения, перегрев или даже разрушение элементов системы.

Анализ устойчивости электрических цепей проводится на основе их операторных передаточных функций, представленных в виде отношения полиномов:

$$H(p) = \frac{W(p)}{V(p)} = \frac{b_m p^m + b_{m-1} p^{m-1} + \cdots b_1 p + b_0}{p^n + a_{n-1} p^{n-1} + \cdots a_1 p + a_0}.$$

Полином знаменателя $V(p)$ представляет собой характеристический полином. Корни характеристического уравнения

$$V(p) = p^n + a_1 p^{n-1} + \cdots a_{n-1} p + a_n = 0$$

совпадают с полюсами операторной передаточной функции p_k и определяют свободную (собственную) составляющую реакции цепи:

$$f_{\text{св}}(t) = \sum_{k=1}^{n} A_k e^{p_k t}.$$

Для анализа устойчивости активной цепи были использованы два основных критерия устойчивости: критерий устойчивости Гурвица и критерий устойчивости Найквиста.

Согласно критерию устойчивости Гурвица, в знаменателе операторной передаточной функции любой устойчивой цепи должен быть полином, корни которого расположены в левой полуплоскости комплексной плоскости. Этот полином называется полиномом Гурвица.

Критерий Найквиста применяется для анализа устойчивости систем с обратной связью. Он основан на построении годографа петлевого усиления цепи и проверке его положения относительно критической точки (1, j0). Если годограф не охватывает эту точку, система устойчива.

Исследование вопросов устойчивости ARC-цепей было предложено провести на основе использования интегрированной программной среды Mathcad и Fastmean. Известно, что компьютерные технологии обучения позволяют использовать наиболее оптимальные возможности человеко-машинного взаимодействия в формате студент-персональный компьютер (ПК) [3-5].

В лабораторном практикуме студентам для анализа была предложена ARC-цепь. Необходимо исследовать данную цепь на устойчивость, используя два критерия устойчивости, перечисленные выше.

Поставленная задача решалась следующим образом. Сначала проводился символьный анализ цепи с использованием программы Fastmean, в результате которого было получено выражение для операторной передаточной функции цепи (рис. 1).

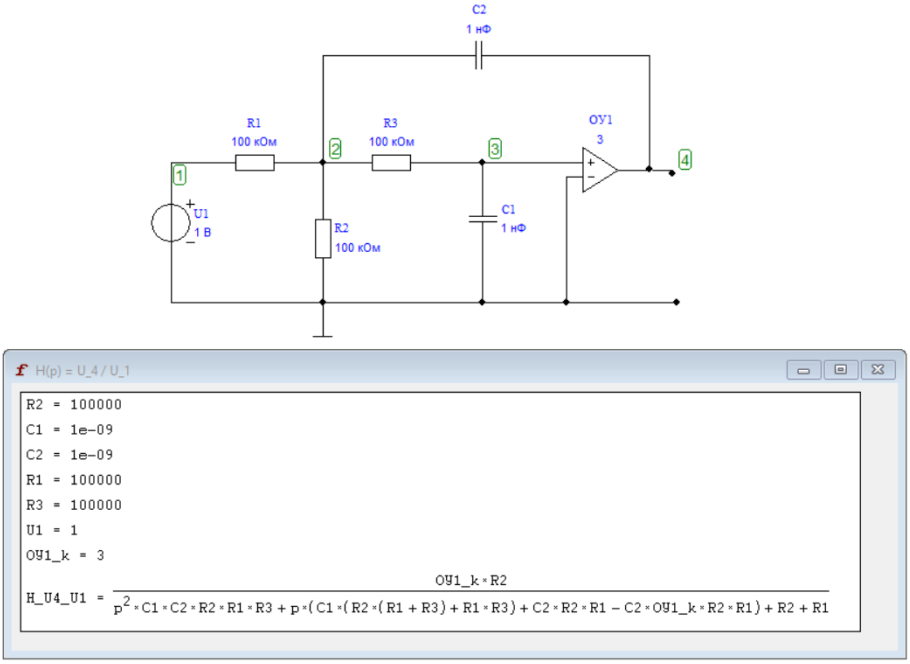


Рис. 1. Нахождение операторной передаточной цепи с использованием символьного метода в программе Fastmean

По критерию устойчивости Гурвица корни полинома знаменателя операторной передаточной функции должны лежать в левой полуплоскости. Корни знаменателя были найдены в программе Mathcad:

– в общем виде

$$H(p) := \frac{K}{p^2 \cdot R^2 \cdot C^2 + p \cdot (4 - k) \cdot C \cdot R + 2}$$

Given

$$p^2 \cdot R^2 \cdot C^2 + p \cdot (4 - k) \cdot C \cdot R + 2 = 0$$

$$\text{Find}(p) \rightarrow \begin{pmatrix} \dfrac{\dfrac{C \cdot R \cdot \sqrt{k^2 - 8 \cdot k + 8}}{2} - 2 \cdot C \cdot R + \dfrac{C \cdot R \cdot k}{2}}{C^2 \cdot R^2} & \dfrac{2 \cdot C \cdot R + \dfrac{C \cdot R \sqrt{k^2 - 8 \cdot k + 8}}{2} - \dfrac{C \cdot R \cdot k}{2}}{C^2 \cdot R^2} \end{pmatrix}$$

– численно

$$k := 3 \qquad R := 10^5 \qquad C := 10^{-9}$$

$$p^2 \cdot R^2 \cdot C^2 + p \cdot (4 - k) \cdot C \cdot R + 2 \text{ solve} \rightarrow \begin{pmatrix} -5000 + 5000i \cdot \sqrt{7} \\ -5000 - 5000i \cdot \sqrt{7} \end{pmatrix}$$

Далее было определено значение коэффициента усиления операционного усилителя (ОУ), при котором активная цепь будет устойчивой и иметь корни характеристического уравнения, которые лежат в левой полуплоскости:

$$R := 10^{5} \quad C := 10^{-9}$$

Given

$$-2 \cdot C \cdot R + \frac{C \cdot R \cdot k}{2} < 0$$

$$\text{Find}(k) \rightarrow k < 4$$

Следующим этапом было исследование устойчивости активной цепи с использование критерия устойчивости Найквиста.

В программе Fastmean были построены схема (рис. 2) и годограф петлевого усиления ARC-цепи при разных значениях коэффициента усиления ОУ (рис. 3), также было получено символьное выражение для петлевого усиления (рис. 4), позволяющее определить, при каком значении коэффициента усиления ОУ годограф петлевого усиления не охватывает точку с координатами (1, j0) на комплексной плоскости.

Далее определялось значение частоты ω_0, при котором $\mathrm{Im}B(j\omega) = 0$. По виду годографа петлевого усиления студент должен сделать вывод об устойчивости ARC-цепи.

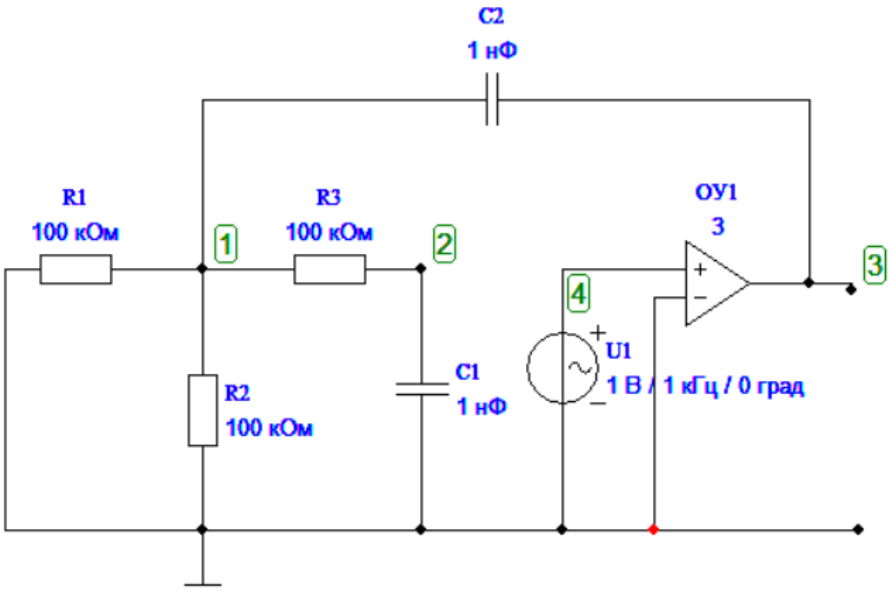


Рис. 2. Схема петлевого усиления ARC-цепи

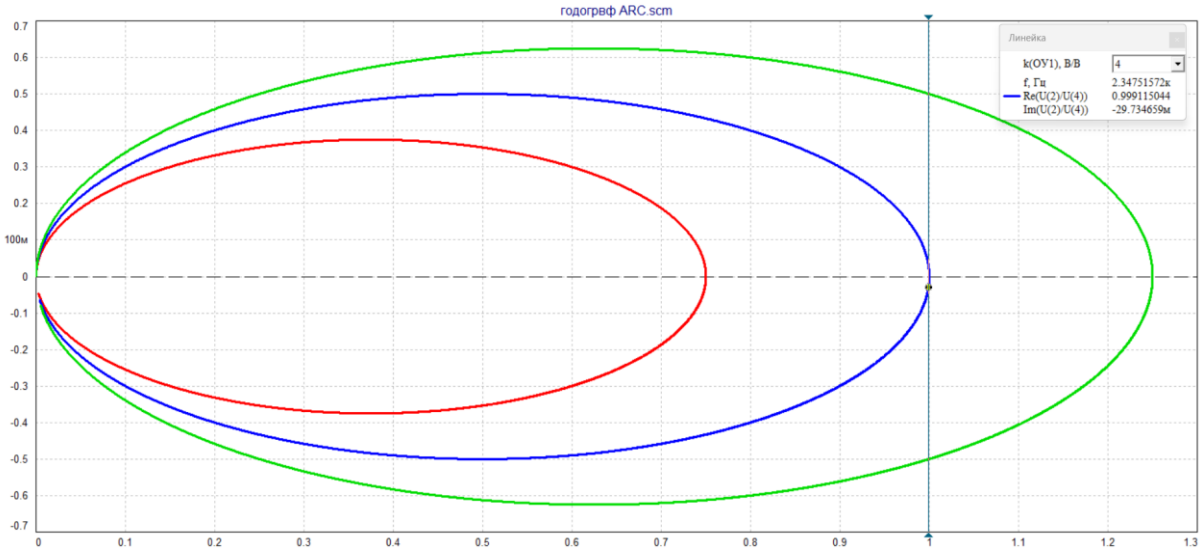


Рис. 3. Годограф петлевого усиления ARC-цепи при разных значениях коэффициента усиления ОУ

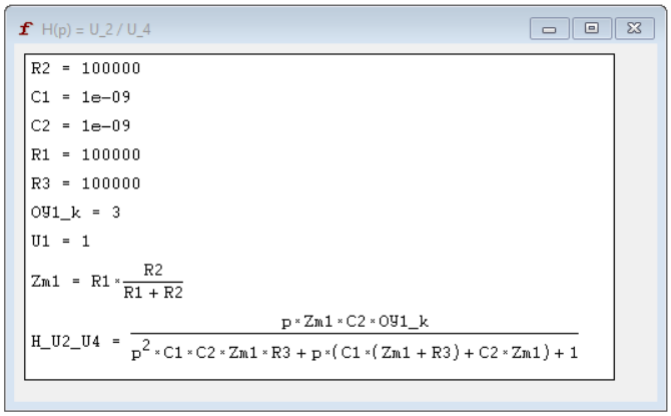


Рис. 4. Символьное выражение для петлевого усиления

Таким образом, виртуальная лабораторная работа по исследованию устойчивости активного четырехполюсника, выполненная в интегрированной программной среде Mathcad и Fastmean, позволяет сократить время на сложные расчеты, обеспечить наглядность полученных результатов при исследовании различных критериев устойчивости, что способствует расширению и углублению возможностей традиционных методов обучения, позволяет студенту овладеть важным инструментом для анализа и проектирования электронных систем.

Список используемых источников:

1. Оганесян А. А. Устойчивость электрических цепей. М.: Радио и связь, 1985.
2. Dorf R. C., Bishop R. H. Modern Control Systems. Pearson, 2016.
3. Зайцева З. В., Логвинова Н. К. Компьютерный расчет линейных и нелинейных цепей при постановке виртуальных лабораторных работ // Актуальные проблемы инфо-

телекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. С. 401-406.

4. Зайцева З. В., Логвинова Н. К. Виртуальный лабораторный практикум для технических дисциплин при дистанционном обучении // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. С. 218-223.

5. Зайцева З. В., Логвинова Н. К. Возможности человеко-машинного взаимодействия в обучающей среде технического вуза // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 558-563.

DEVELOPMENT AND CREATION OF A VIRTUAL LABORATORY PRACTICUM FOR STUDYING THE STABILITY OF ACTIVE TWO-PORT NETWORKS

Zaitseva Z.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

The development and creation of a virtual laboratory practicum for studying the stability of ARC circuits based on the use of the Mathcad and Fastmean integrated software environment is discussed. It is shown that the use of computer technologies, which allow for simulation during laboratory work, enhances the clarity and effectiveness of mastering the material when studying various stability criteria.

Key words: *laboratory practicum, ARC circuits, stability criteria, integrated software environment, process simulation*

УДК 654.026
ГРНТИ 49.01.11

АНАЛИЗ СОВРЕМЕННЫХ СРЕДСТВ УНИЧТОЖЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ КАК АРХИТЕКТУРЫ СЕМАНТИЧЕСКОЙ ИНТЕРОПЕРАБЕЛЬНОСТИ ОБСТАНОВКИ НА ПОЛЕ БОЯ В ТАКТИЧЕСКОМ ЗВЕНЕ УПРАВЛЕНИЯ

В. Г. Иванов, В. П. Михайлов, Д. С. Алленов, В. В. Чабаненко

Департамент информационных систем МО РФ

Анализ опыта практического обнаружения различных модификаций БЛА позволяет службам безопасности отделить их из числа сторонних моделей и выявить интересующие характеризующие факторы отдельного БЛА, функционал которого влияет на выполнение разноплановых задач. Разведывательные возможности современных БЛА связаны со стремительным их развитием, что в свою очередь требует соответствующего развития средств их обнаружения и идентификации.

идентификация летательных средств, разведывательные системы, информационные системы, передача данных, электромагнитная доступность

Введение

На сегодняшний день службы безопасности Российской Федерации не готовы эффективно противостоять разведывательно-ударным действиям БЛА соперника, поскольку существующие средства противовоздушной обороны (ПВО), которые предназначены для крушения больших воздушных целей на высотах 2,5-10 км не рассчитаны для обнаружения и идентификации летательных аппаратов малых размеров [1]. Кроме того, применение существующих активных ПВО средств отражения воздушных целей не всегда является экономически целесообразным и эффективным [2].

Целью исследования является разработка подходов к борьбе с БЛА различных классов на основе проведенного анализа современных средств и способов устранения БЛА ведущих стран мира.

Эффективность применения средств ПВО зависит не только от дальности обнаружения БЛА, но и от возможности их распознавания (идентификации), а также передачи распознанного (идентифицированной) ориентира на средства ПВО.

Определение класса БЛА позволит принять решение по применению средств ПВО, которые будут как экономически обоснованными, так и эффективными. В таблице 1 представлена предложенная в странах западной Европы классификация БЛА [3].

ТАБЛИЦА 1. Классификация БЛА

№	Класс	Категория	Масса, кг	Высота применения, м	Радиус действия, км
1	I	Малые, мини, микро	1-150	60-1500	5-50
2	II	Тактические	(150-600)	до 5500	до 200
3	III	Ударные	(>600)	10000-20000	до 6000

Для эффективного применения зенитных средств неизменной является задача обнаружения и идентификации БЛА. В органах безопасности остается частично не решенными вопросы возможности обнаружения и идентификации БЛА I и II классов, а без этого невозможно принять решение по эффективному применению зенитных средств поражения. Идентификация БЛА зависит от степени его заметности, которая определяется величиной его сигнатур в радиочастотном, инфракрасном и видимом диапазонах, а также сигнатуры акустической. Кроме того, современные БЛА имеют небольшие размеры благодаря применению композитных материалов или пластика со специальной покраской и с особой комбинацией слоев, а их небольшие бензиновые и тем более электрические двигатели мало излучают тепла и работают почти бесшумно.

В настоящее время обнаружение БЛА I и II классов осуществляется посредством радиоэлектронной разведки (радиолокационная система сантиметрового диапазона) и радиоэлектронной разведки методом триангуляции путем засечки частоты канала передачи видеосигнала и определения его позиционирования минимум по двум источникам. Второй метод менее точный, за счет азимутальной погрешности и быстрым переходом на применение БЛА с оптическими катушками, но имеющие большие дальности обнаружения, за счет приема сигнала в пассивном режиме.

Для эффективного устранения БЛА III класса в службах безопасности передовых стран мира применяют зенитные ракетные комплексы, которые способны эффективно устранить как малые, так и большие воздушные цели на высотах 5 – 20 км. Для уничтожения БЛА I и II классов широкое применение получило снаряжение калибров: 23, 35 и 40 мм. Новейшие арсеналы

позволяют создать облако обломков из сотни поражающих элементов, что обеспечивает эффективное устранение БЛА. В комплексе со средством объективного контроля и сопровождения, а также передачи целеуказания об обнаруженном БЛА значительно повышается точность поражения.

Но развитие технологий БЛА ставит перед службами безопасности задачу внедрения новейших средств ПВО для противодействия БЛА. Без полноценного защитного купола, способного противостоять любому классу БЛА, вопрос безопасности всех объектов и подразделений не будет решен.

Улучшение показателей эффективности устранения малоразмерных БЛА возможно путем разработки новейших средств обнаружения, позиционирования их в пространстве, передачи целеуказаний на средства противодействия, поражения, а также внедрения комплекса специальных мероприятий по организации их устранения перспективными и активными средствами.

К перспективным средствам устранения БЛА ведущих стран мира, которые во время испытаний показали свою эффективность, следует отнести: электромагнитное и лазерное противодействие, а также БЛА-перехватчики. К таким образцам следует отнести микроволновую пушку "Phaser" компании Raytheon (США). Указанная система электромагнитного снаряжения предназначена для устранения БЛА I и II классов, которые перемещаются со скоростью от 185 до 370 км/ч. Также существуют образцы электромагнитного противодействия, которые обеспечивают устранение БЛА в радиусе 360°. Например, система "DroneDome" (Израиль) способна идентифицировать БЛА, осуществлять сопровождение целей и автоматическое их устранение, при этом не создавая препятствий для других летательных аппаратов. Это достигается благодаря использованию специальной направленной антенны. Система способна работать в любых погодных условиях и может обнаруживать цели размером до 2 квадратных сантиметров на расстоянии 3,5 км.

Лидером в разработке лазерного оружия противодействия является США. Примеры таких систем:

– система противоракетной обороны Skyguard и Nautilus которая построена вокруг высокоэнергетического тактического лазера - THEL (Tactical High Energy Laser);
– система LaWS (Laser Weapon System) технологический демонстратор высокоэнергетического лазерного оружия, созданного командованием морских систем ВМС США;

– лазерный комплекс Hel (High-Energy Laser) компании Boeing установлен на бронетранспортер Boxer. Комплекс способен обнаруживать, сопровождать и ликвидировать цели как в воздухе, так и на земле. Мощности достаточно для устранения БЛА и ракет малой дальности.

Электромагнитное и лазерное противодействие имеет как преимущества, так и недостатки. К преимуществам использования таких систем можно отнести стоимость и точность цели наведения, к недостаткам зависимость от погодных условий, которые существенно могут ограничить действие лазера и дальность применения в случае с электромагнитным противодействием.

Заключение

Борьба с БЛА требует подхода, который сводится к трем требованиям: обнаружить, распознать и устранить. Первые два шага в этой последовательности на данный момент в основном отработаны за счет совершенствования существующих технологий. В свою очередь устранение БЛА требует одновременно как технических, так и организационных решений. К ним может быть отнесено:

– создание комплексной системы противодействия БЛА, включающих специальные мобильные группы, разнотипные компактные зенитные средства обнаружения и устранения БЛА, со сравнительно высокими разведывательными и огневыми возможностями при обнаружении и стрельбе по малоразмерным целям;
– поиск и обнаружения БЛА необходимо использовать комплекс средств, использующий разные физические принципы, объединенных в единую архитектуру с автоматизацией информационного обмена о воздушной обстановке в масштабе времени, близком к реальному;
– совершенствование (модернизация) существующих образцов ПВО и арсенала к ним в интересах повышения эффективности борьбы с малоразмерными целями;
– разработку перспективных образцов ПВО, в том числе нетрадиционных видов противодействия, для решения задач обнаружения и устранения малоразмерных целей.

Приоритетами в реализации программ разработки современных средств устранения БЛА можно считать использование средств перехвата или устранения с помощью БЛА перехватчиков, которые по своим стои-

мостным показателям значительно ниже или сопоставимы, чем перехватываемая воздушная цель.

Список используемых источников

1. Мохаммад М., Похващев В. Н., Рязанцев Л. Б. Вопросы повышения эффективности противодействия малоразмерным беспилотным летательным аппаратам // Военная мысль. 2022. № 6. С. 45–52.

2. Тикшаев В. Н., Барвиненко В. В. Проблема борьбы с БПЛА и возможные пути ее решения // Военная мысль. 2021. № 1. С. 125-132.

3. Лопин Г. А., Смирнов Г. И., Ткачев И. Н. Развитие средств борьбы с БПЛА // Военная мысль. 2023. № 1. С. 42–50.

REVIEW OF MODERN DETECTION TOOLS UAV

Ivanov V., Allenov D., Chabanenko V., Mikhailov V.
Department of Information Systems of the Ministry of Defense of the Russian Federation

Analysis of the experience of practical detection of various UAV modifications allows the operator to separate them from the number of third-party models and identify the characteristic factors of interest of an individual UAV, the functionality of which affects the performance of diverse tasks. The reconnaissance capabilities of modern UAVs are associated with their rapid development, which in turn requires the corresponding development of means for their detection and identification.

Key words: *aircraft identification, reconnaissance systems, information systems, data transmission, electromagnetic availability*

УДК 621.396.96
ГРНТИ 47.25.15

МЕТОДЫ РАСПОЗНАВАНИЯ ОБЪЕКТОВ ПО СПЕКТРОГРАММАМ В СЕТЯХ СОТОВОЙ СВЯЗИ

К. О. Коровин, Р. А. Алли

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

Малая радиолокационная заметность БПЛА делает непростой задачу их радиолокационного обнаружения из-за их схожести с птицами. Широкое распространение БПЛА в последние годы и их адаптация для ведения боевых действий требует разработки средств оперативного обнаружения БПЛА в воздушном пространстве города. В статье рассматриваются методы обнаружения и в перспективе – распознавания БПЛА по микродоплеровскому смещению. Работа преследует цель сделать краткий обзор одного из методов получения спектрального портрета цели в сетях сотовой связи стандарта 5G NR и предложить методы его дальнейшей обработки. Проведено компьютерное моделирование спектрограммы винтов БПЛА разной конструкции, установлены некоторые зависимости между свойствами частотно-временного портрета винта и его характеристиками.

ISAC, MIMO, 5G NR, микродоплеровский эффект, БПЛА, CNN, ViT

Распознавание спектрального портрета можно проводить по следующему алгоритму: измерение спектра, построение частотно-временного портрета и его классификация.

Для того, чтобы технология совмещенной локации и связи работала, требуется, чтобы система использовала технологию MIMO. С 4-го поколения эта технология используется в сетях связи повсеместно для уплотнения каналов. В системе MIMO количество доступных пространственных потоков канала связи зависит от количества антенн в передающей и приемной антенных решетках. Количество пространственных каналов, которые поддерживает система MIMO, равна количеству антенн в ее наименьшей антенной решетке. Базовые станции и абонентские устройства 4G поддерживают режим работы 4x4 в восходящем канале и 8x8 в нисходящем. Технология привела к аппаратной конвергенции базовых сотовых станций с MIMO радарами. Это позволило использовать базовую станцию как локатор непрерывного излучения, изменив алгоритм передачи и обработки данных [1].

Структура сигнала ISAC в 5G NR

В 5G NR данные передаются пакетами, которые называются радиокадрами. Радиокадр длится 10 миллисекунд. Десять радиокадров составляют один

интервал когерентной обработки. Сам радиокадр состоит из 4-х групп по 5 слотов. Слот – это временной интервал, зарезервированный для определенной цели. Их 3 типа: прием сигнала от мобильного устройства (UL), передача данных от базовой станции на мобильное устройство и (DL) и специальный временной слот, который служит временным буфером между этими двумя режимами работы, предотвращая помехи. Слоты передаются группами по 5 в строгом порядке: DDDSU. Длительность одного слота – 0,5 миллисекунд. Каждый из них состоит из 14 OFDM символов, длительностью 33,3 микросекунды. Такая временная структура сигнала называется TDD (Time Division Duplex) [2].

Ширина полосы каждого канала составляет 30 кГц. Такие каналы формируют полосу в 100 МГц [3].

После того, как БС обнаруживает неизвестную летающую цель, она передает сигналы связи цели в слотах DL, одновременно принимая эхо. В этом режиме зондирования извлеченные микродоплеровские характеристики являются однозначными [2].

Передаваемый базовой станцией сигнал можно описать формулой:

$$s(t) = \sum_{n=1}^{N}\sum_{m=1}^{M} D_{TX}(n,m) \times e^{j2\pi n\Delta f t} \times rect\left(\frac{t - mT_s}{T_s}\right) \qquad (1)$$

Формула описывает комбинацию частот и временных интервалов, с помощью которых передается сигнал, а $D_{TX}(n,m)$ – символ данных, который передается как m OFDM символ, модулированный на поднесущую n, также называемый символом комплексной модуляции. Δf – интервал между поднесущими, а $T_s = \frac{1}{\Delta f} + T_g$ обозначает общую продолжительность одного OFDM-символа. $T_g . rect\ (\cdot)$ – прямоугольное окно с единичной поддержкой [4].

Сигнал ISAC распространяется в свободном пространстве и отражается от цели. Во временной области излучаемый сигнал описывается как $s(t)e^{j2\pi f_c t}$, где – центральная частота приемопередатчика. Если значительная часть принятого сигнала была отражена от окружающих предметов, то принятый сигнал будет зависеть от времени, расстояния до абонента и отражателя и иных параметров [1, 3, 4, 5].

Принимаемый сигнал $\tilde{y}(t, R(t), \gamma(t))$ имеет вид:

$$\tilde{y}\big(t, R(t), \gamma(t)\big) = \gamma(t)\, s\left(\frac{2R(t)}{c}\right) e^{j2\pi f_c t} \times e^{\left(-j2\pi f_c \frac{2R(t)}{c}\right)} \qquad (2)$$

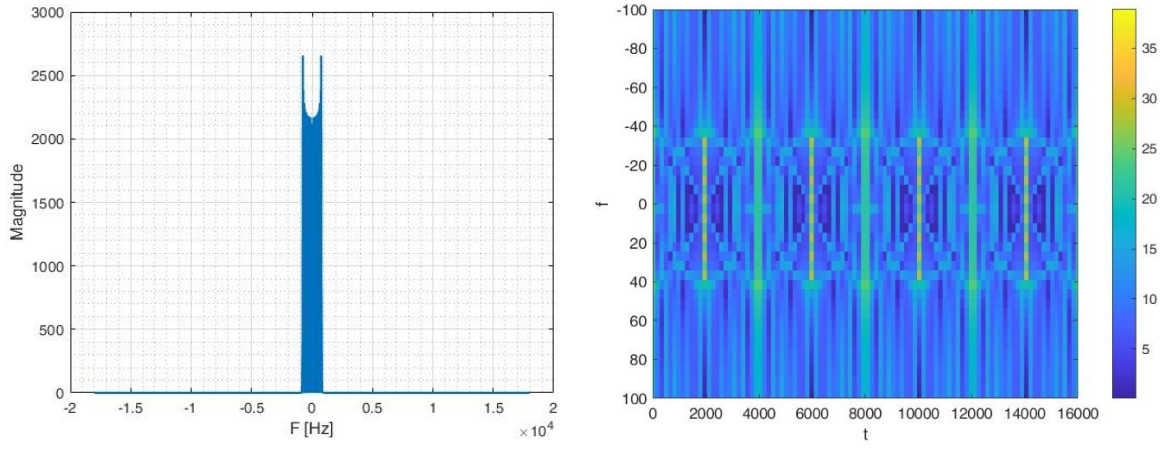
где $\gamma(t)$ – затухание канала. *R(t)* – расстояние от точки рассеяния до базовой станции.

Микродоплеровская модуляция

Эффект Доплера – это эффект, в результате которого частота сигнала отраженного от движущегося предмета изменяется в сторону повышения частоты или ее уменьшения, в зависимости от того, движется предмет в сторону наблюдателя или от него, и чем быстрее скорость объекта относительно линии наблюдения, тем больше это отклонение [4]. Модуляция сигнала, отраженного от вращающегося винта в общем виде, может быть отображена как:

$$s_{\Sigma}(t) = L \cdot e^{-i\cdot\frac{4\pi}{\lambda}\cdot(R_0+z_0\cdot sin(\beta))} \cdot \sum_{k=0}^{K-1} sinc\left(\frac{4\pi}{\lambda}\cdot\frac{L}{2}\cdot cos(\beta)\cdot cos\left(2\cdot\pi\cdot\Omega\cdot t+\varphi_0+\frac{k\cdot 2\cdot\pi}{K}\right)\right) \quad (3)$$

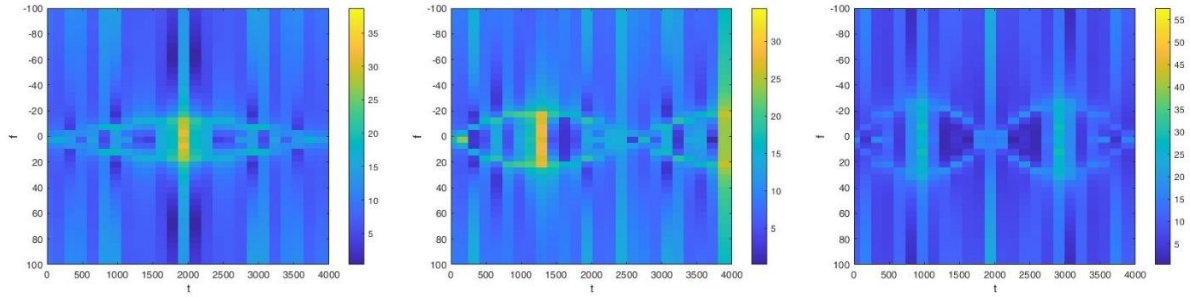
где $s_{\Sigma}(t)$ – отраженный от винта сигнал, L – длина лопасти, λ – длина волны, β – угол возвышения, Ω – скорость вращения винта в оборотах в секунду, φ_0 – начальное положение винта, T – количество лопастей, R_0 – расстояние от радара до цели [4, 5]. Импульсный сигнал с продолжительностью зондирующего импульса в 1 миллисекунду и периодичностью повторения в 0,05 секунды, отраженный от вращающегося винта, выглядит, как показано на рисунке (2а), после применения БПФ ко всему накопленному сигналу сразу (период накопления 16 секунд). Эти данные можно обработать иначе: применим оконную функцию к данным: нарезаем данные на векторы по 2048 символов и применяем к каждому вектору быстрое преобразование Фурье. После этого транспонируем получившуюся матрицу и отображаем в виде тепловой карты (рисунок 2б). Время на графике 2б указано в миллисекундах, а частота в десятках герц, т.е. смещение Доплера здесь составляет почти 4кГц.



а) б)

Рис. 1. а – спектр отраженного от винта сигнала после БПФ по оси абсцисс – частота в Гц, по оси ординат – амплитуда, b – спектр отраженного сигнала после оконного БПФ

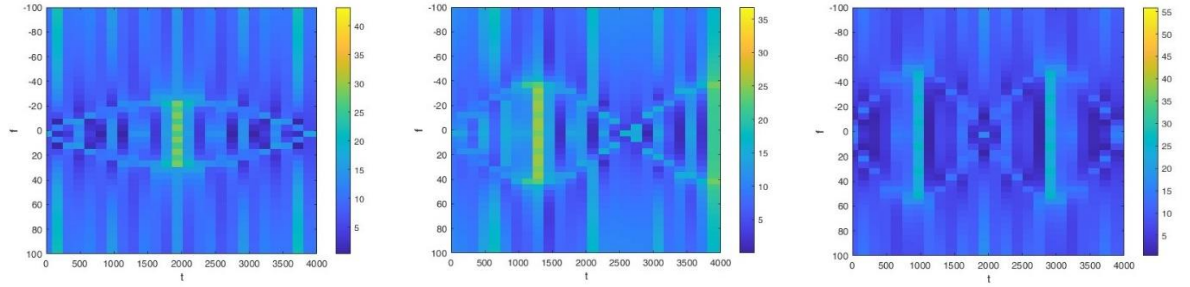
По параметрам модуляции сигнала (рисунки 1б, 2), можно обнаружить летательный аппарат. Винты БПЛА отличаются друг от друга длиной и количеством лопастей, а также скоростью вращения. Можно смоделировать сигнал, отраженный от винтов разного типа, например тех, что представлены на рисунке 2.



а) L = 3,5 дюймов
Ω = 2 об/с
N = 2

б) L = 3,5 дюймов
Ω = 3 об/с
N = 2

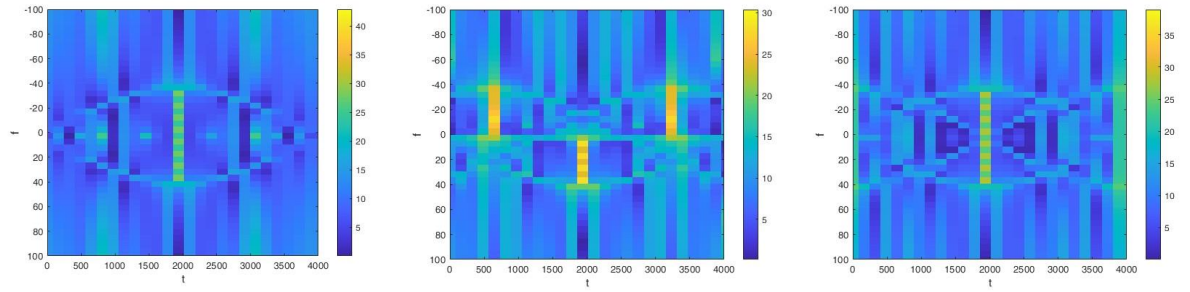
в) L = 3,5 дюймов
Ω = 4 об/с
N = 2



г) L = 6,5 дюймов
Ω = 2 об/с
N = 2

д) L = 6,5 дюймов
Ω = 3 об/с
N = 2

е) L = 6,5 дюймов
Ω = 4 об/с
N = 2



ж) L = 9,5 дюймов
Ω = 2 об/с
N = 2

з) L = 9,5 дюймов
Ω = 2 об/с
N = 3

к) L = 9,5 дюймов
Ω = 2 об/с
N = 4

Рис. 2. Частотно-временные портреты сигнала, отраженного от винтов с разными параметрами

Разрешение, с которой будет снят портрет, зависит от скорости вращения винта и частоты несущей волны при одинаковой дальности. Скорость вращения винта определяет предельные требования к интервалу когерентной обработки (максимум периода), а частота несущей волны – возможности по его минимизации. При увеличении длины лопасти увеличивается допплеровское смещение (рис. 2 а, г, ж). При увеличении скорости вращения винта также увеличивается максимальная скорость, и уменьшается период, за который винт оборачивается на 180 градусов (рис. 2 б, д). При увеличении количества лопастей меняется частотно-временной портрет (рис. 2 з, к).

Классификация частотно-временного портрета.

Последний этап обработки – распознавание частотно-временного портрета. Для этого можно использовать сверточные нейронные сети (CNN) или нейронные сети архитектуры Vision Transformer (ViT) [6]. CNN можно обучить на небольшом наборе данных с помощью аугментации, однако они могут испытывать трудности с низким разрешением. ViT улавливают общие зависимости в изображении, но требуют большого объема данных и мощной вычислительной машины. Отдельно следует отметить перспективность применения алгоритмов дактилоскопирования звука для анализа спектрального портрета [7].

Выводы

В ходе работы было проведено компьютерное моделирование отражения сигнала для винтов БПЛА с разными параметрами, в результате чего был построен радиолокационный частотно-временной портрет с помощью оконного преобразования Фурье спектра сигнала по времени. Продемонстрировано как ведет себя частотно-временной портрет, при изменении параметров винтов БПЛА: длины лопасти, количества лопастей, скорости вращения винта. Показано наличие зависимости параметров частотно-временного портрета от параметров винта, что позволяет предсказывать тип БПЛА по отраженному от него сигналу, если провести классификацию его частотно-временного радиолокационного портрета с помощью нейронных сетей.

Список используемых источников

1. Бакулин М. Г., Крейнделин В. Б. Технологии в системах радиосвязи на пути к 5G. М.: Горячая линия-Телеком, 2024. 279 с.
2. Zhang J., Wang X., Li Y. ISAC for 5G: Vision and Challenges // IEEE Communications Magazine. 2021. Vol. 59. № 5. P. 34-40.
3. Wei J. et al. UAV's Rotor Micro-Doppler Feature Extraction Using Integrated Sensing and Communication Signal [Электронный ресурс] // arXiv preprint. 2024. URL: https://arxiv.org/abs/2408.16415 (дата обращения 15.07.2024).
4. Chen V. The Micro-Doppler Effect in Radar. 2nd ed. Norwood: Artech House, 2019. 568 p.
5. Chen V.C. Radar Signatures of Rotor Blades // Proc. of SPIE on Wavelet Applications VIII. 2001. Vol. 4391. P. 63-70.
6. Wang Z., Liu H., Chen Y. ViT for Radar Spectrogram Classification // IEEE Transactions on Aerospace. 2022. Vol. 30. № 4. P. 210-225.
7. Уильямс, Д., Пурансингх, А., & Саиту, Дж. Эффективная идентификация музыки с использованием ORB-дескрипторов изображения спектрограммы [Электронный ресурс] // EURASIP Journal on Audio, Speech, and Music Processing. 2017. Т. 2017, № 1. 17 с. URL: https://doi.org/10.1186/s13636-017-0114-4 (дата обращения 15.07.2024).

METHODS OF OBJECT RECOGNITION BASED ON SPECTROGRAMS IN CELLULAR NETWORKS

Korovin K., Alli R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The low radar visibility of UAVs makes their radar detection challenging due to their similarity to birds. The widespread use of UAVs in recent years, and their adaptation for combat, necessitates the development of means for rapid UAV detection in urban airspace. This article examines methods for detecting and, in the future, recognizing UAVs based on micro-Doppler shift. The work aims to provide a brief overview of one method for obtaining a spectral portrait of a target in 5G NR cellular networks and to propose methods for its further processing. Computer modeling of spectrograms of UAV rotors of various designs has been carried out, and some dependencies between the properties of the time-frequency portrait of the rotor and its characteristics have been established.

Key words: *ISAC, MIMO, 5G NR, micro-Doppler effect, UAV, CNN, ViT*

УДК 621.396.41
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ ПРОЦЕДУРЫ ЭКВАЛАЙЗИРОВАНИЯ ДЛЯ КОМПЕНСАЦИИ ИСКАЖЕНИЙ В РЭЛЕЕВСКОМ КАНАЛЕ С ЗАМИРАНИЯМИ

В. Е. Коротин, В. С. Вторых

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

В статье рассматривается применение эквалайзирования для компенсации искажений, вызванных Рэлеевским каналом с замираниями. Исследование включает в себя моделирование канала передачи OFDMA-символов и анализ зависимостей вероятности битовой ошибки от отношения сигнал – шум для различных условий распространения и модуляций сигнала. Результаты демонстрируют потенциал эквалайзинга для повышения надежности и качества связи в сложных радио условиях.

эквалайзирование, опорный сигнал, передаточная функция канала, многолучевое распространение

В беспроводных системах связи надежность передачи данных критична. Искажения (амплитудные, частотные, фазовые), вызванные многолучевым распространением сигналов должны быть скомпенсированы для корректной демодуляции.

Для исследования искажений, возникающих при распространении радиоволн в канале связи, используют несколько основных моделей (модель канала Гаусса, модель канала Райса, модель канала Рэлея), отличающихся сложностью и степенью приближения к реальным условиям распространения.

Канал Рэлея (прямая видимость между передатчиком и приемником отсутствует, на прием приходят только отраженные сигналы) является наиболее приближенной к действительности моделью, что определяет ее использование в данном исследовании. Модели каналов Гаусса, Рэлея и Райса представлены на рис. 1 [1].



а) модель Гаусса б) модель Райса в) модель Рэлея

Рис. 1. Описание каналов Гаусса, Рэлея и Райса

В системах множественного доступа с ортогональным частотным разделением (OFDMA) для компенсации искажений амплитуды, частоты и фазы принимаемого сигнала используется процедура эквалайзирования канала.

Суть эквалайзирования заключается в том, что в спектр каждого символа OFDM добавляются специальные опорные поднесущие – пилот-сигналы. Приемник, зная расположение пилотных поднесущих, может оценить искажения, вносимые каналом. По принятым значениям пилотных поднесущих определяется передаточная функция канала, зная которую, восстанавливается спектр отправленного сигнала [2].

Для исследования процедуры эквалайзирования в среде SystemVue создана модель передатчика OFDMA (приемник реализован по обратной схеме аналогично передатчику), а также подсистемы канала с АБГШ и многолучевым распространением. Описание подсистем, а также параметров отдельных блоков представлено на рис. 2-4.

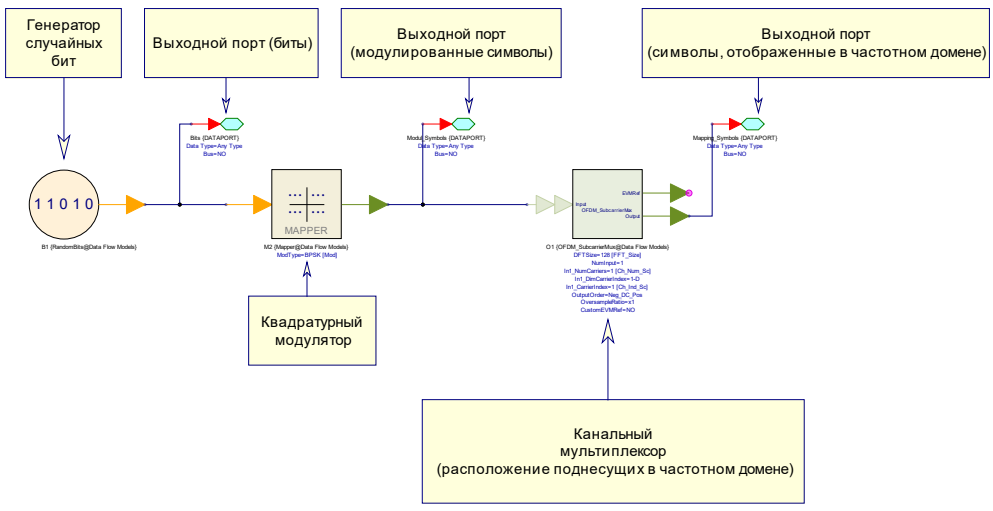


Рис. 2. Подсистема формирования канала

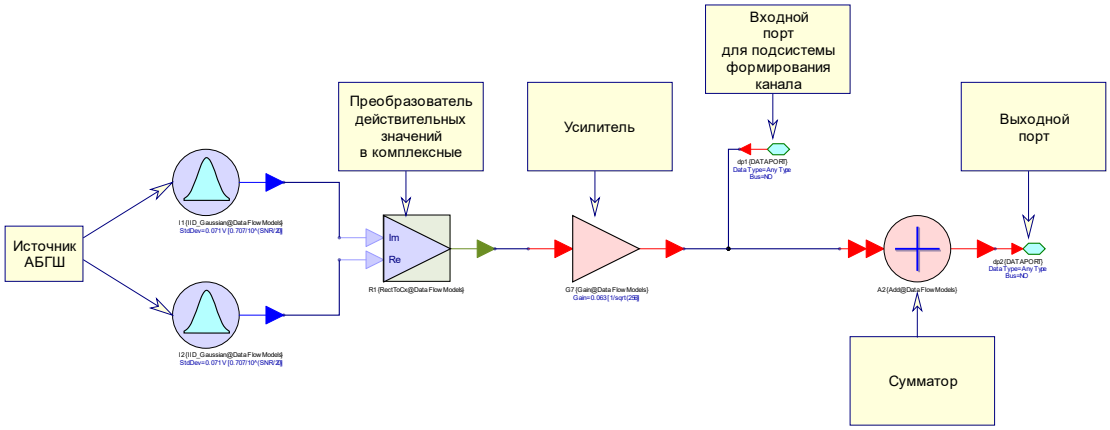


Рис. 3. Подсистема канала с АБГШ

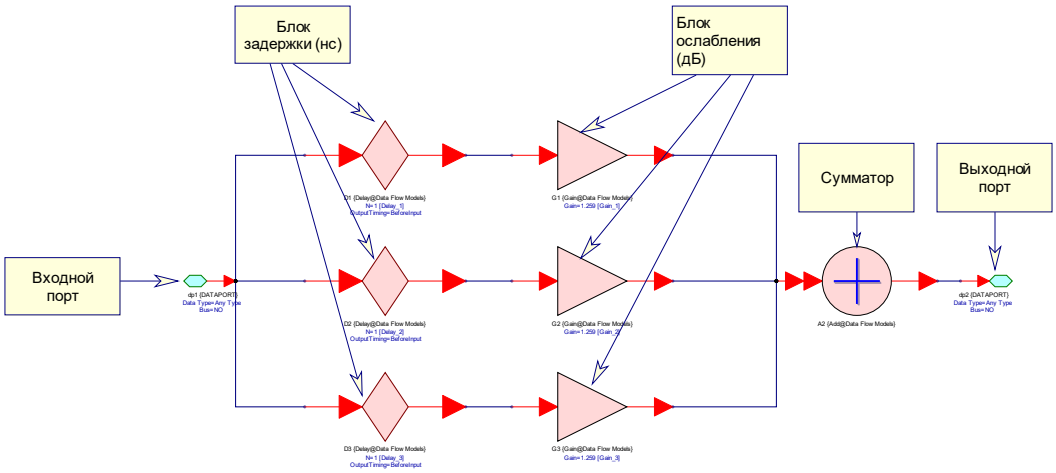


Рис. 4. Подсистема канала Рэлея

Программный код для инициализации параметров модели представлен на рис. 5. Полная модель представлена на рис. 6.

Эквалайзер, представленный на рис. 6, компенсирует искажения в канале следующим образом [3]:

– передаточная функция канала получается перемножением комплексно-сопряженного опорного сигнала (сгенерированного в приемнике) и отсчетов опорного сигнала, извлеченных из принятого OFDMA-символа после ДПФ;
– поскольку передаточная функция канала известна лишь для 41 поднесущей, ее нужно интерполировать (блок Interpolator) на весь спектр OFDMA-символа;
– спектр принятого OFDMA-символа умножается на обратную интерполированную передаточную функцию канала. Для этого от результата интер-

поляции берется обратная функция (блок Inverse_M) и размещается в спектре.

```
FFT_Size=256;   %Размер быстрого преобразования Фурье
CP_Size=16; %Величина циклического префикса

%Расстановка пилот-поднесущих

P_Step=5;   %Период пилотов
P_Left=-100;    %Граница индексации пилотов слева
P_Right=100;    %Граница индексации пилотов справа
Pilot_Ind_Sc=[P_Left:P_Step:P_Right];   %Индексация поднесущих
Pilot_Num_Sc=length(Pilot_Ind_Sc);  %Количество пилотов

Pilot_Value(1:Pilot_Num_Sc, 1)=0.707+1i*0.707;  %Значения пилотов

%%формирование каналов

k=0;
i=0;

for i=-50:50    %Диапазон индексов поднесущих для 1-го канала
    if mod(i, P_Step)~=0    %Пропуск индексов пилотов
    k=k+1;  %Счетчик
    Ch1_Ind_Sc(k)=i;    %Запись индекса
    end;end;

Ch1_Num_Sc=length(Ch1_Ind_Sc);  %Количество используемых поднесущих
Ch1_Mod=2;  %Модуляция для первого канала (QPSK)

k=0;
i=0;

for i=-100:-51  %Диапазон индексов поднесущих для 2-го канала
    if mod(i, P_Step)~=0    %Пропуск индексов пилотов
    k=k+1;  %Счетчик
    Ch2_Ind_Sc(k)=i;    %Запись индекса
    end;end;

Ch2_Num_Sc=length(Ch2_Ind_Sc);  %Количество используемых поднесущих
Ch2_Mod=3;  %Модуляция для второго канала (QAM-16)

k=0;
i=0;
```

```
k=0;
i=0;

for i=51:100
    if mod(i, P_Step)~=0
    k=k+1;
    Ch3_Ind_Sc(k)=i;
    end;end;

Ch3_Num_Sc=length(Ch3_Ind_Sc);
Ch3_Mod=4;

%Параметры задержки и ослабления в многолучевом канале связи

Beam_1_Delay=4;
Beam_1_Gain=-5;

Beam_2_Delay=10;
Beam_2_Gain=-10;

Beam_3_Delay=20;
Beam_3_Gain=-20;
```

Рис. 5. Инициализация параметров модели

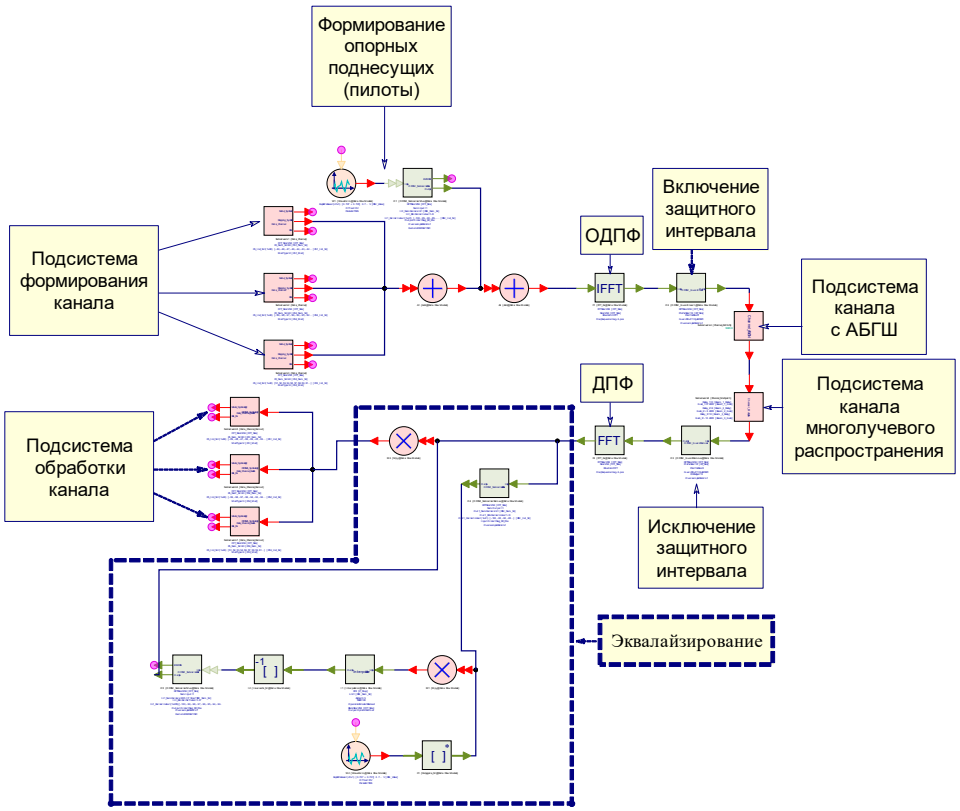


Рис. 6. Модель для исследования процедуры эквалайзирования

Для проверки корректности работы модели вначале необходимо построить зависимости вероятностей битовой ошибки (BER) от отношения сигнал-шум (SNR) в канале с АБГШ и сравнить с теоретическими данными. Данные зависимости приведены на рис. 7.

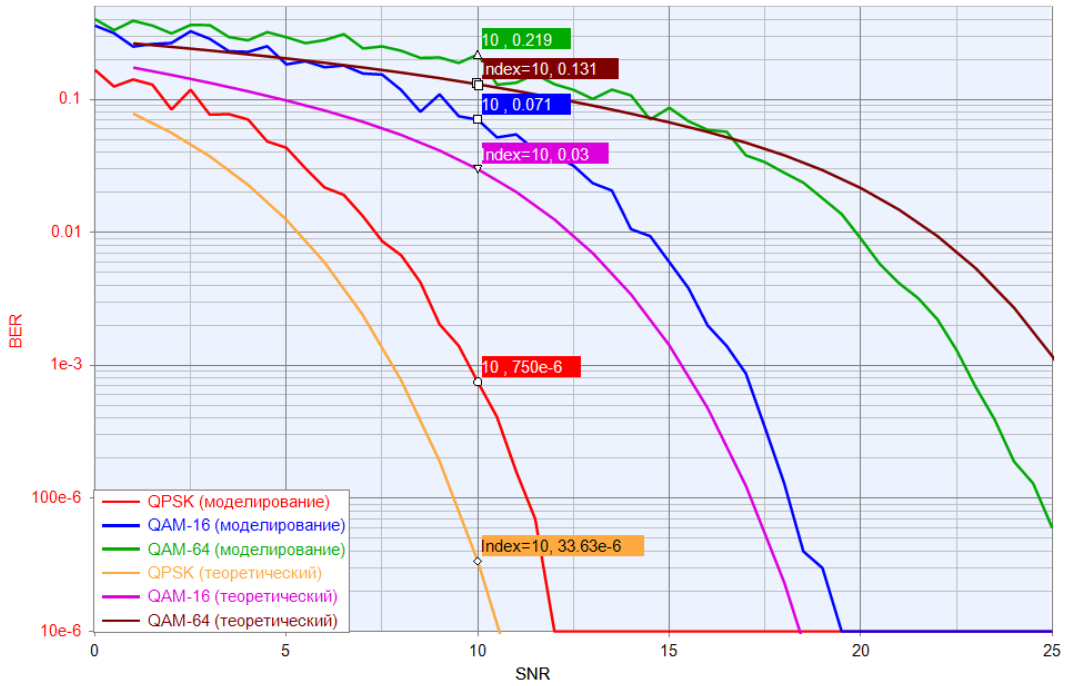


Рис. 7. Зависимость вероятности битовой ошибки от отношения сигнал – шум для канала с АБГШ

На рис. 8 приведены зависимости BER от SNR для Рэлеевского канала с замираниями.

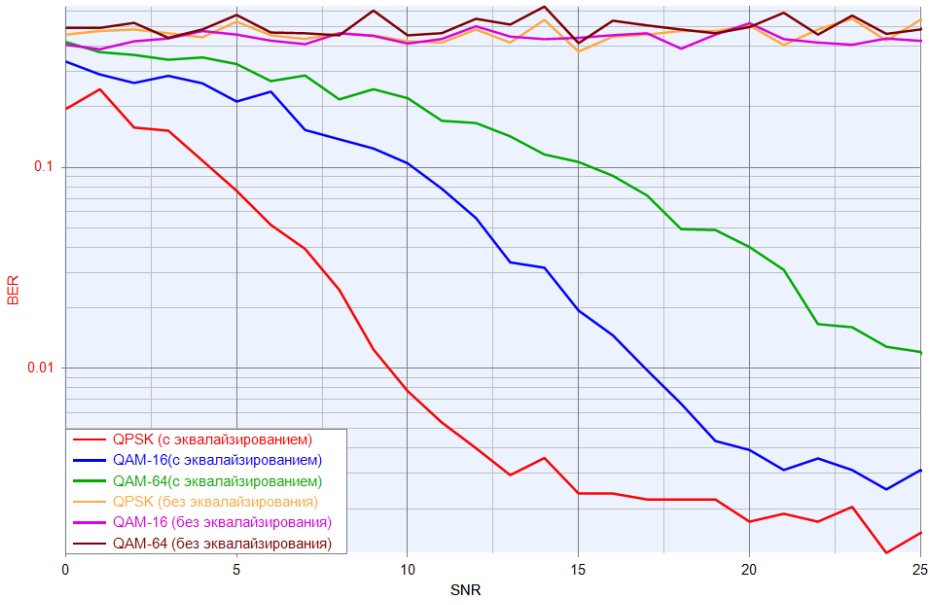


Рис. 8. Зависимость вероятности битовой ошибки от отношения сигнал – шум для канала Рэлея с замираниями

Анализируя зависимости, представленные на рис. 7, можно сделать вывод, что спроектированная модель адекватна. Значения вероятностей битовой ошибки для различных типов модуляций близки к теоретическим.

Для компенсации искажений, вызванных Рэлеевским каналом с замираниями необходимо эквалайзирование. Без применения данной процедуры, корректная демодуляция сигнала невозможна, что следует из анализа зависимостей, приведенных на рис. 8.

Крутизна падения характеристик на рис. 8 показательна. Для улучшения помехоустойчивости, помимо эквалайзирования, требуется помехоустойчивое кодирование. Также, улучшения качества эквалайзирования можно достичь, экспериментируя с различными способами размещения опорных поднесущих и методами интерполяции.

Полученная модель может быть использована для исследования различных методов эквалайзирования, включая “слепые” алгоритмы [4], а также найти применение для изучения систем с неортогональным множественным доступом.

Список используемых источников

1. Семенова А. И., Завьялов С. В., Смирнова Е. Н. Разработка метода оценки эффективности приема многочастотных сигналов в условиях многолучевого распространения // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А С. Попова: меж вуз. сб. науч. тр.

2. Ковалев В. В., Покаместов Д. А. Способы улучшения эквалайзирования в системах связи с OFDM // Доклады ТУСУР, 2018. Т. 21. № 1.

3. Крюков Я. В., Рогожников Е. В., Шибельгут А. А. Основы построения систем беспроводного широкополосного доступа: учебно-методическое пособие для практических занятий и самостоятельной работы, 2015. 37 с.

4. Джиган В. И. Адаптивная фильтрация сигналов: теория и алгоритмы. Москва: Техносфера, 2013. 528 с. ISBN 978-5-94836-342-4.

INVESTIGATION OF AN EQUALISATION METHOD FOR THE COMPENSATION OF DISTORTION IN A RAYLEIGH CHANNEL WITH FADING

Korotin V., Vtorykh V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the use of equalisation to compensate for the distortion caused by the Rayleigh channel in the case of fading. The research includes modelling of the OFDMA symbol transmission channel and analysis of bit error rate versus signal-to-noise ratio for different propagation conditions and signal modulations. The results demonstrate the potential of equalisation for reliability and communication quality improvement in challenging radio environments.

Key words: *equalisation, reference signal, channel transfer function, multipath propagation*

УДК 621.396.41
ГРНТИ 49.31.29

ИССЛЕДОВАНИЕ ФАКТОРОВ ФОРМИРОВАНИЯ ЗОН ПОКРЫТИЯ, ХАРАКТЕРНЫХ ДЛЯ РАДИОСИСТЕМ, ИСПОЛЬЗУЮЩИХ ТЕХНОЛОГИЮ OFDM

В. Е. Коротин, В. С. Вторых

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

В данной статье представлено исследование взаимосвязи между характеристиками систем радиосвязи на основе технологии OFDM (ортогональное частотное мультиплексирование) и радиусом их зон покрытия. Особое внимание уделено выбору величины защитного интервала (GI) или циклического префикса (CP). Статья обосновывает выбор оптимальной величины GI/CP для различных типов OFDM-систем, в зависимости от их назначения и требуемых размеров зоны обслуживания. Проведенный анализ способствует более глубокому пониманию механизмов работы современных OFDM-систем и факторов, влияющих на их зону покрытия. Рассматриваются не только энергетические показатели, но и другие существенные аспекты, определяющие размеры и форму зоны покрытия.

радиодоступ, OFDM, циклический префикс, защитный интервал, радиус зоны покрытия, межсимвольная интерференция, временное рассеяние

При анализе особенностей формирования зон покрытия в различных системах необходимо учитывать не только энергетические характеристики системы, но также ее помехозащищенность и особенности радиоинтерфейса. Ограничения по размеру зон покрытия могут определяться, например, защитным временным интервалом в системах с временным разделением каналов, препятствующий наложению соседних каналов из-за разности хода сигнала синхронизации к обслуживаемым станциям, находящимся на разном удалении от центрального координатора (базовой станции). Следовательно, важно учитывать эти аспекты при анализе и формировании зон покрытия для систем радиодоступа на базе технологии OFDM.

Общеизвестно, что такие системы умеют успешно справляться с межсимвольной интерференцией (временным рассеянием – в нотации некоторых источников) благодаря копированию некоторой части конца символа в межсимвольный промежуток времени, образуемый с предыдущим символом. Данный межсимвольный промежуток называют циклическим префиксом (CP – cyclic prefix) – в E-UTRA [1], 5G NR [2] либо защитным интервалом (GI – guard interval) – в IEEE 802.11 [3], IEEE802.16 [4] – рис. 1.

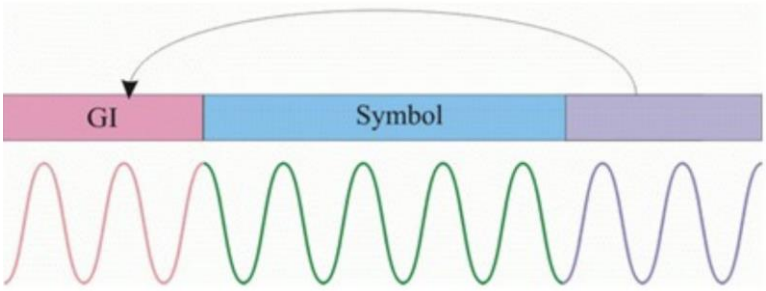


Рис. 1. Формирование защитного интервала (циклического префикса)

Очевидно, что величина защитного интервала должна выбираться в зависимости от желания скомпенсировать ту или иную разность хода, прямого и задержанного лучей – то есть ограничить интервал наложения соседних символов только величиной межсимвольного промежутка, заполняемого копией конечной части последующего символа и формирующего указанный защитный интервал (циклический префикс). Таким образом, вопрос о величине защитного интервала сводится к решению вопроса о том, от какой разности хода интерферирующих лучей следует предусмотреть защиту. Очевидно, что величина защитного интервала влияет на производительность системы радиодоступа из-за передачи дублированной информации, что приводит к снижению скорости пользовательского доступа:

$$\frac{1}{T} - \frac{1}{(T+G)} \qquad (1)$$

или в G/T раз, где: T – длительность символа, G – величина защитного интервала. Например, в стандарте IEEE 802.11a/g при величине защитного интервала 0,8 мкс и длительности символа 3,2 мкс снижение скорости достигало 25% (кстати говоря, численно равного относительной величине защитного интервала ¼ – традиционной форме указания величины защитного интервала в виде правильной дроби).

Следовательно, правильный выбор относительной величины защитного интервала ограничен сверху и является продуктом компромисса между производительностью и иммунитетом к межсимвольной интерференции. Указанный выше пример, пожалуй, является первой реализацией защитного интервала в публичной системе, поэтому рассмотрение вопроса об обоснованности выбора величины защитного интервала логично начать с нее.

Рекомендации из [5] указывают на то, что радиоволны могут распространяться от передатчика к приемнику через различные трассы, каждая из которых имеет свою временную задержку, зависящую от длины трассы. Эти сигналы с задержкой образуют линейный фильтр с изменяющимися во времени характеристиками. При моделировании задержки радиоканала предполагается, что он

описывается своей импульсной характеристикой, которая представляется в виде функциональной зависимости плотности мощности от дополнительной задержки относительно первого обнаруженного сигнала (профиль задержки мощности). Эти профили задержки мощности характеризуются параметрами, вычисленными по усредненным профилям по поверхности. Интересен параметр среднеквадратичного значения разброса задержки, который определяется по индивидуальным профилям и затухает по экспоненте, и его можно использовать вместо профиля задержки мощности [5]:

$$h(t) = \begin{cases} e^{-\frac{t}{S}} \text{ для } 0 \le t \le t_{max} \\ 0 \text{ в противном случае} \end{cases} \quad (2)$$

где: S – среднеквадратичное значение разброса задержки; t_{max} – максимальная задержка; $t_{max} >> S$.

Характерные значения параметра разброса задержки, полученные с помощью усредненных профилей задержки для трех видов помещений, представлены в таблице 1. Эти значения основаны на измерениях на частотах 1900 МГц и 5,2 ГГц [5]. В столбце B таблицы 5 представлены наиболее часто встречающиеся медианные значения, в столбце *A* – более низкие, но не минимальные, значения, которые также возникают достаточно часто, а в столбце *C* – самые высокие значения задержки, которые возникают весьма редко. Значения, приведенные в таблице, характерны для максимального размера вероятных помещений каждого типа.

ТАБЛИЦА 1. Среднеквадратичные значения параметра разброса задержки

Частота	Условия приема	A (нс)	B (нс)	C (нс)
1 900 МГц	Внутренние помещения жилых домов	20	70	150
1 900 МГц	Внутренние служебные помещения	35	100	460
1 900 МГц	Внутренние помещения промышленных зданий	55	150	500
5.2 ГГц	Внутренние служебные помещения	45	75	150

Как показывают приведенные в таблице 1 данные, выбранный в стандарте IEEE 802.11a/g защитный интервал 800 нс согласуется с экспериментальными результатами.

Список используемых источников

1. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; LTE Physical Layer - General Description (Release 8), 2011. 44 с.

2. 5G; NR; Physical layer; General description (3GPP TS 38.201 version 15.0.0 Release 15), 2018. 13 с.

3. 802.11n-2009 - IEEE Standard for Information technology-- Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput, 2009.

4. WirelessMAN®: Inside the IEEE 802.16 Standard for Wireless Metropolitan Area Networks, 2006. 223 с.

5. Рекомендация МСЭ-R P.1238-5 Данные о распространении радиоволн и методы прогнозирования для планирования систем радиосвязи внутри помещений и локальных зоновых радиосетей в частотном диапазоне 900 МГц – 100 ГГц, 2009.

INVESTIGATION OF COVERAGE ZONE FORMATION FACTORS CHARACTERISTIC OF OFDM RADIO SYSTEMS

Vtorykh V, Korotin V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

An investigation of the relationship between the characteristics of radio communication systems based on OFDM (Orthogonal Frequency Division Multiplexing) technology and the radius of their coverage areas is presented in this paper. Particular attention is paid to the choice of the guard interval (GI) or cyclic prefix (CP). The paper justifies the choice of the optimal value of GI/CP for different types of OFDM-systems, depending on their purpose and the required size of the service area. The analysis contributes to a deeper understanding of the mechanisms of operation of modern OFDM-systems and the factors affecting their coverage area. Not only energy performance is considered, but also other essential aspects that determine the size and shape of the coverage area.

Key words: *radio access, OFDM, cyclic prefix, guard interval, coverage radius, intersymbol interference, temporal scattering.*

УДК 621.396.67
ГРНТИ 47.45.99

МИКРОВОЛНОВЫЙ ЭЛЛИПТИЧЕСКИЙ ФИЛЬТР С РЕАЛИЗАЦИЕЙ НА МИКРОПОЛОСКОВЫХ РЕЗОНАТОРАХ С ЧЕТВЕРТЬВОЛНОВЫМИ ИНВЕРТОРАМИ СОПРОТИВЛЕНИЙ

А. Р. Кубалова

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

Представлен алгоритм расчета модифицированного ЭФ СВЧ с четвертьволновыми инверторами импедансов с реализацией на микрополосковой линии. Исследуются возможности дополнительной миниатюризации устройства путем реализации на микрополосковой линии.

эллиптический фильтр, СВЧ фильтр, микрополосковая линия (МПЛ), инверторы импедансов, полосно-пропускающий фильтр, электромагнитное моделирование

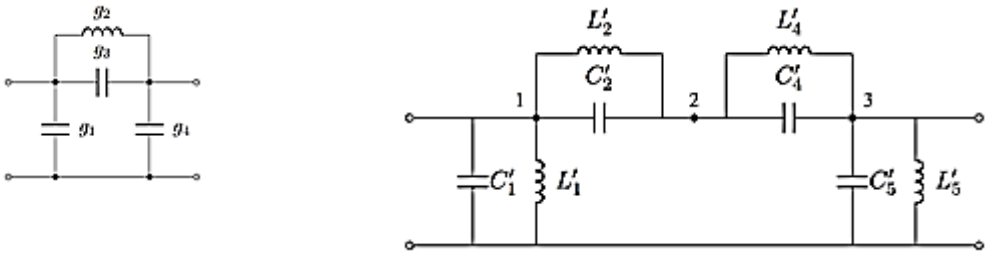
Расчет ЭФ с четвертьволновыми инверторами сопротивлений на МПЛ можно свести к следующим этапам [1]: а) частотное преобразование от фильтра-прототипа нижних частот (ФПНЧ) к полосно-пропускающему фильтру (ППФ); б) преобразование узловых проводимостей ППФ методом Нортона, не искажающее входные и выходные характеристики фильтра; в) включение в схему четвертьволновых инверторов, преобразующих полосно-заграждающие резонансные контуры в их дуальные последовательные цепи [2, с. 370]; г) преобразование резонансных контуров в полосковые шлейфы методом приравнивания параметров крутизны реактивных сопротивлений или проводимостей [2, с. 182–184]; д) масштабирование всех волновых сопротивлений данного фильтра и расчет емкостных цепей согласования с источником и нагрузкой [2, с. 370–373]. Схема П-секции эллиптического ФПНЧ представлена на рисунке 1а. Перейдем от схемы ФПНЧ к ППФ на элементах с сосредоточенными параметрами (рис. 1б), воспользовавшись частотным преобразованием:

$$\Omega \rightarrow a_1 \left(\omega/\omega_0 - \omega_0/\omega\right)$$

где $\omega = 2\pi f$ – циклическая частота, $\omega_0 = 2\pi f_0$ – циклическая центральная частота, $a_1 = f_0/(f_2 - f_1)$, $f_1 = f_0 - w * f_0 /100\ \%$, $f_2 = f_0 + w * f_0 /100\ \%$. Рассчитаем значения элементов ППФ.

Одним из методов полосковой реализации фильтра на рисунке 1б служит добавление четвертьволновых инверторов. Второй узел необходимо привести к эквивалентной Т-образной схеме с проводимостью на землю. Это преобразование осуществляется методом Нортона. Далее все волновые сопротивления должны быть масштабированы до более удобных значений.

На рисунке 2 представлены этапы преобразования внутренней части фильтра по методу Нортона. В схему добавляются два идеальных трансформатора с коэффициентом трансформации $\sqrt{n}$. Цепи, обозначенные пунктирной линией на рисунке 2а, заменяются эквивалентными П-образными схемами (рис. 2б). Шунтирующие емкости и индуктивности узлов складываются.



а) б)

Рис. 1. П-секция эллиптического ФПНЧ (а) и схема эллиптического ППФ на элементах с сосредоточенными параметрами (б)

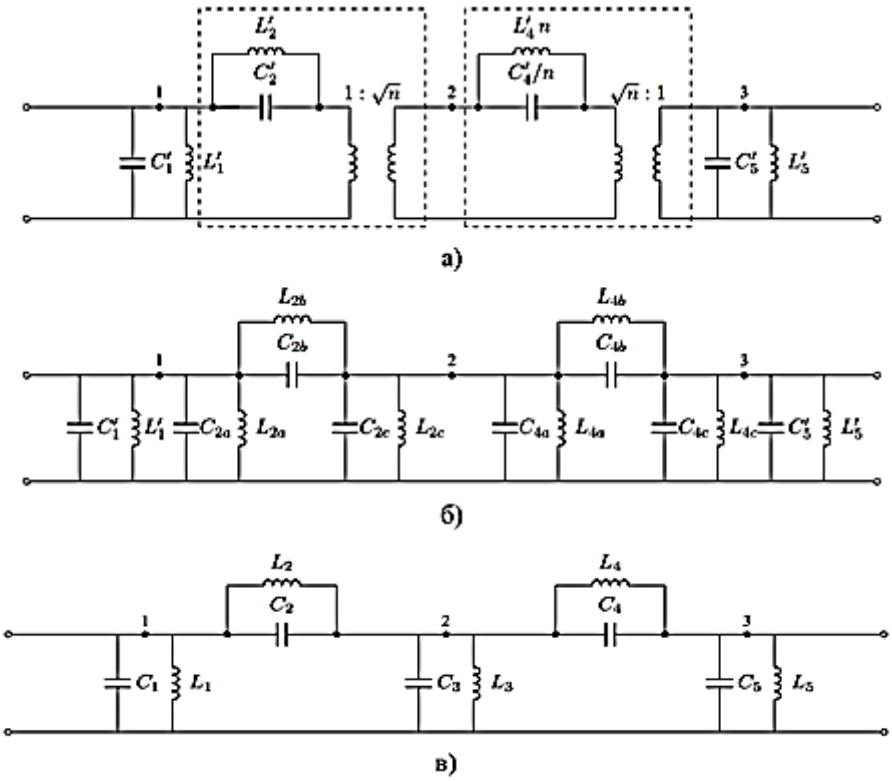


Рис. 2. Преобразование схемы ЭФ на элементах с сосредоточенными параметрами по методу Нортона

В результате получаем схему на рисунке 2в, в которой у каждого узла есть проводимость на землю. Зададимся коэффициентом трансформации $\sqrt{n} < 1$ и рассчитаем значения элементов схемы 2в.

Следующим шагом в схему добавляются четвертьволновые инверторы (рис. 3а) с коэффициентом трансформации $\sqrt{s} < 1$ и рассчитываются новые значения элементов четных резонансных контуров на рисунке 3а.

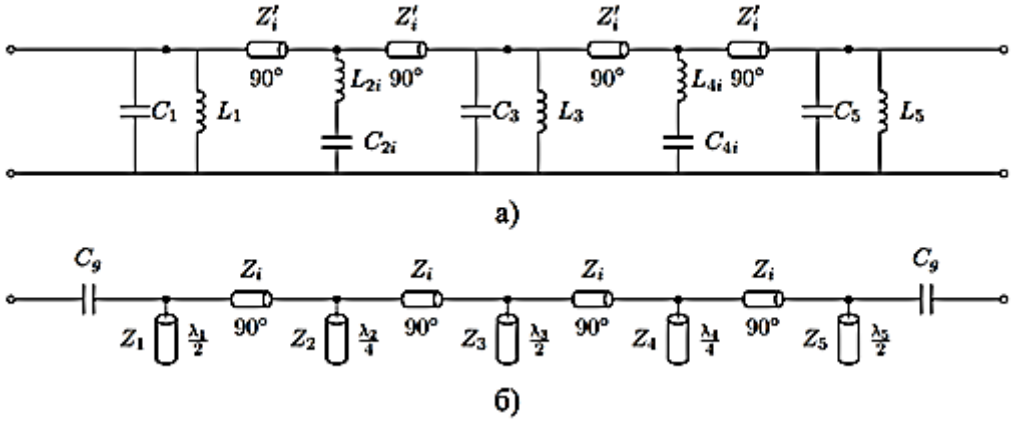


Рис. 3. Преобразование схемы ЭФ на элементах с сосредоточенными параметрами к структуре из полосковых шлейфов

Преобразование резонансных контуров из элементов с сосредоточенными параметрами к полосковым шлейфам осуществляется методом приравнивания параметров крутизны реактивных сопротивлений на частоте резонанса [5, с. 182–184]. Параллельные контуры становятся разомкнутыми отрезками линий передачи длиной $\lambda_0/2$, а последовательные – разомкнутыми шлейфами $\lambda_0/4$, где λ_0 – резонансная длина волны. В результате топология фильтра будет представлять собой полосковые шлейфы, разделенные четвертьволновыми отрезками линий передачи. По результатам анализа влияния параметра $\sqrt{s}$ на АХЧ фильтра было выявлено, что для сохранения равноволновой характеристики в полосе пропускания (ПП) за центральную частоту первой пары инверторов следует взять резонансную частоту первого полуволнового резонатора, а для второй пары – последнего резонатора. С целью получения удобных для реализации на МПЛ физических размеров, все волновые сопротивления фильтра масштабируются на величину $b > 1$. В качестве цепей согласования с источником и нагрузкой используются емкостные инверторы сопротивлений [5, с. 370–373] с коэффициентом трансформации $\sqrt{b}$. Найденные параметры служат входными данными для определения физических размеров модифицированной топологии ЭФ СВЧ с четвертьволновыми инверторами.

Электрическую длину фильтра можно уменьшить вдвое путем смещения емкостных трансформаторов к месту соединения инверторов с крайними шлейфами. Для компенсации паразитных влияний, создаваемых изгибами микрополосковых шлейфов, используют такие коэффициенты трансформации, при которых волновые сопротивления и проводимости инверторов и крайних полуволновых шлейфов были эквивалентны [2]. Граничные условия на концах полуволнового полоска будут совпадать для канонической и модифицированной конструкций (рис. 4).

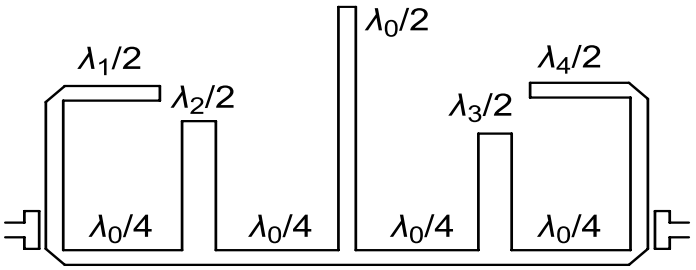


Рис. 4. Модифицированная структура СВЧ ЭФ с инверторами

Разработана компактная модификация узкополосного ЭФ СВЧ с четвертьволновыми инверторами сопротивлений. Электрическая длина фильтра снижена в два раза. Благодаря реализации на МПЛ, используется только один слой диэлектрика.

Список используемых источников

1. Кубалова А. Р., Томашевич С. В. Синтез и моделирование микроволновых фильтров. СПб.: Издательство СПбГУТ, 2012. 216 с.

2. Маттей Д. Л., Янг Л., Джонс Е.М.Т. Перевод с английского под общей редакцией. Л. В. Алексеева и Ф. В. Кушнира. Фильтры СВЧ, согласующие цепи и цепи связи. Т. 1. М.: Связь, 1971. 421 с.

MICROWAVE ELLIPTICAL FILTER IMPLEMENTED ON MICROSTRIP RESONATORS WITH QUARTER-WAVE RESISTANCE INVERTORS

Kubalova A.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunications

A numerical example of the calculation of a modified microwave elliptical filter with quarter-wave resistance inverters implemented on a microstrip line is presented. The possibilities of additional miniaturization of the device are being investigated by implementing it on a microstrip line and using a dielectric with ε_r=10. Filter models were calculated and manufactured according to the developed methodology. The results of electromagnetic simulation and experimental research are presented.

Key words: *microstrip line, impedance inverters, band-pass filter, electromagnetic simulation*

УДК 004.421
ГРНТИ 47.14.17

ИСПОЛЬЗОВАНИЕ СПУТНИКОВОЙ СВЯЗИ VSAT ДЛЯ ИНТЕГРАЦИИ С ПЛАТФОРМОЙ RIGSPACE В ЦЕЛЯХ МОНИТОРИНГА БУРОВЫХ ОПЕРАЦИЙ НА УДАЛЕННЫХ НЕФТЯНЫХ СКВАЖИНАХ

А. Н. Ликонцев, Д. С. Попов

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

В условиях глобальной цифровизации нефтегазовая отрасль сталкивается с задачей повышения эффективности и безопасности буровых операций, особенно на удаленных и труднодоступных месторождениях. Одним из перспективных решений является использование спутниковой связи VSAT (Very Small Aperture Terminal) для интеграции с цифровыми платформами, такими как Rigspace. Эта технология обеспечивает мониторинг и управление буровыми операциями в режиме реального времени, что особенно актуально для регионов с ограниченной инфраструктурой связи.

Rigspace, спутники, VSAT, нефтескважина

Специфика использования VSAT на нефтяных скважинах

Спутниковая связь VSAT широко применяется в нефтегазовой отрасли благодаря своей способности обеспечивать надежную связь в условиях удаленности и экстремальных климатических условий. Основные особенности применения VSAT на нефтяных скважинах:

– удаленность и труднодоступность – месторождения часто расположены в регионах без развитой наземной инфраструктуры;
– экстремальные условия – низкие температуры, высокая влажность и другие факторы требуют высокой надежности оборудования;
– разнородность данных – необходимость передачи телеметрии, видео и голосовых данных;
– требования к связи – высокая пропускная способность, минимальные задержки, безопасность и устойчивость к помехам.

Основные компоненты VSAT-системы:

– терминал VSAT – антенна диаметром 1,2–2,4 м, спутниковый модем с поддержкой протоколов TCP/IP, блок питания (автономный, с возможностью работы от генераторов или солнечных батарей) [3];

– центральная станция (хаб) – управляет трафиком и маршрутизацией данных;
– спутник – геостационарный (например, "Ямал"), работающий в Ku-диапазоне (10,7–14,5 ГГц) или C-диапазоне (4–8 ГГц);
– технические параметры включают скорость до 50 мбит/с (downlink) и задержку 500–700 мс, система также обеспечивает безопасность данных и устойчивость к помехам.

Платформа Rigspace и ее роль в нефтедобыче

Rigspace – это облачная цифровая платформа, разработанная для оптимизации процессов бурения и добычи нефти и газа [1]. Она объединяет данные, аналитику и инструменты управления, предоставляя операторам возможность контролировать буровые операции в реальном времени. Пример на рис. 1.

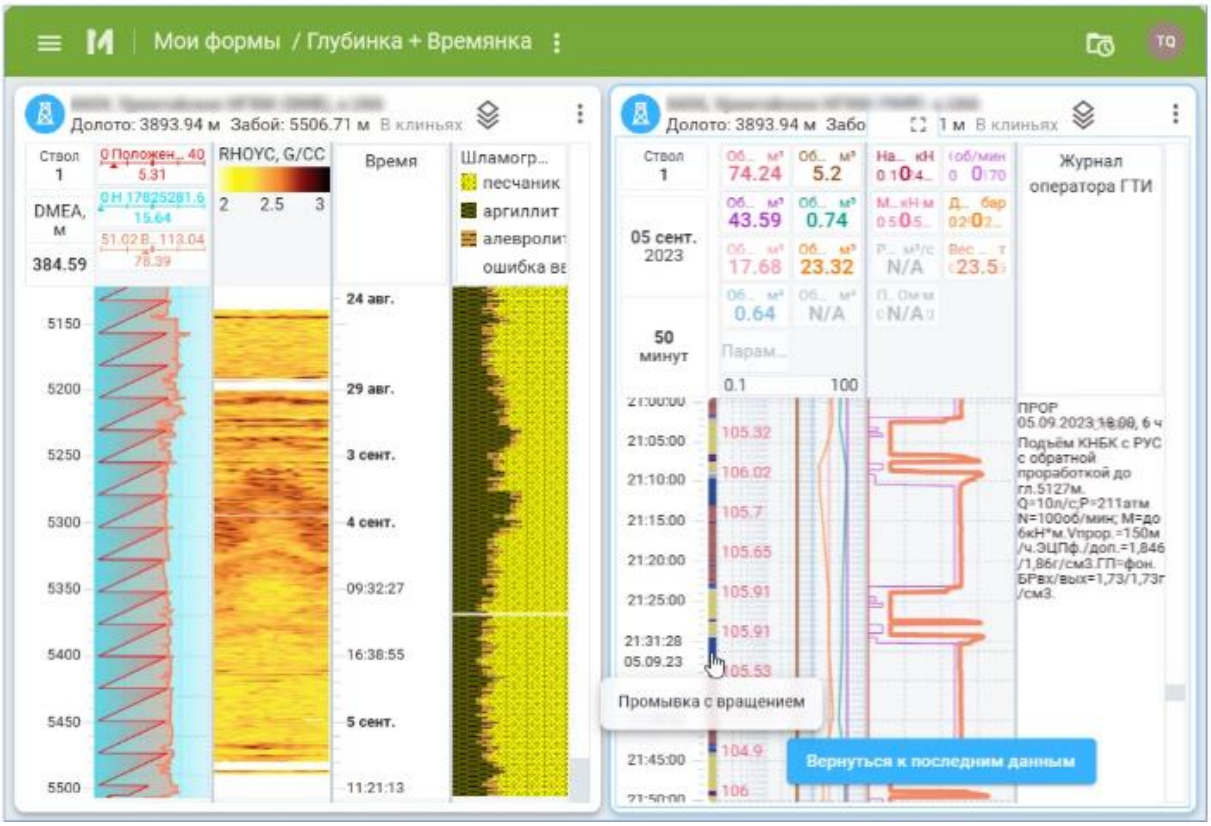


Рис. 1. Форма для мониторинга данных в Rigspace

Основные функции Rigspace – контроль параметров бурения: скорости, давления, температуры, анализ данных для оперативных решений, а так же удаленное управление и координация работ [2].

Интеграция VSAT с Rigspace: технические аспекты

Интеграция VSAT с платформой Rigspace включает следующие этапы:

1. Установка VSAT-терминалов. На буровой платформе устанавливаются спутниковые антенны и модемы, обеспечивающие подключение к интернету.

2. Настройка сети. Создание локальной сети на буровой установке для подключения всех датчиков и систем к VSAT-терминалу.

3. Интеграция с Rigspace. Данные с буровой установки передаются через VSAT на серверы Rigspace, где они обрабатываются и анализируются.

4. Техническая поддержка и обслуживание, после запуска системы важно обеспечить ее постоянное техническое сопровождение. Пример показан на рис. 2.



Рис. 2. Блок-схема передачи данных

Автоматизация передачи данных телеметрии в компании «Тетра-Софт-Сервис»

В рамках проекта автоматизации передачи телеметрических данных с нефтяных скважин на платформу Rigspace, был разработан и реализован алгоритм комбинирования экспоненциального скользящего среднего (EMA) и медианного фильтра. Этот алгоритм был написан на языке программирования Python, что позволило эффективно обрабатывать данные в реальном времени и оптимизировать передачу через каналы связи с ограниченной пропускной способностью (VSAT). Анализ требований заказчика.

Цели – автоматизировать сбор и передачу данных, снизить нагрузку на каналы связи, интегрировать с Rigspace.

Передача ключевых параметров – давления, температуры, уровня жидкости, скорости бурения и пр.

Ограничения – использование VSAT с ограниченной пропускной способностью.

Разработка решения

1. Экспоненциальное скользящее среднее (*EMA*) – это метод сглаживания данных, который придает больший вес последним наблюдениям. Это делает *EMA* более чувствительным к изменениям в данных, что полезно для обнаружения резких изменений параметров (например, скачков давления или температуры).

$$EMAt = \alpha \cdot xt + (1-\alpha) \cdot EMAt-1 EMAt = \alpha \cdot xt + (1-\alpha) \cdot EMAt-1, \quad (1)$$

где *EMAt* – текущее значение *EMA*, x*t* – текущее значение данных, EMAt-1 – предыдущее значение *EMA*, α – коэффициент сглаживания (обычно между 0 и 1). С увеличением α возрастает вес последних данных.

2. Медианный фильтр – это метод устранения шумов в данных. Он заменяет текущее значение на медиану из окна соседних значений. Это полезно для удаления выбросов (аномалий), которые могут возникать из-за ошибок датчиков или помех.

Комбинирование EMA и медианного фильтра

Для достижения наилучших результатов можно комбинировать оба метода рис. 3. Алгоритм состоит из двух основных этапов:

1. Применение медианного фильтра для устранения шумов и выбросов в данных.

2. Вычисление экспоненциального скользящего среднего (EMA) для сглаживания данных и выделения трендов.

Пример сценария:

Давление на скважине: 180, 190, 200, 210, 220, 1000, 230, 240, 250 бар.

Медианный фильтр удаляет выброс (1000 бар).

EMA вычисляет тренд: 180, 185, 190, 195, 200, 205, 210, 215, 220.

Если давление превышает 200 бар, данные передаются на сервер.

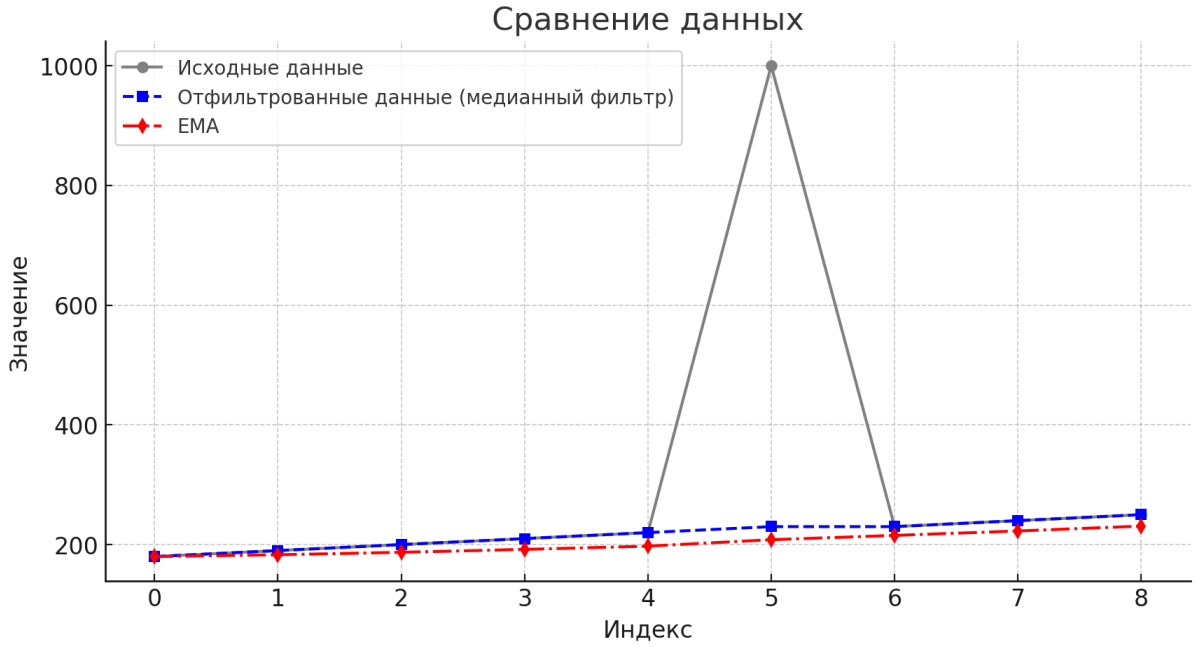


Рис. 3. График сравнения данных фильтров

Применение в проекте

Данный алгоритм был успешно внедрен в систему автоматизации передачи телеметрических данных на нефтяных скважинах. Его использование позволило:

– уменьшить объем передаваемых данных за счет фильтрации и выделения критических параметров;
– повысить точность данных за счет устранения шумов и выбросов;
– обеспечить передачу данных в реальном времени через каналы связи с ограниченной пропускной способностью (VSAT).

Преимущества интеграции VSAT и Rigspace

– реальный мониторинг – оперативное отслеживание параметров бурения [5];
– безопасность – снижение рисков за счет раннего выявления проблем;
– удаленное управление – координация операций из центрального офиса;
– экономическая эффективность – долгосрочные выгоды превышают первоначальные затраты.
–

Примеры применения

В России, где значительная часть нефтяных месторождений расположена в удаленных и труднодоступных регионах, интеграция спутниковой связи VSAT с цифровой платформой Rigspace нашла широкое применение

[4]. Ниже приведены конкретные примеры использования этой технологии на российских месторождениях:

1. Месторождение в Западной Сибири (Ханты-Мансийский автономный округ). Результатом является сокращение времени простоя буровых установок на 20% за счет оперативного выявления и устранения неполадок.

2. Месторождение на полуострове Ямал (Ямало-Ненецкий автономный округ). Полуостров Ямал известен своими экстремальными климатическими условиями, где температура зимой может опускаться ниже -50°C, а инфраструктура связи практически отсутствует.

Результаты

Снижение затрат на бурение на 15 % за счет оптимизации использования бурового раствора и энергии.

Уменьшение количества аварийных ситуаций на 30 % благодаря раннему обнаружению отклонений.

Заключение

Интеграция спутниковой связи VSAT с платформой Rigspace обеспечивает надежный мониторинг и управление буровыми операциями на удаленных нефтяных скважинах. Эта технология повышает безопасность, оптимизирует процессы и снижает затраты, что особенно важно для труднодоступных регионов России. Перспективы развития включают внедрение 5G, Интернета вещей и искусственного интеллекта.

Список используемых источников

1. Rigspace User Guide. Digital Solutions for Drilling Operations [Электронный ресурс], 2021. URL: https://tetra-soft.ru/rigspace-monitoring (дата обращения 26.01.2025).

2. Akinwale Eso1, Omorogiuwa Eseosa Real-Time Effective Monitoring and Control in Oil and Gas Industry Using SCADA Technology as a Management Tool // MAT Journals, 2022. Vol. 8 (2). PP. 22–38. URL: https://www.researchgate.net/publication/362048204_Real-Time_Effective_Monitoring_and_Control_in_Oil_and_Gas_Industry_Using_SCADA_Technology_as_a_Management_Tool (дата обращения 26.01.2025).

3. Портненко М. А., Степанов Е. Г., Шамаев И. А., Ермаков К. В. Диагностический мониторинг объектов энергетики, нефтегазовой, нефтеперерабатывающей и химической промышленности – путь повышения промышленной безопасности // 2023. URL: https://3minut.ru/images/PDF/2015/16/diagnosticheskij-monitoring-ob-ektov-energetiki-neftegazovoj-neftepererabatyvayushchej.pdf (дата обращения 26.01.2025).

4. Павлович Ю. Л., Долгушина Л. В., Кабакова Е. С., Литвинов Р. В. Методы мониторинга состояния нефтегазовых объектов// 2025. URL: https://apbt-sibpsa.ru/wp-content/uploads/2025/v1/1(17)_16-30.pdf (дата обращения 26.01.2025).

5. Антонец К. В. Комплексный мониторинг нефтегазовых загрязнений // IACJ. 2021. № 1. URL: https://cyberleninka.ru/article/n/kompleksnyy-monitoring-neftegazovyh-zagryazneniy (дата обращения 26.01.2025)

USING VSAT SATELLITE COMMUNICATIONS TO INTEGRATE WITH THE RIGSPACE PLATFORM IN ORDER TO MONITOR DRILLING OPERATIONS AT REMOTE OIL WELLS

Likontsev A., Popov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of global digitalization, the oil and gas industry face the challenge of improving the efficiency and safety of drilling operations, especially in remote and hard-to-reach fields. One of the promising solutions is the use of VSAT (Very Small Aperture Terminal) satellite communications for integration with digital platforms such as Rigspace. This technology provides real-time monitoring and management of drilling operations, which is especially important for regions with limited communication infrastructure.

Key words: *Rigspace, satellites, VSAT, oil well*

УДК 621.39
ГРНТИ 49.33.29

К ВОПРОСУ РЕШЕНИЯ ЗАДАЧИ О МНОГОПРОДУКТОВОМ ПОТОКЕ В ИНТЕЛЛЕКТУАЛНОЙ СИСТЕМЕ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

А. Г. Любимов

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

Существует класс распределенных систем, для которых задачи структурно-параметрического анализа и синтеза целесообразно решать с использованием интеллектуальных систем поддержки принятия решений. В качестве модели в таких системах часто предлагается использовать математическую модель сети с многопродуктовым потоком. Классические методы решения задачи о многопродуктовом потоке основаны на определении максимального потока в путевой форме. В работе показан подход к решению задачи в т-мерном векторном пространстве области допустимых значений многопродуктового потока.

модель сети с многопродуктовым потоком, область допустимых значений многопродуктового потока, многомерное векторное пространство

Существует класс распределенных систем, для которых целевое функционирование существенно зависит от показателей специально создаваемой или арендованной транспортной инфраструктуры. К таким системам, главным образом, относятся телекоммуникационные, транспортные, энергетические и другие системы. Основу транспортной инфраструктуры составляют транспортные сети.

Очевидно, что для принятия обоснованных управленческих решений в конкретных условиях функционирования транспортной сети, необходимо оперативно разрабатывать и оценивать множество альтернативных вариантов по некоторому целевому функциональному или обобщенному показателю. В качестве такого инструмента, как правило, предлагается использовать системы поддержки принятия решений (СППР). Выбор наиболее информативного показателя (целевой функции) транспортных сетей, для применения в задачах анализа и синтеза, решаемых в интеллектуальных СППР, остается актуальным.

Основным функциональным показателем производительности транспортных сетей можно считать величину потока, передаваемого в интересах,

в общем случае, большого количества пользователей. Множество пользователей в сети в каждый момент времени представляет собой совокупность корреспондирующих пар, в каждой из которых один из пользователей выступает источником (истоком) некоторого частного потока, а другой – потребителем (стоком) этого потока. Следовательно, частные потоки имеют направление. В общем случае, роли пользователей в корреспондирующей паре могут меняться местами, что приведет к изменению направления и возможно величины частного потока. Частные потоки корреспондирующих пар в сети существуют независимо друг от друга. Общий поток в сети, представляющий собой совокупность частных потоков, будем называть многопродуктовым потоком, а транспортную сеть – МП-сетью.

Здесь и далее термин «поток» представляет собой некоторую абстракцию, физический смысл которой будет иметь место для конкретных транспортных сетей.

Можно показать, что функциональные возможности МП-сети по передаче многопродуктового потока, с одной стороны, определяется структурой сети, а с другой – расположением истоков и стоков на этой структуре. В качестве функциональной характеристики МП-сети, предлагается использовать понятие пропускной способности. Под пропускной способностью МП-сети или отдельных элементов ее структуры будем понимать предельно допустимые значения многопродуктового потока и частных потоков корреспондирующих пар (исток–сток). Для одной и той же структуры сети значения многопродуктовых потоков могут существенно отличаться при изменении расположения корреспондирующих пар на этой структуре. Аналогичные результаты следует ожидать при изменениях в структуре сети с неизменным расположением корреспондирующих пар. Пропускную способность можно считать наиболее информативной характеристикой в реальных условиях функционирования МП-сетей.

Модель МП-сети, в общем виде, представим в виде взвешенного неориентированного графа $G=\{A,B\}$, где $A=\{a_1,..,a_n\}$ – множество узлов, $B = \{b_{ij}: i,j = 1,..,n;\ i\neq j\}$– множество ребер. На МП-сети может быть организовано m корреспондирующих пар (сток–исток) из множества $\{a_s,a_t:s,t = 1,..,n;s \neq t\}$ В качестве веса ребра b_{ij} примем пропускную способность c_{ij}, соответствующую предельно допустимому значению передаваемого по ребру потока. Каждая корреспондирующая пара узлов (a_s,a_t) создает независимый частный поток f_{st}, исходящий от узла a_s и направляемый по сети к узлу a_t (обратное верно).

Задача о максимальном многопродуктовом потоке в путевой форме формулируется в следующем виде [1]:

максимизировать

$$\sum_{k=1}^{m} f_{st}^{k}, \tag{1}$$

при ограничениях

$$\sum_i x_{ij}^k - \sum_i x_{ji}^k = \begin{cases} 0, \text{если } j \neq s,t, \\ f_{st}^k, \text{если } j = s,t. \end{cases},$$

$$\sum_{k=1}^{m} x_{ij}^k \leq c_{ij}.$$

Здесь x_{ij}^k некоторая часть потока f_{st}^k, направляемая по ребрам МП-сети. Разность потоков, водящих в некоторый узел a_j и выходящий из него равна нулю, если этот узел не является узлом корреспондирующей пары (a_s,a_t). Суммарный поток от всех корреспондирующих пар по ребру b_{ij} не может превышать его пропускную способность c_{ij}.

Задачу (1), как правило, предлагается решать с использованием методов линейного программирования. Однако такой подход к решению задачи о многопродуктовом потоке в путевой форме имеет больше теоретическое значение, нежели практическое применение. Во-первых, задача в такой постановке имеет большую размерность, а во-вторых, максимум целевой функции будет соответствовать некоторому варианту (далеко не единственному) распределения частных потоков в МП-сети. Для аргументированного принятия управленческих решений требуется рассмотрение, как правило, нескольких альтернативных вариантов.

Анализ МП-сети, в конкретных условиях функционирования, можно представить в виде постановки следующих задач с использованием СППР.

Задача 1. Оценить возможности существующей структуры МП-сети для передачи частных потоков для выделенной группы корреспондирующих пар узлов.

Задача 2. Определить наиболее «слабые» места в структуре МП-сети, ограничивающие реализацию предъявленных требований по передаче частных потоков.

Вторая задача является следствием первой задачи, если реализовать предъявленные требования корреспондирующих пар по передаче частных потоков в полном объеме не представляется возможным.

Задача 3. Оценить варианты реконфигурации (восстановления, развития и т.п.) структуры МП-сети по реализации требований корреспондирующих пар по передаче частных потоков.

В настоящей работе предлагается подход к решению задачи о многопродуктовом потоке на основе свойств разрезов (сечений) и рассекающих множеств потоковых сетей.

В частном случае, для одной выделенной корреспондирующей пары узлов (a_s,a_t) оценка пропускной способности МП-сети может быть эффективно решена известными алгоритмами в рамках теоремы Форда-Фалкерсона о максимальном потоке и минимальном разрезе [2].

Максимальный поток в сети для корреспондирующей пары узлов (a_s,a_t) равен пропускной способности минимального разреза (сечения) МП-сети:

$$(f_{st})_{max} = (\sum c_{ij})_{min},\ b_{ij} \in S_{st},$$

где S_{st} – некоторое сечение сети (из множества возможных сечений), нарушающее связность корреспондирующей пары узлов (a_s,a_t) в МП-сети и обладающее минимальной суммарной пропускной способностью входящих в него ребер.

В общем случае, в МП-сети одновременно существуют потоки множества корреспондирующих пар узлов (имеет место многополюсная МП-сеть). Известно, что решение задачи для многополюсной МП-сети можно получить путем расчета минимальных по пропускной способности сечений (разрезов) для каждой пары узлов отдельно одним из известных алгоритмов комбинаторной оптимизации [3, 4].

Одним из наиболее эффективных методов решения задачи расчета максимальных потоков в многополюсной МП-сети является построение потоко-эквивалентной сети в виде дерева минимальных сечений Гомори-Ху [1].

На рисунке 1 представлены две потоко-эквивалентные МП-сети, одна из которых реализована в виде дерева минимальных сечений.

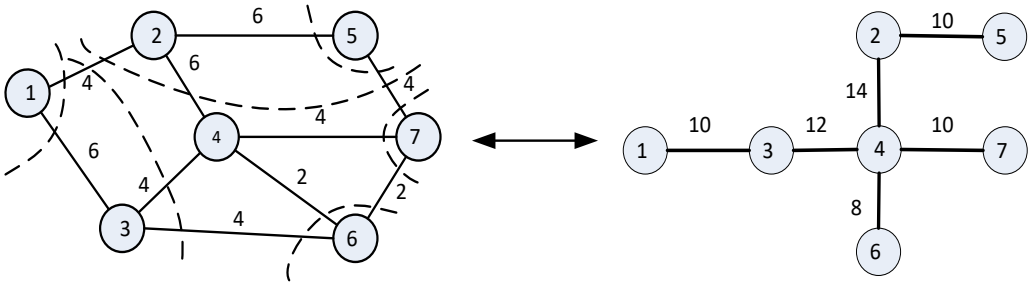


Рис. 1. Потоко-эквивалентные сети

На дереве минимальных сечений каждое ребро, например b_{34}, представляет собой множество ребер $\{b_{12},b_{34},b_{36}\}$ исходной МП-сети, входящих в сечение. При этом значение пропускной способности $c(b_{34}) = 12$ определяет

максимальное значение потока, который может обеспечить МП-сеть с данной структурой между множеством узлов $\{a_1,a_3\}$ и множеством узлов $\{a_2,a_4,a_5,a_6,a_7\}$. Аналогичным образом можно получить полную характеристику МП-сети по передаче потоков в любой комбинации корреспондирующих пар узлов.

Определение предельных (граничных) значений множества максимальных частных потоков $\{f_{st}^k\}$ является необходимым, но, как будет показано ниже, не достаточным условием для полной оценки возможностей МП-сети по пропускной способности. Остается не выясненным главный вопрос: какие существуют в МП-сети ограничения на одновременную передачу частных потоков?

Реализация максимального значения частного потока для каждой корреспондирующей пары узлов (a_s,a_t) возможна при условии, что потоки других корреспондирующих пар полностью отсутствуют или не создают ограничений на маршрутах его передачи. Следовательно, в МП-сети можно выделить некий общедоступный («разделяемый») ресурс пропускной способности, обеспечивающий одновременную полную или частичную реализацию требований по передаче потоков на множестве заданных корреспондирующих пар узлов $\{a_s,a_t\}$.

По аналогии со свойством минимального разреза для двухполюсной сети (теорема Форда-Фалкерсона), введем понятие минимального рассекающего множества для многополюсной МП-сети.

Минимальное рассекающее множество (МРМ) многополюсной МП-сети – это множество ребер с минимальной суммарной пропускной способностью, удаление которых из сети приведет к нарушению связности для заданного множества корреспондирующих пар узлов.

Принимая во внимание, что суммарная пропускная способность МРМ представляет собой «разделяемый» ресурс МП-сети, можно записать условия совместного существования частных потоков для m пар из множества $\{a_s,a_t\}$ в виде:

$$\begin{gathered}(f_{st}^1)_{max} \le (\sum c_{ij})_{min},\ b_{ij} \in S_{st}^1;\\ (f_{st}^{m-1})_{max} \le (\sum c_{ij})_{min},\ b_{ij} \in S_{st}^{m-1};\\ (f_{st}^m)_{max} \le (\sum c_{ij})_{min},\ b_{ij} \in S_{st}^m;\\ (\sum_{k=1}^m f_{st}^k)_{max} \le (\sum c_{ij})_{min},\ b_{ij} \in Z_{st}.\end{gathered} \qquad (2)$$

Система из m+1 неравенств (2) представляет собой область допустимых значений множества частных потоков $\{f_{st}^k\}$, реализуемых в МП-сети одновременно, где:

($S_{st}^k, k = 1, \dots, m$) – минимальные разрезы МП-сети для каждой пары корреспондирующих узлов из множества $\{a_s,a_t\}$;

$Z_{\{st\}}$.– минимальное по суммарной пропускной способности рассекающее множество ребер для всех пар корреспондирующих узлов из множества $\{a_s,a_t\}$.

Предлагается многопродуктовый поток в МП-сети рассматривать в качестве вектора $\vec{F}$ в m-мерном пространстве области допустимых значений (2). При этом область допустимых значений представляет собой m-мерное конечное векторное пространство $V = \{\overrightarrow{f_{st}^1}, \dots, \overrightarrow{f_{st}^m}\}$.

В общем виде вектор

$$\vec{F} = \alpha_1\overrightarrow{f_{st}^1} + \alpha_2\overrightarrow{f_{st}^2} + \dots + \alpha_m\overrightarrow{f_{st}^m},$$

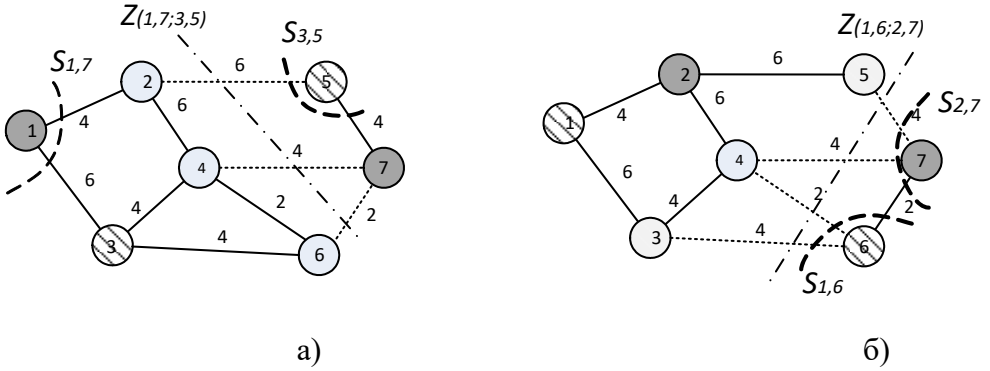
для заданных m-пар в МП-сети, можно представить в виде линейной комбинации векторов [5], описывающих частные потоки корреспондирующих пар узлов из множества $\{a_s,a_t\}$, где:

$\alpha_1, \alpha_2, \dots, \alpha_m$ – коэффициенты, соответствующие значениям частых потоков $\{f_{st}^k; k = 1, \dots, m\}$,

$\overrightarrow{f_{st}^1}, \overrightarrow{f_{st}^2}, \dots, \overrightarrow{f_{st}^m}$ – *базис* векторного пространства области допустимых значений частных потоков МП-сети.

Множество значений коэффициентов $\alpha_1, \alpha_2, \dots, \alpha_m$ в пределах области допустимых значений представляет собой множество распределений частных потоков, реализуемых в МП-сети одновременно.

Для иллюстрации предлагаемого подхода на рисунке 2 приведены два варианта организации корреспондирующих пар узлов на одной и той же МП-сети: $\{(a_1,a_7),(a_3,a_5)\}$ – вариант на рис.2а; $\{(a_2,a_7),(a_1,a_6)\}$ – вариант на рис. 2б.



а) б)

Рис. 2. Варианты организации корреспондирующих пар узлов на МП-сети

Пунктирными линиями на МП-сети показаны минимальные разрезы для каждой пары корреспондирующих узлов и минимальные рассекающие множества ребер, удаление которых из сети разрывает все возможные маршруты передачи частных потоков.

Области допустимых значений частных потоков для МП-сети составляют (на рис. 3 обозначены штриховкой):

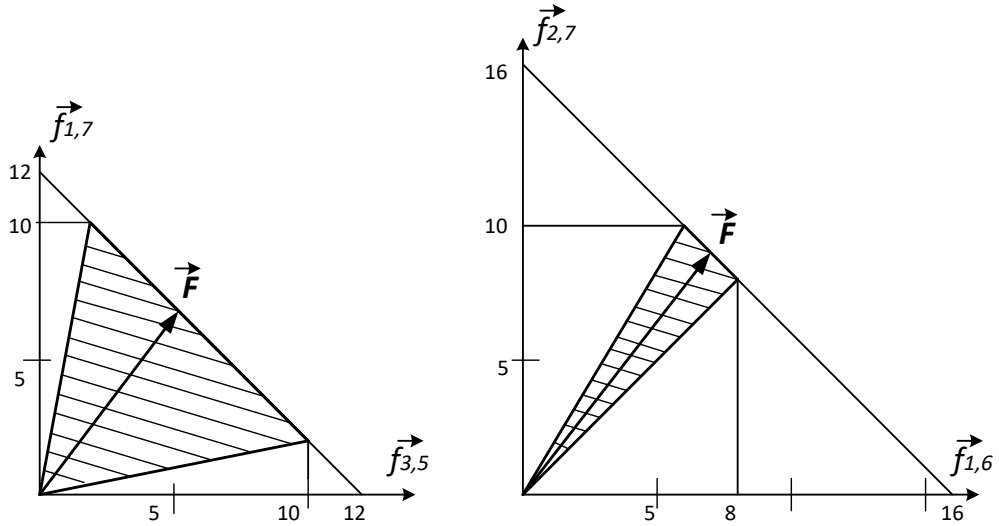
– для множества $\{(a_1,a_7),(a_3,a_5)\}$ (рис. 3а):

$$(f_{1,7})_{max} \le (\sum c_{ij})_{min} = 10,\ b_{ij} \in S_{1,7};$$
$$(f_{3,5})_{max} \le (\sum c_{ij})_{min} = 10,\ b_{ij} \in S_{3,5};$$
$$(f_{1,7} + f_{3,5})_{max} \le (\sum c_{ij})_{min} = 12,\ b_{ij} \in Z_{(1,7;3,5)},$$

– для множества $\{(a_2,a_7),(a_1,a_6)\}$ (рис.3б), соответственно:

$$(f_{2,7})_{max} \le (\sum c_{ij})_{min} = 10,\ b_{ij} \in S_{2,7};$$
$$(f_{1,6})_{max} \le (\sum c_{ij})_{min} = 8,\ b_{ij} \in S_{1,6};$$
$$(f_{2,7} + f_{1,6})_{max} \le (\sum c_{ij})_{min} = 16,\ b_{ij} \in Z_{(2,7;1,6)}.$$

Как следует из рисунка 3, векторные пространства области допустимых значений многопродуктового потока существенно зависят от пространственного расположения корреспондирующих пар узлов на МП-сети.



а) б)

Рис. 3. Векторные пространства частных потоков МП-сети

В заключение отметим, что область допустимых значений многопродуктового потока для сложившейся структуры МП-сети является наиболее

информативной характеристикой. Поэтому предлагается при решении задач оперативного управления транспортными сетями включить алгоритм расчета пропускной способности на основе модели МП-сети в программное обеспечение интеллектуальной СППР.

Список используемых источников

1. Ху, Т. Целочисленное программирование и потоки в сетях / Пер. с англ. П. Л. Бузыцкого [и др.]; Под редакцией А. А. Фридмана. М.; Мир, 1974. 519с.

2. Потоки в сетях/ Л. Р. Форд, Д. Р. Фалкерсон /Пер. с англ. И. А. Вайнштейна. М.; Мир, 1966. 276 с.

3. Корте Б, Фиген Й. Комбинаторная оптимизация. Теория и алгоритмы / Перевод с англ. М. А. Бабенко. М.: МЦНМО, 2015. 720 с. ISBN 978 5 4439 0281 4.

4. Асанов М. О. Дискретная математика: графы, матроиды, алгоритмы: учебное пособие / М. О. Асанов, В. А. Баранский, В В. Расин. 3-е изд., стер. Санкт-Петербург: Лань, 2020. 364 с. ил. (Учебники для вузов. Специальная литература). Текст: непосредственный. ISBN 978 5 8114 4998 9.

5. Якунина О. В. Многомерная геометрия: учебное пособие / О. В Якунина. Пенза. Изд-во ПГУ, 2013. 156с. ISBN 978-5-94170-592-4.

ON THE ISSUE OF SOLVING THE PROBLEM OF MULTI-PRODUCT FLOW IN AN INTELLIGENT DECISION SUPPORT SYSTEM

Lyubimov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

There is a class of distributed systems for which it is advisable to solve the problems of structural parametric analysis and synthesis using intelligent decision support systems. It is often suggested to use a mathematical model of a network with a multi-product flow as a model in such systems. Classical methods for solving the problem of a multi-product flow are based on determining the maximum flow in the travel form. The paper shows an approach to solving the problem in an m-dimensional vector space of the range of acceptable values of a multiproduct flow.

Key words: *a network model with a multi-product flow, the range of acceptable values of a multi-product flow, a multidimensional vector space*

УДК 004.942
ГРНТИ 28.17.23

ИНФОРМАЦИОННАЯ КОМПЛЕМЕНТАРНОСТЬ ТОПОЛОГИЧЕСКИХ ЭЛЕМЕНТОВ ПОЛУПРОВОДНИКОВ

Л. М. Макаров

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

Актуализация проблемы создания полупроводниковых приборов, способных улучшить технические показатели различных аппаратов и систем инициализирует разработку информационных моделей, априорно устанавливающих возможность создания прогрессивных технологий изготовления различного по функциональным признакам изделий микроэлектроники.

Исследуя известные и широко распространенные на практике технологические процессы создания полупроводниковых приборов, показана возможность посредством математической модели априорно устанавливать компонентный состав полупроводника, обеспечивающий необходимый уровень эксплуатационных показателей.

математическая модель, полупроводниковые приборы, микроэлектроника

Полупроводниковые материалы представляют обширную область специальных атомарных композиций, для которых характерно высокая степень вариабельности электрических и физических свойств, что и является основой для технологических процессов создания современных образцов микроэлектроники. Современные технологии производства полупроводниковой продукции реализуются на элементах с субмикронными размерами тонких пленок.

Полупроводник представляет материал, по удельной проводимости занимающий промежуточное место между проводниками и диэлектриками. Хорошо известным свойством полупроводников является увеличение электрической проводимости с ростом температуры.

К числу полупроводников относятся многие простые вещества (германий, кремний, селен, теллур, мышьяк и другие), огромное количество сплавов и химических соединений (арсенид галлия, нитрид галлия, сплав КРТ (кадмий-ртуть-теллур), теллурид кадмия, теллурид висмута и др.).

Полупроводники широко используются при создании электронных приборов.

Комплементарность в контексте полупроводников следует рассматривать при условии наличия двух полупроводниковых приборов, обладающих идентичными техническими характеристиками, но имеющих противоположные проводимости.

Полупроводниковые материалы позиционируются в четырех кластерах. В перовом кластере рассматриваются кристаллические полупроводники, образованные из атомов и молекул одного химического элемента. Здесь традиционно используются германий, кремний, селен, бор. Второй кластер полупроводников образуют материалы из окислов металлов. Наибольшее распространение в технологии создания полупроводников получили закись меди, окись цинка окись кадмия, двуокись титана. Третий кластер полупроводников образуют атомарные конструкции на основе соединений химических элементов из третьей и пятой групп химической таблицы элементов Д. И. Менделеева. В типовом исполнении изделий микроэлектроники используют антимониды индия, галия и алюминия. В четвертом кластере полупроводники представлены кристаллическими соединения серы, селена и теллура.

Серийное производство полупроводников реализуются двумя методами: создания монокристаллов и поликристаллов. Следует отметить, что и в том и другом случае предусматривается серия процедур легирования полупроводникового материала. Легирование полупроводников рассматривается как специальная технологическая процедура ограниченного введение в полупроводник примесей или структурных дефектов с целью изменения физических, электрических, магнитных оптических, механических свойств. Направленное изменение одного или нескольких из рассмотренных свойств позволяет улучшить технические показатели рабочего процесса полупроводника. Наибольшее распространение в технологии создания полупроводниковых приборов получили эмпирические методы [1, 2].

Для получения кристаллов n- и p- типа проводимости кристаллы легируют электрически активными примесями. Активная примесь – добавка представляет собой композит, валентность которого отличается от валентности основных замещаемых атомов на единицу.

У полупроводниковых соединений $A^{III}B^{V}$ элементы V группы замещаются примесями VI группы (S, Se, Te), которые являются донорами, а элементы II группы (Zn, Cd), замещают, соответственно, атомы III группы в соединении и являются акцепторами.

А в случае легирования соединений $A^{III}B^{V}$ кремнием и другими примесями IV группы, проявление донорных или акцепторных свойств будет зависеть от того, в узлах какой подрешетки расположен атом примеси. В структуре математической модели создания новой структуры полупроводника это устанавливается посредством выбора соответствующей дислокации внедряемого композита. Так при замещении таким атомом III-валентного Ga он будет проявлять донорные свойства, а при замещении V-валентного As – акцепторные.

В технологии эмпирического метода изменения свойств полупроводника легирование обычно осуществляют непосредственно в процессах выращивания монокристаллов и эпитаксиальных структур. Примесь вводится в расплав, раствор или газовую фазу. Расчет необходимого содержания примеси требует знания количественных показателей связи между всеми компонентами. Отсутствие полного набора показателей атомарных связей порождает необходимость использовать эмпирический метод легирования.

В технологическом процессе для получения тонких легированных слоев используется ионная имплантация. **Ионное легирование полупроводников** (ионная имплантация) рассматривается как **способ введения атомов примесей в поверхностный слой материала** (например, пластины полупроводника или эпитаксиальной пленки) **посредством потока ионов, обладающих высокой энергией** (10–2000 кэВ) [1, 2, 3, 4].

Процесс ионной имплантации реализуется по специальной технологии создания мощных потоков имплантируемой примеси, направленных на атомарную решетку подложки создаваемого полупроводника. Мощный поток имплантируемого вещества обладает высоким уровнем кинетической энергии, который создает «дефекты» в структуре подложки, которые изменяют электронные свойства кристалла, а, следовательно выполняет функцию легирующей примеси.

Технология ионного легирования широко распространена и позволяет создавать многочисленные типы микросхем БИС и СБИС. Получаемые легированные слои (пленки) полупроводников характеризуются субмикронными размерами вдоль поверхности без использования маски и толщиной легированного слоя менее 0,1 мкм с высокой воспроизводимостью концентрационного профиля легирования [4].

Интенсивная ионная обработка подложки полупроводника воспроизводит необходимые электрофизические показатели структуры, но при этом отмечается изменение топологии пленок.

Процесс ионного внедрения сопровождается интенсивным дефектообразованием, поскольку энергия падающего иона на несколько порядков превышает энергию смещения атомов мишени. Возникающие при этом дефекты характеризуются вариативным набором показателей, которые называют радиационными. Простейшие дефекты (одиночные вакансии и междоузельные атомы) имеют малые времена жизни при температурах, близких к комнатной. Но при релаксации они взаимодействуют между собой и с примесями, образуя различные электрически активные комплексы, устойчивые и к воздействию повышенных температур. Эти комплексы вносят в запрещенную зону полупроводника донорные и акцепторные уровни, компенсируя легирующую примесь.

Принимая это, вынимание проводят термическую обработку (отжиг) полупроводника, тем самым обеспечивая стабилизацию позитивных показателей. Относительно несложные технологические процедуры производства элементов микроэлектроники в настоящее время активно развиваются, где на смену эвристическим рецептам синтеза полупроводниковых структур приходит компьютерное моделирование, в частности реализуемое на основе известных методов случайных величин – названный Монте-Карло [5].

С развитием вычислительной техники совершенствуются технологии моделирования профилей внедренной примеси для различных комбинаций ион-мишеней [6]. Поверхность и приповерхностные слои любой фазы обладают свойствами, отличными от свойств объема фазы. На поверхности и в приповерхностных слоях протекают процессы, связанные с фазовыми переходами. Особые свойства поверхности и приповерхностных слоев, а также процессы адсорбции и десорбции играют доминирующую роль в формировании свойств полупроводниковых приборов, размеры которых соизмеримы с толщиной приповерхностного слоя. Процессы самопроизвольного выравнивания концентраций ингредиентов в поверхностном слое полупроводника характеризуется как диффузный, термодинамический. В теоретическом отношении это хорошо известные модели [3].

Термодинамической характеристикой объекта, в частности, полупроводника, является поверхностная энергия, которая отождествляется с работой по созданию равновесной поверхности единичной площади на границе раздела фаз. Элементарная единица площади позиционируется квадратом. Квадрат, как элементарная единица поверхности в декартовой системе координат, обладает четырьмя идентификаторами, которые традиционно раз-

мещают в вершинах. Термодинамический квадрат позволяет в иллюстративной форме обсуждать многочисленные состояния динамической системы, в качестве которой могут рассматриваться полупроводниковые структуры, воспроизводимые с использованием разных химических элементах.

Введем в рассмотрение топологический квадрат – кластер, в вершинах которого размещены показатели элементов кластера. Сохраняя общность суждений, отмечаем наличие возможности использовать базовые положения дифференциальной топологии, оперирующей представлениями ограниченного множества элементов на плоскости, представленного в виде правильного многоугольника и окружности (рис. 1). В этом случае реализуется функционал, устанавливающий взаимосвязь параметров квадрата и окружности. Запишем функционал в виде [6]:

$$AD * CD + AD * DC = AC * BD \quad (1)$$

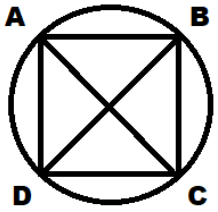


Рис. 1. Образ топологического кластера

Действительно, взаимная связь параметров квадрата и окружности проявляется на сопряженных понятиях диагонали и диаметра. Тождество в выражении (1) достигается в случае равенства метрик: диагонали квадрата и диаметру окружности. В терминах информационной энтропии это характеризует наличие свойства абсолютной эмерджентности для всех элементов образующих периметры рассматриваемых фигур.

Формально представим выражение (1) в виде:

$$\begin{gathered} AD * CD + AD * DC = a \\ AC * BD = b \\ ABS\,(a - b) = E \end{gathered} \quad (2)$$

В таком случае, очевидно, что эмерджентность следует рассматривать как свойство двух объектов, каждое из которых позиционируется парой элементов, наделенное формальным правилом сочетания (2) [5, 7, 8]. Констатируем, что два множества или классы А и В равномощны, тогда и только

тогда, когда между ними существует взаимно однозначное соответствие – биекция. Равномощность характеризуется биекцией в процедуре сопоставления двух множеств с произвольными по определению элементами, а это означает, что одно множество содержит столько же эквивалентных элементов, сколько и другое.

Понятия биекции и эмерджентности сопоставимо с термодинамическим описанием состояния объекта. Действительно, низкий показатель эмерджентности характеризует малое различие состояний в топологии элементов кластера. Можно сказать, что это строго компактная структура, демонстрирующая высокий уровень взаимной связи элементов кластера, активация которых потребует значительных энергетических затрат. В противоположность этому состоянию возможно обнаружить большой по значению показатель эмерджентности, что естественно, характеризует наличие высокий активности – различия элементов кластера.

Введенные понятия позволяют воспроизвести серию формальных оценок структурных образований полупроводников. Рассмотрим типичный случай. Так, например, в [9] рассмотрены примеры из области технологий создания полупроводниковых приборов на основе химических элементов: германия, кремния, бора, углерода, фосфора, серы и других в том числе и органических соединений. Типичными элементами для изготовления полупроводника являются кремний и германий. В твердотельной электронике получил широкое распространений атомарный кремний, который обладает значительным количеством сводных электронов, а следовательно, большим показателем проводимости.

Рассмотрим типичный (N-P-N) кремниевый транзистора на основе химических элементов Si- B- Si (рис. 2). Позиционируем топологию транзистора в формате квадрата (табл. 1).

ТАБЛИЦА 1. Топология полупроводника Si- B- Si

	Атомарная конструкция – химические элементы		
	Si	B	Si
Позиция	14	5	14
Количество электронов	28	11	28

Проведем расчет показателя эмерджентности E по выражению (2). Имеем: E=168.

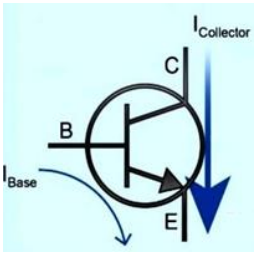


Рис. 2. Схема кремниевого транзистора

Осуществим построение имитационной модели полупроводника – кремниевого транзистора с использование технологии легирования. Внесем в топологическую схему полупроводника мышьяк (As). В этом случае имеем топологию: SiAs-B-SiAs.

По выражению (2) проведем расчет показателя эмерджентности: E = 3024.

ТАБЛИЦА 2. Топология полупроводника SiAs – B- SiAs

	Атомарная конструкция – химические элементы		
	Si +As	B	Si +As
Позиция	14/33	5	14/33
Количество электронов	28/75	11	28/75

По выражению (2) проведем расчет показателя эмерджентности: E = 3024

Изменим топологическую схему воспроизведений полупроводника и внесем легирующую добавку – сурьму (Sb).

ТАБЛИЦА 3. Топология полупроводника SiSb – B- SiSb

	Атомарная конструкция – химические элементы		
	Si +Sb	B	Si +Sb
Позиция	14/51	5	14/51
Количество электронов	28/122	11	28/122

По выражению (2) проведем расчет показателя эмерджентности: E = 4996.

Очевидно, что из серии проведенных расчетов лучший результат, по показателю эмерджентности, представлен в таблице. 3. Что характеризует высокие динамические свойства полупроводника – транзистора.

Действительно, следует отметить, что воспроизведение полупроводниковой структуры пленки на основе сурьмы (Sb) позволяет получить транзистор с лучшим показателем эффективности обеспечения рабочих процессов в многочисленных схемах вычислительной сети ($E_{4996} > E_{3024}$). Такой тип транзистора широко используется в цифровых схемах с малым уровнем входного сигнала [10, 11].

Развитие типичных элементов и сборок на основе полупроводниковых материалов актуализирует проблему поиска новых образцов, способных значительно расширить возможности компьютерной техники. Поиск новых технологических решений в создании полупроводников требует увеличения периода исследовательских работ. Эвристика, составляющая основу таких технологических процедур, инициализирует развитие формальных методов исследования и поиска необходимых полупроводниковых структур. Представленная имитационная модель полупроводника достаточно полно обеспечивает формирование суждений о подвижности электронных носителей, что способствует априори воспроизвести желаемую структуру транзисторов с учетом рассматриваемых проблем приема, усиления и передачи данных.

Список используемых источников

1. Березин А. С., Мочалкина О. Р. Технология и конструирование интегральных микросхем. М.: Радио и связь, 1992. 320 с.

2. Черняев В. Н. Технология производства интегральных микросхем и микропроцессоров. М.: Радио и связь, 1987. 464 с.

3. Романовский М. Н. Технологические процессы микроэлектроники. Томск: ТУСУР, 2002. 190 с.

4. Таиров Ю. М. Технология полупроводниковых и диэлектрических приборов / Ю. М. Таиров, В. Ф. Цветков. СПб.: Лань, 2002. 422 с.

5. Павлов П. В. О распределении введенных атомов и радиационных дефектов при ионной бомбардировке кремния (расчет методом Монте-Карло) // ФТТ, 1966, т. 8, в. 9, С. 2679-2687.

6. Макаров Л. М., Поздняков А. В. Семантическое позиционирование кластеров информационных пакетов. Информационные технологии и телекоммуникации. 2023. Т. 11. № 3. С. 49-61.

7. Вик Дж. У. Теория гомологий. Введение в алгебраическую топологию. Пер. с англ. М.: МЦНМО, 2005. 288 с.

8. Хаусдорф Ф. Теория множеств / Пер. с нем. М.: Ленанд, 2023. 304 с.

9. Шалимова К. В. Физика полупроводников. М.: Ленанд. 2021. 400 с

10. Смирнов Ю. Л. Транзистор это очень просто. М., 1972.

11. geeksforgeeks.org. URL: https://www.geeksforgeeks.org/difference-between-npn-and-pnp-transistor-with-interesting-facts/ (дата обращения 10.02.2025).

INFORMATION COMPLEMENTARITY OF TOPOLOGICAL ELEMENTS OF SEMICONDUCTORS

Makarov L.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The actualization of the problem of creating semiconductor devices capable of improving the technical performance of various devices and systems initializes the development of information models that a priori establish the possibility of creating advanced manufacturing technologies for various functional microelectronics products.

By examining the well-known and widespread in practice technological processes for creating semiconductor devices, it is shown that it is possible to establish a priori the component composition of a semiconductor by means of a mathematical model that ensures the required level of performance.

Key words: *mathematical model, semiconductor devices, microelectronics*

УДК 621.311.61
ГРНТИ 47.14.17

АККУМУЛЯТОРНЫЕ БАТАРЕИ АБ-18 ДЛЯ Р-187-П1 «АЗАРТ»: СОВРЕМЕННОЕ РЕШЕНИЕ ДЛЯ ВОЕННЫХ РАДИОСТАНЦИЙ

В. П. Макогон, А. А. Негурица, Д. И. Лукьяненко

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

Статья посвящена литий-ионным аккумуляторным батареям, разработанным для портативных радиостанций. В материале подробно рассматриваются их ключевые технические характеристики, преимущества перед другими типами аккумуляторов, а также их возможности для зарядки. Основное внимание уделено уникальным особенностям литий-ионной технологии, включая высокую энергетическую плотность, минимальный саморазряд, отсутствие эффекта памяти и удобство эксплуатации.

литий-ионные аккумуляторные батареи, радиостанция Р-187-П1 «Азарт»

Аккумуляторные батареи являются важнейшим компонентом для обеспечения автономной работы портативных радиостанций. Одним из передовых решений в этой области стали аккумуляторные батареи АБ-18, разработанные специально для радиостанции Р-187-П1 «Азарт» (рис. 1). Эти батареи отличаются увеличенной емкостью, продуманной конструкцией и рядом технических преимуществ.



Рис. 1. Портативная радиостанция Р-18-П1 «Азарт»

Литий-ионные аккумуляторы, используемые в АБ-18, имеют значительные преимущества перед другими типами аккумуляторов, такими как

никель-кадмиевые (Ni-Cd) и никель-металл-гидридные (Ni-MH): их высокая энергетическая плотность позволяет уменьшить размеры и вес батарей, при этом запас энергии остается неизменным [1]. Наиболее важным достоинством, по сравнению с другими является минимальная саморазрядка, что делает их идеальными для использования в устройствах, где требуется длительное сохранение заряда при нечастой эксплуатации [2]. Таким образом, литий-ионные батареи затмевают своих конкурентов на рынке, что делает их незаменимыми для современных мобильных и военных приложений.

Высокая плотность энергии, компактность, длительное время работы, способность поддержки технологии быстрой зарядки, повышенная экологическая безопасность ввиду малого количества вредных компонентов и, конечно же, более высокий ресурс циклов зарядки-разрядки – все эти особенности литий-ионных аккумуляторов, позволяют применять их в современных мобильных и портативных устройствах [3]. Вкупе эти качества позволяют минимизировать время простоя, а также делают их универсальными.

Одним из важнейших отличий от других типов аккумуляторов является отсутствие эффекта памяти [4]. Эффект памяти – это явление, из-за которого аккумуляторы сохраняют наименьший уровень заряда вследствие частой либо неполной зарядки [5]. Поскольку литий-ионные аккумуляторы лишены этого недостатка, это повышает его конкурентоспособность по сравнению с другими типами.

В данный момент на рынке представлен широкий ассортимент зарядных устройств. Весь спектр можно условно разделить на 2 категории:

1) портативные зарядные устройства;

2) стационарные универсальные зарядные станции.

Современные производители способны обеспечить надежное, качественное и безопасное восстановление заряда, а также решают проблему подбора оптимального варианта как для полевых условий, так и для базовой инфраструктуры.

Наличие разъема Type-C (рис. 2) делает АБ-18 более универсальным в плане вариативности при зарядке, а также делает его уникальным на рынке, ввиду распространенности данного разъема и существования большого количества кабелей для подключения.

Тактико-технические характеристики разработанных батарей АБ-18 обеспечивают их надежную работу в полевых условиях и имеют следующие параметры:

1) емкость батареи составляет 18–20 А·ч;

2) время работы увеличено до 17 часов;

3) ток заряда до 3 ампер;

4) время зарядки от 6 до 9 часов.

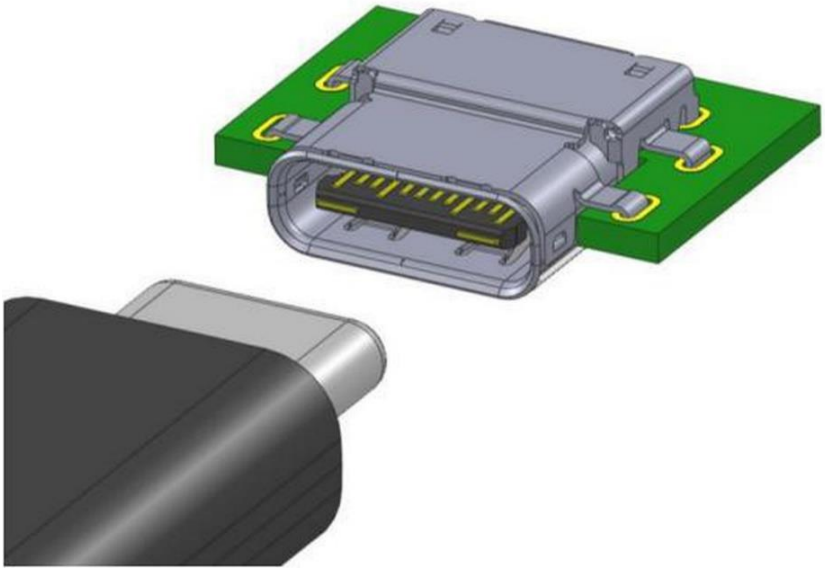


Рис. 2. Внешний вид платы с разъемом Type-C

Благодаря данным характеристикам, появляется возможность минимизировать простои из-за необходимости постоянной подзарядки, что в свою очередь показывает универсальность и эффективность разработанного изделия.



Рис. 3. Внешний вид аккумуляторной батареи АБ-18

Батареи АБ-18 (рис. 3) предоставляют ряд значительных улучшений по сравнению с предшествующими моделями:

1) наличие разъема Type-C упрощает подключение и совместимость с современными зарядными устройствами;

2) объем батареи вырос на 1,5 раза, что существенно увеличивает время автономной работы;

3) более легкая конструкция облегчает транспортировку и использование оборудования.

4) батарея надежно фиксируется в радиостанции, предотвращая выпадение в ходе эксплуатации.

5) помогает оперативно отслеживать уровень оставшейся энергии благодаря индикатору заряда.

Аккумуляторные батареи АБ-18 для Р-187-П1 «Азарт» представляют собой современное и высокоэффективное решение, соответствующее требованиям современных военных операций. Увеличенная емкость, универсальность зарядки и продуманная конструкция делают их неотъемлемой частью экипировки современных войск. Такие батареи позволяют обеспечивать надежную связь даже в самых сложных условиях, повышая автономность и мобильность подразделений.

Литий-ионные технологии продолжают совершенствоваться, предлагая все более мощные, легкие и надежные аккумуляторы, что делает их идеальным выбором для военных нужд и других критически важных сфер применения.

Список используемых источников

1. Кулова Т. Л., Скундин А. М. Проблемы развития литий-ионных аккумуляторов в мире и России //Электрохимическая энергетика. 2023. Т. 23. №. 3. С. 111-120.

2. Забудский А. И. и др. Как ухаживать за литий-ионными аккумуляторами //Роль научно-исследовательской работы обучающихся в развитии АПК. 2022. С. 234-240.

3. Мельник А. А. и др. Обзор огнетушащих средств при тушении литий-ионных батарей // Сибирский пожарно-спасательный вестник. 2021. №. 2. С. 33-35.

4. Кирилюк А. А., Ноздрачев А. В. Никель-кадмиевые и никель-металлогидридные аккумуляторы. общие сведения, способы заряда, правила эксплуатации // Информационные технологии как основа эффективного инновационного развития. 2021. С. 38-42.

5. Кебеков Т. В., Гобозов М. Д. Литиевые вторичные химические источники тока, анализ и сравнение литий-ионных аккумуляторов и литий-полимерных аккумуляторов // Научное обозрение. 2021. С. 80-83.

AB-18 BATTERIES FOR R-187-P1 "AZART": A MODERN SOLUTION FOR MILITARY RADIO STATIONS

Makogon V., Neguritsa A., Lukyanenko D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is devoted to lithium-ion rechargeable batteries developed for portable radios. The material discusses in detail their key technical characteristics, advantages over other types of batteries, as well as their charging capabilities. The focus is on the unique features of lithium-ion technology, including high energy density, minimal self-discharge, no memory effect, and user-friendliness.

Key words: *lithium-ion rechargeable batteries, radio station R-187-P1 "Azart"*

УДК.621.396.6
ГРНТИ 47.47

МОДЕЛИРОВАНИЕ ЦИФРОВЫХ ПРЕОБРАЗОВАНИЙ ПРИ КОГЕРЕНТНОМ СИНТЕЗЕ ЧАСТОТ С ПОМОЩЬЮ ЛОГИЧЕСКИХ ЭЛЕМЕНТОВ

Ю. А. Никитин

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

Рассмотрен варианты когерентного преобразования при цифроаналоговом синтезе частот с помощью логических элементов «AND», «OR», «XOR». Моделирование структур и получаемых спектров производится с помощью пакета схемотехнического моделирования Microcap 12. Результаты моделирования показывают, что цифровой смеситель на логическом элементе «XOR» является полным аналогом четырехквадрантного перемножителя сигналов.

пассивный цифровой синтез частот, спектр, рациональное число, цепная дробь, логические элементы, перемножение сигналов, диофантово уравнение, тракт приведения

В современных цифроаналоговых синтезаторах частоты все колебания – выходные и вспомогательные – образуются из одного высокостабильного опорного колебания с помощью когерентных преобразований. В частности, при чисто цифровом синтезе преобразованиям подвергают частоты следования входных двухуровневых импульсных последовательностей, например, меандров со спектрами вида [1]:

$$\underline{A(t) = \sum_{m=-\infty}^{m=\infty} \frac{sin\left(\frac{m\pi}{2}\right)}{m\pi} exp(jm2\pi PF_s t);} \quad (1)$$

$$B(t) = \sum_{k=-\infty}^{k=\infty} \frac{sin\left(\frac{k\pi}{2}\right)}{k\pi} exp(jk2\pi QF_s t);$$

Формула (1) справедлива для понижения частоты f_a с помощью дополнительного колебания подставки с частотой f_b.

Цифровое преобразование частоты подразумевает использование в качестве операционных узлов цифровой элементной базы, а именно логических элементов. При этом выделение полезного сигнала может осуществляться аналоговым способом, например, линейной фильтрацией.

Цифровая логическая микросхема «сумматор по модулю 2» (если с инверсией – то «исключающее ИЛИ»), реализует булеву функцию:

$$C = \bar{A}B + A\bar{B} = A \oplus B.$$

Возможны другие варианты логических преобразований исходных двухуровневых последовательностей – логические конъюнкция и логическая дизъюнкция:

$$C = A \cap B;$$
$$C = A \cup B.$$

Если представить логические сигналы не в виде набора {0,1}, а в виде {-1,1} то все возможные соотношения входных сигналов *A* и *B* в результате их логических преобразований можно свести к таблице 1.

ТАБЛИЦА 1. Соотношения знаков на выходе логических элементов

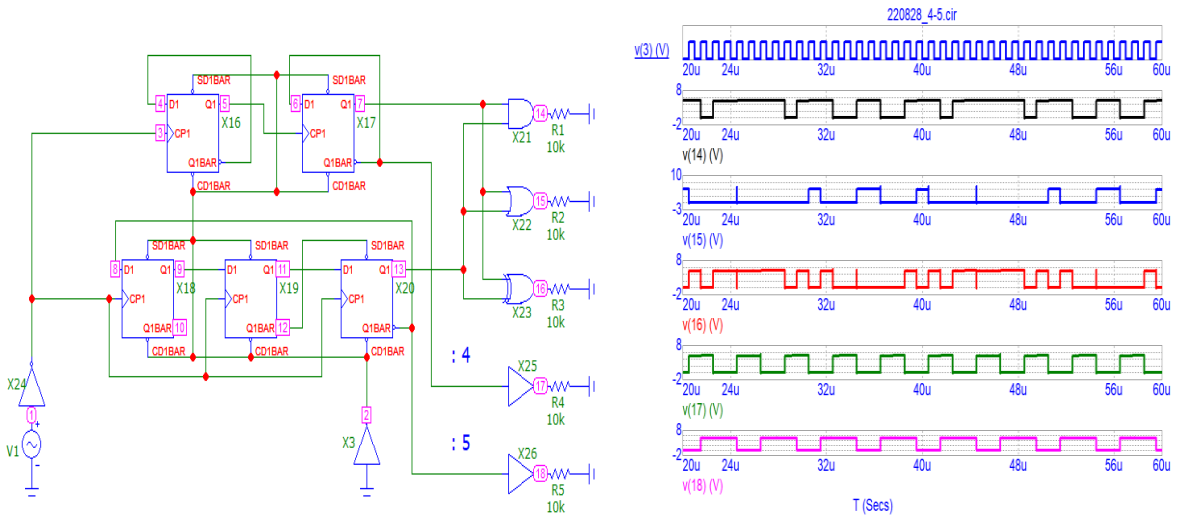
A	B	C	&	1	*XOR*
−1	−1	−1	−1	−1	−1
1	−1	1	−1		1
−1	1	1	−1	1	1
1	1	−1	1	1	−1

В таблице 1 приведены логические преобразования, выполняющих функции «И» (&, AND), «ИЛИ» (1, OR) и «сумматор по модулю 2» (⊕,) или логическая схема «исключающее ИЛИ» (*XOR*). Из анализа таблицы 1 следует, что только логическое преобразование «*XOR*» соответствует всем возможным сочетаниям знаков сигналов *A* и *B* на входе аналогового перемножителя.

Схемотехническая модель цифрового логического перемножения в пакете *Microcap* 12 для проверки уровней спектральных компонент на выходах «&», «1», «*XOR*» (таблица 1) приведена на рисунке 1а; временные диаграммы ее работы приведены на рисунке 1б.

В таблицах 2 – 4 и на рисунках 2 – 4 амплитуды спектральных компонентов отнормированы относительно уровня первой гармоники идеального меандра того же логического уровня; коэффициенты парциальных делителей частоты равны $N_1 = 4$ и $N_2 = 5$ во всех рассматриваемых случаях.

В таблице 2 и на рисунке 2 приведен случай распределения спектральных компонентов на выходе логической схемы «2И-НЕ. Относительный уровень первой гармоники равен – 8,7дБ$_{ИМ}$.



а) б)

Рис. 1. Проверка уровней полезных компонентов спектра на выходах логических схем таблицы 6.11; а) модель; б) временные диаграммы работы для случая $N_1 = 4$, $N_2 = 5$

ТАБЛИЦА 2. Спектр на выходе логической схемы «2И-НЕ»

Номер гармоники выходной частоты схема «2И-НЕ»	1	2	3	4	5	6	7	8	9	10	11	12	13
Относительный уровень, дБН	0	– 31,6	– 8,4	+ 2,7	+ 4,5	– 27,5	– 10,3	– 7,8	– 3,4	– 34,5	– 5,1	– 8,7	– 21,7

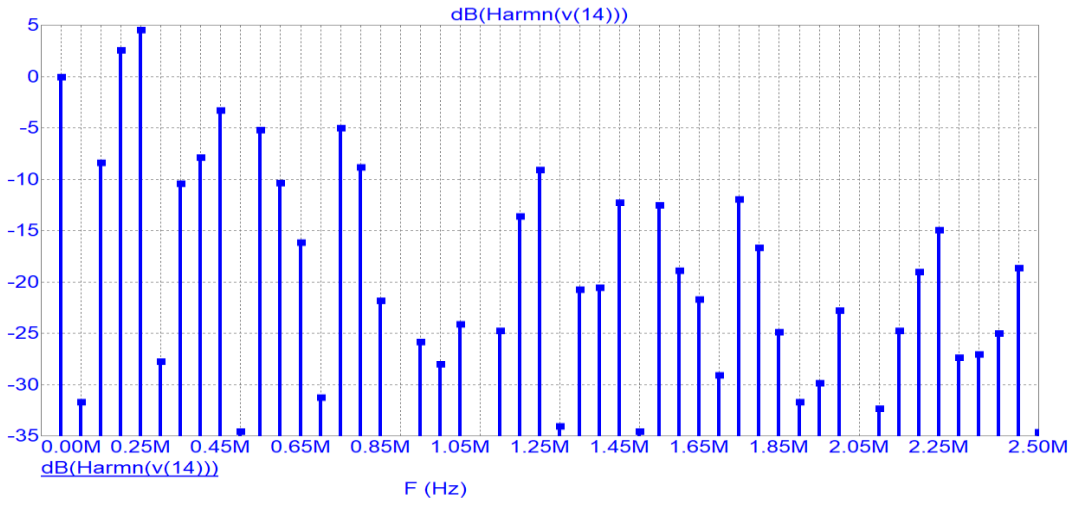


Рис. 2. Спектр на выходе логической схемы «2И-НЕ»

В таблице 3 и на рисунке 3 приведен случай распределения спектральных компонентов на выходе логической схемы «2ИЛИ-НЕ». Относительный уровень первой гармоники равен – 8,7дБИМ.

ТАБЛИЦА 3. Спектр на выходе логической схемы «2ИЛИ-НЕ»

Номер гармоники выходной частоты схема «2ИЛИ-НЕ»	1	2	3	4	5	6	7	8	9	10	11	12	13
Относительный уровень, дБН	0	– 19,9	– 7,4	+ 2,1	+ 0,7	– 22,5	– 13,3	– 8,1	– 4,2	– 32,4	– 5,12	– 11,8	– 18,4

В таблице 4 и на рисунке 4 приведен случай распределения спектральных компонентов на выходе логической схемы «*XOR*». Относительный уровень первой гармоники равен – 2,44дБИМ.

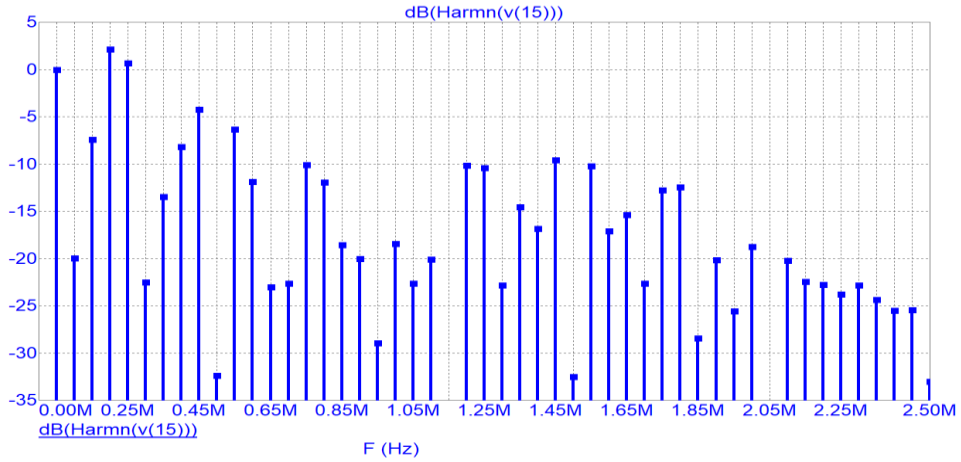


Рис. 3. Спектр на выходе логической схемы «2ИЛИ-НЕ»

ТАБЛИЦА 4. Спектр на выходе логической схемы «XOR»

Номер гармоники выходной частоты схема «Искл.ИЛИ»	1	2	3	4	5	6	7	8	9	10	11	12	13
Относительный уровень, дБН	0	– 37,3	– 8,8	– 30,3	– 11,0	– 30,0	– 9,8	– 36,1	– 2,9	– 40,2	– 4,8	– 42,0	– 15,0

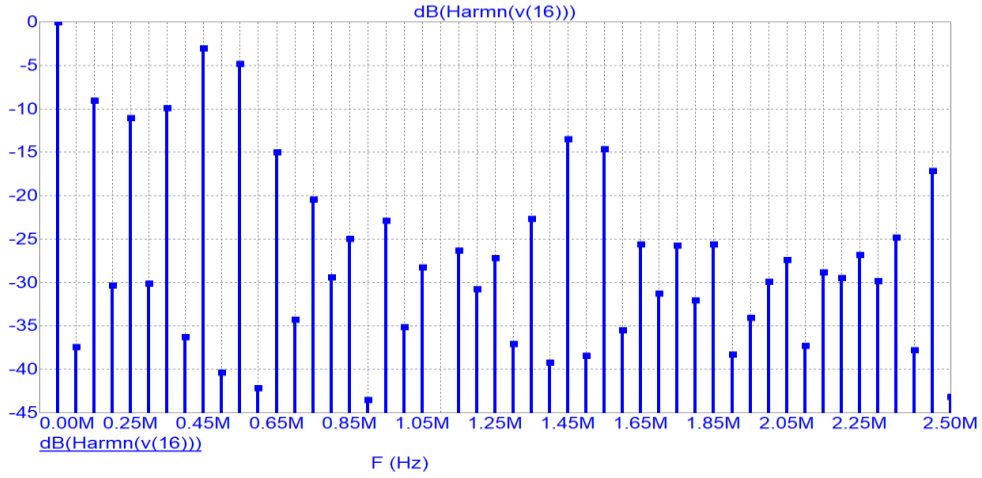


Рис. 4. Спектр на выходе логической схемы «*XOR*»

В соответствии с формулами (1) спектр на выходе цифрового перемножителя на основе логического элемента «XOR» можно записать в виде:

$$C(t) = \sum_{k=-\infty}^{k=\infty} \sum_{m=-\infty}^{m=\infty} \frac{sin\left(\frac{k\pi}{2}\right) sin\left(\frac{m\pi}{2}\right)}{km} exp[2\pi(mP - kQ)F_s t].$$

Аргумент экспоненты в правой части последнего выражения есть диофантово уравнение, которое описывает спектральный состав выходного колебания. Полезным сигналом является колебание $C(t)$ с разностной частотой $\cos[2\pi(P - Q)F_s t]$.

Коэффициенты при частоте шага сетки F_s определяются решением диофантова уравнения (уравнения в целых числах) $mP + kQ = |L \pm x|$, решение которого ищется в виде [1]:

$$m = |S + 1| + Qz;$$
$$S = (-1)^{r-1} \pm x.$$

где $L = P - Q$ – полезная компонента спектра выходного колебания; $x = 0,1,2,\ldots, L\text{-}1$; $z = 0, \pm1, \pm2, \ldots$; $Q = |L \pm x|$; $P_{r\text{-}1}$ – числитель предпоследнего члена разложения (всего r членов) числа $N = P/Q$ в цепную дробь по алгоритму Евклида.

Коэффициенты деления параллельно включенных СИ (рисунок 5) выбирают близкими, как правило, $|N_1 - N_2| = 1$. Тогда эквивалентный коэффициент деления N в нониусной ячейке ТП будет определяться произведением N_1N_2. Например, при $N_1 = 8$ и $N_2 = 8 + 1/3$ эквивалентный коэффициент деления $N = 200$.

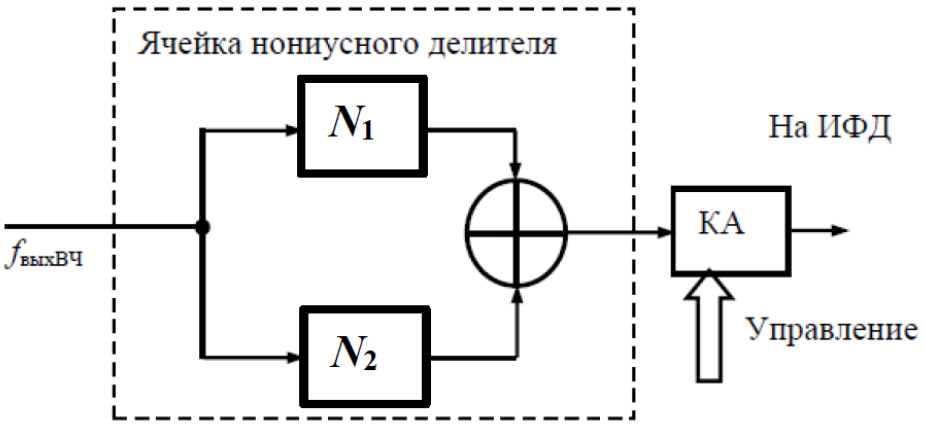


Рис. 5. Цифровая нониусная ячейка деления

Применение «цифровых» смесителей целесообразно, прежде всего, в нониусных ТП умножающих колец ИФАП и в цифро-аналоговых ТП с вычитанием.

При прочих равных условиях относительный уровень шумов в ТП с цифровым смесителем будет ниже, чем в ТП с аналоговым смесителем.

Список используемых источников

1. Никитин Ю. А. Теория цифроаналогового синтеза частот с помощью конечных автоматов: [монография] / Ю. А. Никитин. СПб.: СПб ГУТ, 2024. 342 с. ISBN 978-5-89160-322-6.

USING THE METHOD OF COMPLEX PERIODIC GRID FUNCTION TO FIND THE SPECTRUM OF PACKS OF PULSES

Nikitin Yu.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper considers variants of coherent conversion in digital-to-analog frequency synthesis using the logical elements "AND", "OR", "XOR". Modeling of structures and obtained spectra is performed using the Microcap 12 circuit simulation package. The modeling results show that a digital mixer on the logical element "XOR" is a complete analogue of a four-quadrant signal multiplier.

Key words: *passive digital frequency synthesis, spectrum, rational number, continued fraction, logical elements, signal multiplication, Diophantine equation, reduction path*

УДК 654.739
ГРНТИ 49.33.29

СТРУКТУРНАЯ НЕОДНОРОДНОСТЬ НЕУПОРЯДОЧЕННЫХ ДИЭЛЕКТРИКОВ ЭЛЕМЕНТОВ ЭЛЕКТРОННОЙ БАЗЫ И ИХ ЭКСПЛУАТАЦИОННЫЕ ХАРАКТЕРИСТИКИ

Ю. С. Остроумова[1], С. Д. Ханин[2]

[1]Военно-медицинская академия им. С. М. Кирова
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В контексте развития физико-технологических основ формирования диэлектрических материалов с неупорядоченной структурой для функциональных элементов с необходимыми токовыми и надежностными характеристиками акцентируется внимание на сопряженной с неупорядоченностью структурной неоднородности. Анализируется влияние, которое оказывает на транспортные свойства аморфных оксидов тантала и ниобия структурная неоднородность на разных ее уровнях. Определяются и обосновываются технологические средства улучшения и повышения временной стабильности токовых характеристик емкостных элементов.

структурная неоднородность, электрическая проводимость, устойчивость к электротепловому нагружению, токовые и надежностные характеристики

Проблема улучшения токовых и надежностных характеристик функциональных структур электроники с неупорядоченным диэлектриком была и остается в центре внимания многих исследователей. Если ранее решение этой проблемы относилось только к функциональным структурам емкостных элементов, то в последнее время она приобретает принципиальное значение в плане прогресса в создании субмикронных быстродействующих транзисторов интегральной электроники [1-3]. В научном плане интерес представляют ответственные за формирование токовых и надежностных характеристик относительно малоизученные транспортные явления в неупорядоченных высокоомных материалах.

Для изыскания возможностей конструктивного решения проблемы устанавливалась связь между транспортными явлениями в неупорядоченных диэлектриках и отличительными, сопряженными с неупорядоченностью, особенностями их структуры и определись возможности управления последней технологическими средствами.

В качестве опорного объекта в работе выступают аморфные диэлектрические пленки оксидов тантала и ниобия, получаемые методом электрохи-

мического оксидирования металла. Выбор этих материалов обусловлен следующими соображениями. Во-первых, их значимостью в электронике как функционального материала обладающих рекордно высокими удельными параметрами конденсаторов, а также сенсоров, переключательных устройств и, что весьма важно, перспективных для применения в качестве подзатворного диэлектрика МДП-структур. Во-вторых, предопределяемой наличием в составе указанных оксидов переходных элементов и характерными для металлооксидных конденсаторов условиями нагружения относительно простотой модификации состава и структуры материала. В-третьих, представительностью как неупорядоченного материала с сильной локализацией носителей заряда.

Замысел работы состоит в том, что проследить влияние сопряженной с неупорядоченностью структурной неоднородности на разных ее уровнях: микроскопическом, промежуточном (наноразмерном) и макроскопическом на процессы электронного и ионного переноса и на основе полученных результатов сформулировать рекомендации по улучшению и повышению временной стабильности токовых характеристик.

Первой и очевидной причиной возникновения структурной неоднородности является отсутствие дальнего порядка в атомном строении неупорядоченного диэлектрика, что делает последний случайно неоднородным на микроскопическом уровне. Это предопределяет прыжковый механизм электронного транспорта [4]. Выразительным проявлением последнего в рассматриваемых материалах являются нестационарные и нелинейные явления переноса: долговременная релаксация изотермического тока, широкодиапазонная частотная зависимость динамической проводимости и эффект уменьшения неомической проводимости при увеличении напряженности электрического поля [5-7]. Еще одним важным следствием связанной с отсутствием дальнего порядка неоднородности является облегченное формирование выступающих как носители заряда поляронов с размером порядка амплитуды колебаний структурных частиц (сверхмалых поляронов) [8,9], что проявляется в прогнозируемом характерном отклонении в температурной зависимости прыжковой проводимости на постоянном токе от аррениусовской и изменении при повышении температуры верхней граничной частоты эффекта падения неомической проводимости с увеличением напряженности поля, а также в гауссовом пике в спектре оптического поглощения с характерной для неупорядоченной системы с поляронным транспортом энергией [10].

Наряду с неоднородностью на микроскопическом уровне, отсутствие дальнего порядка в неупорядоченной структуре приводит к возникновению неоднородностей нанометровых размеров. На наличие такой неоднородности указывают результаты рентгенодифрактометрии, согласно которым при большем, по сравнению с кристаллом, среднем координационном числе атома металла и меньшем межатомном расстоянии металл-кислород плотность аморфного оксида ниже, чем кристаллического. Еще одним указанием является обнаруживаемая методом рентгеновской фотоэлектронной спектроскопии тонкая структура 1s-уровня кислорода, свидетельствующая о неэквивалентности его окружения [5].

Фундаментальные представления о строении некристаллических веществ, а также обнаруженная в работе [11] присущая кристаллам высокая электрооптическая чувствительность стекол дают основания полагать, что строение оксида в наноразмерных областях локального разрежения кристаллоподобна. В пользу этой гипотезы говорят и данные кластерного моделирования электронного строения оксидов тантала и ниобия как двухкомпонентной системы с параметрами ближнего порядка компонентов, отвечающих аморфному и кристаллическому оксидам [5, 6].

Наличие структурной неоднородности нанометровых размеров создает условия для образования каналов длиннопробежной диффузии ионов, что с определенностью проявляется в транспортных свойствах при катодной поляризации оксида в контакте с водородосодержащим электродным материалом, прежде всего, в присущей металлооксидным структурам асимметрии вольт-амперной характеристики относительно полярности приложенного напряжения, и при анодной поляризации в течение длительного времени – в электрическом старении оксида в контакте с водным раствором электролита [12-15]. В обоих режимах имеет место транспорт ионов: в первом – водорода, что регистрируется методом ядерных реакций; во втором – кислорода из электролита, что следует из данных вторичной ионной масс-спектрометрии.

В обоих процессах ионный транспорт происходит по локальным каналам, причем в случае инжекции водорода при высокой плотности тока наблюдается термическая кристаллизация оксида. Последнее является еще одним указанием в пользу частичной упорядоченности аморфного оксида в наноразмерных областях разрежения.

В результате указанных ионных процессов в оксиде возникает макроскопическая неоднородность, приводящая к существенному, в случае катод-

ной поляризация – катастрофическому, увеличению тока утечки. Наряду с электростимулированным фазообразованием, сопряженным с протеканием ионного тока существенную роль здесь играет более высокая, по сравнению с аморфным оксидом, электронная проводимость кристаллов.

Другим фактором, предопределяющим структурную неоднородность, является нестехиометрия состава оксидов, проявляющаяся в образовании структурных дефектов в неупорядоченном оксиде типа кислородных вакансий и возможной их кластеризации [16].

Как свидетельствуют результаты расчета энергетического спектра кластерной модели, в которой из кластера извлекались атомы кислорода, и рентгеновской фотоэлектронной спектроскопии частичного восстановленного посредством термообработки оксида, при возрастании концентрации дефектов нестехиометрии в запрещенной зоне увеличивается количество заполненных электронами состояний, причем центрами локализации носителей являются катионы переходного металла в непредельной степени окисления. Как следствие, с увеличением степени нестехиометрии происходит повышение находящегося в области локализованных состояний уровня Ферми и отвечающее этому экспоненциально сильное возрастание прыжковой электронной проводимости.

Агрегация дефектов нестехиометрии может являться причиной возникновения наноразмерных областей локального разрежения. На это указывает, в частности, качественное отличие поведения неомической проводимости кристаллического металлооксида от аморфного, состоящее в отсутствии обусловленного перестройкой путей протекания тока отмеченного выше эффекта уменьшения проводимости с ростом напряженности электрического поля. Заметим, что на агрегацию дефектов нестехиометрии в кристаллах оксидов переходных металлов указывают, как отмечала в своих работах В. А. Иоффе, результаты электронного парамагнитного резонанса.

Исходя из сказанного, следует, что конструктивные в плане улучшения токовых и надежностных характеристик технологические воздействия на структуру оксида должны быть направлены на повышение структурной однородности и снижение дефектности нестехиометрии.

В качестве таких воздействий предложены и апробированы постростовая восстановительная термообработка оксида с последующим реоксидированием, химико-термическая постростовая обработка в парах сильного окислителя, формовка оксида в электролите, содержащем сильный окислитель [17]. Результаты рентгеновской фотоэлектронной спектроскопии ва-

лентных и остовных электронов и EXAFS-спектроскопии свидетельствуют о том, что использование указанных технологических приемов способствует достижению желаемых изменений в строении оксида.

Соответствующая сформулированным рекомендациям модификация технологии формирования оксидов, как показал эксперимент, позволяет добиться существенного (до полутора порядков величины) уменьшения тока утечки и повышения устойчивости токовых характеристик в условиях длительного электротеплового нагружения емкостных элементов при обеих полярностях приложенного напряжения.

Общий итог работы состоит в выработке и реализации системного подхода к характеризации структуры функциональных неупорядоченных диэлектриков на предмет определения неоднородности на разных уровнях ее организации, влияния неоднородности на транспортные свойства и ее генезиса как следствия протекания транспортных процессов и выявлении возможностей технологического решения задач улучшения токовых и надежностных характеристик емкостных элементов электронной базы.

Список используемых источников

1. Зверев Г. И. Физические основы кремниевой наноэлектроники. М.: БИНОМ. Лаборатория знаний, 2017. 240 с.

2. Гриценко В. А., Исламов Д. Р. Физика диэлектрических пленок механизмы транспорта заряда и физические основы приборов памяти: Монография. Новосибирск: Параллель, 2017. 351 с.

3. Красников Г. Я. Конструктивно-технологические особенности субмикронных МОП-транзисторов. Москва: Техносфера, 2011. 800 с.

4. Bottger H., Bryksin V. Hopping Conduction in Solids. VCH, 1985. 472 p.

5. Физика и технология наноструктурированных функциональных материалов: Монография / Под ред. С. Д. Ханина и Ю. А. Кумзерова. СПб.: Издательство Военной академии связи, 2023. 392 с.

6. Физика неупорядоченных и наноструктурированных оксидов и халькогенидов металлов: Монография / Под ред. Г. А. Бордовского. СПб.: Изд-во РГПУ им. А. И. Герцена, 2011. 382 с.

7. Ханин С. Д. Физика транспортных NNN явлений в функциональных материалах металлооксидной электроники // Сборник материалов Международной научно-практической конференции «Карбышевские чтения». Тюмень: ТВВИКУ, 2021. Т. 4. С. 157-162.

8. Брыксин В. В., Ханин С. Д. Сверхмалые поляроны в аморфном оксиде тантала // Физика твердого тела, 1993. Вып. 8. С. 2266-2270.

9. Брыксин В. В. Оптическое внутризонное поглощение в неупорядоченных системах при сильном электрон-фононном взаимодействии // Физика твердого тела, 1982. Т. 24. В. 4. С. 1110-1117.

10. Khanin S. D. Kinetic Electronic Phenomena in Metal Oxide Dielectric Films // Materials Science Forum, 1993, V. 185-188. P. 563-572.

11. Таганцев Д. К. Физико-химические основы разработки стеклообразных материалов и элементов для фотоники. Автореф. Дисс…докт. хим. наук. СПб., 2010. 49 с.

12. Ханин С. Д. Структурная неоднородность и транспортные свойства некристаллических металлооксидных материалов // Техника радиосвязи, 2023. Вып. 2(57). С. 76-82.

13. Ханин С. Д. Имплантационно-стимулированные процессы в функциональных элементах оксидных конденсаторов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. СПб.: СПбГУТ, 2024. Т. 4. С. 858-863.

14. Ханин С. Д. Факторы формирования кинетических свойств металлооксидных диэлектрических материалов электронной компонентной базы // Актуальные проблемы инфотелекоммуникаций в науке и образовании. СПб.: СПбГУТ, 2024. Т. 4. С. 869-873.

15. Ханин С. Д. Электрическое разрушение аморфных металлооксидов в структурах емкостных элементов // Необратимые процессы в природе и технике: XII Всероссийская конференция. М.: МГТУ им. Н. Э. Баумана, 2023. Т. 1. С. 253-255.

16. Кофстад П. Отклонение от стехиометрии, диффузия и электропроводность в простых оксидах металлов. М.: Мир, 1975. 396 с.

17. Ханин С. Д. Физические основы и методы диагностики и управления транспортными свойствами некристаллических металлооксидных материалов в структурах емкостных элементов // Труды XX Международной научной конференции «Физика твердого тела». Минск, 2023. С. 170-172.

STRUCTURAL HETEROGENEITY OF DISORDERED DIELECTRICS OF ELECTRONIC BASE ELEMENTS AND THEIR OPERATIONAL CHARACTERISTICS

Ostroumova Yu., Khanin S.
Military medical academy of S.M. Kirov
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of the development of physical and technological foundations for the formation of dielectric materials with a disordered structure of functional elements with the necessary current and reliability characteristics, attention is focused on the structural heterogeneity associated with disorder. Based on the results of studies of amorphous tantalum and niobium oxides, the influence exerted on transport properties by structural heterogeneity at its different levels is analyzed. Technological means for improving and increasing the time stability of the current characteristics of capacitive elements are determined and substantiated.

Key words: *structural heterogeneity, electrical conductivity, resistance to electrothermal loading, current and reliability characteristics*

УДК 535.14
ГРНТИ 29.31.15

ИЗБРАННЫЕ ВОПРОСЫ КВАНТОВОЙ ОПТИКИ: НЕОДНОЗНАЧНОСТЬ ЗАКОНА СМЕЩЕНИЯ ВИНА

Ф. Ф. Павлов

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

Как известно, любой спектр можно определять различными способами, рассматривая спектральную плотность излучения абсолютно черного тела как функцию частоты или длины волны. Это соответствует нелинейной замене переменных для функции спектральной плотности. Получившиеся в результате замены спектральные функции имеют существенно различные формы и пиковые положения. Рассматриваются различные варианты решения неоднозначности закона смещения Вина с учетом анализа средних значений длин волн, частот и энергии чернотельных фотонов, а также приведения формулы Планка к одному стандарту в логарифмической шкале. Все формулы получены в аналитическом виде для дальнейшего исследования, что абсолютно не типично для стандартных изложений в вузовских материалах по квантовой оптике.

закон смещения Вина, формула Планка, спектральная плотность излучения

Как известно, формула Планка, описывающая равновесную спектральную плотность излучения абсолютно черного тела в шкале длин волн, имеет вид [1]

$$u_\lambda = \frac{16\pi^2\hbar c}{\lambda^5}\frac{1}{e^{\frac{2\pi\hbar c}{\lambda kT}}-1} = \frac{k^5T^5}{2\pi^3\hbar^4c^4}\frac{z^5}{e^z-1}, \quad (1)$$

где $\hbar = \frac{h}{2\pi} = 1{,}054\cdot10^{-34}$ Дж · с – редуцированная постоянная Планка, $k = 1{,}38\cdot10^{-23}\,\frac{\text{Дж}}{\text{К}}$ – постоянная Больцмана; $\text{с} = 3\cdot10^8\,\frac{\text{м}}{\text{с}}$ – скорость света в вакууме, T – температура абсолютно черного тела в Кельвинах; $z = 2\pi\hbar\nu/kT = 2\pi\hbar c/\lambda kT$.

Также часто используется равновесная спектральная плотность в шкале частот [1]:

$$u_\nu = \frac{16\pi^2\hbar\nu^3}{c^3}\frac{1}{e^{\frac{2\pi\hbar\nu}{kT}}-1} = \frac{2k^3T^3}{\pi\hbar^2c^3}\frac{z^3}{e^z-1}. \quad (2)$$

Полная объемная плотность энергии теплового излучения (закон Стефана-Больцмана) равна

$$u = \int_0^\infty u_\lambda d\lambda = \int_0^\infty u_\nu d\nu = \frac{4}{c}\sigma T^4, \quad (3)$$

где $\sigma = \frac{\pi^2 k^4}{60c^2\hbar^3} T^4 = 5{,}67 \cdot 10^{-8} \frac{\text{Вт}}{\text{м}^2\text{К}^4}$ – постоянная Стефана-Больцмана.

Для вычисления спектральной плотности в шкале частот (2) необходимо было сделать замену λ = c/ν в формуле (1) и учесть, что $d\nu = -\frac{c}{\lambda^2} d\lambda$, и тогда $u_\nu d\nu = -u_\nu \frac{c}{\lambda^2} d\lambda = u_\lambda d\lambda$.

Максимум спектральной плотности в шкале длин волн (1) находится из условия $\frac{du_\lambda}{d\lambda} = 0$, дающее соотношение для длины волны

$$\lambda_m = \frac{2\pi\hbar c}{kT(W(-5e^{-5}) + 5)} = \frac{(0{,}002898 \text{ м} \cdot \text{К})}{T}, \quad (4)$$

называемое законом смещения Вина, и соответствующей ей частоты

$$\nu_m = \frac{\text{c}}{\lambda_m} = \left(1{,}0346 \cdot 10^{11} \frac{\text{Гц}}{\text{К}}\right) \cdot T, \quad (5)$$

где $W(-5e^{-5}) \approx -0{,}0349$ – значение *W*-функция Ламберта *W*(*x*)=LambertW(*x*) при $x = -5e^{-5} \approx -0{,}03369$; здесь и везде используется система СИ и температура *T* измеряется в Кельвинах; все формулы помимо численных значений приводятся в аналитическом виде (с оговоркой, что не все функции выражаются в элементарных функциях).

Аналогично, максимум спектральной плотности в шкале частот (2) находится из условия $\frac{du_\nu}{d\nu} = 0$, дающее соотношение для частоты

$$\nu'_m = \frac{kT(W(-3e^{-3}) + 3)}{2\pi\hbar} = \left(5{,}8789 \cdot 10^{10} \frac{\text{Гц}}{\text{К}}\right) \cdot T. \quad (6)$$

и соответствующей ей длине волны

$$\lambda'_m = \frac{c}{\nu'_m} = \frac{(0{,}0050994 \text{ м} \cdot \text{К})}{T}, \quad (7)$$

где $W(-3e^{-3}) \approx -0{,}17856$ – значение *W*-функция Ламберта *W*(*x*) = LambertW(*x*) при $x = -3e^{-3} \approx -0{,}1494$.

Таким образом, положение максимума зависит от шкалы, для которой определяется спектральная плотность. Видно, что произведение длины

волны (4) на частоту (6) не равно скорости света, при этом получается интересная формула, полученная в аналитическом виде:

$$\lambda_m \cdot \nu'_m = \frac{W(-3e^{-3}) + 3}{W(-5e^{-5}) + 5} c = 0{,}5682 \cdot c, \qquad (8)$$

То есть длина волны λ_m, соответствующая максимуму u_λ по длинам волн, не совпадает с длинной волны c/ν'_m, отвечающая максимуму u_ν по частоте, и $\lambda'_m = 1{,}76 \cdot \lambda_m$.

Примечательно, что, хотя на самом деле Солнце белое, максимуму распределения по длине волны при $T = 5800$ К соответствует длина волны λ_m = 500 нм (цвет циан!), тогда как максимуму распределения по частоте соответствует частота $\nu'_m = 3{,}41 \cdot 10^{14}$ Гц (инфракрасный диапазон). В данной статье не обсуждается цвет Солнца из закона смещения Вина, и этому простому, но неоднозначному, вопросу будет посвящена отдельная публикация. Единственное, что стоит сказать, что если найти максимум функции $u_\lambda \cdot e^{-\tau(\lambda)}$ из условия $\frac{d(u_\lambda \cdot e^{-\tau(\lambda)})}{d\lambda} = 0$, где $\tau(\lambda)$ – оптическая толщина атмосферы, которую при молекулярном рассеянии (закон Рэлея $\tau(\lambda) \sim 1/\lambda^4$) можно представить в виде пропорции $\tau(\lambda) = \tau_{Sun} \cdot \left(\frac{\lambda_{Sun}}{\lambda}\right)^4$, то длина волны, соответствующая максимуму будет равна $\lambda_m = 572$ нм (желтый цвет). Здесь учтено, что оптическая толщина безоблачной атмосферы по нормали на длине волны $\lambda_{sun} = 500$ нм (максимум внеатмосферного чернотельного излучения) принята равной τ_{sun}= 0,26.

На рис. 1 приведены графики спектральных плотностей (1) и (2) при температурах T = 5800 К и T = 4000 К.

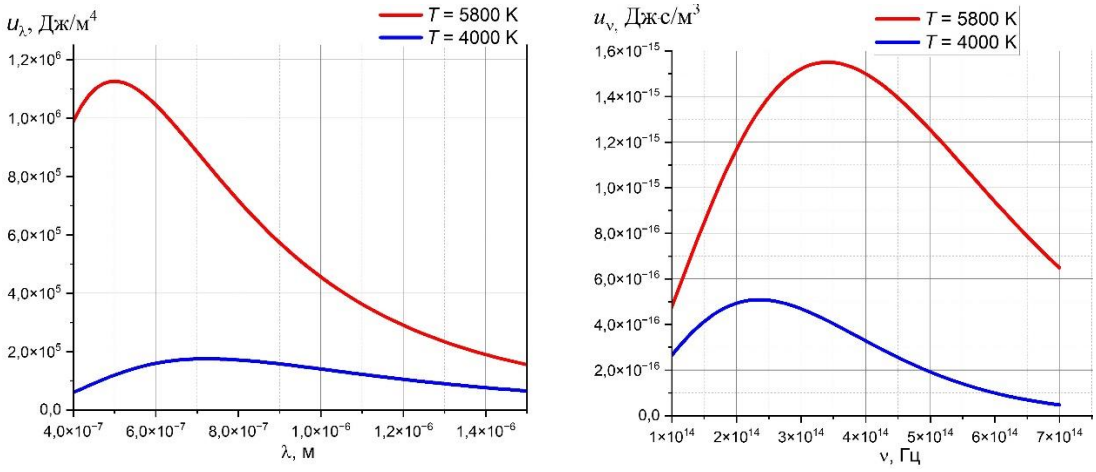


Рис. 1. Графики формулы Планка в зависимости от длины волны и частоты

Разве формула Планка не определена достаточно хорошо, что независимо от того, как мы ее строим, мы должны приходить к одним и тем же качественным выводам об источнике?

Проанализируем средние значения длины волны, частоты и энергии чернотельного фотона, а также рассмотрим построение формулы Планка в едином стандарте с использованием ln(λ) или ln(ν) в качестве независимой переменной.

В некоторых работах предлагается использовать среднюю энергию излучаемых фотонов вместо закона смещения Вина, так как, по утверждению авторов [2]: «средняя энергия фотона служит и педагогическим целям лучше, и имеет ясный физический смысл». Однако, как мы убедимся позже, такой подход тоже не совсем корректен, так как неоднозначность остается.

I. Средние значения вместо максимальных

Вместо максимальных значений длины волны (4) и частоты (6) сделаем поэтапный анализ средних значений энергии чернотельного фотона, длины волны и частоты.

1. Средняя энергия одного чернотельного фотона.

Чтобы найти среднюю энергию одного чернотельного фотона $\langle E_\gamma \rangle$, нужно объемную плотность энергии поля излучения (3)

$$u = \int_0^\infty u_\nu d\nu = \frac{4}{c}\sigma T^4 = \frac{\pi^2 k^4}{15c^3\hbar^3} T^4 = \left(7{,}57 \cdot 10^{-16}\ \frac{\text{Дж}}{\text{м}^3\text{К}^4}\right) \cdot T^4$$

поделить на концентрацию фотонов [3]

$$n_\gamma = \int_0^\infty \frac{u_\nu}{h\nu} d\nu = \frac{2k^3\zeta(3)}{\pi^2 c^3 \hbar^3} T^3 = \left(2{,}03 \cdot 10^7\ \frac{1}{\text{м}^3\text{К}^3}\right) \cdot T^3,$$

где $\zeta(3) \approx 1.202$ – значение дзеты-функции Римана $\zeta(n)$ при $n = 3$.

Тогда получим выражение

$$\langle E_\gamma \rangle = \frac{u}{n_\gamma} = \frac{\pi^4}{30\zeta(3)} kT \approx 2{,}7 \cdot kT = \left(3{,}729 \cdot 10^{-23}\ \frac{\text{Дж}}{\text{К}}\right) \cdot T. \qquad (9)$$

Казалось бы, при представлении закона смещения Вина в форме излучения черного тела в терминах фотонов, нет двусмысленности относительно того, какую формулу для длины волны (4) или (7) следует рассматривать, но в дальнейшим мы убедимся, что это не так.

2. Средняя длина волны.

Для средней длины волны чернотельного фотона получается следующая формула в аналитическом виде

$$\langle\lambda\rangle = \frac{\int_0^\infty \lambda u_\lambda d\lambda}{\int_0^\infty u_\lambda d\lambda} = \frac{60c\hbar\zeta(3)}{\pi^3 kT} = \frac{2{,}326}{kT}c\hbar = \frac{(0{,}005326\ \text{м}\cdot\text{К})}{T}. \qquad (10)$$

Если представить среднюю энергию $\langle E_\gamma \rangle$ в виде $hc/\langle\lambda\rangle$, то тогда получим выражение

$$\langle E_\gamma \rangle = \frac{hc}{\langle\lambda\rangle} = 2{,}7\cdot kT, \qquad (11)$$

в точности совпадающее с формулой (9).

Примечательно, что при T = 5800 К (Солнце) $\langle\lambda\rangle = 918$ нм (инфракрасный диапазон).

Далее оценим дисперсию длины волны по формуле

$$D(\lambda) = \frac{\int_0^\infty (\lambda - \langle\lambda\rangle)^2 u_\lambda d\lambda}{\int_0^\infty u_\lambda d\lambda} = \langle\lambda^2\rangle - \langle\lambda\rangle^2 = \frac{10c^2\hbar^2}{k^2T^2} - \frac{3600c^2\hbar^2\zeta(3)^2}{\pi^6 k^2T^2} =$$
$$= \frac{4{,}5893c^2\hbar^2}{k^2T^2} = \frac{2{,}4\cdot 10^{-5}}{T^2}.$$

Тогда среднеквадратичное отклонение длины волны будет равно

$$\sigma = \sqrt{D(\lambda)} = \frac{2{,}1423c\hbar}{kT} = \frac{(0{,}004905\ \text{м}\cdot\text{К})}{T}. \qquad (12)$$

Если данное среднеквадратичное отклонение принять за меру разброса относительно среднего значения $\lambda = \langle\lambda\rangle \pm \sigma$, то можно заметить, что среднее значение (10) близко к своему среднеквадратичному отклонению (12) $\langle\lambda\rangle \sim \sigma$ и относительна ошибка равна $\delta\lambda = \sigma/\langle\lambda\rangle = 92\ \%$.

Таким образом, можно сделать вывод, что кривая формулы Планка настолько широкая, а пик настолько монотонный, что по всей малой ширине видимой полосы спектр вблизи пика фактически плоский, и закон смещения Вина интерпретируется слишком широко.

3. Средняя частота.

Аналогично найдем среднюю частоту чернотельного фотона в аналитическом виде

$$\langle \nu \rangle = \frac{\int_0^\infty \nu u_\nu d\nu}{\int_0^\infty u_\nu d\nu} = \frac{180kT\zeta(5)}{\pi^5\hbar} = \frac{0{,}60992}{\hbar}kT = \left(7{,}986 \cdot 10^{10}\ \frac{\text{Гц}}{\text{К}}\right) \cdot T, \quad (13)$$

где $\zeta(5) \approx 1.0369$ – значение дзеты-функции Римана $\zeta(n)$ при $n = 5$.

Примечательно, что при $T = 5800$ К (Солнце) $\langle \nu \rangle = 4{,}63 \cdot 10^{14}$ Гц (красный цвет).

Можно заметить, что произведение средней длины волны (10) на среднюю частоту (13) не равно скорости света, и получается интересная аналитическая формула

$$\langle \nu \rangle \cdot \langle \lambda \rangle == \frac{10800 \cdot \zeta(5) \cdot \zeta(3)}{\pi^8} c = 1{,}4187 \cdot c. \quad (14)$$

То есть, неоднозначность закона смещения Вина, вытекающая из-за того, что произведение длины волны λ_m, соответствующей максимуму функции (1) на частоту ν'_m, отвечающей максимуму функции (2), не равно скорости света (формула (8)), сохраняется и для средних значений длины волны и частоты.

Как известно, в основе гипотезы Планка лежит утверждение, что свет испускается чередою отдельных порций, квантов энергии, и энергия одного кванта пропорциональна частоте излучения $E_\gamma = h\nu$. Поэтому оценим среднюю энергию одного чернотельного фотона по формуле:

$$\langle E_\gamma \rangle = h\langle \nu \rangle = 3{,}83 \cdot kT = \frac{1{,}4187hc}{\langle \lambda \rangle} \neq \frac{hc}{\langle \lambda \rangle}, \quad (15)$$

которая, как видно, не совпадает с формулой (9).

Таким образом, среднюю энергию одного чернотельного фотона нельзя использовать в качестве альтернативы закону смещения Вина, потому что неоднозначность остается – фотоны имеют разную среднюю энергию (11) и (15). Это тянется от несовпадения максимальных значений частот и длин волн, и таким образом неоднозначность даже в средних энергиях фотонов остается.

II. Распределение спектральной плотности излучения по логарифмической переменной

Предлагается использовать $\ln(\lambda)$ или $\ln(\nu)$ в качестве независимой переменной [4]. Такой тип графика часто называют «спектральным распределением по дробной полосе пропускания».

Если независимая переменная выбрана логарифмической (ln(λ) или ln(ν)), то соответствующие функции Планка достигают пика в одном и том же месте. Поэтому при таком представлении формулы не возникает двусмысленности относительно того, какую из них следует рассматривать. Фактически, эти графики имеют одинаковые пики, потому что они являются идентичными графиками. Легко увидеть, что $d(\ln\lambda) = \frac{d\lambda}{\lambda} = -d(\ln\nu) = \frac{d\nu}{\nu}$. Отрицательный знак возникает, поскольку увеличение частоты соответствует уменьшению длины волны.

Если ввести безразмерную переменную $z = \frac{h\nu}{kT} = \frac{2\pi\hbar\nu}{kT} = \frac{2\pi\hbar c}{\lambda kT}$ планковское распределение можно задать в виде

$$\nu u_\nu = \lambda u_\lambda = \frac{k^4T^4}{\pi^2 c^3\hbar^3}\frac{z^4}{e^z - 1}.$$

Тогда среднее значение z, соответствующее средней энергии фотона (15), будет равно $\langle z\rangle = \frac{h\langle\nu\rangle}{kT} = 3{,}83$, чему соответствует средняя частота (13). При этом $\langle z\rangle \neq \frac{hc}{\langle\lambda\rangle kT} = 2{,}7$ для средней энергии фотона (11).

На рис. 2 показан график $\frac{\nu u_\nu}{T^4}$ от z от ln(z) в качестве независимых переменных. Таким образом получается единая кривая для описания излучения черного тела для всех температур. Значение $\langle z\rangle$, соответствующее средней энергии фотона, отображается на рис. 2 в виде вертикальной линии.

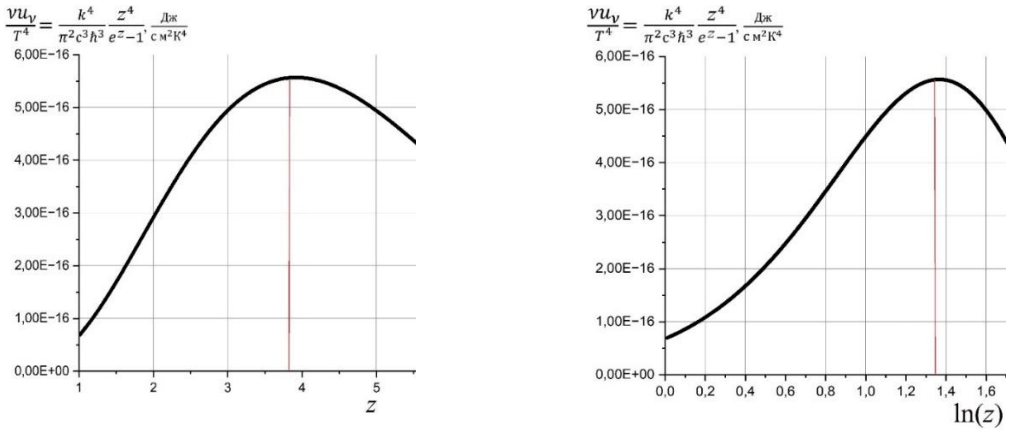


Рис. 2. Графики распределения приведенной равновесной спектральной плотности в зависимости от безразмерной переменной z и ln(z)

В данной работе рассмотрен большой спектр вопросов, связанный с двойственностью закона смещения Вина, который может быть стимулом для дальнейшего исследования; обозначены все острые проблемы; новизна

заключается в том, что все решения получены в аналитическом виде, чего не встречается в учебниках и публикациях, посвященных данному вопросу.

Список используемых источников

1. Матвеев А. Н. Оптика. М.: Высш. шк., 1985, 351 с.
2. Jonathan M. Marr, Francis P. Wilkin. A better presentation of Planck's radiation law // Am. J. Phys. 2012. 80. P. 399-405. arXiv:1109.3822. DOI: 10.1119/1.3696974
3. Иванов В. В., Кривов А. В., Денисенков П. А. Парадоксальная Вселенная: 175 задач по астрономии. СПб.: Изд. СПбГУ, 1997, 144 с.
4. Zhang Z. M., X. J. Wang X. J. Unified Wien's displacement law in terms of logarithmic frequency or wavelength scale // J. Thermophys. Heat Transfer. 2010. Vol. 24. PP. 222–224. DOI: 10.2514/1.45992 EDN: MZWNNT

SELECTED TOPICS IN QUANTUM OPTICS: AMBIGUITY OF THE WIEN'S DISPLACEMENT LAW

Pavlov F.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

As is known, any spectrum can be defined in various ways, considering the spectral density of radiation of an absolutely black body as a function of frequency or wavelength. This corresponds to a nonlinear change of variables for the spectral density function. The spectral functions obtained as a result of the change have significantly different shapes and peak positions. Various options for resolving the ambiguity of the Wien displacement law are considered, taking into account the analysis of average values of wavelengths, frequencies and energies of blackbody photons, as well as reducing Planck's formula to a single standard in a logarithmic scale. All formulas are obtained in analytical form for further study, which is absolutely not typical for standard presentations in university materials on quantum optics.

Key words: Wien's displacement law, Planck's law, spectral energy density

УДК 004.8
ГРНТИ 28.23.01

ОСНОВНЫЕ ПОДХОДЫ К РЕШЕНИЮ ПРОБЛЕМ РАСПОЗНАВАНИЯ МЕДИАДАННЫХ

О. И. Пантюхин, Д. Ю. Изотов, Р. В. Яровой

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

Статья посвящена основным подходам к решению проблем распознавания медиаданных, включая машинное и глубокое обучение, обработку естественного языка и комбинированные методы. Приводится сравнительный анализ этих подходов, описываются их преимущества и ограничения. Подчеркивается важность выбора подходящего метода для конкретных задач и перспективы дальнейшего развития технологий распознавания медиаданных.

распознавание медиаданных, машинное обучение, обработка естественного языка, мультимодальные данные, классификация

Объем медиаданных растет экспоненциально, охватывая изображения, видео, аудио и текстовую информацию, что в свою очередь имеет большое влияние в различных сферах, включая социальные медиа, здравоохранение, финансы и безопасность, но для эффективного использования медиаданных необходимы мощные инструменты для их анализа и интерпретации.

Распознавание медиаданных представляет собой сложный процесс, включающий автоматическое извлечение и классификацию информации из различных типов мультимедийного контента [1], что требует применения современных технологий и алгоритмов, способных обрабатывать большие объемы данных с высокой точностью и скоростью.

Основные проблемы, связанные с распознаванием медиаданных, возникают из-за разнообразия содержимого и условий неопределенности. Под условиями неопределенности авторским коллективом подразумевается неблагоприятная для распознавания обстановка, например шумные области. Решение этих проблем является основной задачей для повышения качественных показателей обработки и распознавания медиаданных, а также для повышения области их применения.

Область применения технологии распознавания медиаданных определяется исходя из задач, которые обладают своими характеристиками, спе-

цификой и определенными трудностями. Основные направления применения технологии выделены ниже.

Технология распознавания изображений включает в себя классификацию, сегментацию и идентификацию элементов. Автоматическая обработка, включающая в себя локализацию объектов и определения границ, осложняется посредством вмешательства искажений и шумов.

Распознавание видеоданных является более комплексной задачей, по сравнению с распознаванием изображений, так как информация, поступающая на считывающие элементы системы, меняется динамически, из-за чего повышаются требования и к вычислительным мощностям в том числе.

Особенности распознавания аудиоданных, в том числе человеческой речи, заключаются в таких факторах, как шумовые помехи, вариации произношения, акценты и интонационные особенности говорящих.

Основные сложности распознавания текста сводятся к классификации текстовых данных, извлечения смысловой информации, эмоциональной окраски текста и учета контекста. Из-за вышеперечисленных особенностей, повышается сложность моделей распознавания в робототехнических системах.

Исходя из вышеперечисленных направлений распознавания и их особенностей, реализация системы распознавания медиаданных подразумевает использование разнообразных подходов, каждый из которых обладает своими преимуществами и ограничениями. Выбор конкретной методики с использованием машинного обучения определяется спецификой задачи и техническими требованиями.

Машинное обучение представляет собой совокупность алгоритмов, способных адаптироваться к данным для выполнения конкретных задач распознавания. Традиционные методы, такие как деревья решений, алгоритмы опорных векторов и кластеризация методом k-средних, демонстрируют эффективность при работе с ограниченными наборами данных и простыми задачами классификации, однако ограничения классических подходов приводят к недостаточной производительности при работе с объемными и сложными массивами [2].

Глубокое обучение базируется на использовании многослойных нейронных сетей, способных моделировать сложные зависимости внутри данных. Конволюционные нейронные сети нашли широкое применение в задачах распознавания изображений и видеоматериалов благодаря своей способности выявлять пространственные признаки. В то же время рекурентные нейронные сети успешно реализуются в обработке звуковых сиг-

налов и текстовых потоков, что делает их незаменимыми в области анализа последовательностей.

Обработка естественного языка (Natural Language Processing, NLP) сосредоточена на анализе и интерпретации текстовых данных. Современные архитектуры, такие как BERT и GPT, демонстрируют высокую точность в части касающейся классификации текстов, автоматического перевода и извлечения информации. В то же время, NLP сталкивается с такими особенностями, как многозначность слов и необходимость учета контекста [3].

Интеграционные подходы объединяют преимущества различных методов для повышения точности и эффективности систем распознавания медиаданных. Мультимодальные системы, например, сочетают анализ изображений, звука и текста для формирования более комплексного понимания контента.

Каждый из указанных методов занимает свое уникальное место в арсенале решений проблем распознавания медиаданных. Применение данных систем определяется спецификой конкретных задач и доступными ресурсами – от ограниченных вычислительных мощностей до необходимости обработки больших объемов информации.

Каждый из этих подходов имеет свое место и значимость в решении проблем распознавания медиаданных и используется в зависимости от конкретных задач и доступных ресурсов.

В таблице 1 представлено сравнение подходов к распознаванию медиаданных.

ТАБЛИЦА 1. Сравнение подходов к распознаванию медиаданных

Подход	Преимущества	Ограничения	Примеры применения
Машинное обучение	- простота реализации - эффективность на небольших и умеренных объемах данных - понятность алгоритмов	- снижение точности на сложных наборах данных - ограниченные возможности обработки нелинейных зависимостей	- базовая классификация изображений - простой анализ текста
Глубокое обучение	- высокая точность на сложных данных - автоматическое извлечение признаков - хорошая масштабируемость	- высокие требования к ресурсам - долгое время обучения - сложность интерпретации моделей	- распознавание лиц - анализ видео - обработка звука

Подход	Преимущества	Ограничения	Примеры применения
Обработка естественного языка (NLP)	- обработка сложных текстовых структур - высокая точность в классификации и генерации текста	- зависимость от качества данных - сложности в обработке многозначных слов и контекста	- автоматический перевод - анализ тональности
Комбинированные подходы	- улучшенная точность и эффективность - возможность работы с мультимодальными данными	- сложность разработки и интеграции - высокие требования к ресурсам и данным	- системы распознавания контента в социальных сетях - автономные системы безопасности

Обработка медиаданных в настоящее время представляет собой одну из наиболее приоритетных задач. Из тех технологий, которые могут быть использованы в данной задаче (обработка медиаданных) – искусственный интеллект (компьютерное зрение, NLP, глубокое обучение) – представляет большой спектр возможностей [4], в тоже время необходимо помнить, что в одном конкретном методе решения есть свои достоинства, а есть недостатки и для того, чтобы нивелировать их лучшим вариантом является комбинирование различных подходов к решению поставленной задачи, а с учетом скорости развития технологий (повышение качества и эффективности существующих алгоритмов, создание новых, превосходящих существующие, технологий) – все перечисленное будет способствовать более всеобъемлющему улучшению и покрытию все большего числа сфер жизни.

Список используемых источников

1. Ячная В. О., Луцив В. Р., Малашин Р. О. Современные технологии автоматического распознавания средств общения на основе визуальных данных // Компьютерная оптика. 2023. № 2. С. 287-305.

2. Полетаевая Н. Г. Классификация систем машинного обучения // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2020. № 1. С. 5-22.

3. Цитульский А. М., Иванников А. В., Рогов И. С. NLP – обработка естественных языков // StudNet. 2020. № 6. С. 467-475.

4. Гавриленко Н. Г., Заворовский И. А. Адаптация методов теории распознавания образов в решении задач по анализу поведения человека // Известия Тульского государственного университета. Технические науки. 2025. № 1. С. 189-200.

MAIN APPROACHES TO SOLVING MEDIA DATA RECOGNITION PROBLEMS

Pantukhin O., Izotov D., Yarovoy R.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the main approaches to solving media recognition problems, including machine and deep learning, natural language processing and combined methods. A comparative analysis of these approaches is given; their advantages and limitations are described. The importance of choosing a suitable method for specific tasks and prospects for further development of media recognition technologies are emphasized.

Key words: *media recognition, machine learning, natural language processing, multimodal data, classification*

УДК 004.8
ГРНТИ 28.23.01

СИСТЕМЫ РАСПОЗНАВАНИЯ МЕДИАДАННЫХ: ОБЛАСТИ ПРИМЕНЕНИЯ И РЕШАЕМЫЕ ЗАДАЧИ

О. И. Пантюхин, Д. Ю. Изотов, Р. В. Яровой

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

Статья посвящена анализу систем распознавания медиаданных, охватывая их ключевые области применения и решаемые задачи. В работе рассмотрены основные технологии, такие как машинное обучение, обработка естественного языка и компьютерное зрение, которые играют основную роль в развитии этих систем. Описаны практические задачи, решаемые с помощью этих технологий, включая улучшение поиска и классификации контента, автоматизацию процессов в сфере безопасности, здравоохранения и образования, а также повышение доступности медиаматериалов для различных категорий пользователей.

системы распознавания медиаданных, машинное обучение, обработка естественного языка, компьютерное зрение

В современном мире объем цифровой информации растет с невероятной скоростью, и медиаданные занимают значительную часть этого потока. Медиаданные включают в себя изображения, аудио, видео и текстовые файлы, которые требуют автоматизированных методов для их эффективного анализа и управления. Системы распознавания медиаданных стали ключевыми инструментами в решении этих задач, обеспечивая возможность идентификации, классификации и извлечения полезной информации из различных типов мультимедийных источников.

Современные системы распознавания медиаданных базируются на ряде передовых технологий, которые обеспечивают автоматическое извлечение и обработку информации из мультимедийных файлов. Основные технологии, используемые в этих системах, включают машинное обучение, обработку естественного языка (NLP) и компьютерное зрение.

Машинное обучение (ML) играет ключевую роль в распознавании медиаданных. Используя алгоритмы классификации и кластеризации, системы могут автоматически распознавать объекты на изображениях, идентифицировать говорящих по голосу и классифицировать текстовые данные. Глубокое обучение, являющееся подмножеством ML, позволяет создавать

сложные нейронные сети, которые способны анализировать огромные объемы данных и обучаться на их основе [1].

В разрезе современного мира NLP системы используются в большом количестве направлений – анализ обработка и распознавание текстовых данных (комментарии на различных информационных ресурсах, проверка текста книг на разного рода этических моментов), различного рода медиаданных (видео, звук). В некотором роде, NLP позволяет понимать системе текстовые данные, классифицировать, переводить и писать (создавать) их.

Такое направление в области искусственного интеллекта (ИИ) как компьютерное зрение позволяет системам распознавать и классифицировать объекты на таких типах данных как изображения или видео. Оно (компьютерное зрение) находит применение во многих областях, в качестве примера можно привести анализ медицинских снимков (обнаружение и классификация различных аномалий), в системах безопасности (детекция несанкционированного проникновения на объект), автопилотируемые объекты (автомобили под управлением ИИ, роботы-доставщики) и в других разного рода задачах.

Исходя из вышеперечисленного (которая является малым множеством из большого подмножества) ИИ представляет собой уникальную технологию, которая позволяет разного рода системам «понимать, воспроизводить» информацию не на основе строго заданной логики, а за счет «обучения», что в свою очередь позволяет улучшить показатели связанные с задачей по заданным метрикам качества.

На основе вышесказанного, основой для создания систем распознавания медиаданных идеально подойдут технологии ИИ, которые обладают ресурсами для решения задач в различных сферах.

Исходя из тех фактов, что системы распознавания медиаданных (СРМ) могут обрабатывать аудиоданные, видео, изображение, то можно выделить несколько основных областей, в которых они могут быть использованы:

– в интернете: в таком необъятном «пространстве» существует безграничное множество информации, которое не может быть легко проанализирована небольшой группой специалистов на предмет наличия в ней разного рода запрещено информации, которая нарушает законы, нормы этики и морали, в этом случае могут быть задействованы СРМ для обнаружения, классификации и извещения, а также (при необходимости) устранения подобного контента;
– в медицине: правильно «обученные» СРМ могут служить подспорьем в медицинской практике для анализа снимков (МРТ, КТ), ЭКГ, где они

(СРМ) могут детектировать, идентифицировать и ставить соответствующий диагноз;

– системы безопасности: СРМ могут быть использованы на разного рода объектах в целях идентификации нарушения границ охраняемого объекта (детекция проникновения незарегистрированных лиц на режимный объект) [2];
– системы распознавания медиаданных применяются для автоматического создания субтитров и учебных материалов, с целью повышения доступности образовательного контента для людей с нарушениями слуха и автоматизации создания обучающих материалов на разных языках;
– в маркетинге и рекламе системы распознавания медиаданных помогают анализировать предпочтения пользователей и персонализировать контент. Системы анализируют действия пользователей на веб-сайтах и показывают рекламу, которая соответствует их интересам. Таким образом наблюдается увеличение эффективности рекламных кампаний и улучшение пользовательского опыта [3].

Исходя из тех примеров, что приведены выше по тексту, можно сделать вывод, что СРМ создают обширный потенциал для дальнейшего развития. Системы такого типа могут раскрыть свой необузданный функционал во множестве направлений – будь то анализ изображений, распознавание и транскрибация аудиоматериалов, классификация объектов в различных видеорядах – все перечисленное помогает решать повседневные задачи, которые на протяжении всего времени отвлекают людей от их рабочих задач, на которых необходимо акцентировать внимание, а ведь в таком стиле СРМ могут быть раскрыты в полной мере.

Основная приоритетная задач СРМ данных состоит в улучшении качества поисковых систем по различным заданным фильтрам за счет совершенствования механизмов классификации и разметки различного рода информации, что в свою очередь ускоряет поиск данных определенных пользователей системы. В качестве примера можно привести базы данных, где СРМ в процессе работы размечает видео согласно заданным категориям, в дальнейшем в базе данных каждое видео помечается определенная категория, что в дальнейшем ускоряет поиск необходимого контента.

В тоже время в качестве примера можно привести следующий вариант использования СРМ: обнаружение плагиата и защита авторских прав. Такой вариант использования реализуется за счет механизмов (заложенных в СРМ) сравнения материалов, впервые поступающих в систему с материалами, которые в системе содержаться, а если совпадение было найдено то,

следовательно, извещаются ответственные лица, что обладает высокой значимостью в музыкальной сфере и киноиндустрии.

Автоматически настроенный процесс создания такого элемента для видео как субтитров или такой вариации как текстовое описание для разного рода видеоконтента в наше время также является задачей со своим высоким приоритетом, которая направлена на появление возможности получения информации людьми с ограниченными возможностями (дефекты слуха, зрения). СРМ, в подобных случаях, а также их вариациях, позволяют создавать как субтитры, так и текстовые описания из разного рода видеоматериалов, что в дальнейшем дает возможность использовать их (видеоматериалы) группам людей, возможности которых ограничены [4].

Достаточное большое количество различных сетевых ресурсов (соцсети, видеохостинги) уже используют СРМ для обработки данных, что упрощает работу модераторов, ведь многие данные уже автоматически фильтруются за счет использования вышеназванных систем, не позволяя «опасным данным» дойти до пользователей, тем самым обезопасив их.

Сведения изложенные выше способны укрепить доверие к СРМ, но они сталкиваются с обильным количеством недостатков, которые еще только предстоит рассмотреть, проанализировать, разработать методы их ликвидации и внедрить для дальнейшего совершенствования СРМ.

Системы распознавания медиаданных (СРМ) обладают следующими преимуществами [5]:

1) повышение эффективности: автоматизированная обработка информации ускоряет процесс получения итогового результата;

2) повышение уровня удовлетворенности пользователей: за счет распознавания контента и его рубрикации достигается качественное повышение рекомендательных систем;

3) автоматизация привычных процессов жизнедеятельности: за счет автоматизации определенных процессов, сотрудники, пользователи могут выполнять более актуальные задачи.

Системы распознавания медиаданных обладают следующими недостатками:

1) низка точность: несмотря на вышеперечисленные преимущества, всегда существует вероятность, что медиаданные могут быть неправильно распознанных в силу различных причин (низкое качество видео, звука и данных другого типа);

2) анонимность данных: из-за использования различных данных, которые могут содержать конфиденциальную информацию, в свою очередь растет риск их утечки из-за неправильно настроенных политик безопасности;

3) необходимо весьма объемное количество обучающих датасетов: т.к. любая модель ИИ обучается на разного рода датасетах, то необходимо упомянуть, что качество модели зависит от самого качества датасета для обучения (количество данных, их качество, отсутствие различного рода «отравленных данных»).

4) вопросы этики: автоматизация процессов распознавания медиаданных в любом случае поднимает вопросы этики, что в свою очередь обязывает разработчиков закладывать различные фильтры для защиты.

Для того чтобы исправить все вышеперечисленные недостатки требуется как разработка новых, так и доработка уже существующих основ СРМ.

В дальнейшем СРМ будут совершенствоваться для различных направлений, в том числе и тех, которые появятся на новых витках развития технологического прогресса.

Список используемых источников

1. Пальмов С. В., Артюшкина Е. С. Глубокое обучение: определение и отличительные особенности // Форум молодых ученых. 2020. № 3 (43). С. 311-315.

2. Малыгин М. А. Обнаружение и распознавание лиц человека на изображениях с камер видеонаблюдения // Столыпинский вестник. 2023. № 5. С. 2882-2893.

3. Сушкина А. С., Щербенко Е. В., Алешина О. Г. Применение цифровых технологий в маркетинге // Вестник Алтайской академии экономики и права. 2020. № 11 (часть 1) С. 131-138.

4. Азаренко К. А., Каунг М. Н., Белов Ю. С. Обзор методов для распознавания действий человека // E-Sci. 2019.

5. Шапиро Л. Компьютерное зрение. М.: БИНОМ. Лаборатория знаний, 2013. 752 с.

MEDIA DATA RECOGNITION SYSTEMS: APPLICATION AREAS AND PROBLEMS TO BE SOLVED

Pantukhin O., Izotov D., Yarovoy R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the analysis of media recognition systems, covering their key areas of application and the tasks they solve. The work considers the main technologies, such as machine learning, natural language processing, and computer vision, which play a major role in the development of these systems. Practical tasks solved with the help of these technologies are described, including improving the search and classification of content, automating processes in the field of security, healthcare, and education, as well as increasing the availability of media materials for various categories of users.

Key words: *media recognition systems, machine learning, natural language processing, computer vision*

УДК 004.896
ГРНТИ 28.17.33

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА ГЕОИНФОРМАЦИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

П. А. Прокофьев

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

В работе представлена методика оценки качества геоинформационного программного обеспечения. Рассматриваются количественные и качественные критерии оценки ПО. Предложенный подход включает в себя применение стандартов ГОСТ, а также использование методик, характерных для геоинформационного ПО. Даны рекомендации по улучшению процесса оценки качества геоинформационного программного обеспечения.

ГИС, пространственные данные, картография, географические объекты, оценка качества

Геоинформационные системы (ГИС) играют важную роль во многих отраслях, в частности связанных с пространственно-распределенными объектами и производствами. Однако отсутствие специализированных стандартов для оценки качества такого ПО осложняют его внедрение в государственные и коммерческие структуры. В данной работе представлена методика, объединяющая существующие стандарты и специфику работы с пространственными данными. Цель исследования – предложить универсальный подход к оценке качества ГИС, учитывающий как технические характеристики ПО, так и специфику геопространственных данных.

В настоящее время не существует специальных стандартов качества программного обеспечения, относящегося к области геоинформатики. Однако существует ряд смежных стандартов, которые могут быть положены в основу методики оценки геоинформационного ПО. К ним относятся:

– ГОСТ Р 25010-2015. Требования и оценка качества систем и программного обеспечения. Модели качества систем и программных продуктов [1].
– ГОСТ Р 57773-2017. Пространственные данные. Качество данных [2].

В качестве одного из способов оценки качества предлагается использовать алгоритм аддитивной свертки [3], применяя показатели, указанные в [1], а также используя метод экспертных оценок. Алгоритм включает в себя следующие шаги.

1. Составление набора критериев, являющихся самыми важными для потребителя.

2. Оценка выполнения критерия в интервале от 0 до 1.

3. Выставление коэффициентов значимости критериев. Коэффициенты распределяются в интервале от 0 до 1.

4. Расчет аддитивной суммы интегральной оценки по формуле:

$$O = \sum_{i=1}^{n}(Z_i \cdot K_i),.$$

где O – интегральная оценка заявленного продукта; n – количество критериев сравнения программы согласно таблице критериев; Z_i – значение выполнения i-го критерия (1 – выполнен, 0 – не выполнен); K_i – коэффициент значимости критерия сравнения (принимает значения от 0 до 1).

В таблице 1 приведен пример результата оценки программы по методике, указанной выше.

ТАБЛИЦА 1. Пример оценки качества ГИС с использованием взвешенных оценок

№ п/п	Название характеристики	Значение параметра	Оценка выполнения	Значимость
1	Эффективность			
1.1	Результативность	Высокая	1	1
2	Производительность			
2.1	Производительность	Высокая	1	1
3	Удовлетворенность			
3.1	Полноценность	Средняя	0,5	1
3.2	Доверие	Высокое	1	1
3.3	Удовольствие	Среднее	0,5	0,5
3.4	Комфорт	Средний	0,5	0,5
4	Свобода от риска			
	Смягчение отрицательных последствий:			
4.1	экономического риска	Высокое	1	1
4.2	риска для здоровья и безопасности	Высокое	1	1
4.3	экологического риска	Высокое	1	1
5	Покрытие контекста			
5.1	Полнота контекста	Высокая	1	1
5.2	Гибкость	Низкая	0	0.25

В данном примере значение показателя составило 8. Максимальная возможная оценка равна 9,25.

В качестве альтернативного способа оценки качества геоинформационного ПО предлагается использовать методику оценки качества эталонных пространственных данных в разных системах с использованием мер качества, указанных в [2]. Алгоритм включает в себя следующие шаги.

1. Выбрать элементы качества данных для сравнения (ГОСТ Р 57773-2017).

2. Собрать набор эталонных данных.

3. Импортировать данные в проверяемые системы.

4. Рассчитать меры качества.

В таблице 2 приведен пример результата оценки программы по методике, указанной выше.

ТАБЛИЦА 2. Пример оценки качества ГИС путем сравнения качества пространственных данных

№ п/п	Мера качества	ГИС 1	ГИС 2
1.1	Коэффициент избыточных элементов	0	0
1.2	Коэффициент избыточных элементов	0	0
2.1	Уровень согласованности с правилами концептуальной схемы	-	0
2.2	Степень согласованности области значений	1	0.8
2.3	Частота конфликтов физической структуры	0	0.11
2.4	Количество недопустимых «разрывов»	-	-
4.1	Степень некорректности классификации	-	0.1

Процедура оценки качества (рис. 1) может включать в себя одну из предложенных методик, однако наилучший результат получается при использовании обоих подходов.

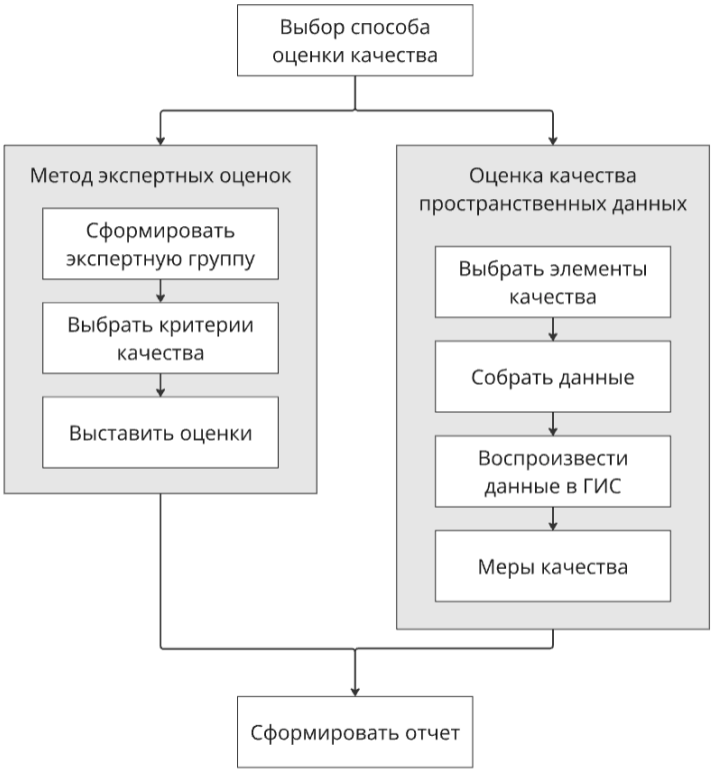


Рис. 1. Процедура оценки качества ГИС

Список используемых источников

1. ГОСТ Р 25010-2015 – Требования и оценка качества систем и программного обеспечения. Модели качества систем и программных продуктов М.: Стандартинформ, 2015. 29 с.

2. ГОСТ Р 57773-2017 – Пространственные данные. Качество данных М.: Стандартинформ, 2017. 133 с.

3. Маслов Ю.Г. О методике сравнения программных продуктов // Информационная безопасность, № 2, 2007 [Электронный ресурс]. URL: https://lib.itsec.ru/articles2/control/ometodike sravneniya programmnih produktov (дата обращения 17.03.2023).

METHOD OF ASSESSING THE QUALITY OF GEOINFORMATION SOFTWARE

Prokofev P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper presents a methodology for assessing the quality of geoinformation software. Quantitative and qualitative criteria for assessing software are considered. The proposed approach includes the use of GOST standards, as well as the use of methods characteristic of geoinformation software. Recommendations are given for improving the process of assessing the quality of geoinformation software.

Key words: *GIS, spatial data, cartography, geographic features, quality assessment*

УДК 621.372.413
ГРНТИ 47.45.99

УСТРОЙСТВА СВЧ НА ПЛАНАРНЫХ НЕРЕГУЛЯРНЫХ ЛИНИЯХ

Э. Ю. Седышев, Е. А. Болдырев, Е. Ф. Иванищева, А. А. Макаров, С. И. Федоров

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

В данной работе рассматривается возможность классификации микроволновых устройств на нерегулярных планарных линиях без связи и со связью. Авторы предпринимают попытку обозначить сферы применения тех или иных видов нерегулярных линий (в том числе и связанных). Работа содержит результаты макетирования и экспериментальных исследований.

микроволновая электроника, СВЧ, планарные линии, связанные линии, устройства частотной селекции, излучатели с нерегулярными «плечами»

Нерегулярные линии СВЧ находят широкое применение в микроволновой электронике, они являются основными элементами делителей мощности, мостовых схем, устройств частотной селекции и согласования.

На сегодняшний день известны работы, посвященные данной тематике. В основном это публикации по отдельным устройствам на *нерегулярных планарных линиях (*НПЛ). Классификация микроволновых устройств по типу применяемых линий и типов связей на данный момент отсутствует.

Для начала рассмотрим основные типы нерегулярных линий, которые наиболее часто используются в микроволновой электронике.

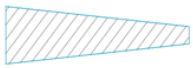
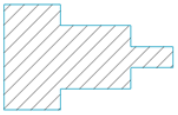
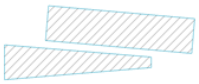
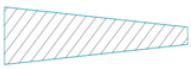
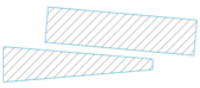
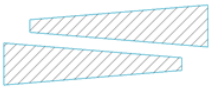
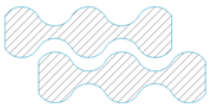
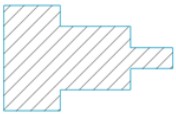
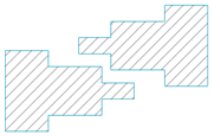
Можно выделить основные два класса НПЛ. К первому классу отнесем НПЛ со скачкообразным изменением волнового сопротивления, этот класс использует интерференцию волны, а в устройствах одновременно существуют как бегущие, так и стоячие волны (смешанная волна). Вторым классом НПЛ может быть класс с плавным изменением волнового сопротивления, эти линии также работают со смешанной волной, хотя уровень согласования у них выше, чем у предыдущих и в устройствах преобладает бегущая волна. Устройства, которые включают в себя скачкообразное и плавное изменение волновых параметров, сегодня практически неизвестны.

Очень хорошо известны в литературе различные инженерные методы расчета волновых сопротивлений [1]. Эти методы легко позволяют рассчитать волновые сопротивления классических регулярных полосковых линий.

При наличии связей и введения эффективных геометрических размеров полные (четная и нечетная моды) сопротивления связанных линий считаются уже с большой погрешностью [2], при этом с ростом связи погрешность расчета возрастает и может достигать 15...25 % [3, 4, 5].

Рассмотрим возможные виды связей между различными типами линий, сведем их в таблицу 1 (Регулярные связи на различных типах линий).

ТАБЛИЦА 1 Регулярные связи на линиях.

	 Прямоугольная линия	 Трапециевидная линия	 Волнообразная линия	 Ступенчатая линия
 Прямоугольная линия	 Линии регулярны		Регулярная связь невозможна из-за формы линий	Регулярная связь невозможна из-за формы линий
 Трапециевидная линия			Регулярная связь невозможна из-за формы линий	Регулярная связь невозможна из-за формы линий
 Волнообразная линия	Регулярная связь невозможна из-за формы линий	Регулярная связь невозможна из-за формы линий		Регулярная связь невозможна из-за формы линий
 Ступенчатая линия	Регулярная связь невозможна из-за формы линий	Регулярная связь невозможна из-за формы линий	Регулярная связь невозможна из-за формы линий	

Регулярные связи довольно широко применяются в устройствах микроволновой электроники. Связанные линии находят широкое применение в узкополосных микроволновых фильтрах, которые широко представлены на рынке, а методики их синтеза известны более 60 лет.

Сразу же оговоримся, что все устройства на НПЛ без связи и со связью носят эксклюзивный характер, общие методики их синтеза отсутствуют. Так, например, ступенчатые устройства согласования представляют собой

каскад убывающих или возрастающих волновых сопротивлений отрезков линий одинаковой длины. По сути, разработчики имеют дело с классической лестничной схемой, которая не дает представления о всех возможных схемах согласования.

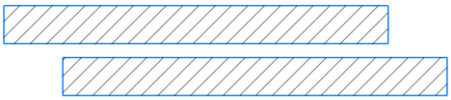
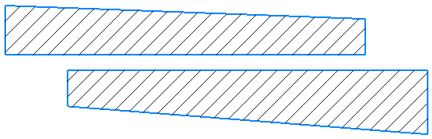
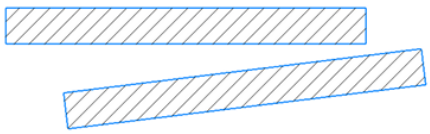
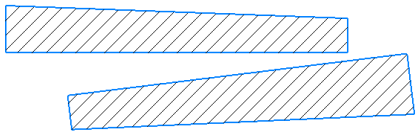
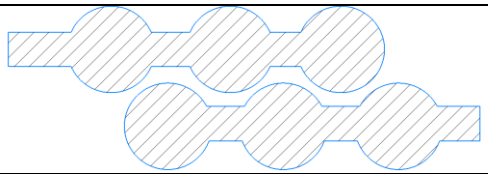
Связь между планарными линиями также можно подразделить на два основных класса. В таблице 2 к первому классу отнесем регулярную связь, а второй класс объединит всевозможные виды нерегулярных связей.

ТАБЛИЦА 2. Виды связи регулярных и нерегулярных линий

Связь первого класса	Связь второго класса
Регулярная связь	Нерегулярная связь Периодическая и непериодическая Симметричная и несимметричная Логарифмическая связь Полиномиальная связь и т.д.

В таблице 3 представлены некоторые из перечисленных видов связи.

ТАБЛИЦА 3. Различные виды связи на регулярных и нерегулярных линиях

Вид связи	Пример
Регулярная связь на регулярной линии	
Регулярная связь на нерегулярной линии	
Нерегулярная связь на регулярной линии	
Нерегулярная связь на нерегулярной линии	
Периодическая связь	

Для того, чтобы понять целесообразность использования нерегулярностей в СВЧ-устройствах, были проведены исследования с полосно-пропускающим фильтром смоделированном на регулярных и нерегулярных линиях с различными видами связи. Для исследования был синтезирован макет «резонатор типа дуга», представляющий собой регулярную линию с регулярной связью (рисунок 1). Дальнейшие изменения геометрии и исследования проводились в САПР RFSim 99.



а б

Рис. 1. а) макет шлейфного резонатора типа «дуга» с регулярной связью; б) экспериментальная АЧХ

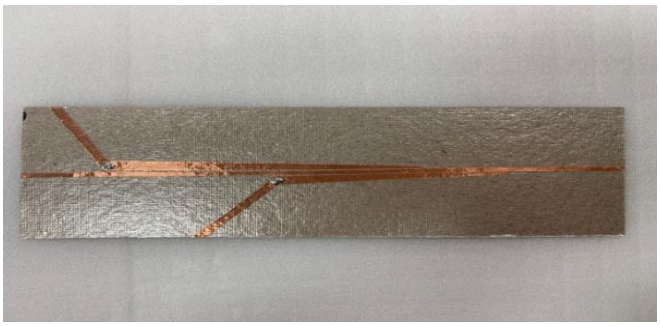
Стоит отметить, что полученные результаты моделирования ППФ в САПР RFSim 99 близки к реальным значениям макета. Результаты проведенных исследований позволяют сделать вывод, что применение нерегулярностей приводит к расширению полосы пропускания и увеличению центральной частоты фильтра.

Интерес к нерегулярным линиям отражен в статьях зарубежных и отечественных авторов. Все чаще возникают идеи создания систем описания связанных линий, которые бы облегчили расчеты. Очевидно, что при наличии периодических изменений волнового сопротивления одиночной линии в ее структуре возникают участки с емкостными и индуктивными параметрами, что отражается на частотно-селективных свойствах структуры в целом, использование же таких линий в паре приводит к устройствам направленного ответвления.

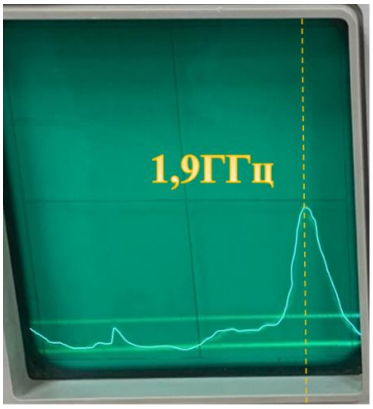
Группе синтеза СВЧ устройств при Санкт-Петербургском государственном университете телекоммуникаций удалось синтезировать ряд устройств мультиплексирования и частотной селекции на нерегулярных линиях без связи и со связью.

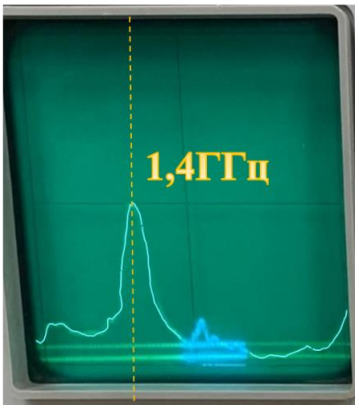
На рисунке 2 представлен макет частотно-зависимого направленного ответвителя и его характеристики.

Данный макет предоставляет возможность ответвлять сигнал на различных частотах по уровню примерно в − 5 дБ, как и в случае классического НО уровень ответвления в первую очередь зависит от уровня связи между ведущей и ответвляющей линией.



а





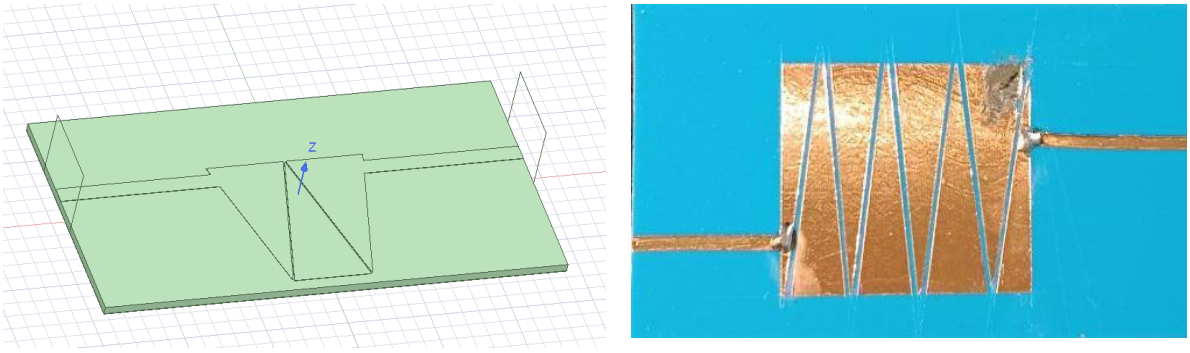
б в

Рис. 2. а) макет направленного ответвителя на нерегулярных линиях, б) характеристика по пути 1-2, в) по пути 1-4

Представленный макет содержит два рабочих плеча, их количество ограничено техническим заданием и габаритами платы. Подобные структуры предлагается использовать в устройствах детектирования сигнала на различных частотах, главной задачей в этом случае является компактное размещение элементов связи и детектирования.

Использование подобных треугольных нерегулярных линий позволяет также синтезировать различные частотно-селективные устройства: фильтрующие делители мощности, патч-фильтры, мультиплексеры и т.д. [6, 7, 8]. Также нашей группой была исследована возможность реализации фильтра на связанных нерегулярных линиях, изготовлен макет и проведены из-

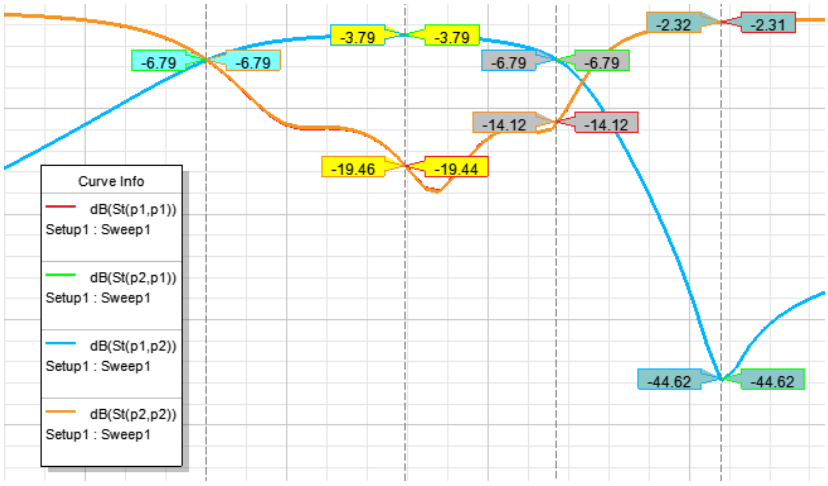
мерения. На рисунке 3 представлена модель устройства и одна из реализаций 8 – элементного фильтра.



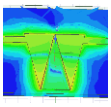
а *б*

Рис. 3. а) модель фильтра на нерегулярных линиях, б) макетное исполнение структуры

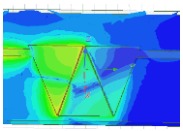
Результаты моделирования структуры показали хорошие результаты согласования в полосе пропускания шириной около 18 %, типичной для данной структуры является близкое положение нуля справа. Размеры модели оставляют возможность подстройки, что важно для микроволновых устройств.



а



б



в

Рис. 4. а) АЧХ фильтра на нерегулярных связанных линиях, б) распределение Е – поля на центральной частоте полосы пропускания, в) в полосе запирания

Довольно перспективной областью применения нерегулярных линий, авторам кажется область интегрированных микроволновых излучателей. Использование нерегулярных линий передачи для согласования широко представлено в инженерной литературе. Как основной пример использование подобного типа линий можно обратиться к четвертьволновому трансформатору на нерегулярной линии с плавным изменением волнового сопротивления [9, 10]. Однако и элементы с несколькими периодами изменения волнового сопротивления показали возможность расширения рабочей полосы даже узкополосных антенн.

Одной из решаемых задач стало исследование неоднородностей, введенных в проводящий слой плоской спиральной антенны Архимеда (рис. 5).

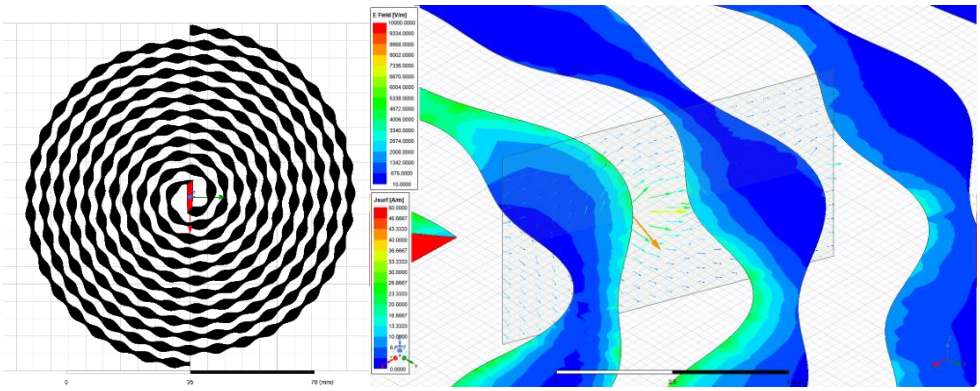


Рис. 5. Модель спиральной антенны с распределением токов и поля в сечении соответствующем активной зоне расчетной частоты

По своей сути проводящая линия спиральной антенны ввиду непропорционального изменения ширины соседних полосков неоднородно видоизменялась [11]. В данном случае классическое описание спиральной антенны Архимеда и рассмотрение ее как некоторого аналога щелевой или копланарной линии затрудняется.

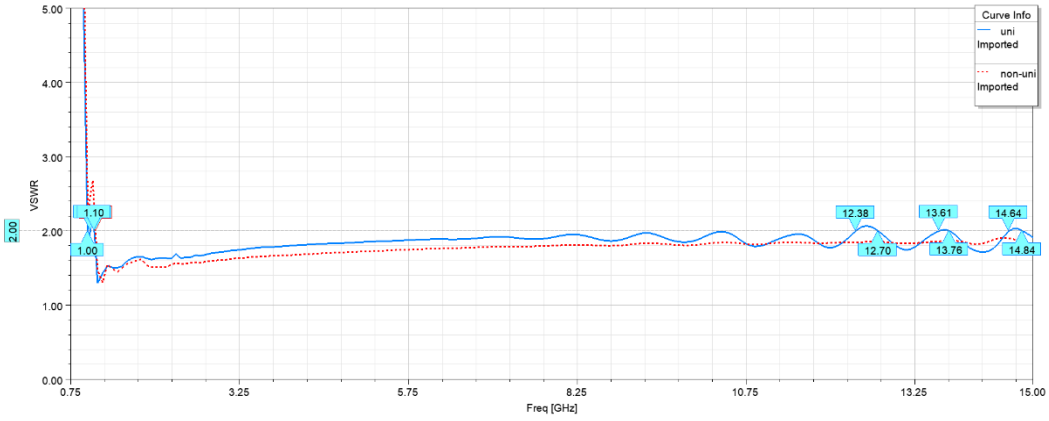


Рис. 6. Сравнение КСВН (1-15ГГц) антенн с постоянной длиной неоднородности (пунктир) и однородной спирали (сплошная линия)

Моделирование проводилось в двух диапазонах 1-15 ГГц (с высокой точностью (и 15-20 ГГц (с более низкой точностью моделирования ввиду ограниченности вычислительных мощностей) (рис. 6). Рассчитанный рабочий диапазон спиральной антенны без неоднородностей составлял порядка 1-20 ГГц.

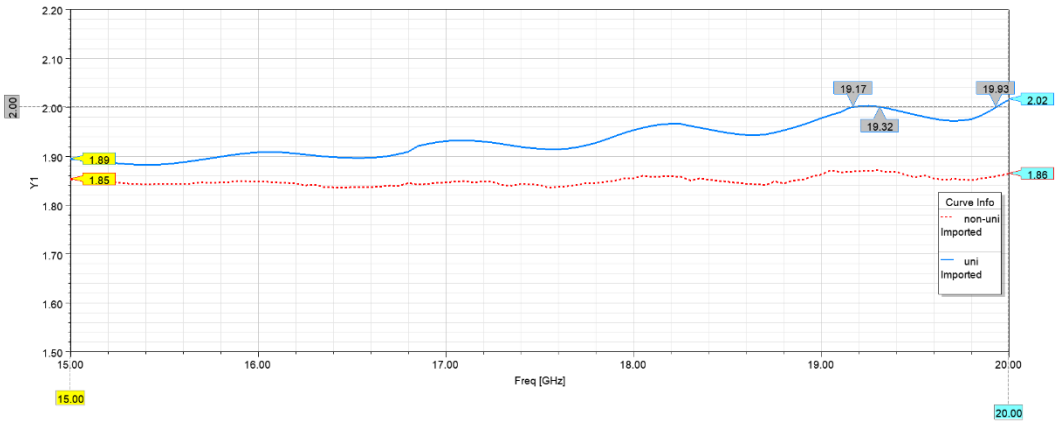


Рис. 7. Сравнение КСВН (15-20 ГГц) антенн с постоянной длиной неоднородности (пунктир) и однородной спирали (сплошная линия)

По итогам моделирования стал очевиден тот факт, что введение неоднородности в спиральную антенну приводит к расширению рабочего диапазона по уровню КСВН без увеличения массогабаритных параметров антенны (рис. 7).

Обобщая результаты работы в целом, можно подчеркнуть, что перед авторами открывается огромный пласт научно-исследовательских изысканий, работы в котором сегодня ведутся во всем мире и весьма противоречиво.

Список используемых источников

1.. Вольман В. И. Справочник по расчету и конструированию СВЧ полосковых устройств / Под ред. В. И. Вольмана. М.: Радио и связь, 1982.

2. Cohu S.B. Characteristic impedance of broadside coupled strip transmission Lines. IEEE Trans., 1960, v. MTT-8, N=11, p. 633-637.

3. Боброва К. В., Булатова И. А., Иванова Е. А., Седышев Э. Ю. Расчет модифицированных линий передач для объемных интегральных схем СВЧ. СПб.: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), 2015. С. 161–170.

4. Гупта К., Гардж Р., Чадха Р. Машинное проектирование СВЧ устройств. М.: Радио и связь, 1987. 432 с.

5. Гвоздев В. И., Нефедов Е. И. Объемные интегральные схемы СВЧ. М.: Наука, 1985. 256 с.

6. Movahedi M. A Compact and Wideband Coupled-Line Coupler with High Coupling Level Using Shunt Periodic Stubs. Radioengineering, 2013. 22(1), 323–327.

7. Jia-Sheng Hong, & Lancaster, M. J. (n.d.). Microstrip triangular patch resonator filters. 2000 IEEE MTT-S International Microwave Symposium Digest (Cat. No.00CH37017). doi:10.1109/mwsym.2000.861002

8. Zhu Y, Wang J, Hong J, Chen J-X & Wu W. Two- and Three-Way Filtering Power Dividers With Harmonic Suppression Using Triangle Patch Resonator', IEEE Transactions on Circuits and Systems I: Regular Papers. 2021. Vol. 68. № 12. PP. 5007-5017. https://doi.org/10.1109/TCSI.2021.3112748

9. Мазепова О. И., Мещанов В. П., Прохорова Н. И., Фельдштейн А. Л., Явич Л. Р. Справочник по элементам полосковой техники. М.: Связь, 1979. 336 с.

10. Баскаков С. И. Радиотехнические цепи с распределенными параметрами: учебное пособие для студентов радиотехнических специальностей вузов / С. И. Баскаков. Изд. 2-е. Москва : URSS, 2011. (Классика инженерной мысли: радиотехника). ISBN 978-5-397-02265-1.

11. Farahani Maryam & Mohammad-Ali-Nezhad, Sajad. A novel UWB printed monopole MIMO antenna with non-uniform transmission line using nonlinear model predictive // Engineering Science and Technology, an International Journal. 2020. 23. 10.1016/j.jestch.2020.05.006.

MICROWAVE DEVICES ON PLANAR IRREGULAR LINES

Sedyshev E., Boldyrev E., Ivanischeva E., Makarov A., Fedorov S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In this paper, the possibility of systematization of microwave devices on irregular planar lines (NAL) without communication and with communication is considered. The authors attempt to identify the areas of application of certain types of irregular lines (including related ones). The work contains the results of mock-up and experimental studies. microwave electronics, microwave, planar lines, connected lines, frequency selection devices, radiators with irregular "arms".

Key words: *microwave electronics, microwave, planar lines, coupled lines, frequency selection devices, emitters with irregular "shoulders"*

УДК 621.373.1
ГРНТИ 47.45.99

СПИРАЛЬНЫЕ АНТЕННЫ НА КОНИЧЕСКОЙ ПОВЕРХНОСТИ В СОСТАВЕ ФАР

Э. Ю. Седышев, Н. И. Глухов, Г. А. Котов, С. И. Федоров

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

В настоящее время развитие беспроводных технологий, включая системы спутниковой связи, увеличивает потребность в антеннах X и Ку – диапазонов. Эти системы должны обеспечивать высокую скорость передачи данных и надежность. Спиральные антенны на конической поверхности отвечают этим требованиям. Антенные решетки на спиральных излучателях перспективны для внедрения в новые поколения телекоммуникационных систем.

спиральные антенны, коническая поверхность, СВЧ-диапазон, широкополосные антенны, компактность и направленность, спутниковая связь и интернет, 5G, IoT, современные материалы и технологии

Спиральные антенны на конической поверхности (рис. 1, 2) представляют собой уникальный класс антенных систем [1, 2, 3, 4], которые сочетают в себе широкополосность, хорошую направленность и компактность. Эти особенности делают их перспективными для использования в современных радиотехнических системах. В данной работе рассмотрены некоторые аспекты, определяющие привлекательность и перспективность таких антенн, а также их потенциальные области применения.

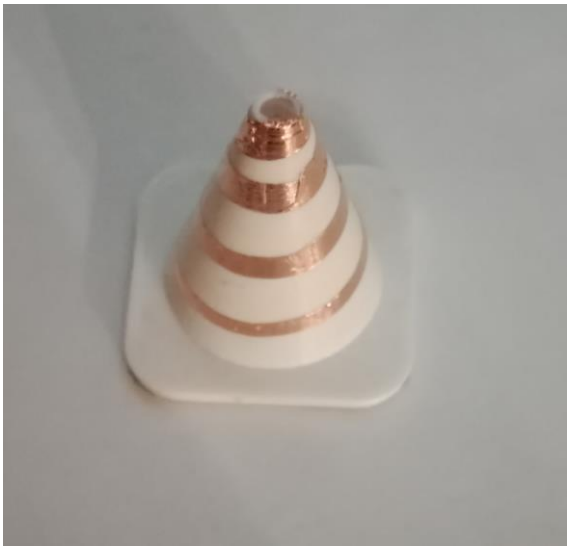


Рис. 1. Макет спирального излучателя на конической поверхности



Рис. 2. Соединение элементов питания внутри конуса

Одним из главных преимуществ спиральных антенн на конической поверхности является их направленность и способность работать в широком диапазоне частот. Это достигается за счет уникальной геометрии антенны, которая позволяет эффективно излучать и принимать сигналы на различных частотах. Такая характеристика особенно востребована в современных системах связи, где требуется поддержка множества стандартов и частотных диапазонов, включая спутниковую связь, радиолокацию и системы беспроводной передачи данных. Расчет различных типов спиралей можно найти в работах сотрудников группы синтеза СВЧ устройств СПбГУТ им. проф. М. А. Бонч-Бруевича [5, 6, 7].

Компактность и эффективность: коническая форма антенны обеспечивает высокую направленность излучения при относительно небольших габаритах. Это делает спиральные антенны привлекательными для использования в мобильных и аэрокосмических системах, где вес и размеры оборудования имеют критическое значение. Например, такие антенны могут быть установлены на борту спутников, беспилотных летательных аппаратов (БПЛА) или в портативных устройствах связи.

Спиральные антенны на конической поверхности демонстрируют высокую надежность и устойчивость к экстремальным условиям эксплуатации, включая перепады температур, вибрации и механические нагрузки. Это делает их идеальными для использования в военных и космических приложениях, где требуется долговечность и стабильность работы. Сами конические элементы могут быть изготовлены как из полимеров, так и керамики.

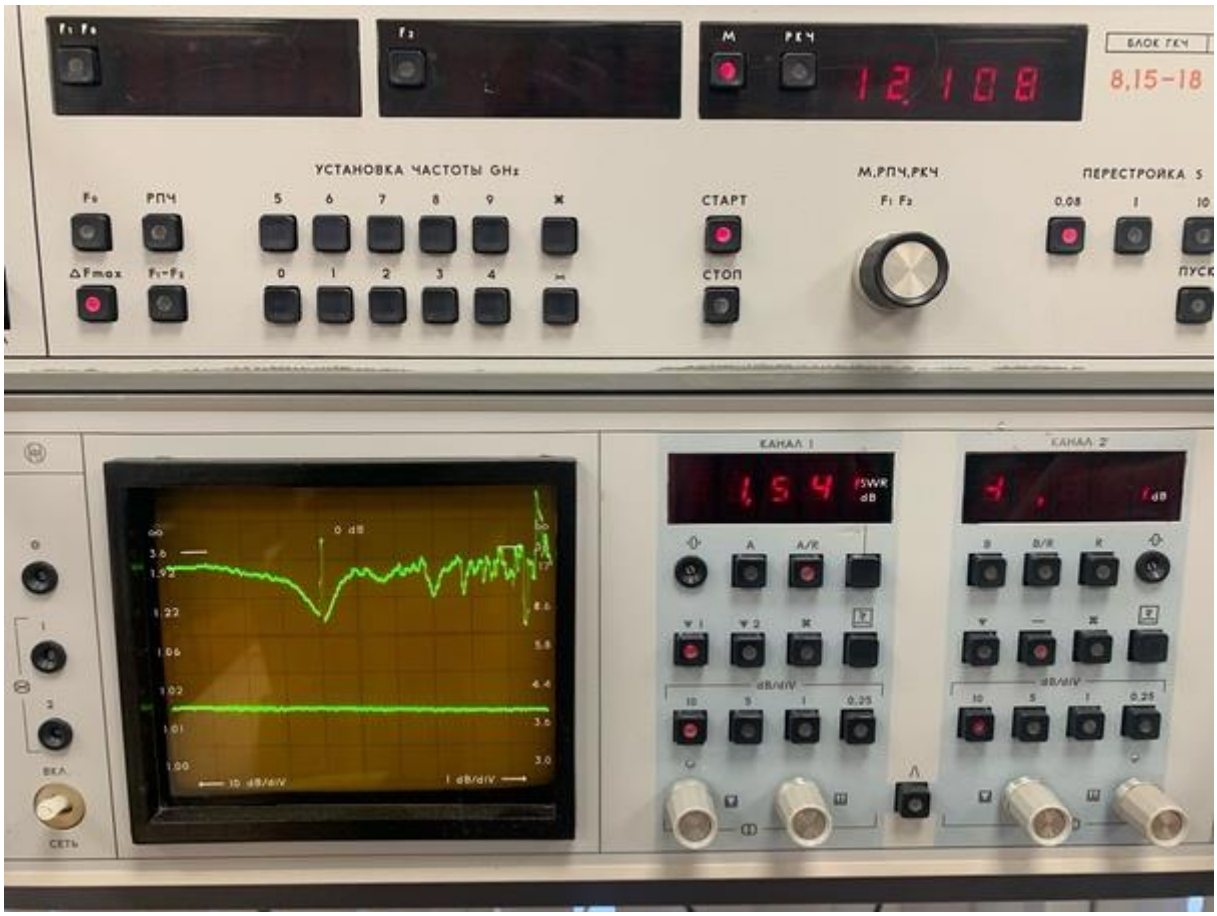


Рис. 3. Частотная характеристика макета излучателя

В рамках данной работы был создан макет одиночного излучателя с образующей конуса 62 мм и радиусом основания порядка 3 сантиметров, диэлектрическая проницаемость материала не превышает 2.2. Макет был изготовлен на 1 частоту за счет использования резонансной системы согласования.

Результаты измерений макета (измерения произведены на панорамном измерителе Р2-116) представлены на рисунке 3, измеренные частотные характеристики следующие: КСВН = 1.6 на частоте 12 ГГц. Характеристика резонансная. Расчетная поверхность для создания ФАР приведена на рисунке 4.

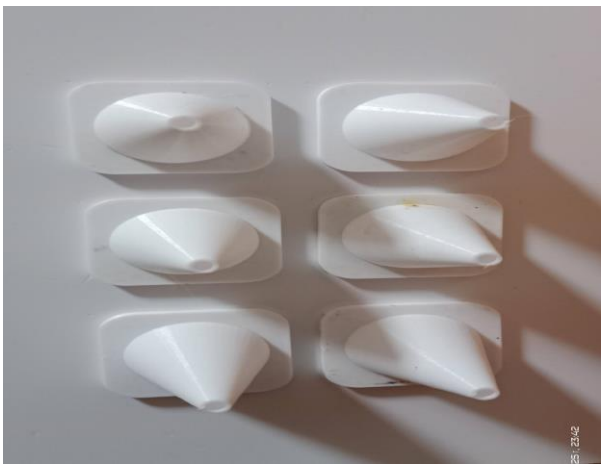


Рис. 4. Общий вид ФАР на конусах

Список используемых источников

1. Ротхаммель К. Антенны. СПб.: Бояныч, 1998. 635 с.

2. Балакирев В. С. Антенны и устройства СВЧ: Учебное пособие. М.: Радио и связь, 2018. С. 45–50.

3. Кинг Р. В., Ву Т. Т. Спиральные антенны: теория и практика. М.: Мир, 2015. С. 120–125.

4. Hansen R. C. Spiral Antennas: A Review // IEEE Transactions on Antennas and Propagation, 2019. Vol. 67. № 5. P. 1234–1245.

5. Ахметов Р. Р., Седышев Э. Ю. Широкополосные контурные антенны для объемных интегральныхсхем СВЧ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017.

6. Покровский Н. А., Седышев Э. Ю. Исследование планарной спирали в ОИС СВЧ. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2017.

7. Покровский Н. А., Седышев Э. Ю. Инженерный метод расчета планарной спиральной антенны СВЧ. Электроника и микроэлектроника СВЧ. Санкт-Петербург, 2017.

SPIRAL ANTENNAS ON A CONICAL SURFACES IN THE COMPOSITION OF FAG

Sedyshev E., Glukhov N., Kotov G., Fedorov S.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

Currently, with the rapid development of wireless technologies such as 5G, Internet of Things (IoT), and satellite internet, there is a growing demand for antenna systems capable of providing high data transfer speeds, reliable communication, and broadband characteristics. Spiral antennas on a conical plane fully meet these requirements due to their unique geometry, compactness, and high efficiency. This makes them one of the most promising solutions for integration into new generations of telecommunication systems.

Key words: *spiral antennas, conical plane, microwave range, broadband antennas, compactness and directivity, satellite communication and radar, 5G and IoT, modern materials and technologies*

УДК 621.396.67
ГРНТИ 47.45.29

ИСПОЛЬЗОВАНИЕ НЕРЕГУЛЯРНЫХ ЛИНИЙ ПРИ СИНТЕЗЕ СПИРАЛЬНЫХ АНТЕНН

Э. Ю. Седышев, С. И. Федоров

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

Синтез широкополосных антенн является актуальной задачей, поскольку они применяются в различных радиотехнических системах. Одним из способов улучшения их характеристик является использование нерегулярных линий, то есть линий передачи с изменяющимся поперечным сечением или электромагнитными свойствами среды. В статье рассматривается влияние нерегулярностей первого типа на рабочие характеристики спиральной антенны.

спиральная антенна, широкополосность, нерегулярные линии

В настоящее время вопрос синтеза широкополосных антенн стоит на повестке дня, т.к. антенны с широкой рабочей полосой находят свое применение в различных радиотехнических системах.

Одним из способов улучшения рабочих характеристик антенны является использование нерегулярных линий. Нерегулярной линией называется линия передачи, в продольном направлении которой изменяется ее поперечное сечение или электромагнитные свойства, заполняющих линию, сред [1]. Одним из примеров полезного устройства, реализуемого на нерегулярной линии, является четвертьволновый трансформатор с плавным переходом (в отличии от классического ступенчатого перехода) [2]. Стоит отметить, что элементы с более сложной геометрией также продемонстрировали возможность улучшения рабочих характеристик антенн [3].

В данной статье основной задачей стояло рассмотрение влияния введенных нерегулярностей в проводящий слой спиральной антенны.

Для исследования влияния нерегулярностей на характеристики спиральной антенны следовало выбрать некоторую исходную структуру для последующей модификации.

За основу была выбрана плоская двухзаходная антенна на спирали Архимеда со следующими параметрами (рис. 1):

1. Ширина проводящей линии – 2 мм;
2. Количество витков – 6;

3. Зона питания - 180°;
4. Диаметр – 100 мм.

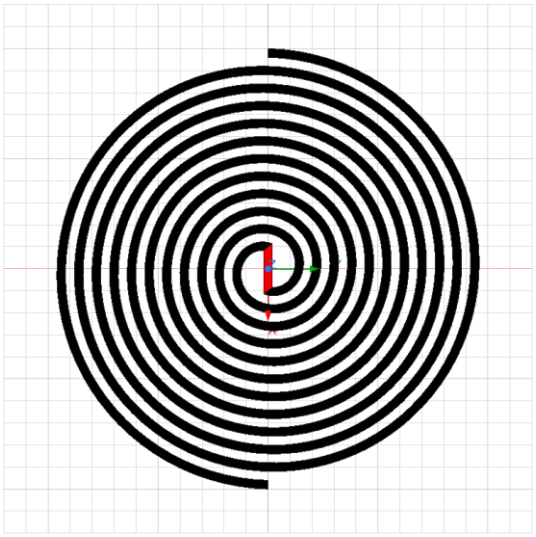


Рис. 1. Немодифицированная спиральная антенна

После моделирования описанной антенны был получен график зависимости КСВН соответствующий ожиданиям (рис. 2). Описанная структура начинает работать на частоте порядка 1.1 ГГц – близкой к рассчитанному значению нижней рабочей частоты. Рассчитанная же верхняя частота составляет порядка 20 ГГц. Для сокращения времени расчёта первичное моделирование проводилось до 15 ГГц. На данной частоте для вышеописанной структуры уже начинало наблюдаться ухудшение рабочих характеристик антенны.

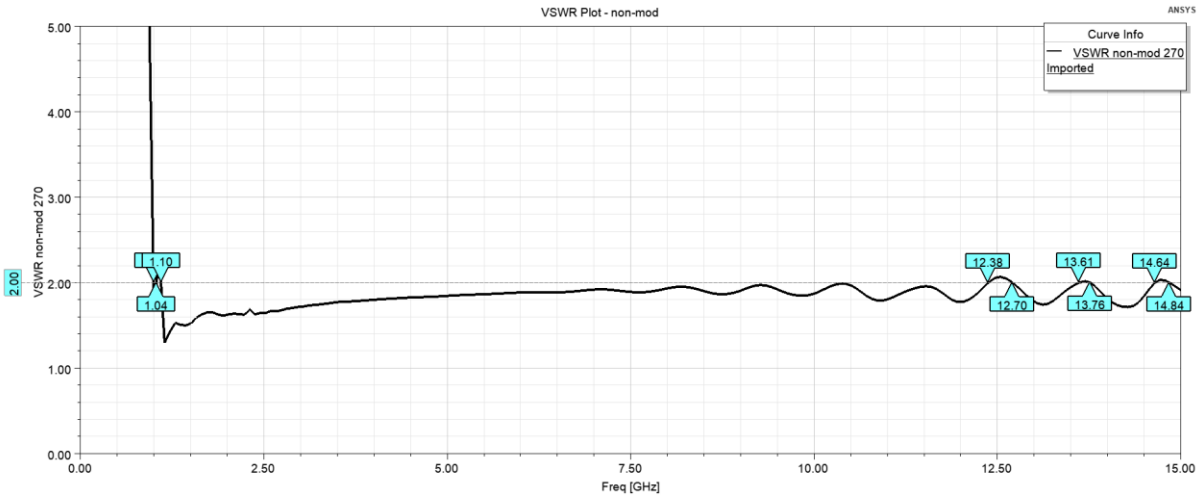


Рис. 2. КСВН немодифицированной спиральной антенны

Следующим шагом следовало ввести в рассчитанную и промоделированную немодифицированную антенну нерегулярность. Для исследования

было выбрано два типа нерегулярностей – оба «гармонические», однако первый вариант обладал одинаковой протяженностью сегмента нерегулярности (рис. 3 а), а второй – изменяющейся пропорционально протяжённости активной зоны спиральной антенны (рис. 3 б).

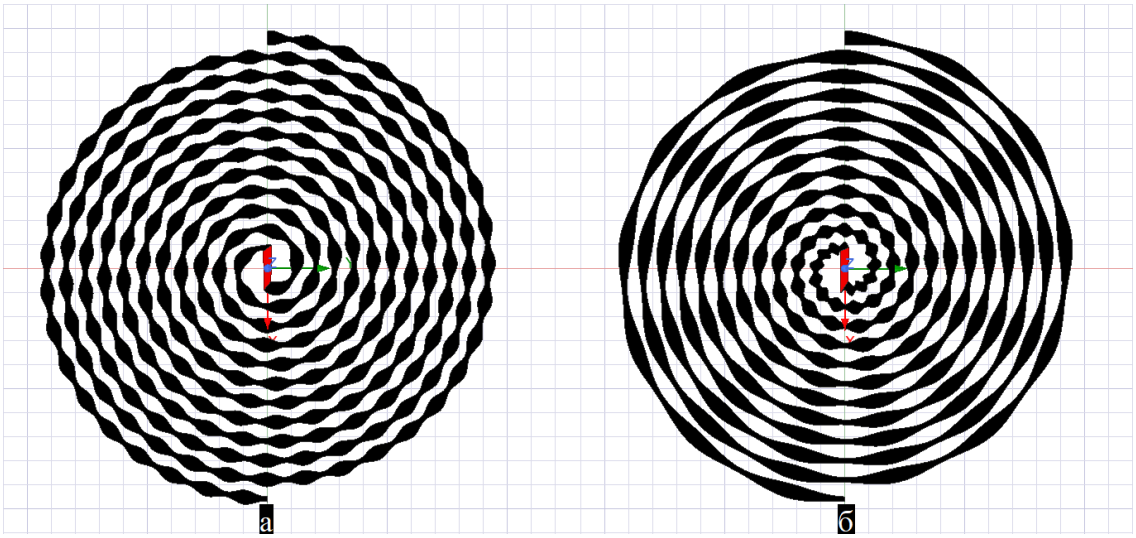


Рис. 3. Спиральные антенны с нерегулярностями: а – одинаковой длинны, б – с изменяющейся длиной

В первом случае нерегулярность (изменение ширины полоска) составляет 1 мм, протяженность каждого сегмента порядка 8.5 мм. Во втором случае длина сегмента с нерегулярностью изменяется в зависимости от положения сегмента на спиральной антенне, а нерегулярность так же составляет 1 мм.

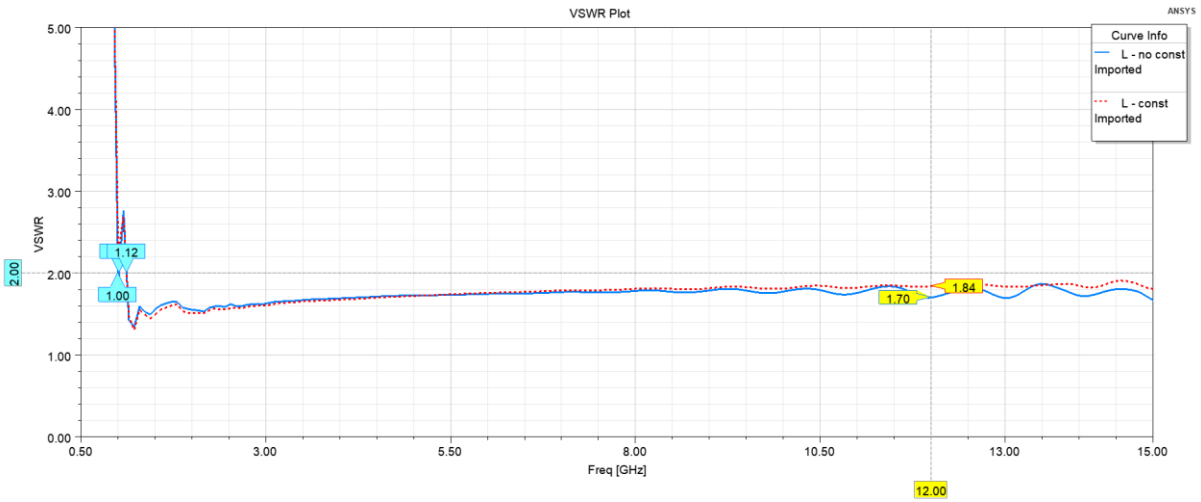


Рис. 4. Сравнение КСВН моделей с постоянной длиной нерегулярности (пунктир) и с нерегулярностью переменной длины (сплошная линия)

Первичное сравнение графиков (рис. 4) практически не показало различий в значении и динамике изменения КСВН, единственным отличием

являлось чуть лучшее его значение в верхней части исследуемого диапазона частот при введении нерегулярностей различной длины.

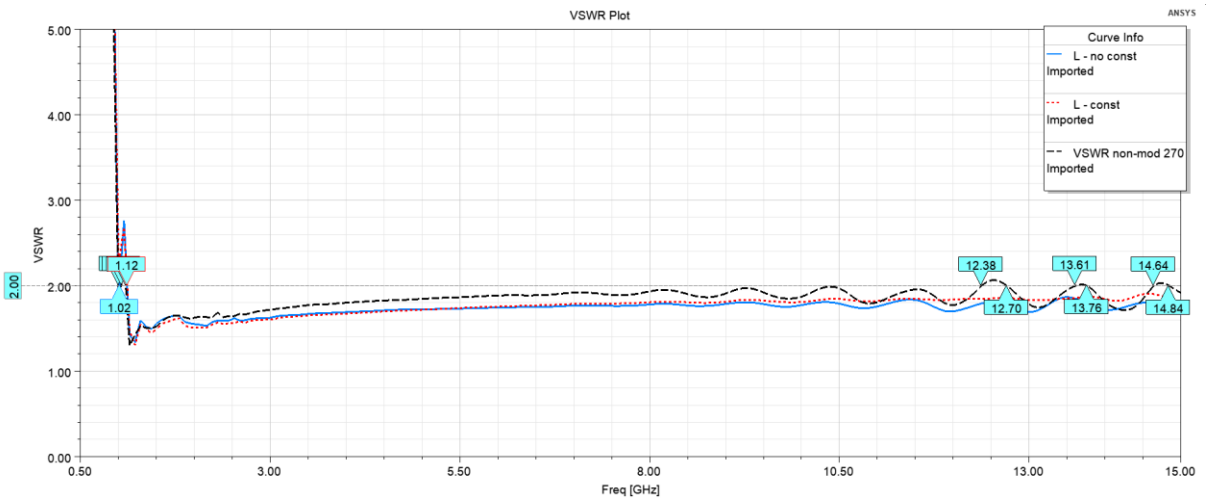


Рис. 5. Наложение графиков рис. 1 и рис. 2

Наложение всех графиков наглядно показало, что по уровню КСВН все три антенны очень схожи, однако динамика изменения графиков в области верхних рабочих частот сподвигла к расширению исследуемого диапазона до 20 ГГц. Данное увеличение, однако сопровождалось понижением точности моделирования ввиду ограниченности вычислительных ресурсов.

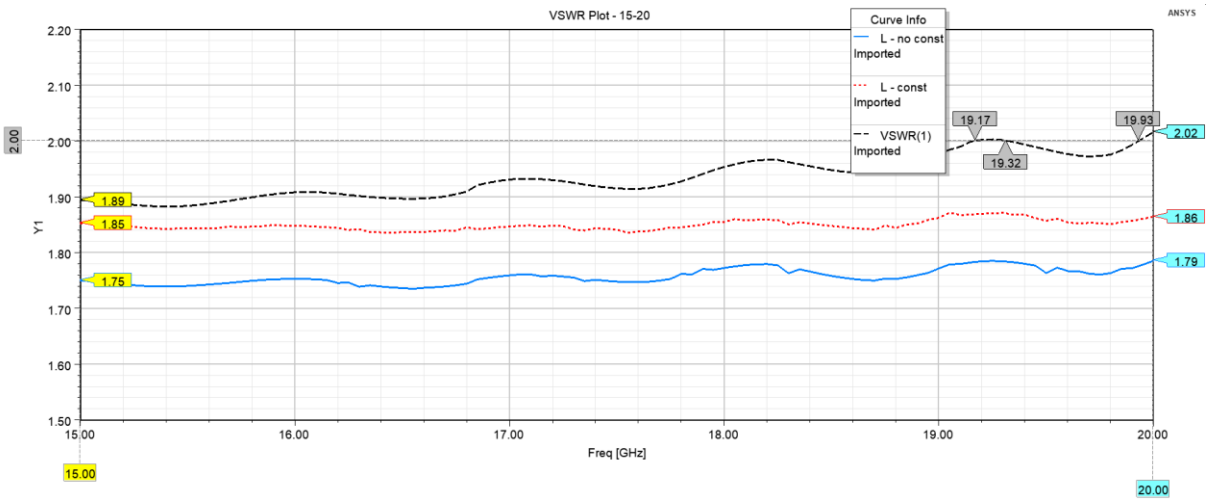


Рис. 6. Зависимость КСВН для трёх случаев в диапазоне 15-20 ГГц

Анализируя полученные зависимости КСВН для диапазона 15-20 ГГц стоит отметить следующие факты:

1. Введение нерегулярностей обоих типов, при сохранении способа питания спиральной антенны, позволяет несколько улучшить КСВН во всем рабочем диапазоне антенны;

2. Введение нерегулярностей обоих типов позволяет несколько расширить рабочий диапазон антенны (по уровню КСВН = 2);

3. Введение нерегулярности с протяженностью вставки пропорциональной длине активной зоны спиральной антенны дает лучшее согласование в области верхних рабочих частот.

Так же стоит упомянуть, что изменение различных параметров в уравнении для нерегулярностей одного типа приводит к появлению целого рода подобных, но отличающихся геометрически структур.

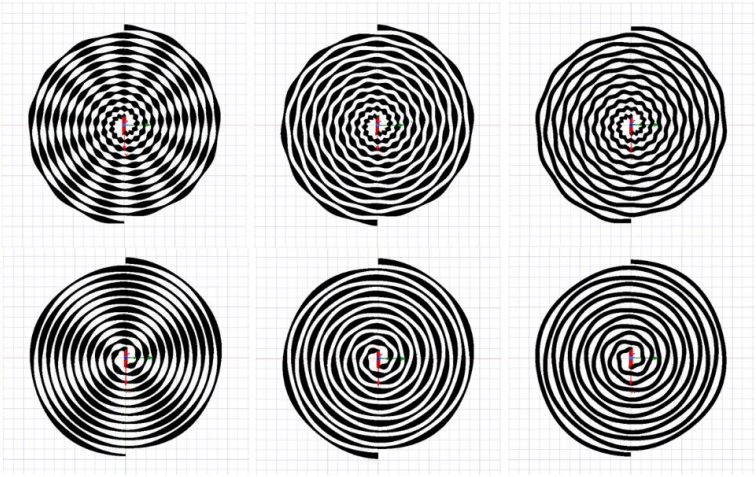


Рис. 8. Варианты спиралей – вариация уравнения для модели с различной длинной нерегулярности

Список используемых источников

1. Сазонов Д. М. Антенны и устройства СВЧ: учебник для вузов. М.: Высш. школа, 1988. 430 с.

2. Баскаков С. И. Радиотехнические цепи с распределенными параметрами: учебное пособие. Изд. стереотип. М.: Книжный дом «ЛИБРОКОМ», 2021. 152 с. (Классика инженерной мысли: радиотехника).

3. Farahani Maryam & Mohammad-Ali-Nezhad Sajad. A novel UWB printed monopole MIMO antenna with non-uniform transmission line using nonlinear model predictive. Engineering Science and Technology, an International Journal. 2020. 23.

USE OF NON-UNIFORM LINES IN SPIRAL ANTENNA SYNTHESIS

Sedyshev E., Fedorov S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The synthesis of broadband antennas is a relevant task, as they are utilized in various radio engineering systems. One of the methods to enhance antenna characteristics is the use of non-uniform lines - transmission lines with variable cross-sections or differing electromagnetic properties of the medium. This article examines the impact of irregularities on the performance of a spiral antenna.

Key words: *spiral antenna, wideband, non-uniform lines*

УДК 621.396.946
ГРНТИ 47.05.15

РАСЧЕТ МИНИМАЛЬНО ВОЗМОЖНОГО РАССТОЯНИЯ МЕЖДУ РАДИОЭЛЕКТРОННЫМИ СРЕДСТВАМИ В БЕСПРОВОДНЫХ СЕТЯХ ВЫСОКОЙ ПЛОТНОСТИ

О. А. Симонина, А. В. Бобровский

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

В докладе показано, что при переходе к сетям высокой плотности пока не существует определения термина "высокая плотность". Таким образом, в настоящее время не заданы минимальные требования к расстоянию между радиоэлектронными устройствами (РЭС), что приводит к вольной трактовке данного термина. Проведенные расчеты границ ближней зоны позволили найти зависимость между частотным диапазоном и минимально допустимым расстоянием между РЭС в сетях высокой плотности.

беспроводные сети высокой плотности, РЭС, частотный диапазон

В настоящее время в некоторых работах принято считать, что сети высокой плотности – это сети на основе стандартов IEEE 802.11, при этом на 1 м^2 расположено одно устройство [1]. Также можно встретить термин «сети сверхвысокой плотности» [2], который относится к сетям 6-го поколения и предполагает возможность размещения до 100 устройств на 1 м^3. Существуют публикации [3], в которых исследуются различные сценарии взаимодействия между устройствами в таких сетях. Сети высокой и сверхвысокой плотности могут быть в том числе гетерогенными, т.е. реализованными с использованием различных технологий. Однако несмотря на то, что данные статьи обозначают большой пласт задач, которые нужно решить для успешного развертывания таких сетей, научно обоснованного определения как сетей высокой плотности, так и сетей сверхвысокой плотности пока не существует.

Для реализации таких сетей необходимо решить несколько задач:

– определение оптимального частотного спектра, как в вопросе ширины, так и в вопросе центральной частоты, для условий значительного количества устройств поблизости и высокой потребности в пропускной способности сети [4];

– подбор оптимального метода доступа к каналу, выбор которого значительно осложнен именно количеством устройств с одинаковым приоритетом [4];
– выбор модуляционно-кодирующей схемы для удовлетворения современных потребностей в пропускной способности, учитывая высокое количество помех от соседних устройств и крайне быстрое изменение характеристик канала, так же является важным фактором;
– организация мобильности абонентов между разными организаторами сетей, учитывая значительное наложение сетей в пространстве и большое количество подвижных абонентов.

Если же планировать реализацию гетерогенной сети, то добавляется значительное количество дополнительных задач [5], таких как синхронизация между различными типами сетей, анализ их взаимного влияния друг на друга в ограниченном пространстве, создание алгоритмов оптимального взаимодействия и выбора типа сети для определенной задачи.

Как видно из работ различных авторов [1-5], для построения сетей высокой плотности существует множество проблем как физического, так и более высоких уровней. Одной из самых важных задач при построении сетей высокой плотности является проблема обеспечения электромагнитной совместимости (ЭМС). Для сетей Wi-Fi такие задачи решаются с использованием изменения архитектуры сети на неоптимальную, с подключением большого количество оконечных устройств к одной точке доступа, что позволяет уменьшить помеховое воздействие [6]. При этом пропускная способность таких сетей, являющихся одноканальными и полудуплексными, напрямую зависит от количества подключенных к точке доступа устройств, и, конечно, с увеличением подключений возможности передачи информации существенно падают. Хотя стандарт IEEE 802.11ax позволяет частично решить эту проблему модернизацией канального уровня, вопрос обеспечения ЭМС в таких сетях также остается нерешенным.

Как видно из тенденции последних пары лет, увеличение количества устройств, и, соответственно, увеличение плотности сетей – процесс неостановимый. Но все же есть определенные факторы, не связанные с желанием потребителя, которые смогут частично ограничить этот рост. Известно, что излучения электромагнитных помех можно рассматривать в ближней и дальней зоне [7]. Данные зоны отличаются тем, что в ближней зоне еще не сформирована электромагнитная волна, ее магнитная и электрическая составляющие рассматриваются отдельно. Соотношение электрической и маг-

нитной составляющих сильно зависит от конструктивных особенностей источника. В дальней зоне электромагнитная волна полностью сформирована, энергия распределена между электрической и магнитной составляющей равномерно. Граница между этими зонами определяется как [8]:

$$r = \frac{\lambda}{2\pi}.$$

Считается, что дальняя зона начинается на расстоянии r ≥ 3λ, на котором электромагнитную волну можно считать полностью сформированной. Зона формирования электромагнитной волны называется переходной [8] (рис. 1).

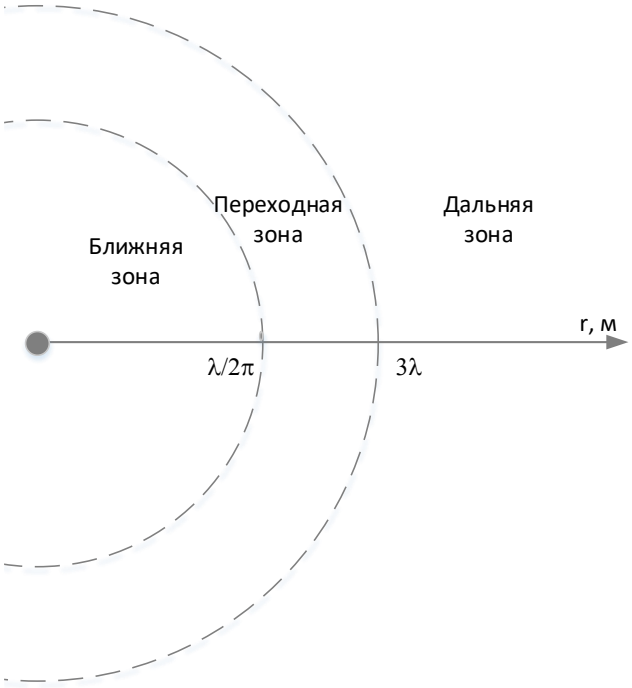


Рис. 1. Граница дальней зоны для точечного излучателя

Таким образом, можно определить границу дальней зоны как критерий для задания минимально возможного расстояния между устройствами в сетях высокой и сверхвысокой плотности. При этом минимальное расстояние будет зависеть от частоты и размеров и геометрических особенностей излучателя.

На начальном этапе примем излучатель как точечный объект с изотропным излучением. Тогда минимально возможное расстояние для устройств высокой плотности в зависимости от частоты можно найти как:

$$r = 3\frac{2{,}99 \cdot 10^4}{F(\text{МГц})}.$$

Рассчитаем минимально возможное расстояние между излучателями в сетях высокой плотности и построим зависимость для части диапазона СВЧ (рис. 2). Таким образом, на частоте, например, 2,4 ГГц устройства не должны быть расположены ближе, чем 37,5 см, что согласуется с принятым в Wi-Fi требованием не более 1 устройства на м^2 [1,6].

Учитывая существование такого типа сетей как BAN (Body Area Network) [9], где устройства расположены крайне близко, и зачастую гораздо ближе, чем 37,5 см из примера выше, для таких сетей необходимо искать другое решение. Это связано с тем, что сети BAN являются сетями очень высокой плотности, где на 1 м^2 может располагаться 5 устройств. Как показано на рис. 2, критическое расстояние между устройствами с ростом частоты уменьшается, следовательно, одним из вариантов для повышения допустимой плотности устройств является переход на значительно большие рабочие частоты несмотря на то, что это может вызывать некоторые технические трудности.

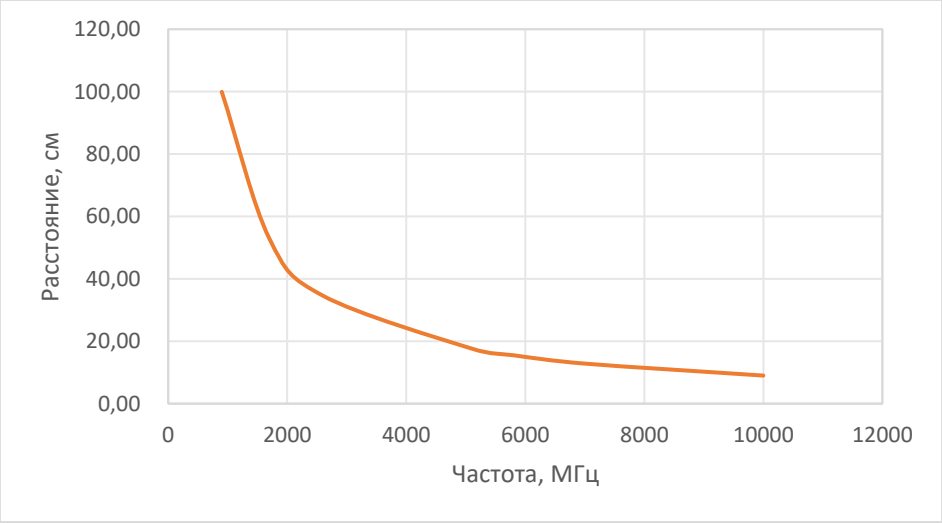


Рис. 2. Зависимость минимально возможного расстояния между устройствами в сетях высокой плотности для популярного диапазона СВЧ

Данный результат не учитывает взаимное расположение устройств, геометрические особенности излучателей, класс излучения и другие характеристики, что требует дальнейших исследований. Минимально возможное расстояние определяет только физические ограничения на взаимное расположение радиоэлектронных средств. Также в дальнейшем имеет смысл разработать методику выбора частотного диапазона и параметров радиосигнала исходя из архитектуры сети и требований к плотности размещения устройств.

Список используемых источников

1. Парамонов А. И., Бушеленков С. Н. Анализ задач и модели многопутевой маршрутизации в сетях интернета вещей // 77-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио: сб. докладов [Электронный ресурс] / СПбГЭТУ «ЛЭТИ». Санкт-Петербург. 2022. С. 117-120.

2. Тонких Е. В., Разработка и исследование методов планирования сетей связи высокой плотности: дис. канд. техн наук: 2.2.15. СПб, 2021. 139 с.

3. Мутханна А. С. А. Модель интеграции граничных вычислений в структуру сети «воздух-земля» и метод выгрузки трафика для сетей интернета вещей высокой и сверхвысокой плотности // Труды учебных заведений связи. 2023. Т. 9. № 3. С. 42-59.

4. Al-Dulaimi A. et al. Planning of ultra-dense wireless networks //IEEE Network. 2017. Т. 31. № 2. С. 90-96.

5. An J. et al. Achieving sustainable ultra-dense heterogeneous networks for 5G //IEEE Communications Magazine. 2017. Т. 55. № 12. С. 84-90.

6. Викулов А. С., Парамонов А. И. Введение в сети Wi-Fi с высокой плотностью пользователей //Информационные технологии и телекоммуникации. 2018. Т. 6. № 1. С. 12-20.

7. Шебалкова Л. В., Ромодин В. Б. Электродинамика, антенны и СВЧ-устройства СБЛ. 2020.

8. Мягков Н. Ю., Кирдяев М. М. Проблемы электромагнитной совместимости //Труды Международного симпозиума «Надежность и качество». 2015. Т. 2. С. 303-305.

9. Chen M. et al. Body area networks: A survey //Mobile networks and applications. 2011. Т. 16. С. 171-193.

CALCULATION OF THE MINIMUM POSSIBLE DISTANCE BETWEEN ELECTRONIC DEVICES IN HIGH-DENSITY WIRELESS NETWORKS

Simonina O., Bobrovskyi A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The report shows that in the transition to high-density networks; there has not yet been a definition of the term "high density". Thus, at the present time, the minimum requirements for the distance between radio-electronic devices have not been set, which results in a loose interpretation of the term. The calculations made it possible to determine the relationship between frequency range and minimum allowable distances between distribution zones for high-density network.

Key words: *high-density wireless networks, radio-electronic devices, frequency range*

УДК 621.396.946
ГРНТИ 47.47.31

ВАРИАНТЫ РЕАЛИЗАЦИИ ПРИЕМНИКОВ ДЛЯ СВЕРХШИРОКОПОЛОСНЫХ СИСТЕМ ИМПУЛЬСНОГО РАДИО С ВРЕМЕННЫМИ СКАЧКАМИ

О. А. Симонина, С. А. Кокин

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

В статье исследуется несколько вариантов приемопередатчиков сверхширокополосных систем на основе импульсного радио. Рассматриваются требования к приемопередатчикам и связанные с ними компромиссы в отношении качественных показателей, пропускной способности, технических средств и вычислительной сложности конкретных практических схем. Поясняется влияние на разработку схемы приемника свойств сверхширокополосного радиоканала, собственных помех и помех от других пользователей, частоты дискретизации и методов модуляции. Сравниваются различные СШП приемники с точки зрения рабочих характеристик и по другим важным критериям. В зависимости от применения и требований к приемопередатчику может быть отдано предпочтение различным схемам приема.

СШП, RAKE приемник, импульсное радио, рабочие характеристики приемника

При оптимальной согласованной фильтрации и упрощенных методах, реализуемых с помощью RAKE приемников (множество параллельных корреляторов с оптимальным объединением) и простых приемников с одним коррелятором, принимаемый сигнал сравнивается с местным образцовым сигналом, который необходим для оценивания принятого сигнала с передачей настроечных последовательностей или «вслепую» [1]. Принимаемый сигнал можно сопоставлять и сам с собой, и в этом случае говорят о приемниках с «автокорреляционной» структурой [2]. Если элемент задержки вносит задержку равную нулю, то это будет детектор энергии, в котором умножитель может использоваться как устройство возведения в квадрат. В дифференциальных детекторах задержка равна разности между моментами поступления последовательных импульсов. В схемах с передачей контрольной частоты TR задержка представляет разность между опорным и информационным символами.

На рисунке 1 представлена обобщенная структурная схема СШП приемника. На ней показаны две возможные точки дискретизации: перед умножителем и после интегратора. Первая дает возможность реализовать полностью цифровые, полностью программируемые и гибкие схемы приемников, а вторая позволяет использовать низкую скорость взятия отсчетов при аналоговой входной цепи.

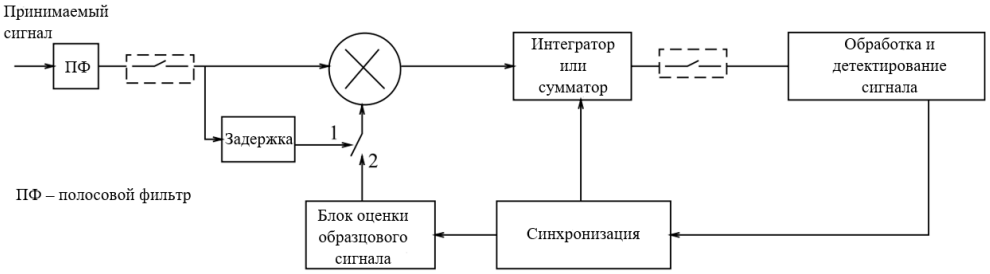


Рис. 1. Обобщенная схема СШП приемника [3]

Оптимальная согласованная фильтрация. Основной принцип согласованной фильтрации заключается в оценке копии принимаемого сигнала и использовании ее в качестве фильтра для получения максимальной помехозащищенности SNR на выходе. В каналах с аддитивным белым шумом согласованная фильтрация обеспечивает оптимальный прием для минимизации вероятности ошибки. Реализовать ее можно с помощью приемника типа RAKE, в котором образцовыми сигналами служат оцениваемые принятые импульсы. Затем производится их оптимальное объединение методом суммирования дифференциально-взвешенных сигналов MRC.

Если шум не белый, как в случае сосредоточенных помех или помех многостанционного доступа, согласованная фильтрация не дает оптимального решения. Наиболее практичный метод подавления помех многостанционного доступа в системах импульсного радио представляют приемники с отбрасыванием импульсов. Они хорошо работают при большом количестве импульсов на символ N и относительно малом количестве искаженных. Приемник с «мерцающим» эффектом [4] предполагает наличие информации о кодовых последовательностях ТН всех пользователей для определения искаженных импульсов и их отбрасывания. Выделители чипов устанавливают оптимальный порог для отсчетов на выходе согласованного фильтра, отбрасывая искаженные импульсы до принятия решения по символу.

Схема с передачей контрольной частоты – TR. Принцип работы таких схем заключается в передаче модулированных импульсов данных вместе с опорным немодулированным импульсом. Если задержка опорного немодулированного импульса меньше, чем время когерентности канала, влияние канала на опорные и информационные импульсы одинаково. Опорные импульсы выполняют функции образцовых сигналов, сопоставляются с информационными импульсами и используются при демодуляции. В данном случае точная оценка параметров канала в приемнике не требуется, что делает системы с передачей контрольной частоты TR привлекательными при передаче по сильно искажающему каналу. Однако схема TR требует точной линии задержки для синхронизации импульсов. Несоответствие задержек ухудшает качество, снижает помехозащищенность SNR и повышает коэффициент ошибок BER. Оно связано с корреляционными свойствами формы принимаемого импульса.

Еще одна серьезная проблема схем TR – использование зашумленных образцовых сигналов для корреляции. Эту проблему можно решить усреднением опорных импульсов для получения «чистого» образцового сигнала. При усреднении нужно учитывать изменения канала, кроме случаев, когда он стационарен. Использование информационных импульсов повышает надежность детектирования символов. Дисперсия шума в образцовом сигнале снижается с увеличением числа усредняемых импульсов.

Дифференциальный детектор работает аналогично схеме с передачей контрольной частоты TR, но вместо опорных импульсов использует информационные импульсы от предыдущего символа [2]. Это требует относительного кодирования передаваемых бит перед модуляцией для хранения информации в разности двух последовательных символов.

Образцовые сигналы содержат шум, ухудшающий характеристики приемника, а задержка, равная длительности символа, снижает стойкость к ошибкам синхронизации. Как и в схемах TR, точность установки задержек в передатчике и приемнике влияет на качественные показатели. Даже небольшая разница задержек существенно ухудшает характеристики.

Детектор мощности представляет собой субоптимальную схему некогерентного приема СШП сигналов импульсного радио, которая может быть реализована с использованием модуляции типа АМН (OOK) или ФИМ (PPM). При использовании АМН устанавливается порог: если мощность ниже порога, принимается "0", если выше – "1". Оптимальный порог находится в точке пересечения функций плотности распределения вероятности энергии сигналов "0" и "1". Характеристики детектора можно улучшить, усреднив сигнал перед подачей на устройство возведения в квадрат, что уменьшает влияние шумов и улучшает помехозащищенность. Усреднение можно реализовать с помощью одной или нескольких линий задержки с изменяемыми или фиксированными межимпульсными интервалами. Также можно использовать цифровые отсчеты при дискретизации сигнала, но это увеличивает частоту взятия отсчетов и требования к аналого-цифровым преобразователям. Усреднение значительно улучшает характеристики детектора.

Еще одно усовершенствование заключается в нахождении точного и простого метода оценивания порога при модуляции АМН (OOK). Выбор порога сильно влияет на характеристики приемника, и обычно используют фиксированный порог. Однако радиоканал и статистика шумов меняются, поэтому целесообразно использовать адаптивный порог, зависящий от мощности сигнала и шума. Как и в случае схемы TR и дифференциального детектора, интервал интегрирования можно адаптировать в зависимости от максимально допустимой задержки в канале [5]. Оптимальный интервал интегрирования, минимизирующий коэффициент ошибок BER, зависит от статистики канала и дисперсии шума. Он меняется в зависимости от защищен-

ности SNR и профиля задержек многолучевого распространения. Адаптивный приемник оценивает статистику канала, сигнала и шума и изменяет интервал интегрирования для оптимизации качественных показателей.

У каждой схемы реализации приемника можно выделить ряд преимуществ и недостатков, представленных в таблице 1.

ТАБЛИЦА 1. Преимущества и недостатки различных реализаций СШП приемника

Вариант реализации приемника	Преимущества	Недостатки
Оптимальная согласованная фильтрация	Отсчеты, полученные в каждом цикле, можно оптимально объединить для улучшения качества детектирования символов	Требует составления матрицы коэффициентов корреляции помех на выходах корреляторов и/или ветвей приемника
	Помеха от одного определенного пользователя влияет только на отдельные его импульсы	Установка правильного порога требует точной оценки канала, для чего часто требуется передача настроечных последовательностей
Схема с передачей контрольной частоты TR	Позволяет с помощью простого приемника накапливать энергию сигнала, содержащуюся во всех составляющих многолучевого распространения	Выигрыш достигается ценой повышения мощности шума в силу особенностей приемника
	Упрощенная схема временного согласования и большая устойчивость к ошибкам рассогласования во времени	Без точной синхронизации в пределах заданного «окна» окажутся как сигнал, так и шум
	Не требует точной синхронизации принимаемых импульсов	Требует точной линии задержки
Дифференциальный детектор	Повышается эффективность использования спектра, а скорость передачи данных удваивается по сравнению со схемой TR	Даже небольшая разница задержек приводит к существенному ухудшению характеристик
Детектор мощности	Не чувствителен к искажениям и нелинейности фазы, вносимым такими устройствами как антенны, усилители или фильтры	Вынужденное применение алгоритма усреднения, что ведет к увеличению частоты взятия отсчетов и повышает требования к аналогово-цифровым преобразователям

Таким образом, для реализации приемника в диапазонах ниже 2ГГц, например, в метровом и дециметровом диапазонах наибольший интерес представляет схема с оптимальной согласованной фильтрацией. Так как качественные показатели приемника можно улучшить, увеличив число трактов, соответствующих основным лучам, а приемник в более низком частотном диапазоне не так требователен к характеристикам АЦП. Тогда будет

иметь место компромисс только между качеством и сложностью, необходимой для конкретной реализации.

В статье исследовано несколько вариантов приемопередатчиков сверхширокополосных систем на основе импульсного радио. Было показано, что каждый вариант приема имеет несколько конкурирующих параметров в смысле характеристик, стоимости, объема аппаратной реализации, вычислительной сложности, пропускной способности, возможностей многостанционного доступа и т. д. В зависимости от применения и требований к приемопередатчику может быть отдано предпочтение различным схемам приема. Методы повышения характеристик некогерентных приемников основываются, главным образом, на оценках некоторых дополнительных параметров каналов, способных сделать этот приемник более когерентным. Для дальнейшего исследования и применения в диапазонах частот ниже 2 ГГц будет использована схемы с оптимальной согласованной фильтрацией.

Список используемых источников

1. Quek T. Q. S., Win M. Z. Ultrawide bandwidth transmitted-reference signaling //2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577). IEEE, 2004. Т. 6. С. 3409-3413.

2. Pausini M., Janssen G. J. M. Analysis and comparison of autocorrelation receivers for IR-UWB signals based on differential detection //2004 IEEE International Conference on Acoustics, Speech, and Signal Processing. IEEE, 2004. Т. 4. С. iv-iv.

3. Arslan H., Chen Z. N., Di Benedetto M. G. (ed.). Ultra wideband wireless communication. John Wiley & Sons, 2006.

4. Fishler E., Poor H. V. Low-complexity multiuser detectors for time-hopping impulse-radio systems //IEEE Transactions on Signal Processing. 2004. Т. 52. №. 9. С. 2561-2571.

5. Akahori H., Shimazaki Y., Kasamatsu A. Examination of the automatic integration time length selection system using PPM in UWB // 2004 International Workshop on Ultra Wideband Systems Joint with Conference on Ultra Wideband Systems and Technologies. Joint UWBST & IWUWBS 2004 (IEEE Cat. No. 04EX812). IEEE, 2004. С. 268-272.

RECEIVER REALIZATION OPTIONS FOR ULTRA-WIDEBAND IMPULSE RADIO SYSTEMS WITH TIME HOPS

Simonina O., Kokin S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper explores several variants of transceivers for ultra-wideband systems based on impulse radio. The requirements to transceivers and related trade-offs in terms of quality, bandwidth, technical means and computational complexity of specific practical schemes are considered. The effects on receiver circuit design of ultra-wideband radio channel properties, intrinsic interference and interference from other users, sampling rate and modulation techniques are explained. Various UWB receivers are compared in terms of performance and other important criteria. Depending on the application and transceiver requirements, different receiving schemes may be preferred.

Key words: *UWB, RAKE receiver, pulse radio, receiver performance characteristics*

УДК 378.147.88
ГРНТИ 14.35.09

АПРОБАЦИЯ МЕТОДИЧЕСКИХ УКАЗАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ «ИЗУЧЕНИЕ ЯВЛЕНИЙ И ЗАКОНОВ ВОЛНОВОЙ ОПТИКИ. ПОЛЯРИЗАЦИЯ СВЕТА. ЗАКОН МАЛЮСА. ЗАКОН БРЮСТЕРА»

И. Е. Скалецкая, Н. Л. Урванцева, Ю. В. Шарихина

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

Работа посвящена апробации в учебном процессе методических указаний для выполнения лабораторной работы «Изучение явлений и законов волновой оптики. Поляризация света. Закон Малюса. Закон Брюстера», входящей в состав комплекта учебно-лабораторного оборудования. Лабораторная установка позволяет исследовать характер поляризации лазерного излучения и экспериментально проверить законы Малюса и Брюстера. Лабораторная работа будет введена в учебный процесс в рамках дисциплин «Физика (спецглавы)» и «Физика конденсированного состояния» в СПбГУТ им. проф. М. А. Бонч-Бруевича.

волновая оптика, закон Малюса, закон Брюстера, лабораторное оборудование

Санкт-Петербургским государственным университетом телекоммуникаций им. проф. М. А. Бонч-Бруевича был приобретен комплект учебно-лабораторного оборудования «Волновая оптика» с целью постановки лабораторных работ на кафедре физики. Лабораторный стенд представлен на рис. 1.

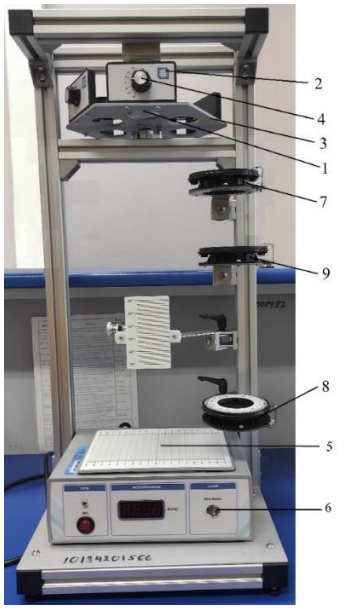


Рис. 1. Лабораторный стенд «Волновая оптика»: 1– источник излучения, 2 – пиктограммы элементов, 3 –турель, 4 – поворотное устройство, 5 – экран, 6 – блок питания, 7, 8 – поляроиды, 9 – пластинка λ/4

Данная установка позволяет изучать явления дифракции, интерференции и поляризации. Для естественного света световой вектор (вектор напряженности электрического поля $\vec{E}$) направлен произвольно в этой плоскости перпендикулярной направлению распространения волны. Для поляризованного света поведение светового вектора в этой плоскости упорядочено [1, 2]. В общем случае получаем эллиптическую поляризацию света. Для создания поляризованного света используют устройства, называемые поляризаторами (поляризационную призму, поляроид) или явление отражения света под углом Брюстера (например, стопа Столетова).

Линейно поляризованный свет можно получить из естественного с помощью кристаллической пластины, обладающей свойством дихроизма (например, из кристалла турмалина). Аналогичным свойством обладают поляроиды − пленки, в состав которых введено небольшое количество одинаково ориентированных кристаллов сульфата йодистого хинина [3]. Направление, в котором поляроид пропускает свет, называют главным направлением.

При вращении поляризатора вокруг направления луча можно проводить анализ поляризации света, измеряя интенсивность прошедшего луча. В этом случае устройство называют анализатором. Если на анализатор падает линейно поляризованный свет, то максимум интенсивности на выходе анализатора наблюдается, если главное направление поляроида совпадает с плоскостью колебаний светового вектора. В случае, когда свет естественный или поляризован по кругу, интенсивность на выходе анализатора не зависит от положения его главного направления.

Пусть вектор напряженности $\overrightarrow{E_0}$ линейно поляризованного света составляет угол φ с главным направлением поляроида. Сквозь поляризатор проходит составляющая $E = E_0 \cos\varphi$. Интенсивность пропорциональна квадрату амплитуды, запишем закон Малюса (1):

$$I = I_0 cos^2\varphi \qquad (1)$$

где I_0 – интенсивность падающего света.

Для естественного света направление вектора $\vec{E}$ в плоскости, перпендикулярной падающему лучу, меняется с частотой ~ 10^{15} Гц. Следовательно, на выходе поляризатора интенсивность света *I*:

$$I = \frac{I_0}{2} \qquad (2)$$

Формулы (1) и (2) не учитывают потери световой энергии в поляризаторе, с учетом которых закона Малюса, принимает вид (3):

$$I = \tau \cdot I_0 \cdot cos^2\varphi, \quad (3)$$

где τ – коэффициент пропускания ($\tau = \frac{I_{max}}{I_0}$).

При выполнении лабораторной работы проводят измерение не абсолютной, а относительной интенсивности излучения I/I_0, где I_0 − постоянная, задаваемая чувствительностью измерительного прибора. Полученные значения относительной интенсивности удобно нормировать, поделив все измеренные значения на максимальное значение относительной интенсивности.

Естественный свет можно представить в виде наложения двух некогерентных линейно поляризованных волн со взаимно перпендикулярными направлениями поляризации (рис. 2).

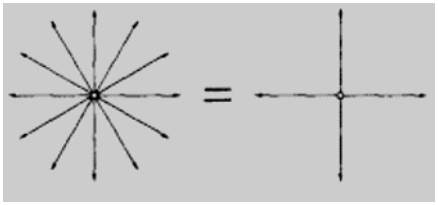


Рис. 2. Вектор напряженности электрического поля естественного света в плоскости перпендикулярной направлению распространения в разные моменты времени

Для естественного света интенсивности этих составляющих одинаковы.

Степень поляризации P частично поляризованного света отношение интенсивности поляризованного света $I_{поляр}$ к полной интенсивности I_o:

$$P = \frac{I_{поляр}}{I_0}.$$

Частично поляризованный свет, как и естественный, можно представить в виде наложения двух некогерентных волн со взаимно перпендикулярными направлениями поляризации (рис. 3).

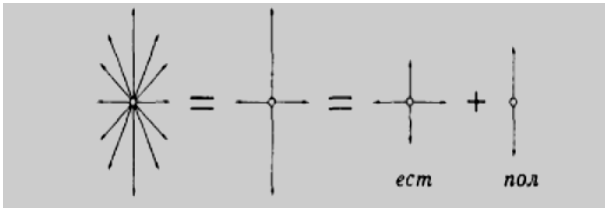


Рис. 3. Представление частично поляризованного света в виде суммы двух некогерентных линейно поляризованных волн

Вертикальные колебания соответствуют максимальной интенсивности I_{max}, а горизонтальные – минимальной I_{min}. Полная интенсивность

$I_0 = I_{max} + I_{min}$, интенсивность поляризованного света $I_{поляр} = I_{max} - I_{min}$. Тогда, степень поляризации для частично линейно поляризованного света:

$$P = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}.$$

В процессе выполнения лабораторной работы студенты определяют степень поляризации P полупроводникового лазера и снимают зависимость интенсивности луча, прошедшего через анализатор от угла поворота, а также определяют вид поляризации лазерного излучения. Полученные результаты позволяют найти коэффициент пропускания поляризатора, сравнить построенные нормированные теоретические и практические зависимости.

Для анализа состояния поляризации рассмотрим плоскую световую волну, распространяющуюся вдоль оси *z*. Пусть вектор $\overrightarrow{E_0}$ составляет с осью *x* угол α. Тогда вектор $\overrightarrow{E_0}$ можно представить в виде суммы $\overrightarrow{E_1}$ и $\overrightarrow{E_2}$:

$$\overrightarrow{E_1} = E_0 \cos\alpha \cos(\omega t - kz + \alpha_1)\,\overrightarrow{e_x}$$
$$\overrightarrow{E_2} = E_0 \sin\alpha \cos(\omega t - kz + \alpha_2)\,\overrightarrow{e_y}$$
$$\overrightarrow{E_0} = E_0 \cos\alpha \cos(\omega t - kz + \alpha_1)\,\overrightarrow{e_x} + E_0 \sin\alpha \cos(\omega t - kz + \alpha_2)\,\overrightarrow{e_y},$$

где ω − круговая частота, k – волновое число ($k = 2\pi/\lambda$), λ – длина волны, α_1 и α_2 – начальные фазы колебаний $\overrightarrow{E_1}$ и $\overrightarrow{E_2}$ в точке с координатой z = 0.

Если составляющие $\overrightarrow{E_1}$ и $\overrightarrow{E_2}$ когерентны ($\alpha_1 - \alpha_2 = \delta = \text{const}$), то поведение вектора $\overrightarrow{E_0}$ упорядочено. Конец вектора будет двигаться в плоскости *xy* по эллипсу. Обозначим фазу вектора $\overrightarrow{E_1}$ за $\gamma = \omega t - kz + \alpha_1$, тогда:

$$E_x = E_0 \cos\alpha \cos\gamma;$$
$$E_y = E_0 \sin\alpha \cos(\gamma + \delta);$$
$$\cos(\gamma + \delta) = \cos\gamma \cos\delta - \sin\gamma \sin\delta;$$
$$\cos\gamma = \frac{E_x}{E_0 \cos\alpha};$$
$$\sin\gamma = \frac{1}{\sin\delta}\left[\frac{E_x \cos\delta}{E_0 \cos\alpha} + \frac{E_y}{E_0 \sin\alpha}\right]$$
$$\frac{E_x^2}{E_0^2 \cos^2\alpha} + \frac{E_y^2}{E_0^2 \sin^2\alpha} - \frac{2E_x E_y \cos\delta}{E_0^2 \cos\alpha \sin\alpha} = \sin^2\delta$$

Таким образом, конец светового вектора описывает эллипс в плоскости, перпендикулярной направлению распространения световой волны.

В частном случае $\delta = 0, \pm\pi, \pm 2\pi, \ldots, \pm m\pi$ эллипс вырождается в прямую:

$$\frac{E_x}{E_0\,cos\,\alpha} = \pm\frac{E_y}{E_0\,sin\,\alpha}$$

Угол, который составляет эта прямая с осью x равен α, если m – четное число, и равен π − α, если m – нечетное. Оба случая соответствуют линейной поляризации.

При $\delta = \pm\pi/2, \pm 3\pi/2, \ldots$ получим уравнение эллипса, ориентированного вдоль осей x и y.

$$\frac{E_x^2}{E_0^2\,cos^2\,\alpha} + \frac{E_y^2}{E_0^2\,sin^2\,\alpha} = 1$$

Большая и малая оси этого эллипса будут равны или $E_0 \cos\alpha$ или $E_0 \sin\alpha$ (в зависимости от угла α). Если $\delta \neq const$, то свет не поляризован.

Таким образом, самый общий вид поляризации – эллиптическая. При этом конец светового вектора описывает эллипс. Частными случаями эллиптической поляризации являются круговая и линейная поляризации.

Плоскополяризованный свет можно получить из естественного с помощью отражения от плоской границы двух диэлектриков.

Граничные условия на границе раздела двух диэлектриков при отсутствии сторонних зарядов и токов проводимости:

$$\begin{cases} E_{1\tau} = E_{2\tau} \\ H_{1\tau} = H_{2\tau} \\ D_{1n} = D_{2n} \\ B_{1n} = B_{2n} \end{cases}$$

Индексами τ и n обозначены тангенциальные и нормальные составляющие вектора напряженности (E и H) и индукции (D и B) электрического и магнитного полей соответственно.

Поле, поляризованное перпендикулярно плоскости падения, обозначим $E_\perp$, поле, лежащее в плоскости падения, $E_\parallel$.

Выполнение граничных условий приводит к следующим зависимостям коэффициентов отражения от углов падения θ_1 и преломления θ_2 [3]:

$$\begin{cases} R_\perp = \dfrac{I'_\perp}{I_0} = \dfrac{sin^2(\theta_2 - \theta_1)}{sin^2(\theta_1 + \theta_2)} \\ R_\parallel = \dfrac{I'_\parallel}{I_0} = \dfrac{tg^2(\theta_1 - \theta_2)}{tg^2(\theta_1 + \theta_2)} \end{cases}$$

Если на границу падает свет с параллельной поляризацией, для которой $\theta_1 + \theta_2 = \pi/2$, то $R_{\parallel}$ становится равным нулю. Отраженный свет при этом полностью поляризован.

Этот угол падения называется углом Брюстера. Используя закон Снеллиуса ($\sin\theta_1/\sin\theta_2 = n_2/n_1$), где n_1 – показатель преломления среды, из которой падает луч, а n_2 – показатель преломления среды, в которую входит луч, получим формулу для определения угла Брюстера:

$$\frac{sin\,\theta_1}{sin\,(^{\pi}/_{2} - \theta_1)} = \frac{n_2}{n_1} = tg\theta_B$$

$$\theta_B = \text{arctg}\frac{n_2}{n_1}$$

Величина этого угла для границы воздух-стекло $\theta_B = 56{,}3^0$ при показателе преломления стекла $n = 1{,}5$.

Естественный свет, падающий на границу раздела под углом Брюстера, после отражения становится линейно поляризованным. Проходящий границу раздела свет поляризован частично.

Если на границу раздела двух диэлектриков под углом Брюстера падает плоско поляризованный свет (например, от лазера) с направлением колебаний вектора Е в плоскости падения волны, то интенсивность отраженной волны становится близка к нулю, так как в падающей волне отсутствует направление колебаний светового вектора, необходимое для создания отраженной волны.

Степень линейной поляризации Р преломленного луча при угле падения, равном углу Брюстера, достигает максимума, но этот луч остается частично поляризованным.

Таким образом, если установить на пути лазерного луча устройство для определения угла Брюстера, то изменяя угол наклона стеклянной пластинки по минимуму интенсивности отраженного луча можно найти угол Брюстера, по его тангенсу определить относительный показатель преломления стекла и сравнить его со справочным значением.

Список используемых источников

1. Борн М., Вольф Э. Основы оптики: пер. с англ. М.: Наука, 1973, 720 с.

2. Сивухин Д. В. Общий курс физики. Оптика: М.: Наука, 1980 г.,752 с.

3. Урванцева, Н. Л. Оптическая физика: учебное пособие / Н. Л. Урванцева. СПб.: СПбГУТ, 2019. 100 с.

TESTING THE METHODOLOGICAL INSTRUCTIONS FOR EXECUTING THE LABORATORY WORK «STUDY OF THE PHENOMENA AND LAWS OF WAVE OPTICS. POLARIZATION OF LIGHT. MALUS' LAW. BREWSTER'S LAW»

Skaletskaya I. E., Urvantseva N. L., Sharikhina Yu. V.
The Bonch-Bruevich St Petersburg State University of Telecommunications

The Bonch-Bruevich St Petersburg State University of Telecommunications purchased a set of educational and laboratory equipment «Wave Optics», transferred to the Department of Physics. The report is devoted to the testing in the educational process of methodological instructions for performing the laboratory work «Study of the phenomena and laws of wave optics. Polarization of Light. Malus' Law. Brewster's Law», which is part of this complex. The laboratory setup allows to study the nature of laser radiation polarization and experimentally verify Malus and Brewster's laws. The laboratory work will be introduced into the educational process within the framework of the disciplines «Physics (special chapters)» and «Physics of Condensed Matter» at The Bonch-Bruevich SPbSUT.

***Key words**: wave optics, polarized light, Malus' law, Brewster's law*

УДК 621.316.7
ГРНТИ 44.39.29

РАЗРАБОТКА МЕТОДИКИ ЧАСТОТНОГО РЕГУЛИРОВАНИЯ И УПРАВЛЕНИЯ ВЕТРОЭНЕРГЕТИЧЕСКИМИ СИСТЕМАМИ

Д. Ф. Ткачев, Г. И. Мурачев

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

В данной статье представлено расширенное исследование методов частотного регулирования энергосистемы, характеризующейся высокой долей ветровой генерации на базе асинхронных генераторов с двойным питанием, а также интегрированными накопителями энергии. С применением программной среды MATLAB/Simulink разработана и проанализирована комплексная модель, включающая алгоритмы первичного согласованного управления и синхронными генераторами, стратегии регулирования в области постоянной мощности, методы нечеткого управления для адаптивной настройки параметров, и принципы оптимизации работы накопителей энергии. Особое внимание уделено анализу влияния коэффициента мощности разгрузки на динамику частотных отклонений, а также эффективности применения нечеткой логики для адаптации параметров регулирования в зависимости от текущих условий работы системы. Исследованы различные методы управления ветроустановками, их преимущества и недостатки, а также проведено моделирование для оценки влияния накопления энергии на устойчивость частоты.

Регулирование частоты, ветроэнергетика, асинхронный генератор с двойным питанием, накопители энергии, MATLAB/Simulink, нечеткое управление

С развитием сложных систем возобновляемых источников энергии (ВИЭ) регулирование частоты и управление работой энергосистемы, работающей на таких источниках, как ветряные турбины, становится все более важным. Различные генераторы, используемые в энергосистеме, могут вызывать колебания частоты, что требует разработки эффективных методов управления. Ветроэнергетика демонстрирует быстрый рост во всем мире, и к 2050 году она может обеспечить значительную долю (40 %) в общей доле возобновляемых источников энергии. Учитывая ограниченность невозобновляемых ресурсов и проблемы изменения климата, переход к более устойчивым формам энергии, включая ВИЭ, становится необходимым. В частности, ветроэнергетические системы играют ключевую роль в поддержке частоты сети, поддержании мощности на номинальной частоте и снижении влияния перебоев в подаче электроэнергии. Поэтому частотное регулирование и управление ветроэнергетическими системами является обязательным.

Традиционные ветряные турбины на базе асинхронных генераторов с двойным питанием (АГДП) не обладают возможностями регулирования частоты вращения, что влияет на инерционный отклик и способность энергосистемы регулировать частоту. Для решения этой проблемы необходимо разработать схему первичного регулирования частоты с переменным коэффициентом для синхронных генераторов (СГ) и АГДП [1, 2].

Ветрогенераторная установка преобразует энергию ветра в механическую, а затем в электрическую. Для изучения влияния ветроаккумулирующей системы необходимо моделировать энергосистему, содержащую такую систему. Модель регулирования частоты, представленная на рисунке 1, использует математические уравнения для описания диапазона влияния и распространения частотных помех.

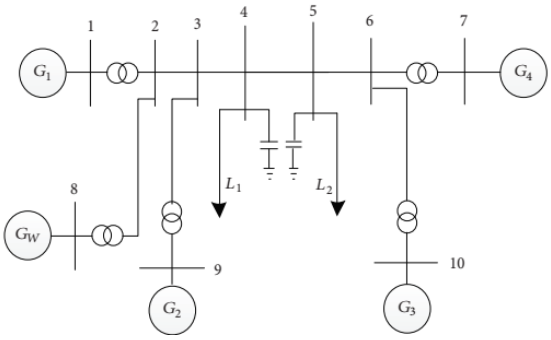


Рис. 1. Структура двухзонной тестовой системы

Для проведения исследований была разработана модель двухзонной электросети, включающая четыре генератора: три синхронных и одну ветряную турбину на базе АГДП [3, 4]. Модель включает в себя:

1. Синхронные генераторы. Три синхронных генератора номинальной мощностью 700 МВт, инерционной постоянной времени 6,5 с.

2. Ветроустановка с АГДП. Модель АГДП включает в себя параметры, определяющие динамику генерации: эквивалентная мощность 800×15 МВт, постоянная времени переменного шага 3 с, номинальная скорость ветра 12 м/с. Изначально АГДП работает в режиме снижения нагрузки на 20 %.

3. Накопители энергии. Модель включает систему накопления энергии, имитирующую работу аккумуляторной батареи с возможностью зарядки и разрядки.

4. Нагрузки. Моделируются две нагрузки с мощностями 1200 МВт и 1800 МВт соответственно, с возможностью импульсного изменения нагрузки.

5. Система управления. В модель включены:

– первичная система согласованного управления. Координированное управление синхронными генераторами и АГДП, обеспечивающее адаптацию параметров управления в зависимости от состояния системы;
– стратегия управления в области постоянной мощности. Регулирование выходной мощности АГДП в области постоянной мощности путем управления углом наклона лопастей;
– система нечеткого управления. Адаптивное регулирование коэффициентов участия ветровой энергии (Kd) и накопителей энергии (Kp) в частотном регулировании на основе нечеткой логики. Входные переменные нечеткой логики – скорость ветра, изменение частоты и отклонение частоты. Разработаны нечеткие правила для определения значений Kd и Kp в зависимости от состояния энергосистемы;
– принцип оптимизации работы накопителя энергии. Управление зарядкой/разрядкой аккумулятора с разделением интервалов работы на основе значения SOC (State of Charge). В период регулирования частоты накопитель работает в диапазоне 20 % < SOC < 80 %. За пределами регулирования частоты устанавливаются пределы для безопасного и эффективного использования накопителя. Применяется логистическая функция для адаптации коэффициента регулирования частоты накопителя энергии в зависимости от его SOC.
– MATLAB/Simulink. Для моделирования динамических процессов использован программный пакет MATLAB с приложением Simulink.

В ходе моделирования проведен анализ влияния различных факторов на работу системы регулирования частоты. В частности, исследованы:

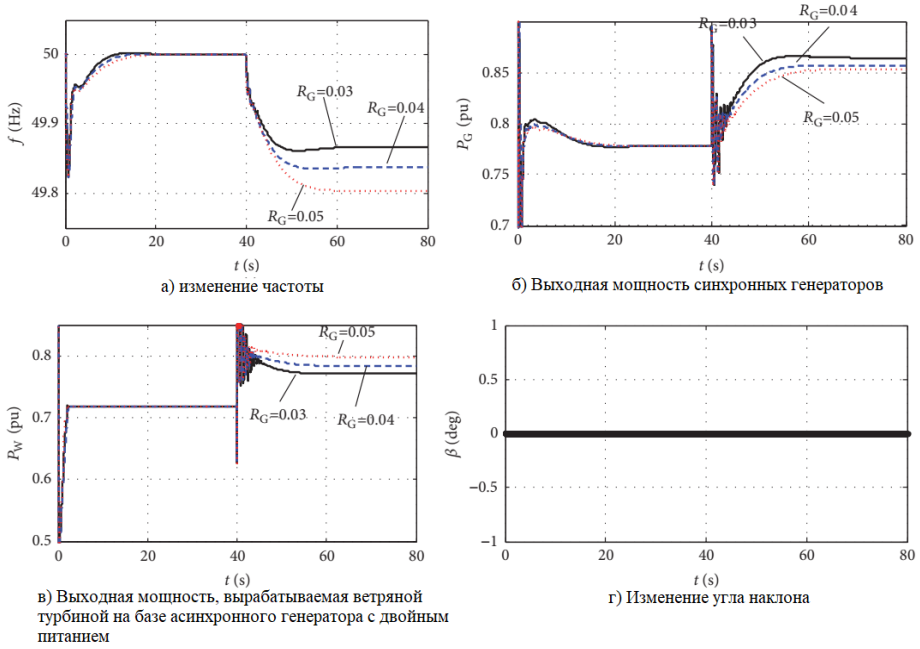
1. Влияние коэффициента мощности разгрузки (Kd). Исследовано влияние различных значений Kd на среднее отклонение частоты и средний коэффициент резервной мощности. Выявлена зависимость оптимального значения Kd от характеристик турбулентности.

2. Работа системы управления в области постоянной мощности. Показано, как алгоритм управления углом наклона лопастей АГДП позволяет участвовать в регулировании частоты в области постоянной мощности.

3. Эффективность нечеткого управления: Продемонстрировано, как использование нечеткой логики для адаптивной настройки коэффициентов Kd и Kp позволяет оптимизировать вклад ветровой генерации и накопителей энергии в регулирование частоты при различных скоростях ветра и возмущениях.

4. Работа системы управления накопителями энергии. Показано, как разработанный принцип разделения интервалов работы с учетом SOC позволяет избежать переразряда и перезаряда накопителей, обеспечивая их надежную и эффективную работу в системе регулирования частоты. На графиках отражены динамические изменения частоты, мощности генерации и SOC накопителей.

5. Динамическое поведение энергосистемы. Анализ динамических характеристик системы при различных сценариях изменения нагрузки показал, как разработанная система управления обеспечивает стабильность и быстродействие регулирования частоты.



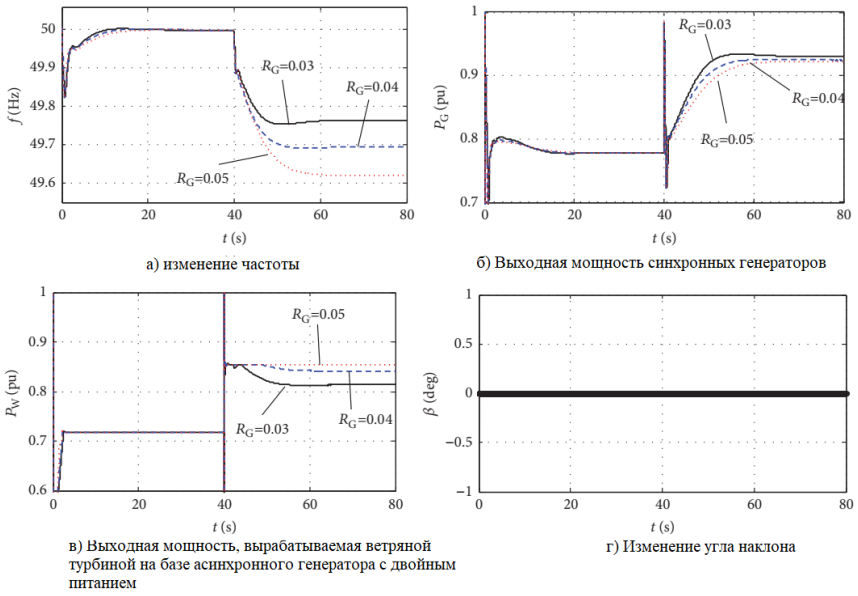
а) изменение частоты
б) Выходная мощность синхронных генераторов
в) Выходная мощность, вырабатываемая ветряной турбиной на базе асинхронного генератора с двойным питанием
г) Изменение угла наклона

Рис. 2. Результаты моделирования участка измерения максимальной мощности при изменении частоты менее 0,2 Гц

На рисунке 2 показано, что мощность регулирования частоты синхронного генератора постепенно уменьшается по мере увеличения коэффициента регулирования (рисунок 2б), в то время как мощность регулирования частоты ветряной турбины на базе асинхронного генератора с двойным питанием постепенно увеличивается (рисунок 2в). С точки зрения восстановления частоты системы, реакция на восстановление частоты является наилучшей, когда устанавливаем корректирующий коэффициент синхронного генератора $R_G = 0{,}03$, как показано на рисунке 2а. Однако, если коэффициент регулирования синхронного генератора невелик, мощность регулирования частоты асинхронного генератора с двойным питанием ограничена, как показано на рисунке 2(в).

Когда устанавливаем R_G = 0,05, частота также может удерживаться в пределах 0,2 Гц, и частота системы остается относительно стабильной. Следовательно, чтобы максимально увеличить мощность регулирования частоты ветряных турбин на базе асинхронного генератора с двойным питанием и в полной мере использовать восстановленную мощность ветряной турбины на базе асинхронного генератора с двойным питанием для регулирования частоты, можем принять R_G = 0,05. Изменение угла наклона также показано на рисунке 2г. Колебания, показанные на рисунке 2, обусловлены тем фактом, что система работает в области контроля максимальной мощности и колебания частоты, превышают 0,2 Гц, так что для этого потребуется несколько переходных периодов Δf.

Для второго случая скорость ветра также составляет 9 м/с. В течение 40 секунд приложенная нагрузка внезапно увеличивается на 600 МВт; отклонение частоты превышает 0,2 Гц. Коэффициенты настройки синхронного генератора используются такие же, как и для первого случая. Соответствующие результаты моделирования показаны на рисунке 3.



а) изменение частоты

б) Выходная мощность синхронных генераторов

в) Выходная мощность, вырабатываемая ветряной турбиной на базе асинхронного генератора с двойным питанием

г) Изменение угла наклона

Рис. 3. Результаты моделирования участка измерения максимальной мощности при изменении частоты более 0,2 Гц

Согласно рисунку 3(а), наилучшая характеристика восстановления частоты достигается при установке R_G = 0,03. Когда изменение частоты превышает 0,2 Гц, система переходит в режим экстренной частотной модуляции, и конечной целью является улучшение эффекта восстановления частоты системы. Все синхронные генераторы и АГДП должны выдавать как можно большую мощность, как показано на рисунках 3б и 3в.

В соответствии с результатом восстановления частоты (рисунок 3а), и изменением угла наклона (рисунок 3(г)), коэффициент регулировки синхронного генератора должен быть установлен равным $R_G = 0{,}03$.

Результаты могут быть использованы для изучения влияния параметров на частотное регулирование [5], [6], [7].

Список используемых источников

1. Hu J. X., Xu G. Y., Bi T. S., Cui H. B. A strategy of frequency control for deloaded wind turbine generator based on coordination between rotor speed and pitch angle // Power System Technology. 2019. 43. PP. 3656–3662.

2. Shi Q., Wang G., Li H. Coordinated Virtual Inertia Control Strategy of Multiple Wind Turbines in Wind Farms Considering Frequency Regulation Capability. Power System Technology. 2019. 43. PP. 4005–4017.

3. Lei D., Yin S. Y., et al. Integrated Frequency Control Strategy of DFIGs Based on Virtual Inertia and Over-Speed Control // Power System Technology, 2015. № 9. PP. 2385-2391.

4. Jiao P. Y., Liu, F., et al. Frequency Regulation Strategy of DFIG in Micro-Grid System Based on Subsection Control // Electrical Measurement & Instrumentation, 2016. № 12. PP. 69-74.

5. Yan X. W., Cui S., and Chang W. F. Primary frequency regulation control strategy of doubly-fed induction generator considering supercapacitor SOC feedback adaptive adjustment[J] // Transactions of China Electrotechnical Society, 2019. Vol. 36. № 05. PP. 1027–1039.

6. C Liu., Q Li., and Wang K. State-of-charge estimation and remaining useful life prediction of supercapacitors // Renewable and Sustainable Energy Reviews. 2021. Vol. 150. № 2. P. 111408.

7. Yin L., Li Y. Fuzzy Vector Reinforcement Learning Algorithm for Generation Control of Power Systems Considering Flywheel Energy Storage // Appl. Soft Comput. 2022. 125, 109149.

DEVELOPMENT OF A METHODOLOGY FOR FREQUENCY REGULATION AND MANAGEMENT OF WIND ENERGY SYSTEMS

Tkachev D., Murachev G.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

This article presents an extensive study of frequency regulation methods for a power system with a high share of wind generation based on doubly-fed induction generators (DFIG), as well as integrated energy storage. A comprehensive model is developed and analyzed using the MATLAB/Simulink software environment, including algorithms for primary coordinated control of DFIG and synchronous generators, control strategies in the constant power region, fuzzy control methods for adaptive parameter tuning, and principles for optimizing the operation of energy storage. Particular attention is paid to the analysis of the impact of the power derating coefficient on the dynamics of frequency deviations, as well as the effectiveness of using fuzzy logic to adapt the control parameters depending on the current operating conditions of the system. Various methods of wind turbine control, their advantages and disadvantages, are investigated, and simulations are conducted to assess the effect of energy storage on frequency stability.

Key words: *Frequency regulation, wind energy, doubly-fed induction generator, energy storage, MATLAB/Simulink, fuzzy control*

УДК 004.896
ГРНТИ 55.30.05

РАЗРАБОТКА ПРОТОТИПА ОПОРНО-ПОВОРОТНОГО МЕХАТРОННОГО МОДУЛЯ СКАНИРУЮЩЕГО ЛАЗЕРНОГО ДАЛЬНОМЕРА МОБИЛЬНОГО РОБОТА

Д. Ф. Ткачев, М. С. Парфенов, В. А. Фукалов

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

Неотъемлемой частью мобильного робота являются датчики, сенсоры и система технического зрения. Они позволяют ему ориентироваться в пространстве, а также преодолевать различные препятствия. Для своевременного обнаружения помех, возникающих перед роботом, применяются следящие лазерные дальномеры – лидары. Однако они имеют определенное разрешение создаваемого ими облака точек. Таким образом при использовании лидара с невысоким разрешением, на определенном расстоянии робот может не увидеть преграды из-за того, что она находилась в промежутке между 2-я точками облака. В результате возникает необходимость разработки высокоточных и надежных систем, позволяющих решить данную проблему.

робототехника, лидар, сканирование, датчик, облако точек, мобильный робот

Одним из наиболее эффективных средств для обеспечения технического зрения роботов являются сканирующие лазерные дальномеры (лидары). Лидар позволяет получать информацию об окружающей сцене в виде облака точек (отображающего положение объектов в трехмерном пространстве относительно сенсора, а также величину отраженного от поверхности объектов сигнала), слабо зависящего от освещения сцены [1]. Лидары применяют как в стационарном, так и мобильном вариантах [2]. Однако точность и разрешение этих облаков точек напрямую зависят от характеристик используемых лидаров. В при использовании устройств с невысоким разрешением могут возникнуть ситуации, когда мелкие объекты, препятствия или неровности дорожного покрытия остаются незамеченными роботом, что может привести к аварийным ситуациям и выходу робота из строя.

В настоящее время на рынке есть компании, предлагающие готовые устройства наклонно-поворотного типа. Среди них выделяются такие компании как Tryosys, 2B Security Systems и Movitherm. После анализа и сравнения характеристик был сделан вывод о том, что существующие на рынке устройства имеют недостатки, такие как: высокая стоимость, избыточная грузоподъемность и высокое энергопотребление. В результате возникает

потребность в разработке собственного опорно-поворотного мехатронного модуля, который бы учитывал эти факторы и способствовал повышению эффективности работы лидара.

Для того чтобы решить проблему наличия слепых зон между отдельными точками создаваемого лидаром облака, его необходимо перемещать в пространстве в различных направлениях, чтобы заполнить промежутки и сделать облако точек более плотным. В работе рассматривались несколько вариантов реализации данных перемещений:

– наклонять лидар вверх и вниз на определенный угол;
– использовать сразу два перемещения и поворот, и наклон.

Структура разработанного опорно-поворотного мехатронного модуля состоит из двух вращательный звеньев, соединенных последовательно. Одно из них предназначено для поворота конструкции вокруг своей оси, а второе для наклона лазерного сканирующего дальномера.

Основным компонентом, приводящим в движение всю систему, является двигатель. Для обеспечения точного позиционирования устройства, а также высокого разрешения шага было решено рассмотреть шаговые двигатели, используемые в станках с ЧПУ, а также 3D принтерах. Наиболее распространенным вариантом является шаговый двигатель типа Nema17. Он имеет разрешение в 200 шагов на оборот, что равно 1.8 градусов на один шаг, момент удержания 0.42 Н*м. малый вес 0.3 кг и цену 1 тысяча рублей.

Для того чтобы управлять шаговым двигателем, а также применять дробление шага для увеличения плавности движения и точности позиционирования, применяются драйверы шаговых двигателей. Популярной и недорогой моделью, обладающей необходимыми техническими особенностями и возможностью управлять выбранным шаговым двигателем, является драйвер A4988. Он работает с напряжениями от 3 В (логическая часть) до 36 В (силовая часть), с максимальным током источника питания до 2 А и позволяет дробить шаг двигателя до 1/16. Для удобства работы с драйвером использовалась плата расширения с тумблерами переключения микрошага.

Для того чтобы управлять всей конструкцией необходим микроконтроллер. В качестве его была выбрана плата Arduino Nano, так как достаточно популярна, доступна и проста в освоении. Она имеет малые габариты 18х45 мм, напряжение питания от 5 до 12 В, порты с поддержкой ШИМ, 22 портами ввода-вывода и тактовой частотой 16 МГц.

Для определения начального положения системы использовался датчик, основанный на эффекте Холла A3144. Он является популярным и ис-

пользуется в качестве квадратурного счетчика, для отслеживания нулевой точки при вращении двигателя. Благодаря ему можно реализовать схему обратной связи по положению. Также он отличается невысокой стоимостью, что, несомненно, является его преимуществом, на ряду с другими датчиками.

Создание 3D модели ОПММ проводилось в CAD программе Autodesk Inventor. В качестве зубчатой передачи была выбрана шевронная передача, так как она обеспечивает минимальный люфт, низкую подверженность вибрациям, плавность перемещения и передачу высокого момента. В шестерне наклонной оси и основании расположились неодимовые магниты для определения начального положения устройства. Также в основании расположен подшипник, позволяющий всей платформе вращаться, а под основанием находится отсек для электроники с 2-мя разъемами для подключения микроконтроллера и питания двигателей. На дне отсека присутствуют ножки для большей устойчивости ОПММ и его дальнейшей фиксации. 3D модель ОПММ представлена на рис. 1.

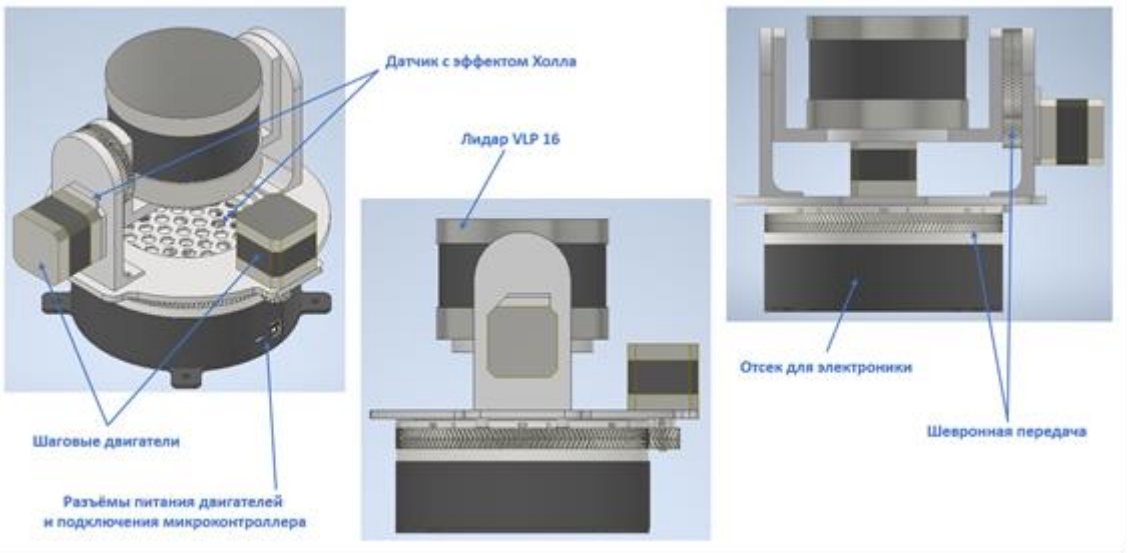


Рис. 1. 3D модель разработанного ОПММ

Моделирование работы ОПММ проводилось в среде разработки Unity 3D [3]. Сначала файл с ранее созданной 3D моделью ОПММ был добавлен в движок. Затем была добавлена сцена и пара объектов, представляющих собой препятствия, которые лидар должен был обнаружить, а также сам лидар. Модель лидара обладает возможностью отображения создаваемого им облака точек. Он был настроен в соответствии с характеристиками реального лидара компании Velodyne – VLP16. Вывод облака точек был задан в отдельном окне.

Для задания вращения ОПММ были написаны и закреплены за определенными осями программы на языке программирования C#. Так как вращение лидара при помощи ОПММ относительно вертикальной оси не дало ощутимых улучшений в плотности облака точек, то было принято решение отказаться от него в рамках данной симуляции.

В программе для вращения лидара относительно горизонтальной оси были заданы пределы, обозначающие зону интереса, где находятся объекты. Попадая при движении в эту зону ОПММ, снижало свою скорость, для увеличения плотности создаваемого облака точек, затем снова возвращал прежнюю.

Детали конструкции изготавливались при помощи печати на 3D принтере с использованием PLA пластика. Данный способ был выбран, потому что он имеет ряд преимуществ, такие как быстрота изготовления, экономичность, гибкость в дизайне и доступность материалов.

После обработки деталей, в соответствующие посадочные места были запрессованы подшипники и магниты. Затем все детали были соединены между собой в единую конструкцию при помощи винтов, на свои места закреплены шаговые двигатели и разъемы под электронику и датчики. После подключения всех проводов к плате расширения, с установленными Arduino Nano и драйверами ШД, электроника была помещена в предназначенный для этого отсек. Внешний вид устройства представлен на рис. 2.



Рис. 2. Внешний вид разработанного ОПММ

После изготовления прототипа были написаны программы управления шаговыми двигателями и загружены в микроконтроллер. Для экспериментов использовались 3 вида программ. Первая для вращения лидара, зафиксированного в заданном положении, относительно вертикальной оси, вторая для наклона лидара относительно горизонтальной оси с фиксированной скоростью и третья для наклона лидара относительно горизонтальной оси с замедлением в зоне интереса. Сначала проходила калибровка начального по-

ложения каждой из осей при помощи поиска магнитного поля датчиками с эффектом Холла, затем начиналось выполнение основной программы. Облако точек, создаваемое лидаром в реальном времени, отображалось при помощи фреймворка ROS 2 и программы для визуализации данных RViz [4]. Эксперименты показали, что разработанный ОПММ справляется с поставленной задачей повышения плотности облака точек в зоне интереса.

Заключение

Изготовление и тестирование прототипа подтвердили соответствие реальных полученных характеристик устройства с прогнозируемыми. Натурные эксперименты продемонстрировали, что ОПММ действительно способен увеличить плотность заполнения облака точек лидара в зонах наибольшего интереса, путем его перемещения в пространстве в различных направлениях в соответствии с заданным законом управления.

Список используемых источников

1. Старобыховская А. А., Лашманов О. Ю., Коротаев В. В. Алгоритм повышения пространственной плотности лидарного облака точек для решения задач автономного вождения автомобиля // Известия высших учебных заведений. Приборостроение, 2021. Т. 64, №7, с. 559

2. Дмитриев В. С., Костюченко Т. П., Янгулов В. С., Теплоухов В. В. Мобильные лидары. Влияние внешних механических воздействий на точность прицеливания лидара // Известия Томского политехнического университета. Инжиниринг георесурсов, 2007. с. 30.

3. Unity 3D [Электронный ресурс] URL: https://learn.unity.com (дата обращения 18.05.2024).

4. Robot Operating System [Электронный ресурс] URL: https://docs.ros.org/en/ rolling/index.html# (дата обращения 18.05.2024).

PROTOTYPE DEVELOPMENT THE PAN-TILT MECHATRONIC MODULE OF THE SCANNING LASER RANGEFINDER OF THE MOBILE ROBOT

Tkachev D., Parfenov M., Fukalov V.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Sensors and a vision system are an integral part of a mobile robot. They allow him to navigate in space, as well as overcome various obstacles. Tracking laser rangefinders, lidars, are used to detect interference in front of the robot in a timely manner. However, they have a certain resolution of the point cloud they create. Thus, when using a low-resolution lidar, the robot may not see the obstacle at a certain distance due to the fact that it was located in the gap between the two points of the cloud. As a result, there is a need to develop high-precision and reliable systems to solve this problem.

Key words: *Robotics, lidar, scanning, sensor, point cloud, mobile robot*

УДК 629.7.014.16
ГРНТИ 49.13.15

РЕЗУЛЬТАТ АНАЛИЗА МЕТОДОВ ИЗМЕРЕНИЯ КОЭФФИЦИЕНТА ШУМА УСИЛИТЕЛЯ ДЛЯ АДАПТИВНОЙ АНТЕННОЙ РЕШЕТКИ РАСПОЛОЖЕННОЙ НА БПЛА

П. Н. Фёдоров, И. В. Галушко, Ю. А. Кудрявцева, К. Н. Следевский

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

Все чаще поднимается вопрос повышения устойчивости приема управляющего сигнала беспилотным летательным аппаратом (БПЛА). Одним из вариантов решения проблем является использование адаптивной антенной решетки на БПЛА. Для корректной работы всей системы, необходимо, чтобы компоненты, используемые в системе, вносили минимальные собственные шумы в принимаемый сигнал.

коэффициент шума, усилители, СВЧ, адаптивная антенная решетка

С каждым годом, несмотря на ограничения, увеличивается применение беспилотных летательных аппаратов (БПЛА), как в гражданской сфере, так и военной. По данным заместителя генерального директора НИЦ «Аэроскрипт» Андрея Яблокова, в России сегодня зарегистрировано более 105 тыс. дронов. Для управления дронами зачастую используются диапазоны частот: 1,2 ГГц, 2,4 ГГц и 5,8 ГГц, которые также используются различными устройствами, создавая помехи. Помехи разделаются на естественные и преднамеренные. К естественным помехам относятся: грозовые разряды, индустриальные помехи, влияние соседних радиосредств. Для БПЛА критичными являются преднамеренные помехи, которые создаются для подавления канала связи между оператором и дроном. Одним из способов борьбы с таким типом помех является использование адаптивной антенной решетки (ААР).

Адаптивная антенная решетка представляет из себя массив антенных элементов, размещенных определенным образом в пространстве, сигналы с которых обрабатываются с использованием специального алгоритма, что позволяет выделить полезный сигнал и исключить помеху. Важным элементом блока управления ААР – является усилитель сигналов, приходящих с входов антенного элемента. В связи с тем, что сигнал на входе может быть существенно ослаблен при удалении БПЛА от источника сигнала, необходимо предусмотреть его усиление до требуемой величины. Поскольку важ-

ным параметром является собственный шум усилителя, то для корректности работы алгоритма и выделения полезного сигнала, необходимо знать его коэффициент шума на каждом этапе работы с сигналом.

Коэффициент шума устройства – отношение сигнал/шум на входе устройства при нормальных условиях к отношению сигнал/шум на выходе устройства [1]. Данное определение может быть выражено в виде следующей формулы:

$$F = \frac{\frac{S_{in}}{N_{in}}}{\frac{S_{out}}{N_{out}}} \quad (1)$$

где, S_{in} – мощность сигнала на входе измеряемого устройства, N_{in} – мощность шума на входе, S_{out} – мощность сигнала на выходе, N_{out} – мощность шума на выходе.

Сам коэффициент шума устройства состоит из нескольких составляющих: теплового шума и дробового шума. Дробовый шум – беспорядочное изменение напряжений и токов относительно их среднего значения в цепях усилителей. Данный шум имеет непрерывное и непредсказуемое воздействие на сигнал из-за хаотичности потока движения электронов. Тепловой шум возникает при флуктуациях электронов в проводниках и имеет однородную структуру на всех частотах. При оценке шума все его источники принято рассматривать как тепловой шум, мощность которого определяется по формуле:

$$P_A = k * T * B \quad (2)$$

где P_A – доступная мощность, k – постоянная Больцмана, T – абсолютная температура, B – полоса частот.

Приняв, что ко входу усилителя подключена согласованная нагрузка при температуре 290 К, то она будет создавать на входе усилителя шум согласно формуле 2. На выходе измеряемого устройства шум усилится на G – коэффициент усиления усилителя, помимо этого усилитель будет иметь собственный шум N_A. Таким образом, формула 1, приобретает вид:

$$F = \frac{(k * T * B * G + N_A)}{k * T * B * G} \quad (3)$$

Данное выражение является определением коэффициента шума, которое официально принято международным Институтом Радиоинженеров (Institute of Electrical and Electronics Engineers (IEEE)).

К основным методам измерения коэффициента шума относятся [2]:
– метод Y-фактора;
– метод генератора сигнала с удвоением мощности;
– метод прямого измерения шума (метод холодного источника).

Метод Y-фактора применяется в большинстве ручных и автоматизированных средств измерения коэффициента шума. В данном методе используется источник шума, который позволяет определить внутренний шум в исследуемом устройстве.

Источник шума, подключается к исследуемому устройству, после чего измеряется выходная мощность при включенном и выключенном источнике шума. Отношение измеренных мощностей называется Y-фактором.

$$Y = \frac{N_2}{N_1} \tag{4}$$

Y-фактор и избыточный коэффициент шума (ИКШ) могут использоваться для измерения крутизны изменения мощности шума исследуемого устройства. Так как калиброванный ИКШ источника шума представляет опорный уровень для входного шума, то можно вывести уравнение для вычисления внутреннего шума исследуемого устройства:

$$N_A = k * T * B * G * \left(\frac{ENR}{Y-1} - 1\right) \tag{5}$$

где ENR – ИКШ.

Из этого возможно вывести выражение, описывающее суммарный шум-фактор устройства:

$$F_{SYS} = \frac{ENR}{Y-1} \tag{6}$$

Метод генератора сигнала с удвоением мощности был популярен, когда не было источников шума, но данный метод все еще остается актуальным в частных случаях, когда Y-фактор может быть очень малым, либо его трудно точно измерить.

При использовании данного метода сначала измеряется выходная мощность устройства, когда на его входе имеется нагрузка при температуре приблизительно 290 К. Затем подключается генератор сигналов с частотой в пределах полосы измерения. Мощность выходного сигнала генератора устанавливается такой, чтобы мощность на выходе устройства увеличилась на 3 дБ. Соответственно шум-фактор устройства вычисляется по формуле:

$$F_{SYS} = \frac{P_{gen}}{k * T * B} \tag{7}$$

где P_{gen} – мощность генератора.

Для использования данного метода необходимо знать шумовую полосу измерителя мощности, также необходимо чтобы выходная мощность измерялась устройством, показывающим истинное значение мощности.

Метод прямого измерения шума используется для измерения устройств с высоким коэффициентом шума. Выходная мощность устройства измеряется при входной нагрузке, находящейся при температуре приблизительно 290 К. Вычислить шум-фактор устройства можно по следующей формуле:

$$F_{SYS} = \frac{N_0}{k * T * B * G} \quad (8)$$

где N_0 – мощность шума.

Измерить коэффициент шума возможно различными методами, которые были рассмотрены в данной статье. Благодаря всем этим способам можно провести сравнительный анализ между различными вариациями разрабатываемых усилителей и выбрать наиболее подходящий. Наиболее подходящим методом, в рамках будущей разработки является метод генератора сигнала с удвоением мощности. Данный метод позволяет проводить измерения вне зависимости от абсолютной точности измерения мощности анализатором спектра, а также исследовать устройства с большим коэффициентом шума. Такой метод позволяет достаточно точно измерить коэффициент шума устройства за исключением случаев с резкими скачками коэффициента шума.

Список используемых источников

1. Бельчиков С. Коэффициент шума. Теория и практика измерений. // Компоненты и технологии. Измерительное оборудование. СПб.: Компоненты и технологии, 2008. С. 196-199.

2. 5952-8255RURU Keysight Technologies Основы измерения коэффициента шума в радиочастотном и микроволновом диапазонах Заметки по применению. С. 12-13.

ANALYSIS OF MEASUREMENT METHODS OF THE AMPLIFIER NOISE FACTOR FOR THE ADAPTIVE ANTENNA ARRAY LOCATED ON THE UAV

Fedorov P, Galushko I., Kudryavtseva A., Sledevskiy K.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The issue of increasing the stability of control signal reception by unmanned aerial vehicles (UAVs) is increasingly being raised. One of the options for solving the problems is to use an adaptive antenna array on the UAV. For the correct operation of the entire system, it is necessary that the components used in the system introduce minimal intrinsic noise into the received signal.

Key words: *noise figure, amplifiers, microwave, adaptive antenna array*

УДК 621.396.6
ГРНТИ 47.45.29

СПОСОБ БОРЬБЫ С АКТИВНЫМИ ПОМЕХАМИ В РАДИОТЕХНИЧЕСКИХ СИСТЕМАХ С ИСПОЛЬЗОВАНИЕМ АДАПТИВНЫХ АНТЕННЫХ РЕШЕТОК

П. Н. Фёдоров, И. В. Галушко, Ю. А. Кудрявцева, И. Е. Титков

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

В условиях специальной военной операции, способы борьбы с активными помехами становятся все более актуальными, так как системы радиоэлектронной борьбы и противодействия постоянно развиваются и появляются новые методы создания помех, которые в свою очередь приводят к срыву выполнения различных боевых и других важных задач. На данный момент существует большое количество типов помех, с которыми необходимо бороться путем применения современных радиотехнических систем.

активные помехи, диаграмма направленности, БПЛА, адаптивные антенные решетки

В данной работе будут рассмотрены те помехи, которые воздействуют на каналы управления БПЛА, так как на данный момент они являются наиболее опасными и актуальными.

Ниже представлены основные цели применения помех:

– выведение из строя систем управления БПЛА;
– нарушение ориентирования и навигации БПЛА;
– создание ложных сигналов навигации;
– противодействие разведывательным силам противника.

В условиях выполнения боевых задач, наибольшее влияние на беспилотные летательные аппараты оказывают активные помехи. Такие помехи создаются искусственно и могут копировать полезный сигнал с некоторыми изменениями. Это приводит к тому, что блок управления, находящийся на борту БПЛА не может отличить помеху от полезного сигнала. Помеха может имитировать команду управления или навигации. Такие помехи генерируются на частоте канала управления или передачи данных [1].

Существует несколько методов борьбы с активными помехами, такие как:

– перестройка по частоте с уплотнением каналов. Данный метод основан на быстрой смене рабочих частот для передачи полезной информации. Такой метод затрудняет возможность создания устойчивой помехи, так как

противник не может быстро адаптировать работу оборудования к постоянному изменению частоты;
- кодовое разделение каналов. Такой метод основан на индивидуальном кодировании сигналов между приемником и передатчиком;
- применение направленных антенн. Такие антенны фокусируют излучение в заданном направлении, что снижает вероятность перехвата и подавления сигнала;
- использование адаптивных антенных решеток. Применение таких систем позволяет ситуативно изменять форму диаграммы направленности антенны. В направлении прихода помехи формируется диаграмма направленности сигнала, это приводит к появлению так называемых «нулей» диаграммы направленности [2].

Наиболее эффективным и современным является метод на основе использования адаптивных антенных решеток. Такой метод имеет высокую эффективность подавления активных помех, так как диаграмма направленности антенны динамически изменяется и увеличивает отношение сигнал / помеха на выходе антенной решетки. Так же стоит отметить гибкость работы адаптивных антенных решеток. Работа таких систем происходит в реальном масштабе времени, что позволяет подстраиваться под изменяющуюся сигнально-помеховую обстановку и выделять сигнал на фоне различных помех.

Ограничением такой системы является ситуация, когда направления прихода помехи и полезного сигнала совпадут, или будут на достаточно близком расстоянии друг к другу, что может привести к непреднамеренному подавлению полезного сигнала. Это связано с тем, что разрешающая способность по углу у адаптивных антенных решеток ограничена формой диаграммы направленности и типом распределения амплитуды сигнала в апертуре антенны [3].

Ниже приведено описание работы системы подавления активных помех с применением адаптивной антенной решетки.

Система выполняет круговое сканирование, такой режим работы называется «режим радара» и применяется с целью обнаружения направления прихода помехи. В процессе сканирования непрерывно формируется диаграмма направленности антенной решетки с выраженным главным максимумом, который направлен в сторону прихода полезного сигнала. Таким образом происходит сканирование сектора, равного 360 градусов с шагом в 1 градус. Для каждого исследуемого сектора происходит расчет сдвигов фаз

на каждом антенном элементе решетки. В зависимости от направления на исследуемый сектор, сдвиги фаз на соседних антенных элементах рассчитываются по схеме, представленной на рисунке 1:

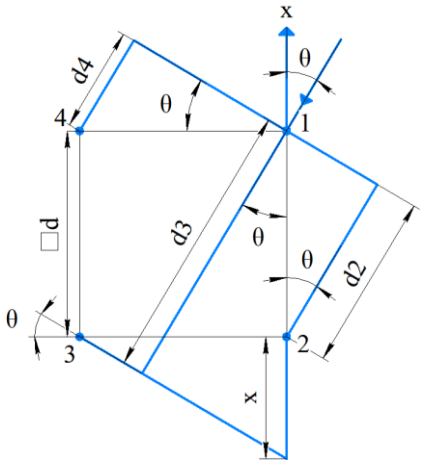


Рис. 1. Схема для определения фазовых сдвигов между принятыми разными антенными элементами сигналами

Перпендикуляры *d1* и *d2* определяются по выражению (1):

$$\begin{cases} d_2 = d \cdot \cos\theta; \\ d_4 = d \cdot \sin\theta. \end{cases} \quad (1)$$

Перпендикуляр *d3* можно определить из соотношения (2):

$$\begin{cases} tg\,\theta = \dfrac{x}{d}; \\ \cos\theta = \dfrac{d_3}{d+x}. \end{cases} \quad (2)$$

Тогда получим следующее выражение для *d3* (3):

$$d_3 = d \cdot (1 + tg\theta) \cdot \cos\theta. \quad (3)$$

Чтобы перевести длину перпендикуляра в разность фаз между первой антенной и другими антеннами необходимо выполнить преобразование (4):

$$\Delta\Phi_{1i} = \frac{2\pi}{\lambda} \cdot d_i, \quad (4)$$

где λ – длина волны заданной рабочей частоты.

Если сдвиг фазы больше нуля, значит сигнал поступил на первый элемент АР раньше, чем на *i*-й элемент. Это физический сдвиг фазы для сигнала, приходящего с того или иного направления.

Определив физические сдвиги фаз между антенными элементами, рассчитывается угол прихода сигнала. Путем суммирования полученных зна-

чений сигналов, приходящих с выходов антенных элементов, формируется суммарная амплитуда сигнала, принятого с указанного направления. Повторив данную операцию для всех возможных направлений прихода сигнала, можно получить диаграмму направленности антенной решетки.

Для визуализации описанного метода, был составлен алгоритм в среде Mathlab, который наглядно демонстрирует «режим радара» и формирование диаграммы направленности антенной решетки.

Данный алгоритм работает по схеме, представленной на рисунке 2. Данная блок-схема позволяет определять направление прихода помехи и подавлять ее. Визуализация метода представлена на рисунке 3. На данном рисунке представлена диаграмма направленности адаптивной антенной решетки, сформированная в результате работы алгоритма подавления помехи [4].

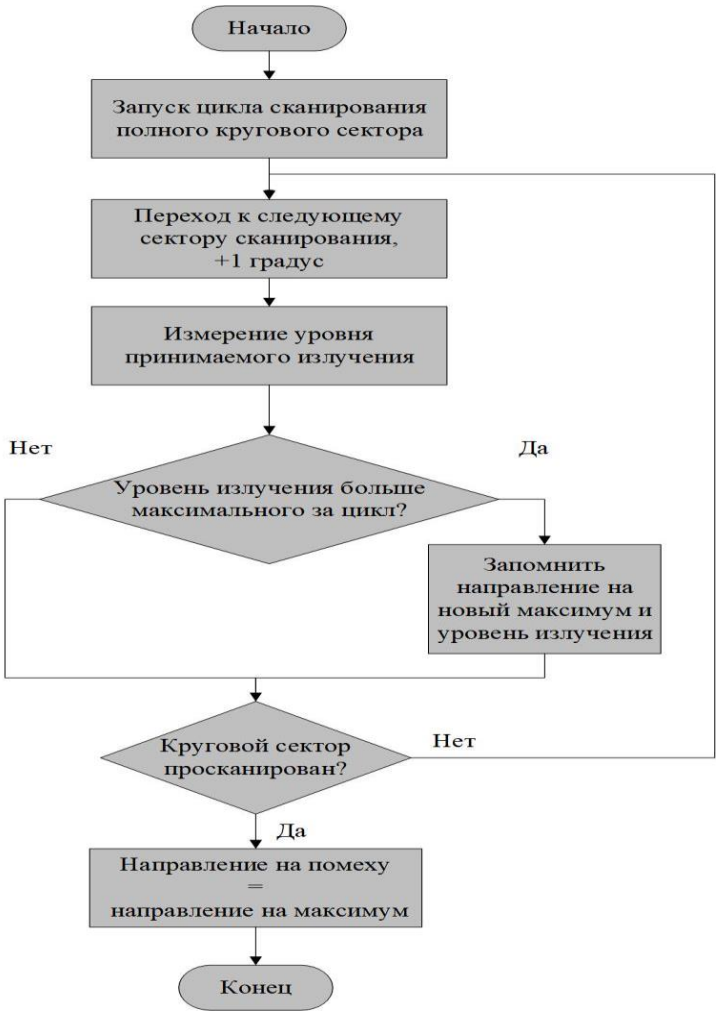


Рис. 2. Блок-схема алгоритма адаптации диаграммы направленности антенной решетки

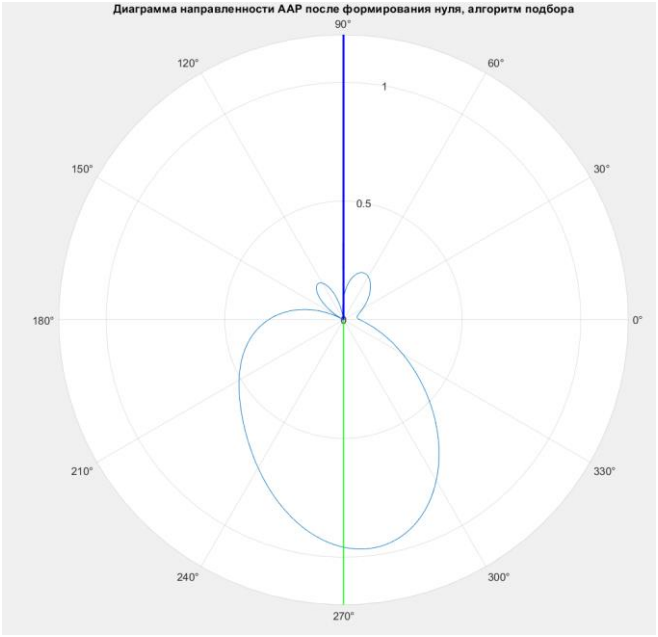


Рис. 3. Визуальное представление алгоритма поиска направления помехи

В данной работе была представлена схема алгоритма адаптации диаграммы направленности ААР, а также рассмотрен метод формирования ДН с учетом фазовых сдвигов между сигналами, поступающими на элементы антенной решетки. Подробно разобрана работа режима кругового сканирования, применяемого для обнаружения направлений помех, что позволяет формировать ДН с главным максимумом в направлении полезного сигнала и подавлять помехи. Разработанный алгоритм в среде MATLAB наглядно демонстрирует эффективность предложенного метода и позволяет визуализировать процесс адаптации ДН.

В заключение хотелось бы отметить, что проведенный анализ метода и реализация алгоритма подтверждают высокую перспективность применения ААР для защиты каналов управления БПЛА от активных помех. Данный метод является наиболее эффективным среди «энергетических» методов подавления помех. Адаптивные антенные системы могут стать основой новых технологий обеспечения устойчивости и надежности каналов связи в условиях сложной радиопомеховой обстановки. Тем не менее, для повышения эффективности таких систем требуется дальнейшее развитие методов адаптации, включая улучшение разрешающей способности и разработку оптимальных алгоритмов обработки сигналов.

Список используемых источников

1. Монзинго Р. А., Миллер Т. У. М77 Адаптивные антенные решетки: Введение в теорию: Пер. с англ. М.: Радио и связь, 1986. 448 с.

2. Марчук Л. А. Пространственно-временная обработка сигналов в линиях радиосвязи. Л.: ВАС, 1991. 135 с.

3. Помехозащищенность радиосистем со сложными сигналами / Г. И. Тузов М.: Радио и связь, 1986. 264 с.

4. Риглер, Комптон Р. Т. Адаптивная антенная решетка для подавления помех // ТИИЭР. 1973. Т. 61. № 6. С. 75-86.

A METHOD OF COMBATING ACTIVE INTERFERENCE IN RADIO ENGINEERING SYSTEMS USING ADAPTIVE ANTENNA ARRAYS

Fedorov P., Galushko I., Kudryavtseva Yu., Titkov I.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

In the context of a special military operation, methods of combating active interference are becoming increasingly relevant, as electronic warfare and counteraction systems are constantly evolving and new methods of jamming are emerging, which in turn lead to disruption of various combat and other important tasks. At the moment, there are a large number of types of interference that need to be addressed through the use of modern radio engineering systems.

Key words: *Active interference, directional pattern, UAV, adaptive antenna arrays*

УДК 004.722
ГРНТИ 49.37.31

ЗАДАЧИ ОПТИМИЗАЦИИ СТРУКТУРЫ СЕТИ РЕТРАНСЛЯТОРОВ НА БАЗЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ПЕРЕДАЧИ ДАННЫХ

А. М. Чуднов, А. Е. Деркач

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

Статья посвящена задачам оптимизации структуры сети ретрансляторов на базе беспилотных летательных аппаратов с целью повышения устойчивости передачи данных в условиях динамически изменяющейся среды. Рассматриваются ключевые аспекты оптимизации, включая формирование системы маршрутных таблиц, кластеризацию сети и управление ресурсами беспилотных летательных аппаратов. Основная цель исследования – максимизация вероятности своевременной доставки сообщений при учете ограниченных ресурсов беспилотных летательных аппаратов, таких как пропускная способность каналов связи, мощность передатчиков и чувствительность приемников.

сеть ретрансляторов, беспилотные летательные аппаратов, сеть обмена данными, устойчивость обмена данными, вероятность, своевременная доставка сообщений

Сети ретрансляторов на базе БПЛА являются перспективным решением для обеспечения устойчивой передачи данных в условиях динамически изменяющейся среды. Основной задачей является оптимизация структуры сети с учетом ограниченных ресурсов БПЛА, включая их технические характеристики и количество. В данной статье рассматриваются задачи оптимизации структуры сети, включая формирование системы маршрутных таблиц, кластеризацию сети и управление ресурсами БПЛА для достижения максимальной эффективности передачи данных. Под эффективностью передачи данных будем понимать своевременность доставки сообщений.

Общая постановка задачи

Оптимизация структуры сети ретрансляторов на базе БПЛА с учетом ограниченных ресурсов и изменяющихся условий среды для достижения максимальной вероятности своевременной доставки сообщений.

Частная постановка задачи

1. Оптимизация системы маршрутных таблиц (ТМП): определение оптимальных маршрутов передачи данных с учетом вероятностно-временных характеристик (ВВХ) обмена сообщениями [1].

2. Кластеризация сети: разбиение сети на кластеры для повышения устойчивости и эффективности передачи данных путем уменьшения ТМП для ускорения расчетов маршрутов.

3. Управление ресурсами БПЛА: учет технических и количественных ограничений БПЛА, таких как пропускная способность каналов связи, мощность передатчиков и чувствительность приемников [2].

Формализация задачи

Для формализации задачи оптимизации введем следующие обозначения:

– потоковая структура сети: определяется распределением потоков $S = (s(\mu))$, где – $s(\mu)$ интенсивность потока данных по маршруту μ.
– ресурс БпЛА: включает ограничения на передающие и приемные средства, задаваемые векторами $U = (u_k)$ и $V = (\upsilon_k)$, где u_k и υ_k – ресурс передающих и приемных средств узла k соответственно.

Задача оптимизации формулируется как максимизация вероятности своевременной доставки сообщений $P(S|C, \Lambda)$ при ограничениях на ресурсы БпЛА:

$$P(S|C, \Lambda) \to max_{S \in S(C)}$$

где $S(C)$ – множество допустимых распределений потоков, определенное канальной структурой C и ресурсами БпЛА.

Методика анализа и оптимизации

Для решения задачи оптимизации используется методика, основанная на анализе вероятностно-временных характеристик обмена сообщениями [1, 3]. Вероятность своевременной доставки сообщений $P(S|C, \Lambda)$ определяется как:

$$P(S|C, \Lambda) = \frac{1}{\lambda_\Sigma} \Sigma_{\mu \in M} s(\mu) P\{t(\mu) \le \tau\},$$

где λ_Σ – суммарная интенсивность потоков, $P\{t(\mu) \le \tau\}$ – вероятность своевременной доставки пакета по маршруту μ, определяемая сверткой распределений времени задержки в линиях связи:

$$P\{t(\mu) \le \tau\} = \Pi_{(k,l)\in\mu} P\{t(k,l) \le \tau | S_{k,l}\}.$$

Для расчета вероятности $P\{t(k,l) \le \tau | S_{k,l}\}$ используется модель системы массового обслуживания (СМО) [4]:

$$P\{t(k,l) \le \tau | S_{k,l}\} = 1 - \exp\left(-\frac{\tau}{T_{k,l}}\right),$$

где $T_{k,l} = \frac{1}{C\prime_{k,l} - S_{k,l}}$ – среднее время задержки пакета в линии связи *(k ,l)*.

Для уменьшения размеров ТМП и ускорения расчетов маршрутов в сети обмена данными ретрансляторов на базе БПЛА можно использовать кластеризацию сети.

Предположим, что на каждом звене передачи (например, внутри кластера) сообщение проходит через *N* узлов (ретрансляторов), причем в каждом узле происходит обработка таблицы маршрутизации. Пусть:

N – количество узлов (или, что эквивалентно, количество таблиц маршрутизации, через которые проходит сообщение). При кластеризации сети *N* может уменьшаться за счет локального принятия решения в каждом кластере;

S – средний размер (количество записей, элементов) таблицы маршрутизации в одном узле;

K – коэффициент, характеризующий затраты времени на обработку одной единицы информации при поиске и анализе записей маршрутизации (сек/бит);

t_{proc} – фиксированное время обработки (помимо поиска по таблице), связанное с формированием/обработкой пакета к узле;

T_0 – базовое время передачи пакета по канальным звеньям (без учета маршрутизации).

Кроме того, при увеличении интенсивности потока данных λ (сообщений/сек) в узле может возрастать время ожидания (очередь) перед обработкой. Применим простейшую модель очередей M/M/1, где среднее время ожидания (среднее время нахождения в системе) описывается выражением:

$$T_{queue} = 1 \,/\, (\mu - \lambda)$$

где μ – пропускная способность узла (максимальное количество сообщений, обрабатываемых в секунду). При условии $\lambda < \mu$.

Итоговая формула передачи сообщения

Принимаем, что время передачи одного сообщения T_{msg} складывается из:

– базового времени передачи по сети T_0;
– суммарного времени обработки на всех *N* узлах, где в каждом узле учитывается время поиска по таблице и служебная обработка, то есть ($t_{proc} + k \cdot S$);

– и дополнительных задержек, связанных с перегрузкой узлов (очередь, T_{queue}).

Таким образом, можно записать приближенную формулу:

$$T_{msg} = T_0 + N \cdot (t_{proc} + k \cdot S) + 1/(\mu - \lambda)$$

Эта формула иллюстрирует, что время передачи сообщения возрастает при:

– увеличении количества узлов N (или при отсутствии эффективной кластеризации, когда N велико);
– увеличении размера таблицы маршрутизации S (при условии линейной зависимости времени поиска);
– увеличении интенсивности трафика λ, приближаясь к пределу узловой пропускной способности μ.

При кластерном формировании сети можно считать, что маршрутизация внутри кластера происходит быстрее (благодаря уменьшенному размеру таблиц и более локальному характеру обмена), поэтому параметр N и S в вышеуказанной формуле можно принять за усредненные по кластерам соответственно.

Зависимость T_{msg} от интенсивности трафика λ при разных значениях размера таблицы маршрутизации S показана на рисунке 1.

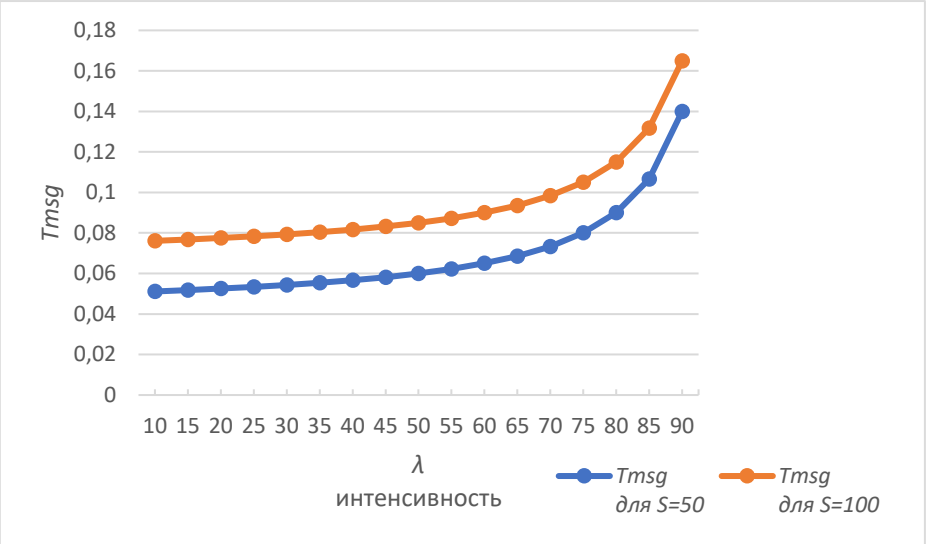


Рис. 1. Зависимость времени доставки одного сообщения от интенсивности трафика при размерах таблиц маршрутизации пакетов 50 и 100 строк

Представленная модель и построенный график позволяют увидеть, как ключевые параметры (количество узлов N, размер таблицы S и интенсивность трафика λ) влияют на общее время передачи сообщения T_{msg}, а также демонстрируют преимущество кластеризации сети (которая снижает N и, возможно, S в локальных кластерах).

Предлагается модель, связывающая время передачи сообщения с количеством и размерами таблиц маршрутизации пакетов, параметрами кластера сети обмена данными (на основе групп ретрансляторов на БПЛА) и интенсивностью потока данных.

Предположим, что:

N – общее число ретрансляторов (БПЛА) в сети;

K – число кластеров (при делении сети на кластеры). Тогда в каждом кластере в среднем $n_{(k)} = N/K$ узлов;

каждый узел хранит в таблице маршрутизации записи только для узлов своего кластера (исключая себя), т.е. число записей $r = n_{(k)}-1$;

sentry – средний размер одной записи маршрутизации (в битах или байтах);

L_{msg} – размер полезной нагрузки передаваемого сообщения (в битах или байтах);

B – пропускная способность канала передачи (бит/с);

I – интенсивность входящего потока данных (количество пакетов в секунду) – значение, влияющее на очереди в устройстве передачи;

k – коэффициент, характеризующий затраты времени на обработку одной единицы информации при поиске и анализе записей маршрутизации (сек/бит).

Можно выделить три составляющие задержки передачи сообщения:

Процессорное время (T_{proc}) на обработку таблицы маршрутизации. Предположим, что на обработку одной записи требуется время k, тогда:

$$T_{\text{proc}} = k(n_{(k)} - 1) \cdot sentry$$

1. Время непосредственно на передачу пакета (T_{tx}). При условии, что суммарный размер пакета складывается из полезной нагрузки и служебных данных, зависящих от количества и размера записей маршрутизации, можно записать:

$$Ttx = L_{\text{msg}} + \frac{(n_{(k)}-1)\cdot sentry}{B},$$

где $(n_{(k)} - 1) \cdot sentry$ – совокупный объем служебной информации, накладываемой на пакет (например, для маршрутизации внутри кластера).

2. Очередь (T_{queue}) – задержка, обусловленная интенсивностью потока данных. Если считать систему приближенно, как M/M/1, где μ сервисная мощность канала (в пакетах/с), то

$$\mu = \frac{B}{L_{\text{msg}}} + (n_{(k)} - 1) \cdot sentry,$$

и средняя задержка в очереди будет: $T_{\text{queue}} = \frac{1}{\mu - I}$, при условии, что $I < \mu$ (иначе система нестабильна).

Таким образом, итоговое время передачи одного сообщения можно записать как:

$$T_{\text{msg}} = T_{\text{proc}} + T_{tx} + T_{\text{queue}} = k \cdot (n_{(k)} - 1) \cdot sentry + L_{\text{msg}} + \frac{(n_{(k)} - 1) \cdot sentry}{B} + \frac{1}{\frac{B}{L_{\text{msg}}} + (n_{(k)} - 1) \cdot sentry - I}.$$

При подстановке $n_{(k)}=N/K$ получаем:

$$T_{\text{msg}} = T_{proc} + T_{tx} + T_{\text{queue}} = k \cdot \left(\frac{N}{K} - 1\right) \cdot sentry + L_{msg} + \frac{\left(\frac{N}{K} - 1\right) \cdot sentry}{B} + \frac{1}{\frac{B}{L_{msg}} + \left(\frac{N}{K} - 1\right) \cdot sentry - I}.$$

Эта формула позволяет оценить, как изменяется время передачи сообщения в зависимости от:

– числа кластеров (K): при увеличении K число узлов в одном кластере (N/K) уменьшается, что сокращает и размер таблицы маршрутизации;
– размер таблиц (через *sentry*) и полезной нагрузки (L_{msg});
– пропускной способности канала (B);
– интенсивности потока данных (I).

Зависимость времени доставки одного сообщения от количества кластеров в сети обмена данными показана на рисунке 2.

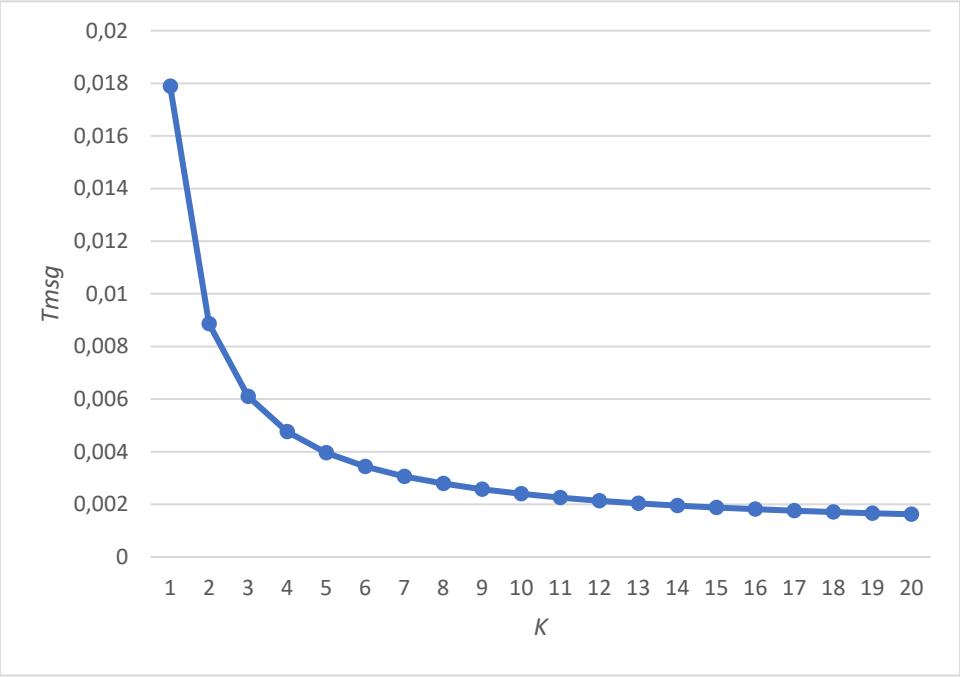


Рис. 2. Зависимость времени доставки одного сообщения от количества кластеров в сети обмена данными

Заключение

Проведен анализ задач оптимизации структуры сети ретрансляторов на базе БПЛА с учетом ограниченных ресурсов и изменяющихся условий среды. Разработанная методика позволяет достичь максимальной эффективности передачи данных за счет оптимизации системы маршрутных таблиц, кластеризации сети и управления ресурсами БПЛА.

Список используемых источников

1. Чуднов А. М., Губская О. А., Кичко Я. В. Методика анализа вероятностно-временных характеристик обмена сообщениями в комплексе беспилотных летательных аппаратов // Известия ТулГУ. Технические науки. 2021. № 11. С. 117–124.

2. Чуднов А. М., Положинцев Б. И., Кичко Я. В. Анализ помехозащищенности обмена данными группы беспилотных летательных аппаратов в условиях оптимизированных помех // Радиотехника. 2022. Т. 86. № 12. С. 33–46.

3. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений // Радиотехнические и телекоммуникационные системы. 2017. № 2. С. 41–49.

4. Чуднов А. М., Путилин А. Н., Попов А. И. Комплексное управление маршрутизацией пакетов и режимами работы радиосредств в неоднородной сети передачи данных // Радиотехнические и телекоммуникационные системы, 2019. № 1. С. 46-56

OPTIMIZATION PROBLEMS OF THE STRUCTURE OF A REPEATER NETWORK BASED ON UNMANNED AERIAL VEHICLES TO INCREASE THE STABILITY OF DATA TRANSMISSION

Chudnov A., Derkach A.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is devoted to the problems of optimising the structure of the drone-based repeater network in order to improve the stability of data transmission in a dynamically changing environment. The key aspects of optimisation are considered, including the formation of a routing table system, network clustering and drone resource management. The main objective of the study is to maximise the probability of timely message delivery while taking into account limited drone resources such as link bandwidth, transmitter power and receiver sensitivity.

Key words: *Repeater network, unmanned aerial vehicles, data communication network, data communication stability, probability, timely message delivery*

КИБЕРБЕЗОПАСНОСТЬ

УДК 004.934
ГРНТИ 20.53.15

РАЗРАБОТКА МЕТОДА НЕЙРОСЕТЕВОЙ СТЕГАНОГРАФИИ ДЛЯ ВСТРАИВАНИЯ МЕДИЦИНСКИХ ДАННЫХ ПАЦИЕНТА В ИЗОБРАЖЕНИЯ

К. Д. Аксенов

ООО «Пространство интеллектуальных решений», г. Новороссийск
Московский государственный технический университет им. Н. Э. Баумана
Кубанский государственный технологический университет

Одним из перспективных подходов, позволяющих решить проблему конфиденциальности медицинских данных, является использование стеганографии – метода сокрытия информации в цифровых объектах. В настоящем исследовании предложен метод нейросетевой стеганографии, позволяющий внедрять текстовые медицинские данные в изображения, который обеспечивает обезличивание данных и позволяет добиться значений метрик точности модели PSNR и SSIM - 30.12 dB и 0.8843 соответственно.

стеганография, нейронные сети, медицинские данные, защита информации, глубокое обучение

Глубокое обучение для медицинской визуализации сталкивается со значительными трудностями при использовании достижений из других областей компьютерного зрения из-за проблем с конфиденциальностью и ограниченного доступа к данным [1-3]. Обеспечение конфиденциальности медицинских данных является одной из наиболее важных задач в области здравоохранения. Информация о пациентах должна оставаться защищенной, в то время как обмен ею между медицинскими учреждениями должен быть оперативным и надежным. Основным решением для защиты данных от подслушивания и угроз является шифрование, которое скрывает исходные данные, превращая их в зашифрованный текст, но которое также может вызвать подозрения из-за видимости вносимых изменений. Одним из перспективных подходов, позволяющих решить эту проблему, является ис-

пользование стеганографии – метода скрытия информации в цифровых объектах. Для обнаружения наличия любого секретного сообщения, скрытого в изображении, используют стегоанализ [4-6].

Глубокое обучение является полезным инструментом в различных приложениях, таких как классификация изображений, автоматическое распознавание речи, распознавание объектов, обработка естественного языка, рекомендательные системы, обработка медицинских данных [7]. Методами глубокого обучения, которые используют в совокупности с методами стеганографии и стегоанализа, являются сверточные нейронные сети (CNN). Стеганография изображений с использованием моделей CNN часто основана на применении архитектуры сети энкодер-декодер [8-13]. Два входа – изображение обложки и секретное изображение – подаются в качестве входных данных в кодировщик для генерации стегоизображения, а стегоизображение – в качестве входных данных в декодер для вывода встроенного секретного изображения. Wu и др. [8, 9] использовали сверточные сети с остаточными блоками и ELU-активацией для встраивания и извлечения скрытого изображения, предлагая функцию потерь для уменьшения шумов. Duan и др. [10] адаптировали U-Net для обработки изображений 256×256 с шестиканальным вводом, объединяя изображения перед подачей в сеть. Van и др. [11] применили H-net и R-net с оптимизацией на основе SSIM и MSE для улучшения качества восстановления. Rahim и др. [12] предлагают параллельную архитектуру для обработки изображений, где признаки объединяются на этапе кодирования. Zhang и др. [13] используют YCrCb пространство, кодируя скрытое изображение в Y-канале, а также применяют комбинированные потери на основе SSIM и MS-SSIM.

В настоящем исследовании предложен метод нейросетевой стеганографии, позволяющий внедрять текстовые медицинские данные в изображения, используемые в медицинских системах. Такой подход обеспечивает обезличивание данных, а также повышает устойчивость к стегоаналитическим атакам.

Для решения этой задачи была разработана гибридная архитектура нейронной сети, включающая энкодер и декодер. Энкодер служит для встраивания текстовой информации в изображение, а декодер – для восстановления этого текста. В качестве исходных данных использовались изображения размером 512x512 пикселей, а текстовые сообщения были ограничены длиной в 100 символов. Для кодирования текстовых сообщений был использован набор всех печатных символов, представленных в библиотеке

Python string.printable. Каждому символу было назначено уникальное значение, а сообщение кодировалось в последовательность чисел. Таким образом, обеспечивалось единообразие и стандартизация входных данных для модели.

Архитектура энкодера состояла из нескольких слоев: слой для обработки текстовой информации, включающий эмбеддинги, полносвязные слои, а также сверточные слои для обработки изображения. После объединения признаков изображения и сообщения полученное скрытое изображение обрабатывалось финальной сверточной сетью для формирования окончательного результата. Декодер, в свою очередь, использовал сверточные слои для извлечения информации из закодированного изображения, а затем использовал полносвязные слои для восстановления исходного текста.

В ходе обработки текстовой информации текстовое сообщение M сначала кодируется в эмбеддинг-пространство:

$$E = Embed(M),$$

где $E \in \mathbb{R}^{L \times d}$ – эмбеддинги текста длины L, с размерностью эмбеддинга d.

Далее изображение преобразовывалось через полносвязный слой:

$$F_m = FC(E),$$

где $F_m \in \mathbb{R}^{H \times W}$ – результат, представленный в пространственном формате (совпадающем с размером изображения).

Исходное изображение I пропускается через несколько сверточных слоев для извлечения признаков:

$$F_i = Conv(I),$$

где $F_i \in \mathbb{R}^{C \times H \times W}$ – карта признаков изображения, C – число каналов.

После обработки, признаки изображения и текста объединяются вдоль канального измерения:

$$F_c = Concat(F_i, F_m),$$

где $F_c \in \mathbb{R}^{(C+1) \times H \times W}$.

После объединения признаков изображения и сообщения полученное скрытое изображение обрабатывалось финальным сверточным слоем для формирования окончательного результата:

$$I_s = Conv_{final}(F_c),$$

где $I_s \in \mathbb{R}^{3 \times H \times W}$ – закодированное RGB-изображение.

Декодер, в свою очередь, использует сверточные слои для обработки закодированного изображения:

$$F_{i_s} = Conv_{decoder}(I_s),$$

где F_{i_s} – промежуточное представление.

Затем полносвязные слои восстанавливают текст:

$$M_r = FC_{decoder}(F_{i_s}),$$

где M_r – восстановленное сообщение.

Модель была обучена с использованием функции потерь, комбинирующей три компонента: потери на основе среднеквадратической ошибки между исходным и закодированным изображением, перцептуальные потери и потери восстановления сообщения. Общая функция потерь была определена как сумма с коэффициентами весов, чтобы сбалансировать влияние каждой из составляющих:

$$\mathcal{L} = \lambda_1 \cdot \mathcal{L}_{MSE} + \lambda_2 \cdot \mathcal{L}_{perc} + \lambda_3 \cdot \mathcal{L}_{msg},$$

где $\mathcal{L}_{MSE} = \|I - I_s\|^2$– среднеквадратичная ошибка между оригинальным и закодированным изображением,

$\mathcal{L}_{perc} = \|\phi(I) - \phi(I_s)\|^2$– перцептуальная ошибка, вычисляемая через функции признаков ϕ, извлекаемых с помощью VGG-19,

$\mathcal{L}_{msg} = -\sum_{i=1}^{N} y_i log(p_i)$ – кросс-энтропийная ошибка для восстановления сообщения.

Для оценки точности модели использовались такие метрики, как PSNR (Peak Signal-to-Noise Ratio) и SSIM (Structural Similarity Index). Метрика PSNR характеризует соотношение мощности сигнала к мощности шума, что позволяет оценить, насколько сильно изображение искажено после внедрения информации. PSNR вычисляется на основе среднеквадратической ошибки (MSE) между исходным изображением I и закодированным изображением I_s:

$$MSE = \frac{1}{H \cdot W \cdot C} \sum_{h=1}^{H} \sum_{w=1}^{W} \sum_{c=1}^{C} (I(h,w,c) - I_s(h,w,c))^2,$$

где H, W и C – высота, ширина и число каналов изображения соответственно.

Затем PSNR рассчитывается по формуле:

$$PSNR = 10 \cdot log_{10}\left(\frac{MAX^2}{MSE}\right),$$

где *MAX* – максимальное возможное значение интенсивности пикселя (например, 255 для 8-битных изображений).

Метрика SSIM сравнивает структурное сходство между изображениями. Она учитывает три компонента: яркость, контраст и структуру. SSIM для двух изображений I и I_s определяется как:

$$SSIM(I, I_s) = \frac{(2\mu_I\mu_{I_s}+C_1)(2\sigma_{II_s}+C_2)}{(\mu_I^2+\mu_{I_s}^2+C_1)(\sigma_I^2+\sigma_{I_s}^2+C_2)},$$

где $\mu_I\mu_{I_s}$ – средние значения интенсивности пикселей в I и I_s,

$\sigma_I^2 + \sigma_{I_s}^2$ – дисперсии интенсивности пикселей в I и I_s,

σ_{II_s} – ковариация между I и I_s,

$C_1 = (k_1L)^2$ и $C_2 = (k_2L)^2$ – небольшие константы для предотвращения деления на ноль (L – динамический диапазон значений пикселей, например, 255 для 8-битных изображений; k_1и k_2– обычно выбираются как 0.01 и 0.03 соответственно).

Обучение алгоритма проводили на рабочей станции с процессором Intel Xeon, с двумя графическими процессорами Nvidia Tesla K80 емкостью 24 ГБ и 64 ГБ оперативной памяти. Использовался язык программирования Python версии 3.7.11. Для обучения и валидации нейронных сетей были использованы библиотека Tensorflow. Применение алгоритма детекции контуров и расчета количественных характеристик было реализовано с помощью библиотеки OpenCV. Статистическую оценку полученных данных, а также построение графиков проводили с использованием библиотек pandas, scipy, matplotlib, seaborn.

В результате оценки точности были получены высокие значения PSNR и SSIM, которые составили 30.12 dB и 0.8843 соответственно. Для изображений высокого качества значения PSNR обычно превышают 30 dB. При этом PSNR в диапазоне 20-30 dB считается удовлетворительным, так как визуальные искажения могут быть заметны. Значения SSIM близкие к 1 (например, 0.8-1.0) указывают на высокое структурное сходство изображений. Таким образом, данные результаты свидетельствуют о минимальном искажении визуальных данных, при котором внедрение текста практически незаметно для человеческого глаза. Применение предложенной модели может обеспечить дополнительный уровень защиты информации при передаче медицинских данных по незащищенным каналам.

Также можно отметить, что предложенный метод нейросетевой стеганографии может быть полезен не только в медицине, но и в других областях,

где требуется обеспечение конфиденциальности данных, например, в правовой и финансовой сферах. В дальнейшем планируется расширение экспериментов с использованием более разнообразных данных, а также исследование возможности применения более сложных архитектур нейронных сетей для повышения устойчивости к атакам и снижения искажений в данных.

Список используемых источников

1. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии / А. В. Красов, Д. Н. Шакин, Н. Н. Лансере [и др.] // Офтальмохирургия. 2022. № S4. С. 92-101. DOI 10.25276/0235-4160-2022-4S-92-101. EDN IYQQXV.

2. Mohammed Adnan, Shivam Kalra, Jesse Cresswell, Graham Taylor and Hamid Tizhoosh. Federated learning and differential privacy for medical image analysis. Scientific reports, 2022, 12(1): 1953.

3. Bell J. H., Bonawitz K., Gascón A., Lepoint T. and Raykova M. Secure single-server aggregation with (poly) logarithmic overhead. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020. PP. 1253–1269.

4. Коржик В. И. Цифровая стеганография: учебник / В. И. Коржик, А. В. Красов. Москва: Общество с ограниченной ответственностью "Издательство "КноРус", 2023. 324 с. ISBN 978-5-406-10970-0. EDN KNKBXU.

5. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных / А. А. Миняев, А. В. Красов, Д. В. Сахаров // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29-33. DOI 10.46418/2079-8199_2020_1_5. EDN ULHTJK.

6. Shi H., Zhang X.-Y., Wang S., Fu G., and Tang J. Synchronizeddetection and recovery of steganographic messages with adversarial learning. Proc. Int. Conf. Comput. Sci. Cham, Switzerland: Springer, 2019. PP. 31–43

7. Hordri N. F., Yuhaniz S. S. and Shamsuddin S. M. Deep learning and its applications: A review. Proc. Conf. Postgraduate Annu. Res. Informat. Seminar, 2016. PP. 1–6

8. Wu P., Yang Y., X. Li. Image-into-image steganography using deep convolutional network. Proc. Pacific Rim Conf. Multimedia. Cham, Switzerland: Springer, 2018. PP. 792–802.

9. Wu P., Yang Y. and Li X. StegNet: Mega image steganography capacity with deep convolutional network. Future Internet. Vol. 10, № 6, p. 54, Jun. 2018.

10. Duan X., Jia K., Li B., Guo D., Zhang E. and Qin C. Reversible image steganography scheme based on a U-Net structure. IEEE Access. Vol. 7. PP. 9314–9323, 2019

11. Van T. P., Dinh T. H. and Thanh T. M. Simultaneous convolutional neural network for highly efficient image steganography. Proc. 19th Int. Symp. Commun. Inf. Technol. (ISCIT), Sep. 2019. PP. 410–415.

12. Rahim R. and Nadeem S. End-to-end trained CNN encoder-decoder networks for image steganography. Proc. Eur. Conf. Comput. Vis. (ECCV), 2018. PP. 1–6.

13. Zhang R., Dong S., and Liu J. Invisible steganography via generative adversarial networks. Multimedia Tools Appl. Vol. 78, № 7. PP. 8559–8575, Apr. 2019.

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

DEVELOPMENT OF A NEURAL NETWORK STEGANOGRAPHY METHOD FOR EMBEDDING PATIENT MEDICAL DATA INTO IMAGES

Aksenov K.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

One of the promising approaches to address the issue of medical data confidentiality is the use of steganography–a method of hiding information within digital objects. This study proposes a neural network-based steganography method for embedding textual medical data into images, ensuring data anonymization and achieving model accuracy metrics with PSNR and SSIM values of 30.12 dB and 0.8843, respectively.

Key words: *Steganography, neural networks, medical data, information security, deep learning*

УДК 004.056.5
ГРНТИ 004.056.5

БИОМЕТРИЧЕСКИЕ ДАННЫЕ И ИХ ВОЗМОЖНОСТИ ДОСТИЖЕНИЯ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ МЕТОДОМ ОДНОРАЗОВОГО ПАРОЛЯ

Ю. М. А. А. Альотум

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

Организации стремятся достичь принципа безопасности в своих технологических системах с меньшими затратами и с высокой эффективностью. В последнее время внимание обращается на использование многофакторной аутентификации, но это дорого. В этой статье мы изучим, как использовать метод одноразового пароля и превратить его в недорогую систему многофакторной аутентификации.

Одноразовый пароль (OTP), многофакторная аутентификация (MFA), динамика нажатия клавиш, биометрические данные

Аутентификация пользователя служит первой линией обороны против фальсификации пользователя, что является серьезным риском безопасности для любой компьютерной системы. Независимо от того, выполняется ли аутентификация онлайн или офлайн, она является важнейшей защитой от несанкционированного доступа к сервису, устройству или данным [1].

Многофакторная аутентификация

Многофакторная аутентификация (MFA) – это процесс входа в систему, который состоит из нескольких шагов и требует от пользователя указать больше информации, а не только пароль.

Поскольку отпечатки пальцев и сканирование радужной оболочки глаза часто чрезвычайно точны в своей разработке и использовании, MFA обычно включает в себя уникальные биологические черты пользователя [2]. Объединение по крайней мере трех различных типов учетных данных является методом повышения безопасности для предотвращения несанкционированного доступа к компьютерному оборудованию и другим важным услугам [1]. Возьмем в пример снятие денег из банкомата (ATM). Фактор знания представлен PIN-кодом, а фактор владения представлен физическим токе-

ном (банковской картой), который пользователь должен предъявить для доступа и снятия средств с личного счета. Рисунок 1 иллюстрирует, как добавление второго биометрического метода [1] может повысить безопасность этой системы.

Уникальные, количественно определяемые признаки, называемые биометрическими, используются для категоризации и характеристики людей. Чтобы защитить различные ресурсы, они могут использоваться для идентификации или верификации. Он отличается от других подходов тем, что обеспечивает большую безопасность (позволяя использовать биометрические данные для защиты от определенных атак, включая фишинг), устраняет необходимость запоминать пароль или другие предметы и символы, которые предоставляют доступ к ресурсам, и его невозможно забыть или потерять [3]. Биометрию можно разделить на две подкатегории: поведенческая и физиологическая биометрия. Физиологическая биометрия использует физические характеристики человеческого тела, включая лицо, вены, отпечатки пальцев или радужную оболочку глаза, для проверки личности. Поведенческая биометрия и физиологическая биометрия могут использоваться с фактором одноразового пароля либо путем генерации случайного пароля на основе этих измерений, либо с использованием его в качестве дополнительного фактора, поскольку этот процесс считается многофакторной аутентификацией [3, 4, 5].

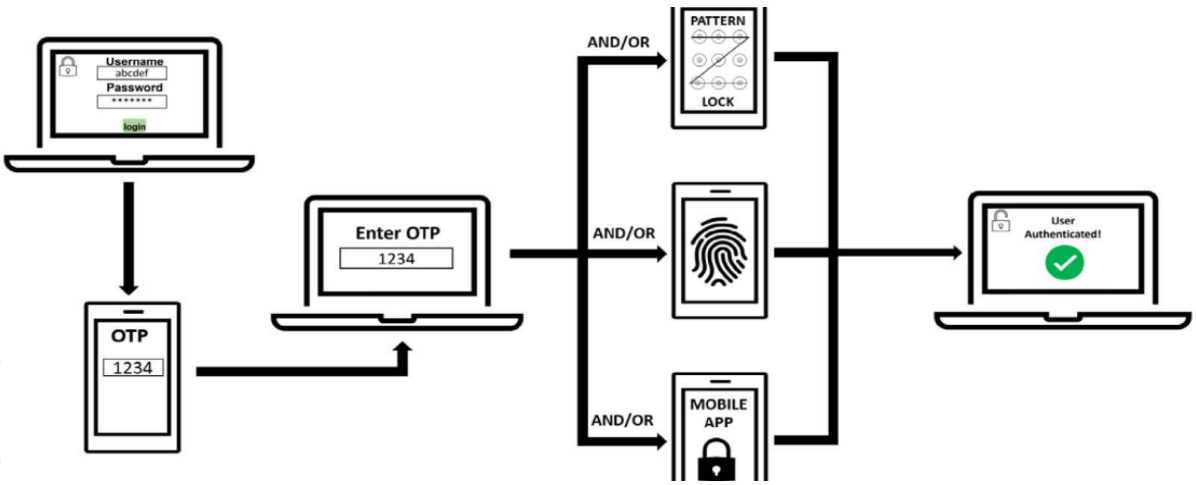


Рис. 1. Многофакторная аутентификация (MFA)

Одним из недорогих методов биометрической аутентификации, которой требуется только существование клавиатуры, является динамика нажатия клавиш, основанная на поведенческих биометрических измерениях пользователя, как показано на рисунке 2.

Происходит процесс анализа действий пользователя при вводе, отслеживая ввод с клавиатуры тысячи раз в секунду с целью распознавания пользователя на основе его ритмических шаблонов ввода текста, и это представляет собой изучение уникального времени в индивидуальном ритме написания [1, 2, 6]. Методы динамики нажатия клавиш не зависят от языка, поскольку функции в первую очередь зависят от того, как пользователь использует клавиатуру, а не от слов, которые он набирает на данном языке [6]. Спиллейн был первым, кто изобрел использование клавиатуры для измерения динамики нажатия клавиш людьми [7]. Первым, кто показал, что динамику нажатия клавиш можно использовать для аутентификации, является Gaines, 1980 [6, 8].

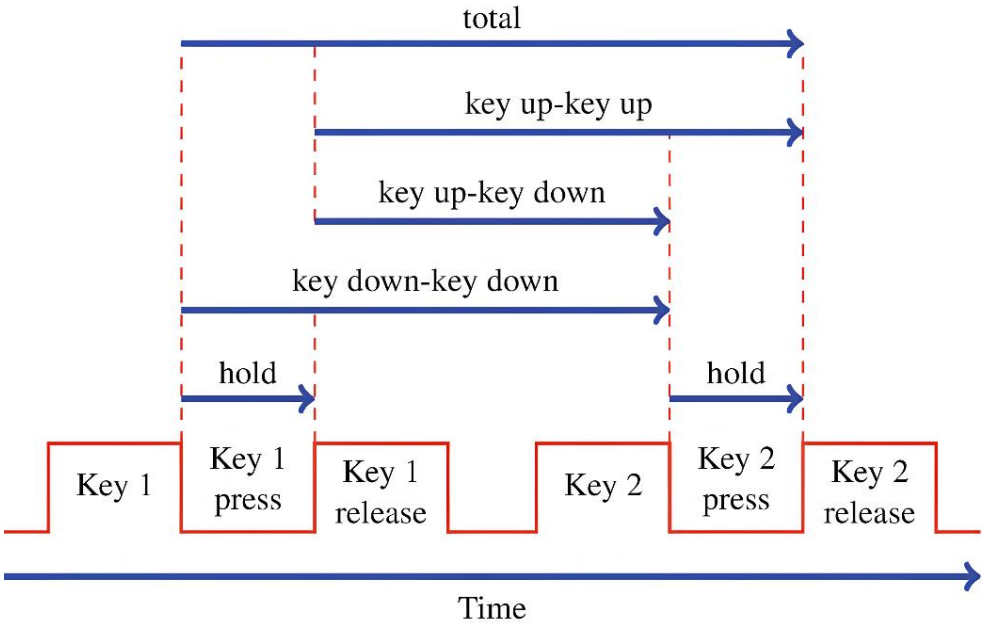


Рис. 2. Принцип извлечения характеристик нажатия клавиш

На этапе обучения динамике нажатия клавиш для каждого пользователя создается специальный порог. Один из способов создания порогового значения – использование манхэттенского и Евклидового расстояния [5].

$$d_T(p,q) = \sum_{i}^{n} |(p_i - q_i)| / \alpha_i$$

$$d(p,q) = \sqrt[2]{\sum_{i}^{n} (p_i - q_i / \alpha_i)^2}$$

где (p, q) –значений временных меток клавши; α_i –все клавиши, введенные на клавиатуре в процессе входа в систему и ввода пароля.

Одноразовый пароль

Благодаря использованию одноразового пароля (OTP) пользователю предоставляется уникальный пароль, который он может использовать только один раз для входа в систему или подтверждения своей личности [1–3].

Тот факт, что пароль действителен только для одного сеанса входа, добавляет еще одну степень защиты. Он больше не действителен после использования, поэтому злоумышленники не могут использовать его снова. Это код символов, который создается автоматически и служит для аутентификации пользователя для сеанса входа [8].

Статические пароли, особенно созданные пользователями, которые могут быть слабыми и использоваться для нескольких учетных записей, менее безопасны, чем пароли, требующие одноразового пароля. Можно заменить традиционную информацию для входа в систему аутентификации или могут использоваться в дополнение к ней для добавления еще одного уровня безопасности [4, 7].

Принцип работы OTP

1. Запрос кода: в рамках дополнительной проверки безопасности система будет требовать ввода одноразового пароля каждый раз, когда пользователь пытается авторизоваться в своей учетной записи или подтвердить выполнение транзакции [4, 5, 8].

2. Отправка кода: по запросу система отправит сгенерированный OTP на устройство, зарегистрированное пользователем. Доставка кода может осуществляться через SMS, электронную почту или специализированные приложения для аутентификации [5].

3. Проверка кода: пользователю необходимо ввести полученный OTP в соответствующее поле. Система проверит корректность введенного кода и подтвердит его соответствие [8].

4. Подтверждение доступа: если введенный OTP совпадает с тем, что был отправлен системой, доступ к учетной записи или транзакции будет предоставлен. В случае неверного или недействительного кода доступ будет отклонен [4], как показано на рисунке 3.

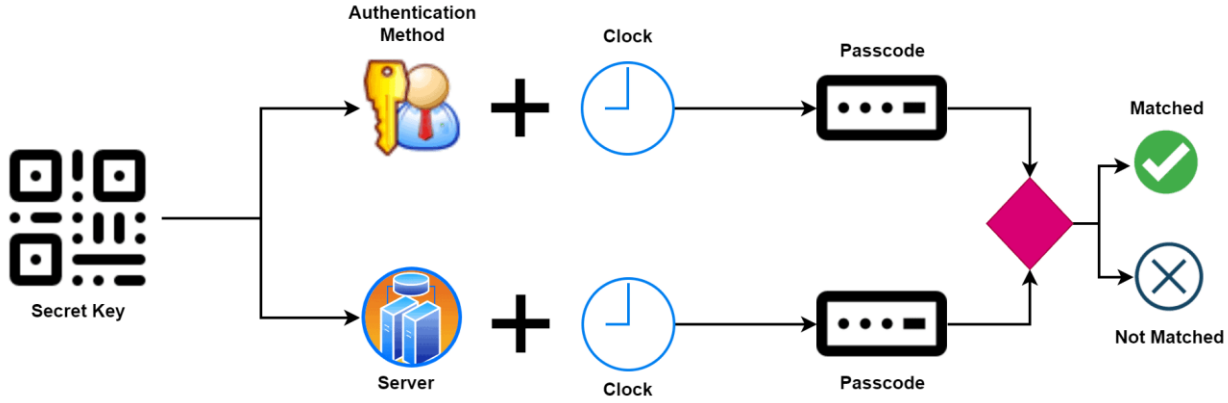


Рис. 3. Принцип работы OTP

Фактор одноразового пароля на основе поведенческо-биометрических данных в многофакторной аутентификации

Добавление третьего фактора в процессы аутентификации считается MFA [6, 8].

Суть MFA заключается в усилении защиты за счет добавления дополнительных уровней безопасности, которые выходят за пределы стандартной пары логина и пароля. Для подтверждения своей личности пользователь должен предоставить дополнительные данные, называемые факторами аутентификации [9, 10, 11]. Эти факторы делятся на основные категории:

1. Фактор знания: информация, известная только пользователю, например, пароль, PIN-код или ответ на секретный вопрос.

2. Фактор владения: физический или виртуальный объект, находящийся в распоряжении пользователя. Это может быть физическое устройство, такое как смарт-карта или USB-токен, или виртуальный элемент, например, одноразовый пароль (OTP), сгенерированный через мобильное приложение для аутентификации

3. Фактор свойства: уникальные биометрические характеристики пользователя, такие как отпечаток пальца, сканирование лица или радужной оболочки глаза.

В системе [8] использовался фактор знания, когда пользователь вводит имя пользователя и пароль. Также использовался фактор владения, где извлекалась динамическая биометрическая информация для нажатий клавиш. Чтобы определить личность человека, написавшего пароль, это тот же человек, который написал правильный пароль, а также определение руки по использованию клавиатуры. В разделе фактора свойства будет использоваться функция одноразового пароля. То же самое, но особым и другим способом,

поскольку система генерирует случайное слово из пароля, введенного пользователем, связанное с динамическими биометрическими данными для измерения нажатия клавиш.

Таким образом, процесс аутентификации основан на поведенческих биометрических данных о нажатиях клавиш, которые пользователь обучил и ввел в процесс проверки.

Соответственно, разные факторы аутентификации использовались неодинаково для конечной цели повышения эффективности безопасности и защиты пользовательских данных от взлома с меньшими затратами.

Список используемых источников

1. Swagatam B., Hafizul I. Quantum-attack-resilience OTP-based multi-factor mutual authentication and session key agreement scheme for mobile users // Computers and Electrical Engineering. 2024. Т. 119. С. 1120–1141.

2. Varasiddhi J. G., Yashwanth P. V., Srinidhi V. B., Ramesh T. K. Smart Door Using Biometric NFC Band and OTP Based Methods // International Conference for Emerging Technology (INCET). 2020. Т. 3. С. 60–64.

3. Красов А. В., Альотум Ю., Ушаков И. А. Аутентификация и идентификация пользователя с использованием биометрической динамики нажатия клавиш на основе «манхэттенского и евклидовского расстояния» // Вестник. 2023. Т 4. С. 49–56.

4. Yousef M. A. A. A. Biometric and behavioral authentication and soft biometrics using keystroke and mouse dynamics // ICAIT. 2023. И. 1. С. 70–75.

5. Альотум Ю. М. А. А., Пешков А. И. Пат. 2024664769 Свидетельство о государственной регистрации программы для ЭВМ Российская Федерация. Программа по многофакторной аутентификации пользователей на основе биометрических динамических методов. – № 2024663318: заявл. 11.06.2024; опубл. 24.06.2024.

6. Seeger M., Bours P. How to Comprehensively Describe a Biometric Update Mechanisms for Keystroke Dynamics. Third International Workshop on Security and Communication Networks (IWSCN) // Электротехника. 2011, Т. 45. С. 48–55.

7. Banerjee S., Woodard D. Biometric Authentication and Identification using Keystroke Dynamics: A Survey.Pattern Recognition Research// Электротехника. 2012. Т. 7. С. 116–139.

8. Hassan S., Selim M., Zayed H. User Authentication with Adaptive Keystroke Dynamics . International Journal of Computer Science Issues // Электротехника. 2013. Т.10, С. 127–135.

9. Maria P., Leandros M., Nick A. Modern Authentication Methods: A Comprehensive Survey // IntechOpen. 2022. Т 2. С. 1–24.

10. Devendra K. One Time Password Security Security System // International Journal of Advance Research and Development. 2020. Т. 2. С. 40–46.

11. Chun Y. H., Shang P. M., Kuan T. C. Using one-time passwords to prevent password phishing attacks // Journal of Network and Computer Applications. 2022. Т. 34. С. 1292–1301.

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

BIOMETRIC DATA AND ITS POTENTIAL TO ACHIEVE MULTI-FACTOR AUTHENTICATION USING ONE-TIME PASSWORD METHOD

Alotoum Y. M. A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Organizations are looking to achieve the principle of security in their technology systems with lower costs and high efficiency. Recently, attention has been drawn to the use of multi-factor authentication, but it is expensive. In this article, we will study how to use the one-time password method and turn it into a low-cost multi-factor authentication system.

***Key words**: One-time password (OTP), multi-factor authentication (MFA), keystroke dynamics, biometric data*

УДК 004.056.55
ГРНТИ 81.93.29

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – КАК МЕТОД ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИИ

И. Н. Бабков

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

Аудит информационной безопасности обеспечивает контроль соответствия уровня защиты информационных ресурсов установленным требованиям в организации. В статье анализируются различные методы аудита, их преимущества и недостатки. Основное внимание уделяется методам, включенным в международные и отечественные стандарты. Отмечаются способы повышения эффективности аудита организаций, в которых внедрены SIEM-системы.

аудит, информационная безопасность, Security Information and Event Management, SIEM

Введение

В современных условиях сохраняется тенденция роста числа кибератак на информационные ресурсы организаций (компаний). Большинство крупных компаний и организаций в целях обеспечения безопасности своих информационных ресурсов и непрерывности бизнеса создают мощные комплексные системы защиты информации (КСЗИ). Выбор механизмов защиты осуществляется специалистами подразделений информационной безопасности (ИБ) и информационных технологий (ИТ), как правило, с учетом модели угроз информационной безопасности, актуальной для конкретной компании.

Согласно аналитическим отчетам, публикуемым различными ИБ-компаниями, количество компьютерных атак постоянно возрастает. Так, например, в отчете компании Positive Technologies эксперты представили исследования актуальных киберугроз в СНГ за 2023 г. и первую половину 2024 г. Согласно отчету, интерес злоумышленников к региону СНГ значимо вырос: во II кв. 2024 г. зафиксировано атак в 2.6 раза больше, чем за аналогичный период годом раньше. Исследователи выявили, что в России наибольшее количество атак на: промышленных предприятиях (11%), телекоммуникациях (10%), госучреждениях (9%), IT-компаниях (7%).

Устойчивая тенденция роста числа атак, в том числе их новых видов, вынуждает компании модернизировать или внедрять новые системы защиты. Соответственно возрастает нагрузка на подразделения ИБ и ИТ.

В этих условиях возникают проблемы:

– обслуживание большого числа систем;
– проведение локального контроля настроек;
– сложность оценки событий ИБ в реальном времени и анализа данных из журналов аудита различных информационных систем (ИС) и средств защиты;
– повышение риска пропуска важных событий и инцидентов ИБ.

SIEM-системы

Ряд из перечисленных проблем можно устранить или ослабить с помощью современных систем управления ИБ, наиболее эффективными из которых являются SIEM-системы (Security Information and Event Management system) – «Система управления информацией и событиями в безопасности» [1, 2]. Эти системы позволяют автоматизировать: процессы управления событиями безопасности, подготовку отчетов по оценке соответствия состояния безопасности нормативным требованиям, а также принятие решений по реагированию на инциденты информационной безопасности. Однако они не могут обнаруживать уязвимости в КСЗИ и ИС (если в составе не подключен сканер безопасности). Решать такие задачи можно в процессе анализа (аудита) ИБ. Кроме того, результаты аудита позволяют дать оценку реальных рисков. С учетом оценки, при необходимости принимается решение об инвестировании в замену или модернизацию систем защиты.

Аудит информационной безопасности

Аудит информационной безопасности (далее – аудит) – независимая экспертиза отдельных областей функционирования организации. Различают внешний и внутренний аудит [3].

Внешний аудит – разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Рекомендуется проводить внешний аудит регулярно, а для многих финансовых организаций и акционерных обществ это является обязательным требованием со стороны их учредителей и акционеров. Это же касается организаций, в составе которых есть крити-

ческие объекты. Внешним аудитом занимаются ИБ-компании, имеющие соответствующие лицензии.

Внутренний аудит – непрерывная деятельность, которая проводится на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка и выполнение которого осуществляется подразделениями службы безопасности и утверждается руководством организации. В план включаются актуальные мероприятия по снижению рисков ИБ. При необходимости план можно скорректировать.

Цели проведения аудита:

– анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов;
– оценка текущего уровня защищенности ИС;
– локализация узких мест (уязвимостей) в системе защиты ИС;
– оценка соответствия ИС существующим стандартам в области ИБ;
– выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Аудит в Системе менеджмента информационной безопасности

Аудит входит как компонент в Систему менеджмента информационной безопасности (СМИБ) стандарта ГОСТ Р ИСО/МЭК 27001-2021. Данный стандарт, как и стандарты ISO/IEC 27005, Cobit и BS 7799-2:2005, используют процессный подход для разработки, внедрения, обеспечения функционирования, анализа, поддержки и улучшения СМИБ организации. Он основан на модели «Планирование (Plan) – Осуществление (Do) – Проверка (Check) – Действие (Act)» (PDCA), которая может быть применена при структурировании всех процессов СМИБ. Модель носит название – цикл Шухарта-Деминга [4].

Функции аудита в модели выполняются на этапе «Проверка (Check)», они требуют:

– выполнять процедуры мониторинга и анализа;
– проводить регулярный анализ результативности СМИБ;
– измерять результативность мер управления для проверки соответствия требованиям ИБ;
– пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения;

– проводить внутренние аудиты СМИБ через установленные периоды времени;
– регулярно проводить руководством организации анализ СМИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;
– обновлять планы ИБ с учетом результатов анализа и мониторинга;
– регистрировать действия и события, способные повлиять на результативность или функционирование СМИБ.

Перечисленные общие требования должны быть реализованы в процессе аудита организации.

Подготовка и проведение аудита в организации

На уровне организации аудит входит в состав административно-организационных мероприятий и, в том числе политику информационной безопасности (ПИБ), проводится с помощью программно-технических мер. При подготовке к определенному аудиту необходимо выбрать: стандарт (или несколько стандартов) информационной безопасности, методику и программу (план) проведения аудита информационной безопасности [3, 5].

При выборе стандарта можно использовать материалы по сравнительному анализу стандартов, определить соответствие требований стандартов и требований КСЗИ организации. Также следует уточнить корпоративную сетевую инфраструктуру, состав оборудования и программного обеспечения. С учетом сравнения, для проведения аудита по методике можно применять стандарты на базе серии ИСО/МЭК 27000.

Проведение аудита делится на этапы, которые носят общий характер для большинства аудитов.

Этапы проведения аудита:
– подписание договорной и исходно-разрешительной документации (в том числе плана проведения аудита);
– сбор информации;
– анализ исходных данных;
– выполнение тестов по аудиту;
– выработка рекомендаций;
– контроль за выполнением рекомендаций;
– подписание отчетных актов.

На основании этапов разрабатывается программа аудита, которая должна быть выполнена в соответствии с договором. Основная цель аудита

состоит в повышении защиты организации, а это возможно, если аудит будет эффективный.

Способы повышения эффективности аудита

1. Максимальный охват корпоративной сети аудитом. Проводится комплексный аудит: КСЗИ; ИС; корпоративная сеть; выполнение ПИБ; внешняя деятельная работников; выполнение организационных мер и т.д.

2. Повышение скорости аудита (для организаций, где есть SIEM). SIEM-системы позволяют автоматизировать: процессы управления событиями безопасности, подготовку отчетов по оценке соответствия состояния безопасности нормативным требованиям, а также принятие решений по реагированию на инциденты ИБ. В результате ускоряется обработка информации и сокращается время проведения аудита.

3. Повышение точности определения уязвимостей. Выявление уязвимостей и узких мест (узлов сетей, версий ОС серверов и компьютеров, а также имитации компьютерных атак) осуществляют сканеры безопасности, например: Nessus, OpenVAS, Retina, Max Patrol. Критерии эффективности сканера: точность идентификации версии ОС, вероятность ложного обнаружения уязвимости, вероятность пропуска существующей уязвимости, скорость сканирования. Оценки уязвимостей приводятся в системах оценки уязвимости, например, в CVSS. Точность оценки очень важна, так как часто встречаются уязвимости с критической степенью риска (имеющие опубликованный эксплоит). Чтобы обеспечить высокую точность надо выбрать оптимальный сканер для аудита.

4. Управление рисками. Проведение оценки реальных рисков информационной безопасности с учетом специфики организации, определение периодичности аудитов. По результатам можно принять решение: снизить риски (обновление систем защиты); принять риски; передать риски сторонней организации (аутсорсинг); отказаться от рисков (изменения в ПИБ). Соответственно решению изменится вид аудита.

5. Тест на проникновение. Аудит «Тест на проникновение» по сравнению с другими аудитами отличается возможностью выбирать сценарий. Тесты на проникновение делятся на 3 вида по наличию исходной информации об объекте: 1-й (отсутствие информации, кроме названия объекта); 2-й (имеется часть информации); 3-й (полная информация). Таким образом, 1-й вид теста по сценарию близок к хакерским атакам, а 3-й наиболее объективный [5].

Выводы

Аудит информационный безопасности, подготовленный с учетом стандарта и специфики организации, обеспечивает контроль реального состояния ИБ организации, по результатам которого разрабатываются рекомендации, направленные на устранение недостатков и рисков.

Повышение уровня защиты организации во многом зависит от эффективности аудита. В целях роста эффективности в процессе аудита необходимо: повысить скорость аудита, повысить точность определения уязвимостей, управлять рисками и выборочно проводить тесты на проникновение.

Список используемых источников

1. Котенко И. В., Саенко И. Б. SIEM-система для управления информацией и событиями безопасности // Защита информации. Инсайд. 2012. № 5. С. 54 – 65.

2. Бабков И. Н. Анализ эффективности SIEM-системы в организации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021. Т. 1. С. 72–77.

3. Петренко С. А. Развитие нормативной базы по технической защите конфиденциальной информации // Защита информации. Инсайд. 2005. №4. С. 28 – 40.

4. Нестеров С. А. Основы информационной безопасности: Учебное пособие. 3-е изд., стер. СПб.: Издательство «Лань», 2017. 324 с. (Учебники для вузов. Специальная литература). ISBN 978-5-8114-2290-6.

5. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с. ил. (Серия «Библиотека программиста»). ISBN 978-5-4461-0662-2.

INFORMATION SECURITY AUDIT – AS AN INCREASING SECURITY ORGANIZATION METHOD

Babkov I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Information security audit ensures that the level of information resources protection meets the established requirements in the organization. The article analyzes various audit methods, their advantages and disadvantages. The main focus is on methods included in international and domestic standards. The ways of the effectiveness auditing increasing in organizations, in which SIEM systems are implemented, are noted.

Key words: *audit, information security, Security Information and Event Management, SIEM*

УДК 004.056.5
ГРНТИ 81.93.29

МЕТОДИКА ПРОТИВОДЕЙСТВИЯ ДЕКОМПИЛЯЦИИ ИСПОЛНЯЕМЫХ ФАЙЛОВ KOTLIN

Г. С. Бударный

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

В настоящее время язык программирования Kotlin набирает популярность. Все чаще используется для разработки мобильных приложений под Android, серверных систем или распределенных высоконагруженных приложений. Kotlin исполняется на виртуальной машине Java, что означает наличие тех же проблем, что и у Java. Легкость декомпиляции android-приложений и последующая компрометация. Необходима методика, которая позволит сохранить работоспособность исполняемых файлов Kotlin и позволит внедрить защиту от декомпиляции.

Kotlin, декомпиляция, обфускация исходного кода

Современные языки программирования, такие как Kotlin, представляют собой ценный интеллектуальный капитал, включающий уникальные алгоритмы, архитектурные решения и новейшие решения. Защита исходного кода имеет стратегическое значение, так как киберугрозы и реверс-инжиниринг ставят под угрозу интеллектуальную собственность, что может привести к экономическим убыткам и утрате конкурентных преимуществ. Kotlin, активно используемый для серверной разработки и Android-приложений, имеет особенности, которые делают его код уязвимым для декомпиляции, что делает актуальной задачу защиты кода от несанкционированного доступа и утечек. В отличие от Java, для Kotlin пока недостаточно инструментов защиты, что требует разработки новых методик для повышения безопасности и продуктивности.

Поскольку Kotlin работает на JVM, он уязвим к декомпиляции, как и Java, что требует применения методов защиты [1]. В силу того, что Kotlin работает на JVM для него актуальны исследования по вложению цифрового водяного знака в class-файлы java-приложений [2-3]. Защита от декомпиляции – ключевой элемент в создании безопасного ПО. В работе исследуются

методы обфускации для минимизации рисков восстановления кода, их интеграция в разработку, создание новой методики защиты и проверка ее эффективности.

Компиляция Kotlin в JVM характеризуется интероперабельностью с Java, что обеспечивает легкую интеграцию с существующими проектами и совместимость с библиотеками [4]. Компилятор генерирует байт-код, оптимизированный за счет inline-функций и современных конструкций, что делает его более компактным и производительным, чем аналогичный код на Java. Строгая типизация и проверки на этапе компиляции, включая null-safety, минимизируют ошибки, но на уровне байт-кода эти механизмы сводятся к стандартным JVM-проверкам. Итоговый байт-код остается уязвимым для декомпиляции и реверс-инжиниринга [5].

Android-приложения разрабатываются на языках Java или Kotlin и поставляются в формате APK, который содержит все необходимые компоненты для установки и работы приложения на устройстве. При разработке исходный код интерпретируется компилятором Java (javac) в байт-код, который сохраняется в class-файлах. При запуске class-файла, JVM, преобразовывает инструкции байт-кода на лету, в машинные инструкции, подходящие для конкретной архитектуры ядра [6].

В Android байт-код компилируется в dex-файлы, оптимизированные для Dalvik или ART, и включается в APK вместе с ресурсами и манифестом. Dalvik исполняет код JIT, а ART использует AOT-компиляцию, что повышает производительность. Dex-файлы уязвимы к декомпиляции, что делает обфускацию важной мерой защиты. Обфускация усложняет анализ кода, изменяя имена, структуру и логику, защищая приложения от утечек данных и фишинга [7].

Оценка инструментов декомпиляции важна для анализа их возможностей, включая поддержку конструкций Kotlin, качество восстановления кода и устойчивость к обфускации [8]. Это помогает разработчикам выявить уязвимые элементы кода и слабости существующих методов защиты. Анализ ограничений и особенностей декомпиляторов позволяет разрабатывать более эффективные методики защиты, учитывая их сильные и слабые стороны при тестировании безопасности приложений. В таблице 1 представлена оценка таких инструментов.

ТАБЛИЦА 1. Эффективность инструментов декомпиляции

Декомпилятор	Новые версии Kotlin	Корутины	лямбда-выражения	Функциональное программирование	inline-функции
JD-GUI	+	-	-	+	-
Jshrink	-	+	-	+	-
Fernflower	+	+	+	-	+
Vineflower	-	+	+	+	+
CFR	-	+	+	-	-
Procyon	-	-	+	-	-
Krakatau	-	-	+	+	-
Jadx	-	+	-	+	+

В эксперименте по оценке инструментов декомпиляции анализировались особенности Kotlin, включая корутины, лямбда-выражения, функциональное программирование и inline-функции [9]. Результаты показали, что даже с незащищенным кодом декомпиляторы с активной поддержкой разработчиков сталкиваются с трудностями, особенно при обработке сложных корутин и функциональных конструкций, где теряется семантика. Инструмент Vineflower продемонстрировал лучшие результаты благодаря широкой поддержке сообщества, что делает его важным ориентиром для разработки эффективных методов защиты кода.

Эффективным способом защиты кода Kotlin от декомпиляции является использование фиктивных методов, затрудняющих работу декомпиляторов [10-11]. Методы высшего порядка forEach и корутины вызывают значительные трудности у инструментов, таких как JD-GUI, Jshrink, Fernflower, Vineflower, CFR, Procyon, Jadx и Krakatau, которые не могут корректно восстановить исходный код.

Предлагается комбинированный подход, включающий вставку фиктивных методик с использованием forEach и корутин в разные части class-файлов. Эти методики не влияют на функциональность приложения, но усложняют анализ кода. Пример фиктивной методики: создание списка, его обработка через forEach и выполнение suspend-функции внутри корутины, которая имитирует сложную обработку данных с вызовами delay и асинхронными операциями.

Комбинированное использование forEach и корутин добавляет многопоточность и дополнительные вызовы, что приводит к появлению в деком-

пилированном коде машин состояний и сложных структур, затрудняя обратную инженерию.

Блок-схема, изображенная на рисунке 1, описывает процесс реализации методики обфускации исходного кода Kotlin.

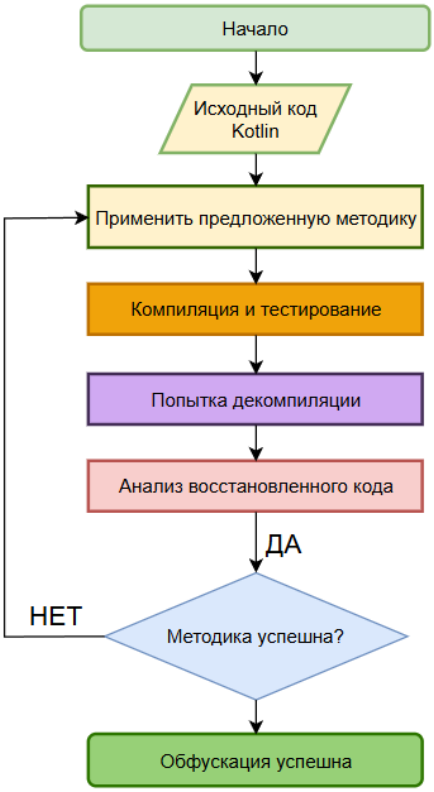


Рис. 1. Блок-схема этапов обфускации исходного кода Kotlin

Декомпиляция кода на Kotlin с использованием инструментов, таких как Vineflower и Jadx, выявила множество проблем. Vineflower заменяет «forEach» на цикл «for», добавляет неинициализированные переменные и некорректные преобразования типов, что искажает логику. Jadx усложняет корутины, добавляет множество лишних структур с переменной «label», параметр «Continuation» и лишние вызовы, что делает код многословным и трудным для понимания. Анализ 15 class-файлов показал, что только 2 из них были декомпилированы с минимальными потерями, тогда как остальные содержали значительные ошибки, потерю структуры и читаемости. Попытка декомпиляции корутин через JD-GUI завершилась внутренней ошибкой.

Использование корутин, методов высшего порядка и фиктивных конструкций доказало свою эффективность в защите кода, усложняя процесс его восстановления. Методика подходит для промышленных проектов, так как делает декомпиляцию трудоемкой и малоперспективной, особенно при использовании сложных конструкций и дополнительных уровней абстракции.

Список используемых источников

1. Шариков П. И. Методика обфускации байт-кода java-приложения с целью его защиты от атак декомпиляцией // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 64-72. DOI 10.46418/2079-8199_2022_1_10. EDN AUOFNA.

2. Хомяков И. Н. Возможность скрытого вложения информации в байт-код Java / И. Н. Хомяков, А. В. Красов // Информационные технологии моделирования и управления. 2014. № 2(86). С. 185-191. EDN RZHODN.

3. Шариков П. И. Исследование устойчивости цифрового водяного знака к атакам направленной декомпиляции составных частей приложения Java // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2022. № 2. С. 100-112. EDN QWHOIV.

4. Bose S. et al. A comparative study: java vs kotlin programming in android application development //International Journal of Advanced Research in Computer Science. 2018. Т. 9. №. 3. С. 41-45.

5. Красов А. В. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполняемые и библиотечные файлы / А. В. Красов, С. И. Штеренберг // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2013. С. 847-852. EDN SMCRAZ.

6. Rao J. et al. Compiled query execution engine using JVM //22nd International Conference on Data Engineering (ICDE'06). IEEE, 2006. С. 23-23.

7. Красов А. В. Методика защиты байт-кода Java-программы от декомпиляции и хищения исходного кода злоумышленником / А. В. Красов, П. И. Шариков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2017. № 1. С. 47-50. EDN ZDBFTL.

8. Шариков П. И. Исследование атаки обфускацией на байт-код java-приложения с целью разрушения или повреждения цифрового водяного знака // I-methods. 2022. Т. 14, № 1. EDN GQGKIV

9. Турушев Т. К. Многофункциональные высокоуровневые языки программирования Java и Kotlin для мобильных приложений / Т. К. Турушев // Теоретические и практические аспекты развития современной науки: теория, методология, практика: Сборник научных статей по материалам VI Международной научно-практической конференции, Уфа, 16 ноября 2021 года. Уфа: Общество с ограниченной ответственностью "Научно-издательский центр «Вестник науки», 2021. С. 55-59. EDN CGOCAC.

10. Шариков П. И. Методика создания и вложения цифрового водяного знака в исполняемые JAVA файлы на основе замен опкодов / П. И. Шариков, А. В. Красов, С. И. Штеренберг // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11, № 3. С. 66-70. EDN YKVPJF.

11. Шариков П. И., Цветков А. Ю., Сигачева В. В., Сиротина Л. К. Исследование и алгоритм предотвращения эксплуатации уязвимостей библиотеки журналирования Log4j в информационных системах java-приложений // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 4. С. 100-106. DOI 10.46418/2079-8199_2023_4_19. EDN BULSOH.

Статья представлена научным руководителем, кандидатом технических наук, и. о. заведующего кафедрой ИБКС СПбГУТ, доцентом Ушаковым И. А.

METHOD FOR COUNTERING DECOMPILATION OF KOTLIN EXECUTIVE FILES

Budarnyy G.
The Bonch-Bruevich St Petersburg State University of Telecommunications

Currently, the Kotlin programming language is gaining popularity. It is increasingly used to develop mobile applications for Android, server systems or distributed high-load applications. Kotlin is executed on the Java virtual machine, which means that it has the same problems as Java. Ease of decompilation of Android applications and subsequent compromise. A technique is needed that will allow maintaining the functionality of Kotlin executable files and will allow implementing protection against decompilation.

Key words: *Kotlin, decompilation, source code obfuscation*

УДК 004.056.5
ГРНТИ 50.07.29

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АНАЛИЗА УЯЗВИМОСТЕЙ В СЕТЕВЫХ ПРОТОКОЛАХ

Н. А. Васильев, Б. С. Лещинский, Д. С. Ситдиков

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

Сетевые протоколы являются основой современных коммуникаций, однако они часто становятся целью злоумышленников, использующих их уязвимости для кибератак. В данной статье рассматривается роль искусственного интеллекта в выявлении и анализе уязвимостей сетевых протоколов. Обсуждаются методы машинного обучения и глубокого обучения, которые помогают автоматизировать и улучшить процесс обнаружения уязвимостей.

искусственный интеллект, анализ уязвимостей, сетевые протоколы, машинное обучение, кибербезопасность, глубокое обучение

Сетевые протоколы составляют основу функционирования современных компьютерных сетей. Их использование обеспечивает передачу данных между устройствами, но вместе с тем они становятся мишенью для кибератак [1]. Уязвимости в протоколах, такие как сниффинг, подмена идентификаторов, SQL-инъекции, атаки типа «отказ в обслуживании», представляют серьезные угрозы для информационной безопасности. С ростом объемов сетевого трафика и сложности атак традиционные методы защиты становятся недостаточно эффективными. На помощь приходят современные подходы, основанные на использовании искусственного интеллекта (ИИ), включая машинное и глубокое обучение [2]. Эти методы позволяют автоматизировать процессы обнаружения угроз, анализировать большие объемы данных и оперативно выявлять аномалии.

Рассмотрим основные сетевые протоколы и типичные уязвимости, связанные с ними.

Основные уязвимости протокола TCP/IP (Transmission Control Protocol / Internet Protocol):

1. Сниффинг (Sniffing) – возможность перехвата данных, передаваемых по сети, что приводит к утечке конфиденциальной информации.

2. Spoofing – атака, при которой злоумышленник подделывает IP-адрес или MAC-адрес, чтобы создать ложное впечатление, что соединение принадлежит доверенному устройству.

3. DoS/DDoS-атаки (Denial of Service / Distributed Denial of Service) – атаки, направленные на перегрузку серверов и сетей.

4. Сегментация и фрагментация: Протокол IP имеет уязвимости в процессе фрагментации пакетов, которые могут быть использованы для обхода фильтрации или для проведения атак.

Основные уязвимости протокола HTTP (HyperText Transfer Protocol):

1. SQL-инъекции – атаки, направленные на эксплуатацию недостатков в обработке пользовательских данных на сервере.

2. XSS (Cross-Site Scripting) – уязвимость, при которой злоумышленники могут внедрять вредоносный скрипт в веб-страницу, что может привести к украденным данным пользователей.

3. CSRF (Cross-Site Request Forgery) – атака, при которой злоумышленник может заставить пользователя выполнить нежелательные действия, используя их права доступа.

Основные уязвимости протокола FTP (File Transfer Protocol):

1. Неправильно обработанные команды могут позволить злоумышленнику выполнить произвольные команды на сервере.

2. Перехват паролей – поскольку FTP передает данные в открытом виде, пароли могут быть легко перехвачены с помощью сниффинга.

3. Проблемы с аутентификацией – использование слабых паролей или отсутствие многофакторной аутентификации может привести к взлому учетных записей.

Основные уязвимости DNS (Domain Name System):

1. DNS Spoofing (Cache poisoning) – злоумышленники могут подменить кэш DNS-серверов, направляя пользователей на фальшивые веб-сайты.

2. DDoS-атаки на DNS-серверы.

Основные уязвимости SSH (Secure Shell):

1. Использование слабых или стандартных паролей для аутентификации может привести к взлому.

2. Man-in-the-middle (MitM) атаки – если SSH-сессия не настроена должным образом, злоумышленник может перехватить и изменить данные, передаваемые по протоколу.

Оценка уязвимостей (0-10) и рисков сетевых протоколов представлена в таблице 1.

ТАБЛИЦА 1. Оценка уязвимости и рисков сетевых протоколов

Протокол	Типы уязвимостей	Риск	Оценка уязвимости
TCP/IP	Сниффинг, Spoofing, DoS/DDoS, Сегментация и фрагментация	Высокий	9
HTTP	SQL-инъекции, XSS, CSRF	Высокий	8
FTP	Необработанные команды, Перехват паролей, Проблемы с аутентификацией	Средний	7
DNS	DNS Spoofing (Cache poisoning), DDoS-атаки на DNS-серверы	Средний	6
SSH	Слабые пароли, Man-in-the-middle атаки	Высокий	9

Основные подходы в области ИИ для анализа уязвимостей сетевых протоколов:

Машинное обучение (ML) активно используется для анализа сетевого трафика с целью выявления аномалий, необычного поведения или атак. Модели машинного обучения способны обучаться на больших объемах данных и находить закономерности, которые трудно обнаружить вручную. Основные подходы включают:

1. Классификация трафика: используются алгоритмы Support Vector Machines (SVM), Random Forest и k-Nearest Neighbors (k-NN) для классификации пакетов данных нормальный трафик или вредоносный трафик [3]. Данные алгоритмы содействуют обнаружению известных атак, таких как DDoS или попытки подбора паролей.

2. Аномалия в трафике. Clustering методы, например, k-means или DBSCAN, обучаются на нормальном трафике и обнаруживают аномалии, которые могут быть результатом атак [4].

Глубокое обучение (DL) позволяет использовать более сложные нейронные сети, которые могут находить глубокие связи в данных. Для анализа сетевых протоколов и трафика используются:

1. Анализ временных рядов – рекуррентные нейронные сети (RNN), а также LSTM могут использоваться для анализа временных зависимостей в трафике, выявляя не только атаки, но и долгосрочные отклонения от нормального состояния [5].

2. Сверточные нейронные сети (CNN) полезны для обработки сложных многомерных данных, таких как изображения или трафик, представленный в виде спектра. CNN могут быть использованы для обработки и классификации сетевых пакетов или для построения моделей выявления атак на основе данных о поведении пользователей [6].

3. Автокодировщики (Autoencoders) используются для создания сжатых представлений данных с целью нахождения скрытых паттернов. Это может помочь в анализе аномалий и в обнаружении новых, неизвестных ранее уязвимостей [7].

Для обработки и анализа текстовых данных, таких как логи сетевых устройств или описания уязвимостей, используются методы NLP:

1. Word2Vec и GloVe – технологии преобразования слов в векторные представления используются для анализа сетевых логов и автоматического поиска описаний уязвимостей, что позволяет ускорить процесс обнаружения угроз [8].

2. BERT и GPT – трансформеры, которые могут быть использованы для глубокого анализа текста, включая поиск уязвимостей, автоматическое извлечение информации и классификацию угроз в логах [9].

Фаззинг – метод тестирования программного обеспечения путем подачи случайных или специально созданных данных с целью выявления ошибок и уязвимостей. ИИ может улучшить фаззинг с помощью генеративных моделей и методов обучения с подкреплением:

1. Генеративные состязательные сети (GANs) могут эффективно генерировать нестандартные и неожиданные данные, которые могут привести к уязвимостям [10].

2. Обучение с подкреплением (RL) используется для оптимизации процесса фаззинга, чтобы фаззинг-процесс становился более целенаправленным и эффективным, что помогает быстрее выявлять уязвимости [10].

Сравнительная характеристика анализируемых подходов по скорости и точности представлена на рисунке 1. Уровень автоматизации подходов представлен на рисунке 2.

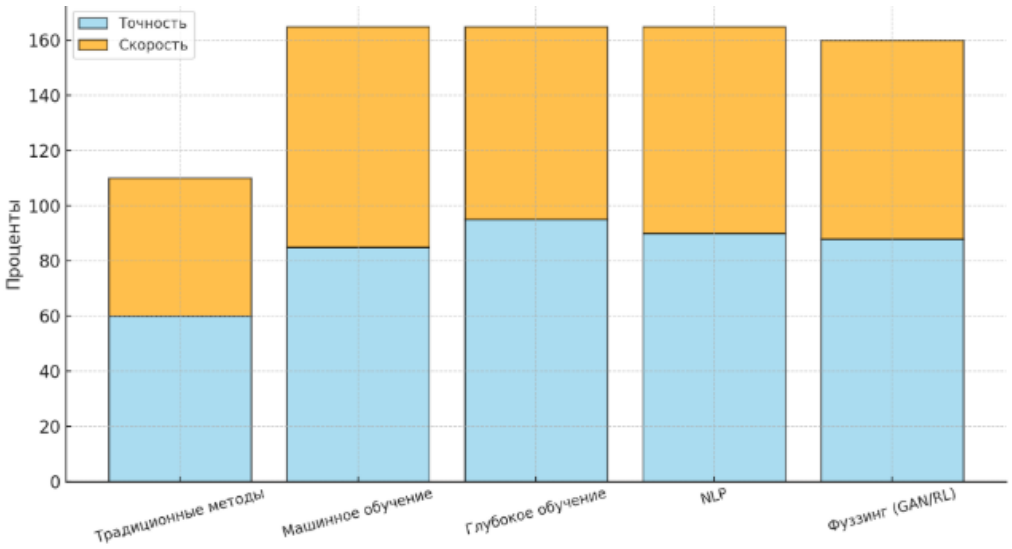


Рис. 1. Сравнительная характеристика подходов по скорости и точности работы

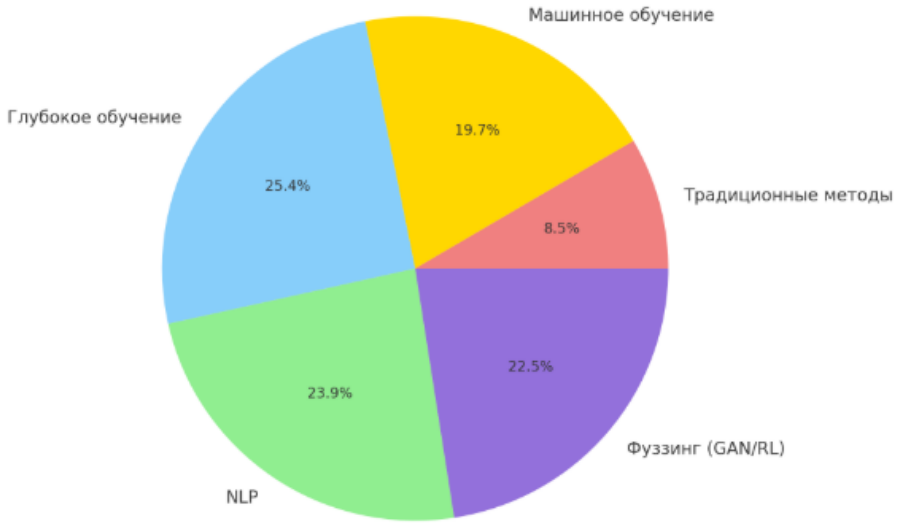


Рис. 2. Уровень автоматизации подходов для анализа уязвимостей

Сетевые протоколы являются важным элементом современных информационных систем, но их уязвимости создают значительные риски для безопасности. В условиях постоянного роста объемов данных и сложности кибератак традиционные методы анализа становятся менее эффективными. Применение искусственного интеллекта, включая машинное и глубокое обучение, открывает новые возможности для автоматизации, повышения точности и скорости обнаружения угроз.

Методы классификации, анализа временных рядов, обработки текстовых данных и фаззинг позволяют эффективно выявлять как известные, так и новые уязвимости. Однако внедрение ИИ-технологий требует тщательно продуманного подхода, включающего обеспечение высокого качества дан-

ных, выбор наиболее подходящих моделей и их настройку для решения конкретных задач. Развитие инструментов ИИ для анализа сетевых протоколов является перспективным направлением, которое позволит существенно повысить уровень кибербезопасности в будущем.

Список используемых источников

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Питер, 2024.

2. Вопросы применения искусственного интеллекта в безопасности / Б. С. Лещинский, Н. А. Васильев, Р. Р. Хабушев, А. Р. Назаров // Искусственный интеллект в решении актуальных социальных и экономических проблем XXI века: Сборник статей по материалам Девятой всероссийской научно-практической конференции с международным участием, Пермь, 17–18 октября 2024 года. Пермь: Пермский государственный национальный исследовательский университет, 2024. С. 77-81. EDN EATNZO.

3. Al Lail M., Garcia A., Olivo S. Machine learning for network intrusion detection–a comparative study //Future Internet. 2023. Т. 15. № 7. С. 243.

4. Vikram A. et al. Anomaly detection in network traffic using unsupervised machine learning approach //2020 5th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2020. С. 476-479.

5. Zhao Z., Xu C., Li B. A LSTM-based anomaly detection model for log analysis //Journal of Signal Processing Systems. 2021. Т. 93. № 7. С. 745-751.

6. Abbasi M., Shahraki A., Taherkordi A. Deep learning for network traffic monitoring and analysis (NTMA): A survey //Computer Communications. 2021. Т. 170. С. 19-41.

7. Li J., Pan Z. Network traffic classification based on deep learning //KSII Transactions on Internet and Information Systems (TIIS). 2020. Т. 14. № 11. С. 4246-4267.

8. Sharma S., Arjunan T. Natural Language Processing for Detecting Anomalies and Intrusions in Unstructured Cybersecurity Data //International Journal of Information and Cybersecurity. 2023. Т. 7. № 12. С. 1-24.

9. Seyyar Y. E., Yavuz A. G., Ünver H. M. An attack detection framework based on BERT and deep learning //IEEE Access. 2022. Т. 10. С. 68633-68644.

10. Chafjiri S. B. et al. Vulnerability detection through machine learning-based fuzzing: A systematic review //Computers & Security. 2024. С. 103903.

APPLICATION OF ARTIFICIAL INTELLIGENCE FOR ANALYZING VULNERABILITIES IN NETWORK PROTOCOLS

Vasiliev N., Leshchinsky B., Sitdikov D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Network protocols are the basis of modern communications, but they often become the target of intruders who use their vulnerabilities for cyberattacks. This article examines the role of artificial intelligence in identifying and analyzing vulnerabilities in network protocols. Machine learning and deep learning methods that help automate and improve the vulnerability detection process are discussed.

Key words: *artificial intelligence, vulnerability analysis, network protocols, machine learning, cybersecurity, deep learning.*

УДК 004.056.55
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

И. В. Гаврилов, Д. А. Баранов

Академия Федеральной службы охраны Российской Федерации

В статье представлены результаты разработки программного средства с децентрализованным подтверждением подлинности информации в системах электронного документооборота на основе протокола консенсуса Clique доказательства авторитета (Proof-of-Authority) на платформе Ethereum. Описаны основные этапы настройки программного обеспечения Geth для создания распределенной блокчейн-сети, включая инициализацию узлов, конфигурацию генезис-блока и обеспечение синхронизации между ними в условиях локальной сети.

умные контракты, блокчейн, распределенная система, система электронного документооборота

Для обеспечения защищенности обрабатываемой в системе электронного документооборота (СЭД) [1] информации могут применяться различные подходы, например, механизм аутентифицированного шифрования с ассоциативными данными, рассмотренный в [2].

С целью создания более универсальной и отказоустойчивой масштабируемой системы с децентрализованным подтверждением подлинности документов в СЭД разработано программное средство, использующее платформу Ethereum на основе алгоритма консенсуса доказательства авторитета (Proof-of-Authority, PoA) [3, 4, 5]. К основным задачам программного средства относятся: обеспечение целостности и подлинности документов, автоматизация процессов согласования и утверждения посредством использования сервиса умных контрактов [6].

Алгоритм работы программного средства подтверждения подлинности информации при загрузке документа в СЭД описывает последовательность действий до проверки статуса документа, включая взаимодействие клиентского приложения, блокчейна и сервиса умных контрактов (рис. 1). В качестве алгоритма хэширования используется ГОСТ 34.11-2018, обеспечивающий создание уникальных идентификаторов документов. Формирование

электронной подписи осуществляется в соответствии с ГОСТ 34.10-2018, гарантирующей аутентичность действий участников.

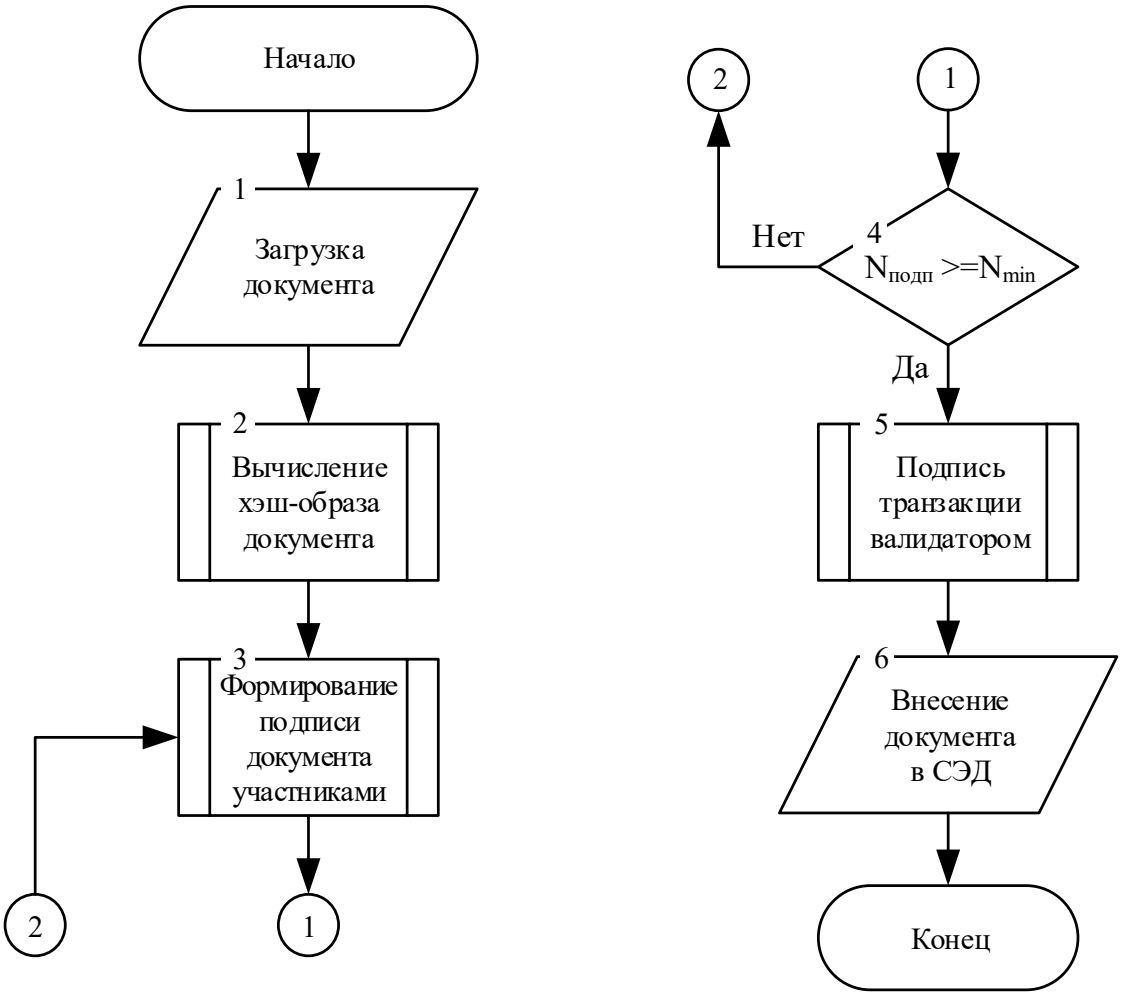


Рис. 1. Алгоритм работы программного средства при загрузке документа в СЭД

Алгоритм работы программного средства (рис. 1) начинается с добавления документа в СЭД через веб-интерфейс, реализованный на JavaScript, пользователем (сотрудником организации). Пользователь вводит содержимое документа или загружает файл (например, PDF) через специальную форму. Программа-клиент обрабатывает этот ввод, подготавливая данные для записи в блокчейн. Для этого программа-клиент вызывает функцию «addDocument» (рис. 1, блок 1) и формирует хэш-образ (рис. 1, блок 2). В программе применяется библиотека Web3.js для подключения к локальному узлу Ethereum с использованием адреса аутентифицированного в системе пользователя в качестве идентификатора.

Хэш-образ документа вычисляется с использованием стандарта ГОСТ 34.11-2018. Для этого программа-клиент использует внешнюю библиотеку «pygost» в Python, поскольку встроенные инструменты Ethereum не поддер-

живают ГОСТ напрямую. Документ до применения функции хэширования преобразуется в байтовый массив. В результате работы блока 2 (рис. 1) формируется хэш-образ длиной 256 бит. Полученный хэш-образ является уникальным идентификатором документа, вносимым в блокчейн.

После загрузки документа начинается процесс его согласования, где участники подписывают документ для подтверждения его подлинности (рис. 1, блок 3). Алгоритм на этом этапе обеспечивает взаимодействие нескольких (многих) пользователей с сервисом умных контрактов через программу-клиент, используя стандарт ГОСТ 34.10-2018 для цифровой подписи [3].

Перед отправкой документа валидатору алгоритм генерирует цифровые подписи участников в соответствии с ГОСТ 34.10-2018. Используемая библиотека Web3.js не поддерживает ГОСТ 34.10-2018 напрямую, поэтому электронная подпись создается с помощью внешней библиотеки «pygost» в Python. Программа-клиент, используя хэш-образ документа, вычисленный по ГОСТ 34.11-2018, формирует электронную подпись на основе закрытого ключа пользователя. Транзакция, содержащая электронную подпись, отправляется в сеть. Сервис умных контрактов записывает адрес отправителя «msg.sender» в массив «signers», а электронную подпись в массив «signatureData» структуры «Document» для последующей верификации вне цепочки.

После каждой подписи программное средство подсчитывает количество элементов в массиве «signers» $N_{подп}$. Если $N_{подп}$ меньше порога N_{min} (условие не выполняется), то статус транзакции остается «pending» (рассматриваемый) и процесс повторяется для следующего участника (рис. 1, блок 4). Если условие выполняется – сервис умных контрактов автоматически изменяет статус транзакции на «approved» (одобрен). Это обновление записывается в текущий блок и подтверждается программами-валидаторами в следующем блоке, который добавляется через 5 секунд в режиме PoA (рис. 1, блок 5).

Описанный процесс загрузки документа в СЭД обеспечивает последовательный сбор всех подписей и их фиксацию в блокчейне, демонстрируя преимущества умных контрактов: процесс утверждения происходит автоматически, без необходимости ручного подсчета подписей или вмешательства администратора. Электронные подписи, сохраненные в массиве «signatureData», могут быть проверены вне цепочки для подтверждения подлинности, что усиливает доверие к системе.

Проверка целостности (подлинности) документа и его состояния может быть проведена пользователями СЭД в любой момент после загрузки и подтверждения статуса документа. Для этого используется два уровня анализа: данные из блокчейна и локальное сравнение. Пользователь через веб-интерфейс вводит идентификатор документа (рис. 2, блок 1). Программа-клиент вызывает функцию «getDocument» сервиса умных контрактов, которая возвращает хэш-образ (ГОСТ 34.11-2018), статус и число подписей. Эти действия позволяет пользователю убедиться, что документ прошел необходимое согласование.

Для проверки целостности алгоритм использует локальные данные. Пользователь загружает оригинальный документ из базы данных через интерфейс. Программа-клиент вычисляет хэш-образ этого документа с помощью ГОСТ 34.11-2018, применяя ту же библиотеку, что и при загрузке (рис. 2, блок 2). Полученный хэш-образ сравнивается с записью в блокчейне (рис. 2, блок 3). Если они идентичны (рис. 2, блок 4), это подтверждает неизменность документа. При расхождении (например, из-за редактирования файла) интерфейс сигнализирует о нарушении, что указывает на попытку подделки (рис. 2, блок 5).

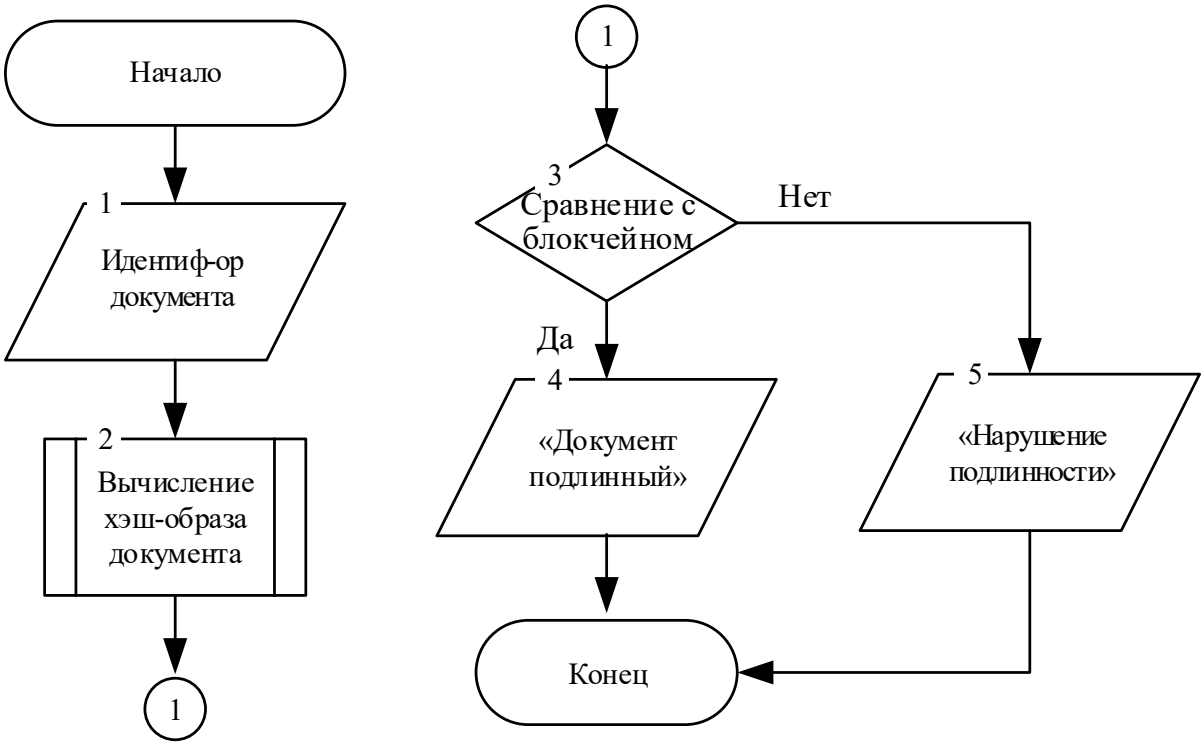


Рис.2. Алгоритм работы программного средства при проверке документа

Целостность цепочки поддерживается на уровне блокчейна. Каждый блок содержит хэш-образ предыдущего блока, формируя непрерывную последовательность. Валидаторы синхронизируют свои копии, и любое изменение данных нарушит эту связь. Пользователь системы сможет убедиться в отсутствии нарушения целостности через программу-клиент, которая отработает автоматически [2].

Отказоустойчивость поддерживается распределенной архитектурой. Если один валидатор выходит из строя, другой продолжает работу, добавляя блоки. При восстановлении отключенный узел синхронизируется через платформу Ethereum, загружая недостающие данные. Это гарантирует непрерывность СЭД даже при сбоях.

Алгоритм предотвращает дублирование подписей: контракт проверяет уникальность адресов в массиве «signers», исключая манипуляции. Записи основных событий («DocumentAdded», «DocumentSigned», «DocumentApproved») создают аудиторский след, доступный для анализа в случае споров.

Таким образом, разработанное программное средство для СЭД на базе Ethereum с PoA обеспечивает безопасность и автоматизацию документооборота. Документы хэшируются по ГОСТ 34.11-2018 и записываются в блокчейн, подписываются по ГОСТ 34.10-2018, а сервис умных контрактов автоматически утверждает их при достижении порога подписей. Проверка статуса и целостности доступна в реальном времени, а безопасность поддерживается PoA и российскими криптографическими алгоритмами. Система сочетает в себе надежность, прозрачность и эффективность, соответствуя современным требованиям к управлению документами.

Список используемых источников

1. Алтухова Н. Ф. Системы электронного документооборота: учебное пособие / Н. Ф. Алтухова [и др.] М.: КНОРУС, 2021. 202 с.

2. Гаврилов И. В., Мартынов Д. А. Программное средство аутентифицированного шифрования в системах электронного документооборота // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция ; сб. науч. ст. в 4 т. / под. ред. А. В. Шестакова; сост. В. С. Елагин, Е. А. Аникевич. СПб.: СПбГУТ, 2022. Т. 2. С. 120-124.

3. Бутерин В. Ethereum: платформа для децентрализованных приложений [Электронный ресурс] // White Paper Ethereum, 2013. URL: https://ethereum.org/en/whitepaper/ (дата обращения 27.03.2025).

4. Сингхал Б. Блокчейн. Руководство для начинающих разработчиков: пер. с англ. / Б. Сингхал [и др.] СПб.: БХВ-Петербург, 2020 288 с.

5. Вуд Г. Ethereum: децентрализованная платформа с поддержкой смарт-контрактов [Электронный ресурс] // Yellow Paper Ethereum, 2014. URL: https://github.com/ethereum/yellowpaper (дата обращения 27.03.2025).

6. Ethereum Foundation. Документация Geth: реализация клиента Ethereum на Go [Электронный ресурс] // Официальный сайт Geth, 2023. URL: https://geth.ethereum.org/docs/ (дата обращения 27.03.2025).

BLOCKCHAIN TECHNOLOGY APPLICATION IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Gavrilov I., Baranov D.
Russian Federation Security Guard Service Federal Academy

The article presents the results of developing a software tool with decentralized confirmation of information authenticity in electronic document management systems based on the Clique Proof-of-Authority consensus protocol on the Ethereum platform. The main stages of setting up the Geth software for creating a distributed blockchain network are described, including initialization of nodes, configuration of the genesis block, and ensuring synchronization between them in a local network.

Key words: *smart contracts, blockchain, distributed system, electronic document management system*

УДК 004.056.53
ГРНТИ 81.93.29

ПРОТОТИП СИСТЕМЫ ЗАЩИЩЕННОЙ IP-ТЕЛЕФОНИИ НА ОСНОВЕ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

И. В. Гаврилов, В. О. Морозов, И. А. Хрущев

Академия Федеральной службы охраны Российской Федерации

В статье представлено описание разработанного программного средства «ИВСТ», позволяющего проводить аутентификацию абонентов системы IP-телефонии до использования голосовой передачи на основе использования российских криптографических алгоритмов шифрования данных и режима выработки имитовставки. Данное программное средство является основой системы защищенной IP-телефонии.

IP-телефония, локальные сети, аутентификация, шифрование, имитовставка.

В настоящее время для аутентификации абонентов в IP-телефонии используют способ, при котором на этапе конфигурирования IP-АТС данные пользователя закрепляется за определенным портом или сетевым адресом в сети [1]. К аутентифицирующим данным в описанном случае относится, например, пароль, а используемые адрес в локальной сети, порт, номер абонента, другие данные пользователя являются идентификаторами. Однако при смене рабочего места у абонента пропадает возможность легитимного пользования сервисами IP-телефонии [2, 3].

В настоящее время аутентификация абонентов IP-телефонии происходит через локальную базу пользователей сети, находящуюся на стороне IP-АТС [4]. При высокой нагрузке, когда все сотрудники в короткий период времени для аутентификации обращаются к IP-АТС, может произойти отказ в обслуживании IP-АТС. Поэтому аутентификацию абонентов IP-телефонии необходимо строить на других принципах.

На рисунке 1 рассмотрена система IP-телефонии с реализованной атакой типа «представление нелегитимного пользователя как легитимного».

Для защиты от указанной атаки авторами предложено применять метод аутентификации по имитовставке (MAC).

Алгоритм выработки имитовставки предполагает генерирацию тега аутентификации фиксированного размера (имитовставки) для данного сообщения. Тег получен из секретного ключа, что делает невозможным под-

мену или изменение нарушителем сообщение без обнаружения. Так получатель может проверить подлинность и целостность сообщения, сравнив выработанную имитовставку с полученной от претендента (используя тот же алгоритм и секретный ключ).

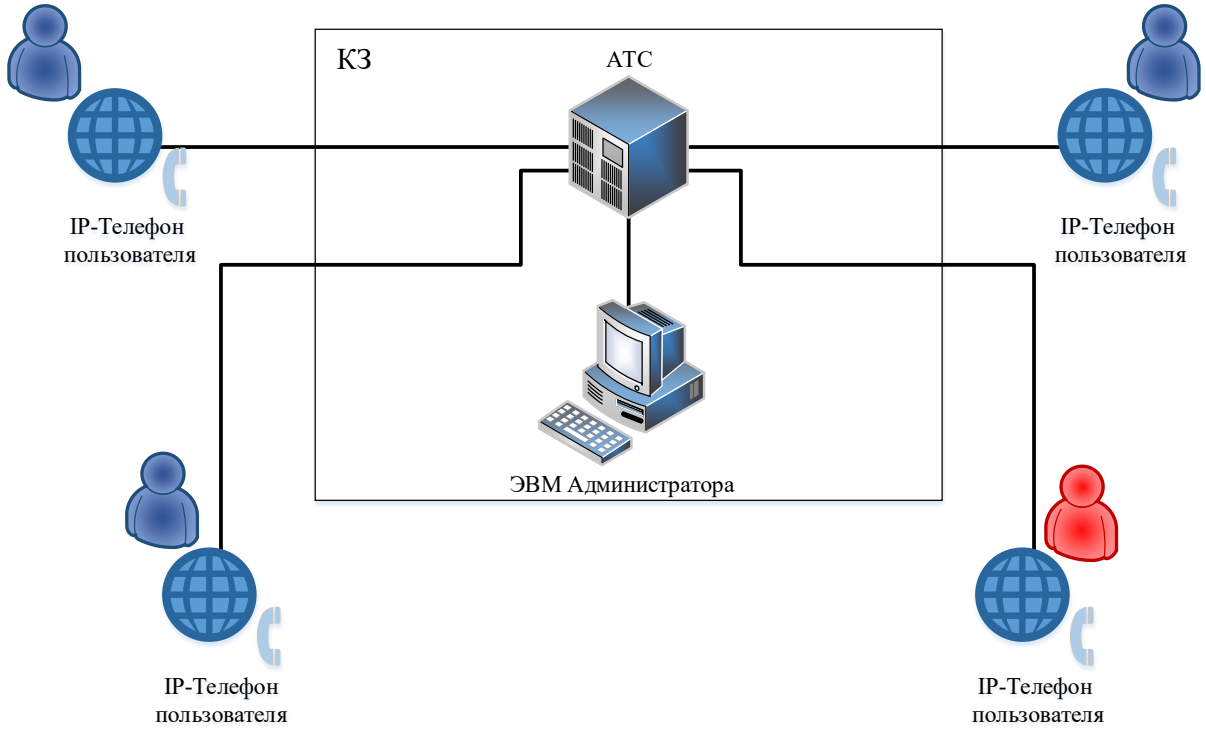


Рис. 1. Общая схема сети IP-телефонии

Для решения проблемы было разработано программное средство для аутентификации пользователей сети с помощью имитовставки «ИВСТ». За основу взят алгоритм криптографический защиты информации «Магма», содержащийся в ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры» [5]. Выбранный алгоритм применяется в криптографических методах обработки и защиты информации, в том числе для обеспечения конфиденциальности, аутентичности и целостности информации при ее передаче, обработке и хранении.

На основании описания работы блочного шифра «Магма», содержащегося в ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации» [6]. Режимы работы блочных шифров" было написано программное средство «ИВСТ».

Программное средство «ИВСТ» выполняет функцию аутентификации пользователей сети и может применяться, как средство устраняющее угрозу информационной безопасности, показанной на рисунке 1.

В качестве набора данных используются:
– логин пользователя;
– индивидуальный пароль пользователя;
– номер телефонного аппарата.

Алгоритм программного средства "ИВСТ" включает предварительный и четыре основных этапа (рис. 2).

На предварительном этапе сетевой администратор IP-телефонии создает базу данных, состоящую из имитовставок, их количество соответствует числу пользователей в сети IP-телефонии. Каждая имитовставка будет выработана из логина, пароля и номера абонента. Информация в базе данных хранится в зашифрованном виде. Программное средство "ИВСТ" на каждом рабочем месте имеет доступ к шифрованной информации, а также в отдельных рабочих местах, где установлены телефонные аппараты IP-телефонии. Так будут созданы места для доступа в сеть помимо стандартных рабочих мест работников.

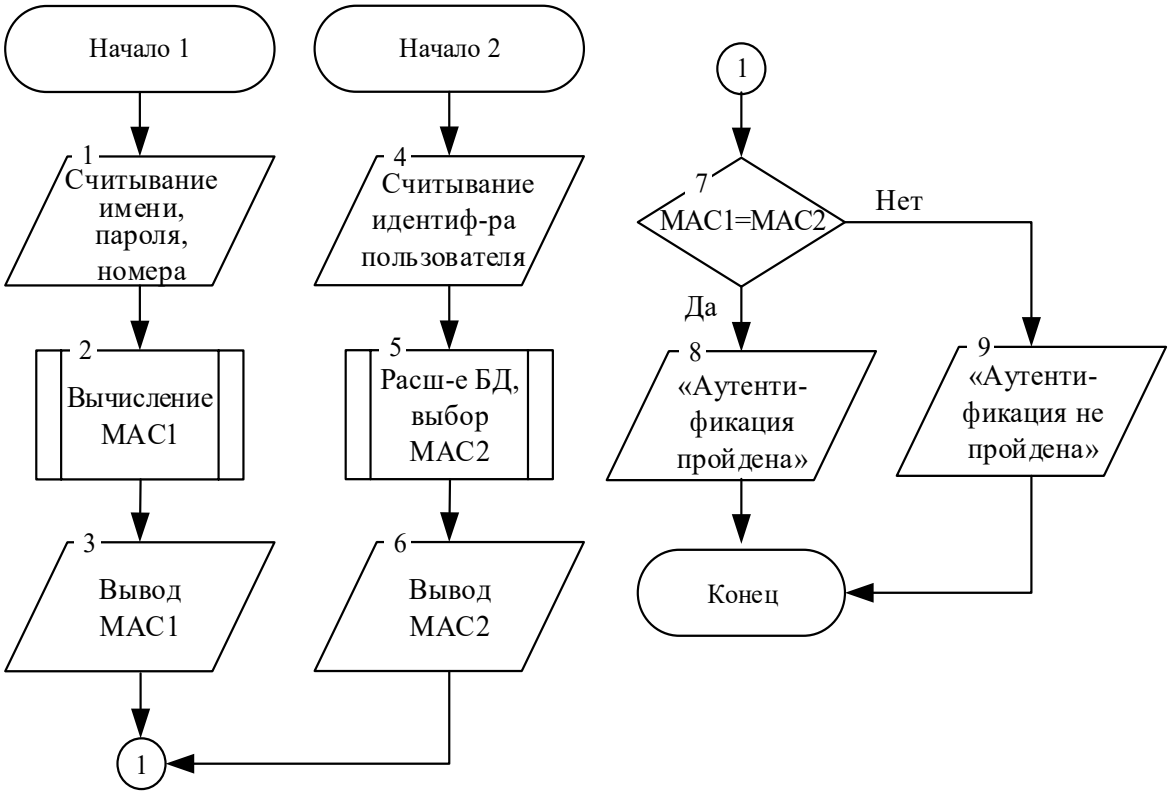


Рис. 2. Алгоритм функционирования программного средства «ИВСТ»

На первом этапе абонент, находящийся вне своего рабочего места пользователь пытается получить доступ к ресурсам сети. Пользователь вводит набор данных (рис. 2, блок 1), после чего программное средство вырабатывает имитовставку MAC1 из этого набора (рис. 2, блок 2).

На втором этапе программное средство «ИВСТ» считывает идентификатор пользователя (рис. 2, блок 4) и расшифровывает информацию из базы данных, хранящейся в памяти (рис. 2, блок 5) с выбором имитовставки MAC2.

На третьем этапе происходит сравнение имитовставок из базы данных и выработанной программным средством пользователя (рис. 2, блок 7). При успешном сравнении пользователь проходит аутентификацию (рис. 2, блок 8) и может пользоваться ресурсами IP-сети. При неудачной попытке доступ не предоставляется, а инцидент информационной безопасности записывается в журнал (рис. 2, блок 9).

На четвертом этапе программное средство «ИВСТ» отправляет конфигурационную исполнительную команду для регистрации номера за конкретным портом на IP-АТС для корректной работы.

Потенциальному нарушителю для пользования сетью IP-телефонии необходимо иметь программное средство «ИВСТ», знать логин, пароль и номер абонента, от лица которого он будет пользоваться ресурсами сети.

Таким образом, можно заключить, что внедрение программного средства «ИВСТ» повышает уровень защиты сети от нарушителей, не позволяя им использовать ресурсы системы IP-телефонии. С помощью предложенного метода аутентификации можно избавляемся от общей базы данных на IP-АТС, что приведет к разгрузке вычислительной способности и позволит использовать менее дорогое серверное оборудование, а с администратора сети снимается часть функций по прописыванию конфигурационного файла IP-АТС, абоненты сети IP-телефонии получают возможность использования ресурсов сети как на своем рабочем месте, так и на другом сетевом узле.

Список используемых источников

1. Билятдинов К. З., Арсеньева А. З., Меняйло В. В. Технологии IP-телефонии: учебное пособие. СПб.: Университет ИТМО, 2022. 166 с.

2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. М.: Мир, 2012. 552 с.

3. Афанасьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов, 2012. 254 с.

4. Рассел Дж. Единая система идентификации и аутентификации. М.: VSD, 2013. 184 с.

5. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2017.

6. ГОСТ Р 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2017.

PROTOTYPE OF A PROTECTED IP TELEPHONY SYSTEM BASED ON THE IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS

Gavrilov I., Morozov V., Hruschev I.
Russian Federation Security Guard Service Federal Academy

The article presents a description of the developed software tool "IVST", which allows authentication of subscribers of the IP telephony system before using voice transmission based on the use of Russian cryptographic algorithms for data encryption and the mode of generating message authentication code. This software is the basis of the secure IP-telephony system.

Key words: *P-telephony, local networks, authentication, encryption, message authentication code*

УДК 004.89
ГРНТИ 81.93.29

АРХИТЕКТУРА ПРОГРАММНОГО ПРОТОТИПА ВИЗУАЛИЗАЦИИ ДАННЫХ БЕЗОПАСНОСТИ ДЛЯ АНАЛИЗА С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ

К. Н. Жернова

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Многие системы обеспечения информационной безопасности, такие как системы обнаружения и предотвращения вторжений для обеспечения сетевой безопасности, используют различные модели визуализации данных в целях представления результатов анализа данных безопасности оператору для принятия окончательного решения. Однако системы на основе нейронных сетей могли бы использоваться для автоматизации процесса анализа промежуточных результатов. Для визуального анализа изображений часто используются сверточные нейронные сети. Они обладают определенными преимуществами и ограничениями. В данном докладе представлена архитектура системы для генерации изображений данных безопасности, учитывающих ограничения сверточных нейронных сетей при анализе изображения.

информационная безопасность, сетевая безопасность, поиск аномалий, визуализация данных, визуальный анализ, нейронные сети.

Введение

Нейронные сети часто используются в сетевой безопасности для обнаружения вторжений [1] – выявления атак и предугадывания поведения сетевого траффика в целях их предотвращения. Обычно для этих целей анализируются данные в текстовом виде в формате таблиц. Однако данные о событиях безопасности также часто могут быть представлены графически.

Технологии компьютерного зрения позволяют анализировать изображения. Например, для визуального анализа во многих исследованиях применяются сверточные [2] и генеративные состязательные [3] нейронные сети. Однако чаще всего нейросетевые модели занимаются поиском объектов на фотографиях и кадрах видеозаписей. Несмотря на это, существует возможность анализировать графические данные безопасности с помощью сверточных нейронных сетей [4]. Это позволит автоматизировать работу оператора приложений безопасности, например, при просмотре промежуточных результатов обработки данных безопасности приложением.

Описание архитектуры

Для того, чтобы повысить точность и оперативность распознавания нейросетевой моделью аномалий в данных безопасности на визуализации, требуется учитывать некоторые характеристики и особенности модели. Например, обработка небольших изображений с меньшим разрешением происходит быстрее, поэтому необходимо соблюдать баланс между весом изображения и его качеством, достаточным для правильного распознавания. Кроме того, визуализация не должна иметь избыточных элементов, которые могут быть расценены моделью как отдельный признак. Основываясь на данных принципах, можно спроектировать модели визуализации, которые нейросетевая модель сможет анализировать более эффективно. Архитектура программного прототипа генерации визуализаций данных безопасности с последующим анализом с помощью нейронных сетей может иметь следующие компоненты:

1) модуль подбора модели визуализации;

2) модуль генерации визуализации;

3) модуль визуального анализа на основе нейронных сетей;

4) графический пользовательский интерфейс, обеспечивающий вывод результата визуального анализа и позволяющий оператору взаимодействовать с другими модулями.

Схема архитектуры прототипа представлена на рис. 1:

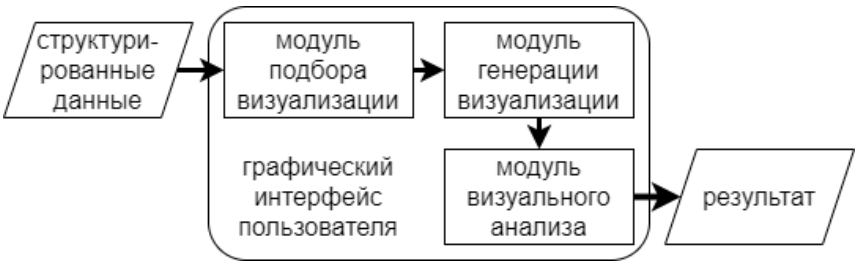


Рис. 1. Архитектура программного прототипа

Последовательность работы программного прототипа выглядит следующим образом. На вход модуля подбора модели визуализации поступают структурированные данные о событиях безопасности. На основе структуры данных первый модуль предлагает оператору возможные модели визуализации, которые отвечали бы задаче безопасности и подходят для отображения такого типа данных. Результат подбора модели отправляется на модуль генерации визуализации, в котором происходит построение графиков, содержащих данные безопасности в форме визуализации. Затем спроектированные графики поступают на модуль визуального анализа, и обученная мо-

дель нейронной сети занимается поиском аномалий на визуализации данных безопасности. В конце результаты анализа отображаются средствами графического интерфейса.

Выводы

В докладе представлена архитектура прототипа системы генерации визуализаций данных безопасности для анализа с помощью нейронных сетей с учетом особенностей сверточной нейронной сети и связанных с ними основными принципами визуализации данных. Полученные результаты позволят автоматизировать работу операторов приложений информационной безопасности.

Дальнейшая работа будет направлена разработку прототипа программного обеспечения, реализующего предложенную архитектуру, и на оценку его эффективности.

Работа выполнена при совместной поддержке РНФ и СПб НФ (проект № 24-21-20058).

Список используемых источников

1. Atefinia R., Ahmadi M. Network intrusion detection using multi-architectural modular deep neural network // The Journal of Supercomputing. 2021. Т. 77. С. 3571-3593.

2. Torres M., Cantu´ F. Learning to see: Convolutional neural networks for the analysis of social science data // Political Analysis. 2022. Т. 30. № 1. С. 113-131.

3. Goodfellow I. et al. Generative adversarial networks // Communications of the ACM. 2020. Т. 63. № 11. С. 139-144.

4. Zhernova K. Visual Malware Recognition Using Artificial Neural Networks // 2024 International Russian Automation Conference (RusAutoCon). IEEE. 2024. С. 1006-1011.

THE ARCHITECTURE OF A SOFTWARE PROTOTYPE FOR VISUALIZING SECURITY DATA FOR ANALYSIS USING NEURAL NETWORKS

Zhernova K.
Petersburg Federal Research Center of the Russian Academy of Sciences

Many information security systems, such as intrusion detection and prevention systems for network security, use various data visualization models in order to present the results of security data analysis to the operator for final decision making. However, neural network-based systems could be used to automate the process of analyzing intermediate results. Convolutional neural networks are often used for visual image analysis. They have certain advantages and limitations. This report presents the architecture of a system for generating security data images that take into account the limitations of convolutional neural networks in image analysis.

Key words: *information security, network security, anomaly detection, data visualization, visual analysis, neural networks*

УДК 004.891.3
ГРНТИ 81.93.29

АНАЛИЗ И КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Д. В. Иванов, К. Г. Налимов

Санкт-Петербургский политехнический университет Петра Великого

Системы искусственного интеллекта на сегодняшний день являются наиболее динамично развивающейся отраслью информационных технологий. Помимо гибких подходов к анализу данных и широких возможностей алгоритмов машинного и глубокого обучения, позволяющих создать модель искусственной нейронной сети для решения огромного спектра прикладных задач, данные технологии несут значительные угрозы информационной и кибербезопасности. В данной работе рассмотрен анализ угроз информационной безопасности, свойственных для систем искусственного интеллекта и приведены подходы к их классификации для дальнейшего построения модели кибербезопасности для информационных систем с применением искусственных нейронных сетей.

искусственный интеллект, информационная безопасность, противодействие угрозам, методы противодействия угрозам информационной безопасности

Процесс моделирования угроз информационной безопасности и прогнозирование возможных векторов кибератак на информационную систему является ключевым процессом при проектировании системы обеспечения информационной безопасности. Данные процессы требуют детального системного и экспертного анализа, учитывающего ряд ключевых факторов: факторы, связанные с функционированием самой информационной системы, такие как технические параметры и отраслевые особенности системы, факторы, связанные с рисками информационной безопасности. Формирование модели угроз является крайне важным и критичными процессом при проектировании информационной системы вне зависимости от ее отраслевого назначения и функционального применения. В случае проектирования информационных систем с применением технологий искусственного интеллекта, таких как искусственные нейронные сети, алгоритмы машинного и глубокого обучения, процессы моделирования угроз информационной безопасности значительно усложняются. Поскольку разработанная модель искусственного интеллекта на основе технологий искусственных нейронных сетей имеет уникальный набор параметров и характеристик, со-

ответственного данная модель помимо выявленных уязвимостей и угроз, свойственных для конкретного типа нейронной сетей, также может обладать уникальными уязвимостями и угрозами, характерными именно для данной модели нейронной сети.

Классические системы информационной безопасности, такие как системы антивирусной защиты, системы криптографической защиты информации, сетевые средства защиты информации, системы обнаружения и предотвращения вторжений, системы мониторинга и управления событиями информационной безопасности способны обеспечить базовый уровень защиты информационной системы с применений технологии искусственной нейронной сети от известных и детально изученных угроз информационной безопасности, но данные механизмы защиты не способны обеспечить защищенность самой нейронной сети от логических и целенаправленных деструктивных воздействий на алгоритм, логику и результаты работы искусственной нейронной сети [1]. Соответственно принципы построения информационной системы с применений технологий искусственного интеллекта требуют принципиально нового подхода.

В данной работе приведен анализ ключевых уникальных угроз для информационной системы с использованием технологий искусственного интеллекта. Классификация угроз базировалась на основных принципах классической информационной безопасности (конфиденциальность, целостность, доступность) пересмотренных в парадигме кибератак на системы искусственного интеллекта. Каждый тип угроз имеет индивидуальную методологию и способы реализации [2].

Были выделены три основные киберугрозы информационных систем с использованием моделей искусственного интеллекта:

1. Угрозы искажения логики работы, влекущие за собой искажение результатов работы модели, как следствие модель искусственного интеллекта проводит некорректную классификацию данных, принимает неверное решение и выдает некорректные ответы. Данный тип угроз может быть реализован атаками «белый ящик», «черный ящик», «серый ящик». Результатами реализации данных угроз могут быть как неумышленный ввод в заблуждение модели искусственного интеллекта, так и целенаправленное воздействие для получения определенного результата, отличного от правильного.

2. Угрозы конфиденциальности модели искусственного интеллекта. Данные тип угроз может быть реализован атаками на информационные ресурсы, используемые для обучения модели искусственного интеллекта, атаками подбора искаженных и ложных значений, позволяющими получить различные артефакты и сведения о функционале модели искусственного ин-

теллекта. Результатом реализации данного типа угроз может быть утечка конфиденциальной информации пользователей информационной системы, получение полного или частичного несанкционированного доступа в информационную систему и использование ее для реализации деструктивных действий.

3. Угрозы извлечения модели искусственного интеллекта. Данная угроза может быть реализована атаками на информационную инфраструктуру размещения информационной системы, где применяется модель искусственного интеллекта, атаки на обучающий набор данных модели и использования подменных данных при взаимодействии с моделью. Результатом реализации данной угрозы может нелегитимное копирование модели искусственного интеллекта, которая функционирует аналогично исходной модели и ее дальнейшее нелегитимное использование как в коммерческих, так и вредоносных целях.

Угрозы могут быть реализованы путем проведения атак на модель искусственного интеллекта при наличии или отсутствии у злоумышленника информации и доступности модели. Таким образом атаки можно классифицировать по признаку наличию у злоумышленника доступа и сведений о модели. В данному случае можно выделить три основных тапа атак:

1. Атака «белый ящик». Реализация атак «белый ящик» возможна при условии наличия у злоумышленника доступа к обучающему набору данных, также злоумышленник обладает целостными знаниями об используемой модели искусственного интеллекта. Атака «белый ящик» является худшим вариантов реализации данной угрозы, поскольку злоумышленник имеет полный доступ к архитектуре, классификатору и обучающим данным модели искусственно интеллекта, что позволяет злоумышленнику кардинально изменить логику работы модели по своему усмотрению. При проектировании модели угроз для данного типа атак к классу нарушителей, способных ее реализовать, следует отнести внутренних нарушителей, разрабатывающих модель искусственного интеллекта, лиц, обеспечивающих функционирование информационной системы с применением искусственного интеллекта, внешних нарушителей с высоким потенциалом, завладевших полной информацией о модели.

2. Атака «черный ящик». Атаки, относящие к типу «черный ящик» являются полной противоположностью класса атак «белый ящик», поскольку у злоумышленника отсутствует какая-либо информация о разрабатываемой модели. При проектировании модели угроз в качестве нарушителей следует рассматривать внешних нарушителей с высоким потенциалом. Для реализации данной атаки злоумышленнику необходимо обладать глубокими знани-

ями и навыками в области технологий искусственного интеллекта, информационных технологий и математики.

3. Атака «серый ящик» является комбинированным вариантом атаки черного и белого ящика, подразумевающего наличия у злоумышленника частичной информации об устройстве модели искусственного интеллекта. При проектировании модели угроз к нарушителям следует относить злоумышленников, определенных для типов атак белый и черный ящик [3].

В таблице 1 приведена классификация наиболее атак и методов их реализации, распределенные по степени владения нарушителем информации о модели искусственного интеллекта. Наименование методов реализации атак переведены с английского языка [4].

ТАБЛИЦА 1. Классификация атак по владению нарушителем информации о модели искусственного интеллекта

Атака	Метод
Атаки «белый ящик»	Алгоритм Бройдена – Флетчера – Гольдфарба – Шанно с ограничением использования памяти
	Метод быстрого градиента
	Базовый итеративный метод
	Атака «полный дурак»
	Метод незначительных изменений
	Алгоритм Карлини-Вагнера
	Метод Вассерштейна
	Метод одношагового целевого класса
	Горячий/холодный метод
	Атака карты значимости на основе Якобиана
	Итеративный метод класса с наименьшей вероятностью
Атаки «черный ящик»	Граничная атака
	Атака с нулевым запросом
	Методы генеративно-состязательной сети
	Вероятностно-взвешенная значимость слов
	Методы генетических алгоритмов
Атаки «серый ящик»	Применяются комбинированные методы атак «белый ящик» и «черный ящик»

Помимо рассмотренных в данной работе угроз и атак при проектировании модели угроз системы искусственного интеллекта и вектора атак следует учитывать следующие параметры информационной системы:

– тип и категория данных, на которые направлен вектор атаки;
– цели и сложность атаки;
– функционально-ролевая модель пользователей и разработчиков системы;
– технологическая модель применения искусственного интеллекта.

Основываясь на приведенной в данной статье аналитической работе, предлагается комплексный подход к анализу и классификации угроз информационной безопасности для систем искусственного интеллекта, начинающийся в первую очередь с определения степени использования алгоритмов искусственного интеллекта в информационной системе [5]. Процент использовании искусственного интеллекта определяется соотношением количества автоматизированных процессов информационной системы с применением алгоритмов искусственного интеллекта к общему количеству процессов:

$$P = \frac{N}{T} * 100\%,$$

где P – процент автоматизации процессов с помощью искусственного интеллекта, N – количество автоматизированных процессов с помощью искусственного интеллекта, T – общее количество процессов.

При дальнейшем проектировании системы кибербезопасности следует учитывать рассмотренные в данной статье угрозы и атаки основываясь на степени автоматизации процессов с применением алгоритмов искусственного интеллекта как на ключевой фактор моделирования угроз.

Список используемых источников

1. Костогрызов А. И., Нистратов А. А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023. № 5(57). С. 9-24.

2. Путято М. М., Макарян А. С. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства // Прикаспийский журнал: управление и высокие технологии. 2020. № 3 (51). С. 94–102.

3. Володин И. В., Путято М. М., Макарян А. С., Евглевский В. Ю. Классификация механизмов атак и исследование методов защиты систем с использованием алгоритмов машинного обучения и искусственного интеллекта // Прикаспийский журнал: управление и высокие технологии, № 2 (54). 2021. С. 91-97.

4. Котенко И. В., Саенко И. Б., Лаута О. С., Васильев Н. А., Садовников В. Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований // Вопросы кибербезопасности. 2024. № 1(59). С. 24-37.

5. Пантелеева Т. А. Возможности и угрозы использования искусственного интеллекта в бизнес-форсайте российских компаний // Проблемы рыночной экономики. 2021. № 1. С. 131-148.

ANALYSIS AND CLASSIFICATION OF INFORMATION SECURITY THREATS IN ARTIFICIAL INTELLIGENCE SYSTEMS.

Ivanov D., Nalimov K.
Peter the Great Saint Petersburg Polytechnic University

Artificial intelligence systems are currently the most dynamically developing information technology industry. In addition to flexible approaches to data analysis and the extensive capabilities of machine learning and deep learning algorithms, which make it possible to create an artificial neural network model for solving a wide range of applied tasks, these technologies pose significant threats to information and cybersecurity. This paper examines the analysis of information security threats inherent in artificial intelligence systems and provides approaches to their classification for further building a cybersecurity model for information systems using artificial neural networks.

Key words: *artificial intelligence, information security, countering threats, methods of countering threats to information security*

УДК 004.891.3
ГРНТИ 81.93.29

ПРОТИВОДЕЙСТВИЕ УГРОЗЕ ОТРАВЛЕНИЯ ДАННЫХ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПУТЕМ ПРИМЕНЕНИЯ МЕХАНИЗМОВ ПРЕДВАРИТЕЛЬНОГО АНАЛИЗА ОБУЧАЮЩИХ ДАННЫХ

Д. В. Иванов, К. Г. Налимов

Санкт-Петербургский политехнический университет Петра Великого

Технологии искусственного интеллекта имеют широкий спектр применения. Важным аспектом при создании системы искусственного интеллекта является задача по обеспечению кибербезопасности. В данном исследовании рассматривается проблема отравления модели искусственного интеллекта злонамеренно искаженными обучающими данными. Проблема в том, что киберпреступник намеренно добавляет вредоносные данные в общий массив обучающих данных, и со временем сама модель искусственного интеллекта становится объектом, способным на деструктивные или злонамеренные действия. Предлагаемый метод противодействия угрозе отравления модели искусственного интеллекта основан на внедрении в саму модель механизмов предварительного анализа обучающих данных с целью обнаружения и блокировки потенциально вредоносной выборки данных. Предложенный метод позволяет снизить вероятность отравления модели искусственного интеллекта.

искусственный интеллект, отравление данных, информационная безопасность, противодействие угрозам, методы противодействия отравлению данных

Угроза отравления системы искусственного интеллекта вредоносными искаженными данными может быть реализована различными способами и методами. Наиболее распространенными методами отравления данных являются добавление шума, вставка ложных объектов, удаление данных, изменение меток классов и модификация структуры данных. Последствия реализации угрозы отравления данных системы искусственного интеллекта могут иметь серьезные последствия для многих сфер человеческой жизни в зависимости от области применения системы [1].

Для систем искусственного интеллекта, распознающих образы и изображения, отравление данных наиболее критично, так как может привести к снижению и потере точности работы модели, как следствие – неверное распознавание объекта, что может позволить злоумышленнику манипулировать системой искусственного интеллекта и успешно обходить действующую систему безопасности и создавать в ней критические уязвимости. Ти-

повая атака отравления данных на примере искусственной нейронной сети представлена на рис. 1 [2].

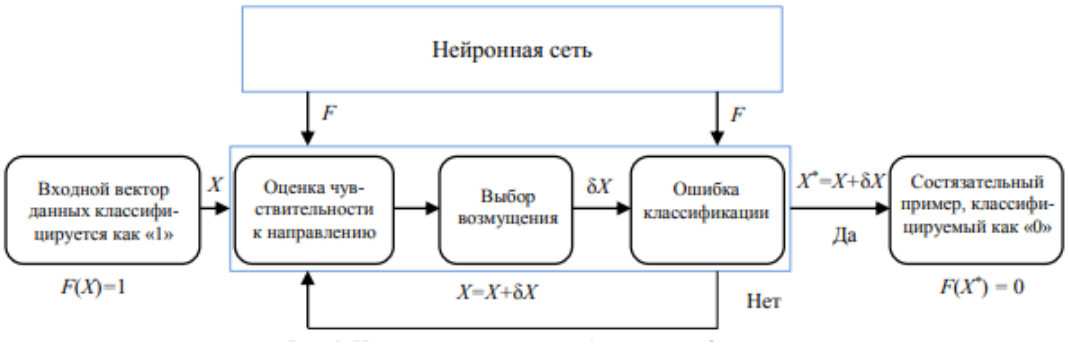


Рис. 1. Атака отравления данных

Методы и модели противодействия угрозе отравления данных систем искусственного интеллекта и алгоритмов машинного и глубокого обучения представляют широкую область для научных исследований. Для противодействия угрозе отравления данных было разработано большое количество методов, позволяющих защитить обучающие данные от целенаправленного искажения.

Были рассмотрены методы, основанные на принципе отклонения негативного воздействия, методы, базирующиеся на вероятностной оценке отравления обучающих данных, методы в основе которых лежит сравнение обучающей выборки данных с эталонным датасетом. Рассмотренные методы реализуемы для защиты от угрозы отравления данных, но имеют свои ограничения и могут допускать реализацию угрозы отравления данных [3].

В данной исследовании предлагается метод, основанный на комплексном анализе угроз отравления данных систем искусственного интеллекта, построенных на базе алгоритмов глубокого обучения. Для реализации данного метода предлагается обучение взаимосвязанных моделей искусственного интеллекта. Выходные данные первой модели нейронной сети используются в качестве входных обучающих данных для последующих моделей. На первом этапе безопасная модель, обученная при помощи данных, содержащих известные признаки атак отравления данных, выполняет функцию фильтрации входящих данных путем исключения отравленных данных и нерелевантных признаков.

В качестве безопасной модели предлагается использовать сверточную нейронную сеть, обученную на корректных изображениях и изображениях,

содержащих признаки отравления, что позволит модели выявлять и классифицировать аномалии в изображениях [4].

При создании модели, позволяющей выявлять признаки отравления данных была выбрана архитектура сверточной нейронной сети глубокого обучения, в качестве сложной адаптивной модели обработки обучающего набора данных, позволяющей выявлять сложные зависимости и нетиповые признаки отравления и искажения обучающей и тестовой выборки, поступающей на вход обучаемой модели. Структура сверточной нейронной сети представлена на рис. 2.

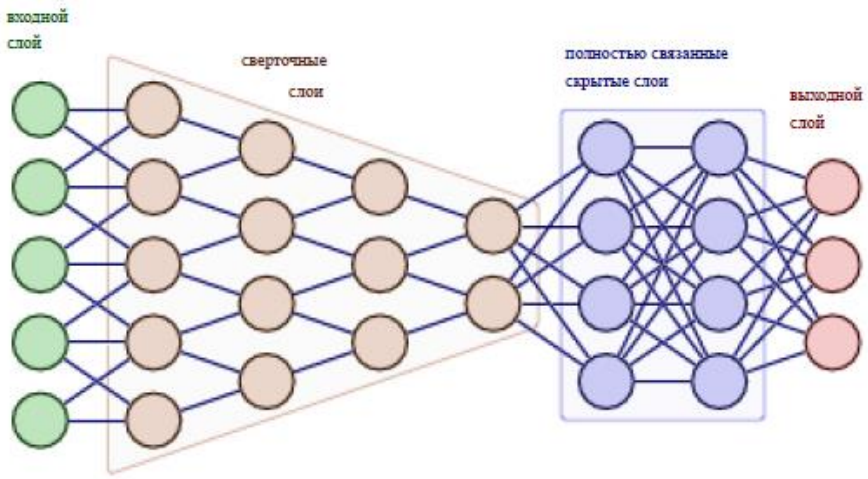


Рис. 2. Структура сверточной нейронной сети

При создании модели, позволяющей идентифицировать отравленные данные ключевой акцент делает на достоверность обучающего набора данных, данные для обучения должны быть экспертно проверены на корректность, что в дальнейшем обеспечит модели высокий процент обнаружения. Последующие модели нейронной сети обрабатывают данные, очищенные от отравления.

Методология обучения сверточной нейронной сети для выявления отравленных данных представлена на рис. 3.

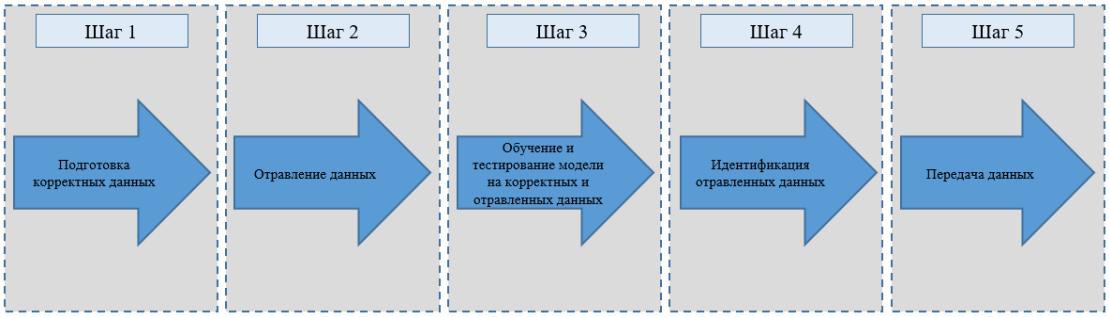


Рис. 3. Методология обучения сверточной нейронной сети

Методология обучения сверточной нейронной сети, предназначенной для выявления признаков отравления данных, представляет собой доработанную классическую методологию глубокого обучения, учитывающая специфику дальнейшей передачи данных в экосистему моделей глубокого обучения с дальнейшей обработкой данных, свободных от отравления.

Данный метод может быть применен для нейронных сетей, используемых для распознавания изображения. Модель безопасной нейронной сети определяет отравленные элементы изображения, далее модели искусственного интеллекта обрабатывают изображение свободное от отравленных данных.

Процесс обучения сверточной нейронной сети для выявления отравления данных включал в себя следующие основные шаги. На первом шаге были выбраны корректные изображения, которые в дальнейшем должны распознавать последующие модели искусственного интеллекта. На втором шаге были произведено отравление данных. На третьем шаге произведено обучение модели сверточной нейронной сети на корректных и отравленных данных. Следующим шагом было тестирование и идентификация признаков отравления при помощи обученной модели. Далее изображения свободные от признаков отравления передаются в последующие модели для дальнейшей обработки. Схема обучения сверточной нейронной сети представлена на рис. 4.

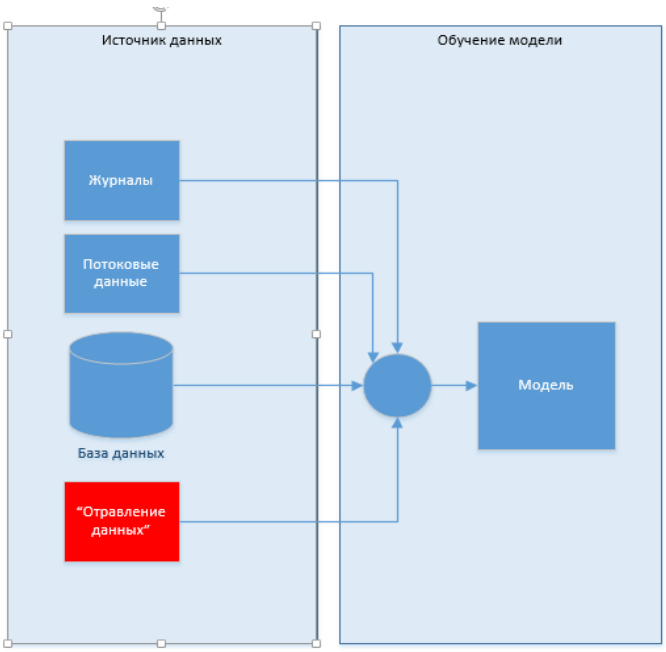


Рис. 4. Обучение модели сверточной нейронной сети

Для эксперимента были использованы цветные изображения дорожных знаков, заимствованные из открытых достоверных источников данных. В качестве достоверного источника были выбраны официальные базы изображений автодорожных знаков. В ходе проведения эксперименты было отобрано 1000 снимков дорожных знаков и проведено отравление различными методами и техниками [5], [6]. Изображения были разделены на 10 классов для каждого типа отравления:

1) добавление триггеров в изображение;
2) зашумление изображения;
3) включение дополнительных объектов в исходное изображение;
4) цветовые манипуляции;
5) световые манипуляции;
6) добавление несвойственных или случайных паттернов;
7) изменение метаданных изображения;
8) добавление прозрачных областей;
9) изменение масштаба изображения;
10) изменение пикселей изображения.

Разработанная модель показала высокую точность обнаружения признаков отравления, которая составила более 75 % в зависимости от типов отравления данных. Наиболее критичными для модели оказались атаки с низким процентом отравления данных.

В данной работе был разработан механизм предварительного анализа обучающих данных на основе сверточной нейронной сети, который позволяет идентифицировать целенаправленное искажение изображения.

Данный механизм может быть использован в качестве инструмента противодействия угрозе отравления данных в экосистеме моделей искусственного интеллекта для распознавания и идентификации изображений.

Список используемых источников

1. Эртель В. Введение в искусственный интеллект. М. «Эксмо», 2019. 448 с.

2. Подтопельный В. В. Особенности моделирования атак на модели машинного обучения с использованием марковских процессов принятия решений // Доклады ТУСУР. 2024. № 2 (том 27). С. 21-30.

3. Ильюшин Е. А., Намиот Д. Е., Чижов И. В. Атаки на системы машинного обучения – общие проблемы и методы // International Journal of Open Information Technologies. 2022. № 10(3). С. 17-22.

4. Костогрызов А. И., Нистратов А. А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023. № 5(57). С. 9-24.

5. Шульга Т. Э., Солопекин Д. А. Распознавание дорожных знаков российского образца с использованием нейронных сетей // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика 2024. № 2. С. 85-95.

6. Смольянинов В. А., Гришунов С. С., Белов Ю. С. Нейросетевая модель для распознавания дорожных знаков // Научное обозрение. Технические науки. 2021. № 3. С. 50-54.

COUNTERING THE THREAT OF DATA POISONING OF ARTIFICIAL INTELLIGENCE SYSTEMS BY USING MECHANISMS OF PRELIMINARY ANALYSIS OF TRAINING DATA

Ivanov D., Nalimov K.
Peter the Great Saint Petersburg Polytechnic University

Artificial intelligence technologies have a wide range of applications. An important aspect in creating an artificial intelligence system is the task of ensuring cybersecurity. This study examines the problem of poisoning an artificial intelligence model with maliciously distorted training data. The problem is that cybercriminals intentionally add malicious data to the general array of training data, and over time, the artificial intelligence model itself becomes an object capable of destructive or malicious actions. The proposed method of countering the threat of poisoning of the artificial intelligence model is based on the introduction of mechanisms for preliminary analysis of training data into the model itself in order to detect and block potentially malicious data samples. The proposed method reduces the likelihood of poisoning the artificial intelligence model.

Key words: *artificial intelligence, data poisoning, information security, countering threats, methods of countering data poisoning*

УДК 004.4
ГРНТИ 81.93.29

ОСНОВНЫЕ ЭТАПЫ АВТОРСКОЙ МЕТОДОЛОГИИ РЕВЕРС-ИНЖИНИРИНГА МАШИННОГО КОДА В ИНТЕРЕСАХ ПОИСКА В НЕМ УЯЗВИМОСТЕЙ

К. Е. Израилов

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Работа посвящена авторской методологии получения высокоуровневых представлений программы, подходящих для анализа экспертом, из ее бинарной формы (т.е. машинного кода). Основным назначением методологии является поиск в программе уязвимостей, ведущих к соответствующим нарушениям информационной безопасности. Кратко описываются основные этапы методологии, а именно, следующие: подготовительные мероприятия, статическое исследование, динамическое исследование, документирование; приводится их графическая схема.

реверс-инжиниринг, программа, уязвимость, методология, этапы

Введение

Наличие уязвимостей в программном обеспечении является актуальной проблемой информационной безопасности. Их эксплуатация (как случайная, так и злонамеренная) является причиной различных информационных угроз. Так, например, наличие ошибок в алгоритмах шифрования данных может приводить к нарушению их конфиденциальности, некорректное использование операций копирования информации – к ее порче и нарушению целостности, а реализация ошибочных вычислений в виде деления на ноль – к программным исключениям и нарушению доступности по выводу данных из программы. Одним из способов противодействия уязвимостям является их обнаружение и исправление. Однако, типичная для программ бинарная форма слабо подходит для статического анализа (в особенности экспертного) и требует перевода в более высокоуровневую – в ее исходный код. При этом, отдельной задачей является получение самого кода программы в случае ее выполнения во встроенных устройствах (а не на персональном или серверном компьютере, где такой код может быть получен средствами операционной системы). Таким образом, поиск уязвимостей программы, в общем случае, является сложной комплексной задачей, требу-

ющей применения не отдельного научно-практического инструментария, а единой методологии (далее – Методология); именно ее основным этапам, выделенным на основании большого авторского опыта и научных публикаций российских и зарубежных авторов, и посвящена данная статья; расширенное же описание Методологии было опубликовано ранее [1, 2, 3].

Этапы методологии

Целевым применением предложенной Методологии является получение более высокоуровневых представлений программы из ее низкоуровневого машинного кода (такой процесс классически называется реверс-инжинирингом) с последующим поиском уязвимостей. Методология была разделена на 4 последовательно выполняемых этапа, описание которых приведено далее.

Этап 1 «Подготовительные мероприятия» предназначен для получения инструкций машинного кода, которые выполняются на устройстве, где они хранятся в виде единого бинарного образа специального формата. При этом, как правило, сам машинный код расположен или в специальных секциях выполняемых программ из состава программной системы образа, или же запакован в него в виде монолитного бинарного участка. Как результат, требуется наличие соответствующих методик – по извлечению образа из устройства, его программной системы, самих программ и их секций. Последними могут являться непосредственно хранящие выполняемый код (так называемые, «.text»), инициализированные и пустые данные («.data» и «.bss»), константы («.rodata») и пр. Полученная таким образом информация передается на следующий этап. Также, анализ программной системы позволяет выявить взаимодействие между ее элементами.

Интуитивно понятная упрощенная схема 1-го этапа с его основными шагами (прямоугольники с прямыми краями), основными (сплошные стрелки) и вспомогательными (пунктирные стрелки) действиями шага над данными, а также самими данными (прямоугольники с закругленными краями), представлены на рис. 1.

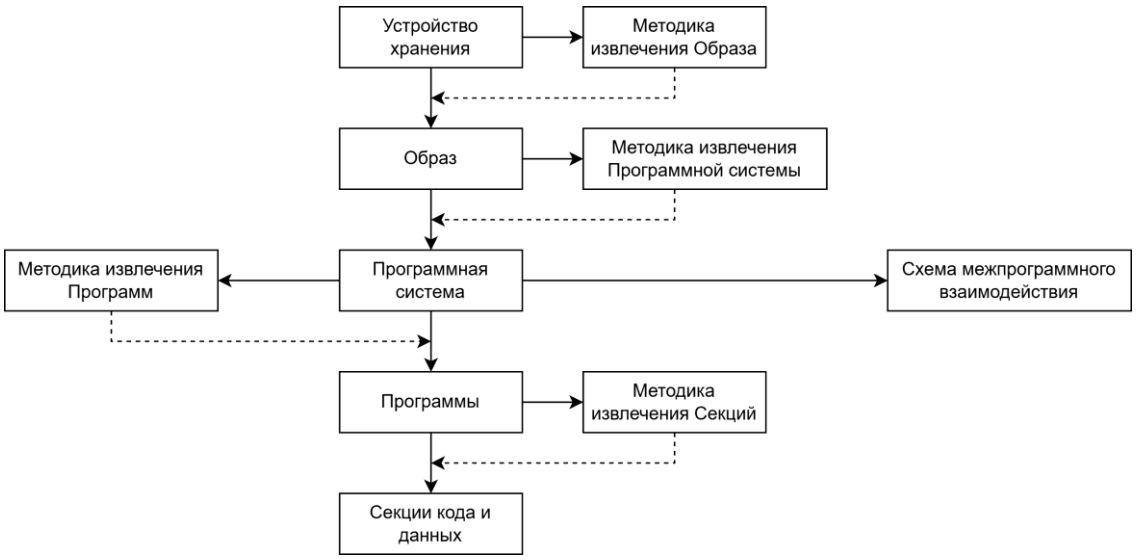


Рис. 1. Упрощенная схема шагов и данных Этапа 1

Таким образом, Этап 1 на входе принимает устройство хранения образа с машинным кодом, а на выходе возвращает секции кода и данных содержащей его программы (или, в случае монолитного образа – две аналогичные области).

Этап 2 «Статическое исследование» предназначен для непосредственного изучения машинного кода без его выполнения – т.е. методами статического анализа. В процессе этого из секций программы выделяется код инструкций процессора, который затем «разбивается» на подпрограммы (т.е. на функции с возвращаемыми значениями или процедуры без них); также выделяются глобальные области данных (аналоги глобальных переменных), используемые алгоритмами машинного кода.

Применение средств декомпиляции позволяет преобразовать подпрограммы, имеющие бинарный вид и не подходящие для ручного анализа, в более человеко-ориентированную форму в виде псевдо-исходного кода. Дальнейшее повышение абстракции позволит восстановить алгоритмы такого кода (например, в виде блок-схем), а также общую архитектуру программного решения или даже его концептуальную модель (как совокупность основополагающих сущностей и их связей). Данная группа шагов является наиболее технически сложной, в осуществлении которой может оказаться востребованным применение искусственного интеллекта, в том числе, за счет авторской генетической декомпиляции [4].

Побочным результатом такого статического анализа может быть выявление внутрипрограммного (или межподпрограммного) взаимодействия, что позволит частично определить и соответствующие интерфейсы (в том числе внешние, обеспечивающие взаимодействие элементов программной си-

стемы, упомянутой при описании Этапа 1). Также, на данном этапе возможна декларация и систематизация реализуемого функционала, а также выявление в коде уязвимостей с применением различных способов поиска [5].

Упрощенная схема 2-го этапа представлена на рис. 2; пунктирным прямоугольником с закругленными краями обозначен блок данных, названных метаинформацией, поскольку они отражают информационные особенности машинного кода с различных разноуровневых аспектов.

Таким образом, Этап 2 на входе принимает секции кода и данных, а на выходе возвращает частичную информацию об интерфейсах (который может использоваться при повторном выполнении Этапа 1 для уточнения информации о программной системе), функционале машинного кода и его уязвимостях.

Этап 3 «Динамическое исследование» достаточно близок к статическому, поскольку имеет такие же шаги, но выполняемые динамически – т.е. путем непосредственного «запуска» кода (как на эмуляторе, так и в отладчике, или даже анализируя лог работы, создаваемые специально внедренным функционалом).

Схема 3-го этапа идентична предыдущему, приведенному на рис. 2.

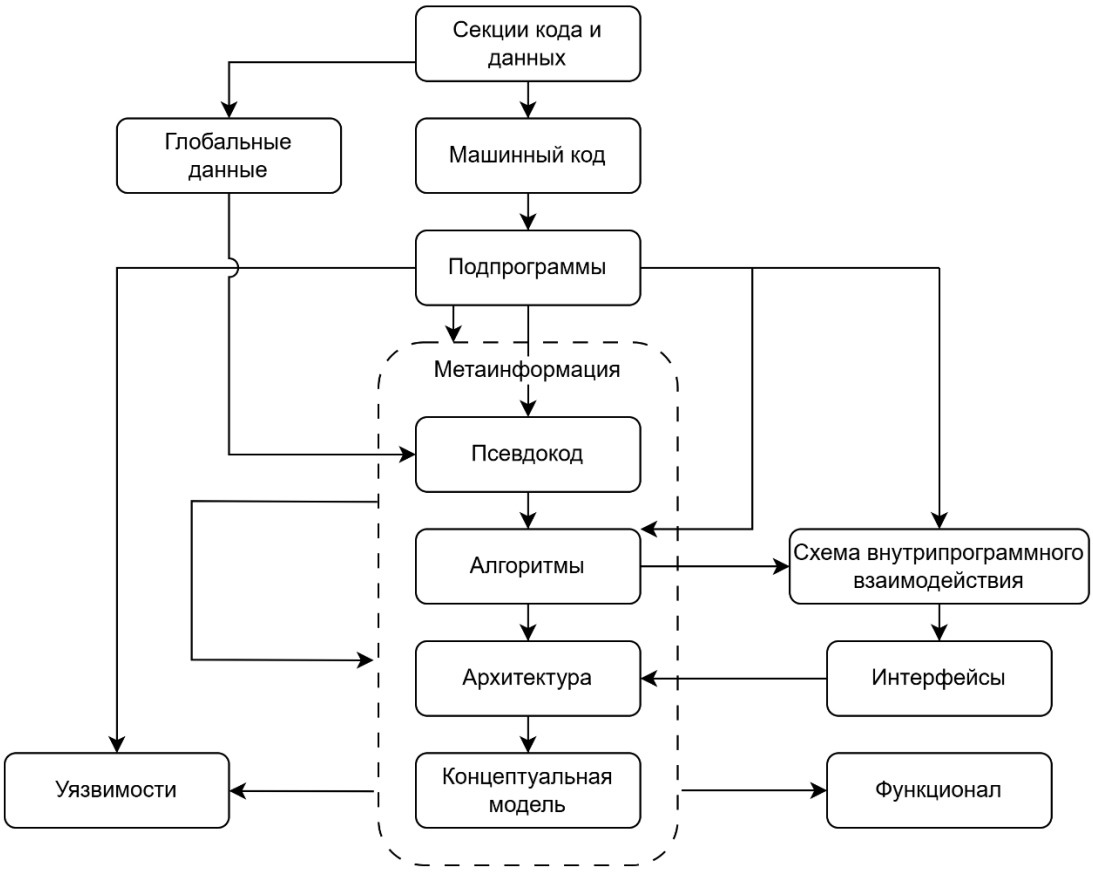


Рис. 2. Упрощенная схема шагов и данных Этапов 2 и 3

Таким образом, вход и выход Этапа 3 аналогичны Этапу 2.

Этап 4 «Документирование» является заключительным и переводит информацию (естественно, важную в аспекте понимания деталей и принципов работы машинного кода и его уязвимостей), полученную на предыдущих этапах, в документированный вид, готовый для анализа экспертами по безопасности; при этом, формализация документации позволит затем применять соответствующие автоматические средства анализа. Так, из выделенных на Этапе 3 уязвимостей можно сформировать их описание, что в последствии позволит оценить и задокументировать безопасность всего образа машинного кода и, следовательно, исследуемого устройства; а описание метаинформации послужит основой для ее более глубокого анализа соответствующими экспертами (например, по архитектурным или иным уязвимостям); итоговая систематизация функционала машинного кода даст полное представление об особенностях работы кода (например, о его возможностях, не отраженных в сопроводительной документации, таких, как наличие небезопасных «бэкдоров», скрытых каналов передачи данных третьим лицам и т.п.).

Упрощенная схема 4-го этапа представлена на рис. 3.

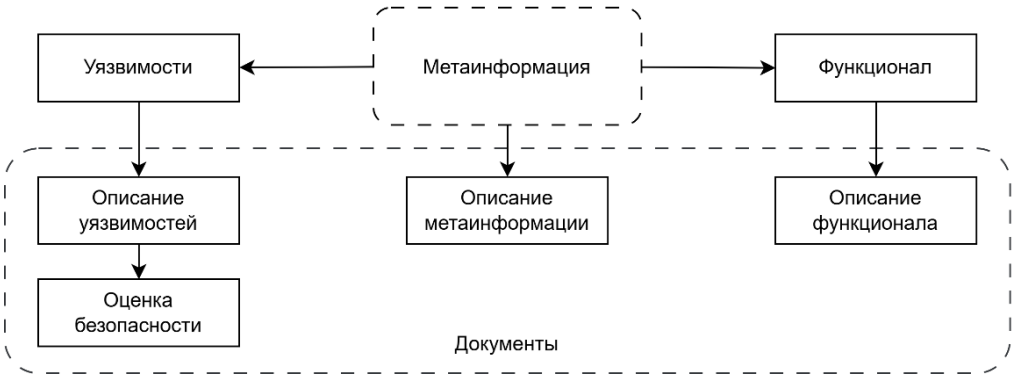


Рис. 3. Упрощенная схема шагов и данных Этапа 4

Таким образом, Этап 4 на входе принимает метаинформацию о структуре и деталях машинного кода, его функционале и уязвимостях, а на выходе формирует соответствующий комплект итоговых документов.

Заключение

В работе кратко описана авторская Методология реверс-инжиниринга, охватывающая все этапы исследования машинного кода – от его получения из устройства хранения и выполнения, до формирования итоговой документации. Основной целью Методологии является оценка безопасности машин-

ного кода путем обнаружения в нем уязвимостей и составления «истинного» функционала. Сама Методология является одним из основных научных результатов более крупного исследования, а ее новизна заключается как в наличии оригинальных шагов, так и в общей систематизации научно-практического опыта, накопленного современными учеными данной предметной области. Продолжением работы может стать более детализированное исследование отдельных шагов Методологии, как с целью разработки новых решений, так и использования существующих.

Список используемых источников

1. Израилов К. Е. Методология реверс-инжиниринга машинного кода. Часть 1. Подготовка объекта исследования // Труды учебных заведений связи. 2023. Т. 9. № 5. С. 79-90. DOI: 10.31854/1813-324X-2023-9-5-79-90.

2. Израилов К. Е. Методология реверс-инжиниринга машинного кода. Часть 2. Статическое исследование // Труды учебных заведений связи // 2023. Т. 9. № 6. С. 68-82. DOI: 10.31854/1813-324X-2023-9-6-68-82.

3. Израилов К. Е. Методология реверс-инжиниринга машинного кода. Часть 3. Динамическое исследование и документирование // Труды учебных заведений связи. 2024. Т. 10. № 1. С. 86-96. DOI: 10.31854/1813-324X-2024-10-1-86-96.

4. Израилов К. Е. Концепция генетической декомпиляции машинного кода телекоммуникационных устройств // Труды учебных заведений связи. 2021. Т. 7. № 4. С. 10–17. DOI:10.31854/1813-324X-2021-7-4-95-109.

5. Израилов К. Е., Гололобов Н. В., Краскин Г. А. Метод анализа вредоносного программного обеспечения на базе Fuzzy Hash // Информатизация и связь. 2019. № 2. С. 36-44.

MAIN STAGES OF THE AUTHOR'S METHODOLOGY OF MACHINE CODE REVERSE ENGINEERING IN THE INTERESTS OF SEARCHING FOR VULNERABILITIES IN IT.

Izrailov K.
Saint Petersburg Federal Research Center of the Russian Academy of Sciences

The work is devoted to the author's methodology for obtaining high-level representations of a program suitable for expert analysis from its binary form (i.e. machine code). The main purpose of the methodology is to search for vulnerabilities in the program that lead to corresponding information security breaches. The main stages of the methodology are briefly described, namely, the following: preparatory activities, static research, dynamic research, documentation; their graphical diagram is provided.

Key words: *reverse engineering, program, vulnerability, methodology, stages*

УДК 007.3
ГРНТИ 44.29.01

ОЦЕНКА ВЛИЯНИЯ НА ИЗМЕНЕНИЕ РАСХОДОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОСЕТЕВОЙ КОМПАНИИ РЕГИОНАЛЬНОГО УРОВНЯ В СВЯЗИ С ВСТУПЛЕНИЕМ В СИЛУ 01.09.2024 ПОЛОЖЕНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА № 185-ФЗ ОТ 13.07.2024 «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ЭЛЕКТРОЭНЕРГЕТИКЕ»

Н. Н. Киселёв[1], С. Н. Смирнов[2]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] Московский Государственный технический университета им. Н. Э. Баумана

В статье рассмотрено влияние изменений, вносимых в федеральный закон «Об электроэнергетике» на деятельность электросетевой компании. Определены возможные векторы развития хозяйственной деятельности организации. Предложен вариант алгоритма действий для адаптации деятельности к изменившимся условиям регулирования со стороны законодательства.

информационная безопасность, электросетевая компания, дистанционное управление технологическими режимами, критическая информационная инфраструктура

Данная статья посвящена оценке влияния новых положений Федерального закона № 185-ФЗ, вступившего в силу 1 сентября 2024 года, на расходы региональных электросетевых компаний в области защиты информации. В условиях стремительного развития технологий и применения цифровых решений в сфере электроэнергетики вопрос информационной безопасности становится крайне актуальным. Электросетевые компании сталкиваются с новыми вызовами, связанными с защитой данных и обеспечением устойчивости своих информационных систем. Основная цель статьи заключается в анализе того, каким образом изменения, предусмотренные законом, повлияют на финансовые и кадровые аспекты работы компаний.

Значение информационной безопасности в электроэнергетике трудно переоценить. Особенно актуальными вопросы информационной безопасности связаны с тем, что электросетевые компании относятся к субъектам критической информационной инфраструктуры, а также той ответственностью, которую накладывает этот статус. Сохранение целостности, конфиденциальности и доступности данных – одни из важных факторов, которые обес-

печивают стабильную работу энергетических объектов. Нормативные изменения, вводимые Федеральным законом № 185-ФЗ, требуют от предприятий не только повышения уровня защищенности информации, но и пересмотра существующих подходов к управлению рисками. Одной из задач статьи является детальный анализ новых требований, предъявляемых законом, и их потенциального воздействия на финансовые затраты компаний на обеспечение безопасности. Другой задачей является предложение алгоритма действий принятия решения о необходимости внесения корректировок в деятельность и планы развития для электросетевых компаний.

Крупные изменения затрагивают не только инвестиции в технологии защиты, но и необходимость повышения квалификации сотрудников и их количество, что также требует значительных ресурсов. Появляющиеся требования к дополнительным мерам безопасности могут привести к увеличению расходов на обучение персонала и переквалификацию. В этом контексте важным является должный анализ кадровой политики компаний и разработки новых программ обучения, соответствующих современным вызовам.

Основным методом данного исследования является анализ действующего законодательства и состояния рассматриваемой организации. В целях сохранения конфиденциальности название организации в данной статье не отражено.

Первым шагом в процессе сбора данных стало определение источников информации. Были выбраны как первичные, так и вторичные источники. К первичным источникам относятся интервью с руководителями и специалистами по информационной безопасности в электросетевых компаниях.

К вторичным источникам относятся существующие отчеты, публикации и данные из открытых источников, таких как тематические исследования и данные о защищаемых активах электросетевой компании.

Анализ положений Федерального закона № 185-ФЗ позволил сформулировать исходя из целей и задач исследования, сформулировать следующие подзадачи:

– сформировать позицию организации относительно требований к функциям системного оператора в части ИБ и ИТ, и какие дополнительные функции накладывает на организацию в части подконтрольных компаний;
– определить влияние статьи 15.1 об обеспечении дистанционного управления технологическими режимами работы и эксплуатационным состоя-

нием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике [1] на потенциальные расходы в области защиты информации и изменения ИТ инфраструктуры организации.

Результаты и обсуждение

Основное внимание уделяется тому, какие конкретные изменения ожидаются в необходимости распределения бюджетных средств в ответ на требования нового законодательства. Эти изменения будут касаться как текущих расходов, так и долгосрочного планирования финансовых ресурсов.

Согласно новым положениями, электросетевые компании обязаны переосмыслить свои подходы к инвестированию в информационную безопасность. Ожидается, что пропорции затрат, выделяемых на защиту информации, существенно увеличатся. Это связано с необходимостью в том числе защиты каналов связи при обеспечении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики. Особенно актуально это для тех объектов и организаций, в которых такой режим управления не реализован. При этом расходы на организацию и осуществление дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики и энергопринимающих установок из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике учитываются при установлении регулируемых цен (тарифов) [2].

Существенным моментом по обеспечению дистанционного управления является класс объектов электросетевого хозяйства. В обязательном порядке оно должно применяться отношении функционирующих в составе Единой энергетической системы России объектов электросетевого хозяйства классом напряжения 220 киловольт и выше. В организации, в интересах которой проводилось исследование такие объекты присутствуют. Дистанционное управление на них организовано.

Кроме этого, дистанционное управление должно применяться в отношении функционирующих в составе технологически изолированных территориальных электроэнергетических систем объектов электросетевого хозяйства классом напряжения 110 киловольт и выше. Данный вид энергосистем сосредоточен в основном на Дальнем Востоке России [3].

При этом следует отметить, что на момент проведения исследования постановление Правительства РФ, которое определит критерии наличия

технической возможности реализации дистанционного управления, а также обязательного минимального состава оборудования и устройств объектов электроэнергетики, в отношении которых осуществляется дистанционное управление [4] находилось в проекте. В такой ситуации не дожидаясь утверждения, сотрудникам служб информационной безопасности и информационных технологий целесообразно провести анализ текущего состояния и довести до сведения руководства организации план возможных организационно-технических изменений, а после утверждения внести корректировки по необходимости.

Согласно статье 3 Федерального закона № 35 «Об электроэнергетике» системный оператор – это системный оператор электроэнергетических систем России [1]. Иными словами, это организация федерального уровня. Таким образом данное положение не относится к электросетевым компаниям регионального уровня.

Важно подчеркнуть, что увеличение объема финансирования в сфере информационной безопасности будет не единственным последствием нового законодательства. Появление жестких требований также обязывает компании проводить ревизию своих существующих бюджетов. Необходимость соответствовать новым стандартам требует пересмотра процессов планирования и учета расходов.

Рекомендации для компаний

С учетом новых требований, установленных Федеральным законом № 185-ФЗ, электросетевым компаниям необходимо разработать стратегию оптимизации расходов на защиту информации. Практические рекомендации, изложенные в данном разделе, помогут предприятиям сократить затраты, не снижая при этом уровня безопасности своих информационных систем.

Первое, на что следует обратить внимание, – это развитие внутренней экспертизы. Инвестиции в обучение персонала позволят укрепить кадровый потенциал в области кибербезопасности. Повышение квалификации сотрудников не только сэкономит средства на аутсорсинговых услугах, но и создает более управляемую среду, адаптированную к специфике компании.

Другой совет заключается в проведении оценки текущего состояния по предлагаемому варианту алгоритма. Регулярный аудит позволит выявить неэффективные технологии и определить области, где возможно оптимальное распределение ресурсов.

– Определить, в каком сегменте находится электросетевая организация: в составе единой энергетической системы России или является технологически изолированной территориальной;
– определить наличие в своем составе объектов электросетевого хозяйства классом напряжения 220 киловольт и выше или 110 киловольт и выше соответственно для каждого сегмента;
– выяснить, осуществляется ли на этих объектах дистанционное управление технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики;
– составить перечень объектов, на которых оперативно-диспетчерское управление не осуществляется или осуществляется с нарушением требований к информационной безопасности; например, информация о состоянии АСУ ТП передается по незащищенному каналу связи;
– разработать план перехода на дистанционное управление технологическими режимами в соответствии с критериями и минимальным составом оборудования;
– оценить стоимость перехода;№
– принять решение о сроках и порядке перехода одновременно с внесением предложений по включению затрат на переход в тариф;
– в случае строящихся объектов классом напряжения 220 киловольт и выше или 110 соответственно для каждого сегмента внести в проекты необходимые корректировки.

В ходе проведенного исследования были проанализированы изменения, вводимые Федеральным законом № 185-ФЗ и их последствия для региональных электросетевых компаний. Основное внимание уделялось влиянию нового законодательства на аспект обеспечения информационной безопасности, а также на финансовые и кадровые стратегии компаний.

Первой важной закономерностью, выявленной в ходе анализа, является то, что вступление в силу данного закона повлечет увеличение расходов компаний на защиту информации. Это связано с необходимостью внедрения современных технологий и обновления существующих систем безопасности.

Дополнительные расходы требуются не только для реализации технологических изменений, но также и для повышения квалификации сотрудников. Инвестирование в обучение персонала является ключевым моментом для успешной адаптации к новым требованиям безопасности. Таким обра-

зом, компании должны понимать, что краткосрочные затраты на обучение и квалификацию могут привести к экономии средств в долгосрочной перспективе, так как квалифицированный персонал способен более эффективно обнаруживать и предотвращать инциденты кибербезопасности.

Второй вывод исследования заключается в том, что компании нуждаются в тщательном анализе своих существующих систем и процессов в области безопасности, чтобы успешно выполнить новые требования. Как один из возможных вариантов проведения такого рода аудита предложен алгоритм, который могут использовать в своей деятельности электросетевые компании регионального уровня. Данный алгоритм прошел апробацию при принятии решения о необходимых корректировках планов развития информационной безопасности и внесения предложений высшему руководству компании в действующей электросетевой организации.

Основные рекомендации заключаются в проактивном подходе к обеспечению информационной безопасности, включая инвестирование в обучение, модернизацию систем и комплексную стратегию управления рисками. Принятие таких мер позволит не только минимизировать потенциальные финансовые расходы, но и повысить уровень доверия со стороны клиентов и партнеров, что, в свою очередь, положительно отразится на репутации компании.

Список используемых источников

1. Федеральный закон от 26 марта 2003 года № 35-ФЗ «Об электроэнергетике» URL: http://www.consultant.ru/document/cons_doc_LAW_41502.

2. Федеральный закон от 13 июля 2024 г. N 185-ФЗ «О внесении изменений в Федеральный закон «Об электроэнергетике» и отдельные законодательные акты Российской Федерации» URL: https://rg.ru/documents/2024/07/19/document-ob-ehlektroehnergetike.html.

3. Постановление Правительства Российской Федерации от 13.08.2018 № 937 «Об утверждении Правил технологического функционирования электроэнергетических систем и о внесении изменений в некоторые акты Правительства Российской Федерации» URL: https://www.consultant.ru/document/cons_doc_LAW_304807/.

4. Постановление Правительства Российской Федерации от 04.12.2024 № 1712 «Об утверждении критериев наличия технической возможности реализации дистанционного управления технологическими режимами работы и эксплуатационным состоянием линий электропередачи, оборудования и устройств объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике и порядка определения наличия указанной технической возможности, а также обязательного минимального состава оборудования и устройств объектов электроэнергетики, в отношении которых осуществляется дистанционное управление из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике» URL: http://publication.pravo.gov.ru/document/0001202412040008.

ASSESSMENT OF THE IMPACT ON CHANGES IN INFORMATION SECURITY COSTS IN A REGIONAL-LEVEL ELECTRIC GRID COMPANY DUE TO THE ENTRY INTO FORCE ON 01.09.2024 OF THE PROVISIONS OF FEDERAL LAW NO. 185-FZ OF 13.07.2024 "ON AMENDING THE FEDERAL LAW "ON ELECTRIC POWER INDUSTRY"

Kiselev N., Smirnov S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
Moscow State Technical University named after N.E. Bauman

The article examines the impact of changes made to the Federal Law "On Electric Power Industry" on the activities of the electric grid company. Possible vectors of development of the economic activity of the organization are determined. A variant of the algorithm of actions for adapting the activity to the changed conditions of regulation by the legislation is proposed.

Key words: *Information security, electric grid company, remote control of technological modes, critical information infrastructure*

УДК 004.051
ГРНТИ 49.43.29

ФОРМИРОВАНИЕ ПОКАЗАТЕЛЕЙ КАЧЕСТВА СИСТЕМ ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ БЕСПРОВОДНЫХ УСТРОЙСТВ СЕМЕЙСТВА СТАНДАРТОВ IEEE 802.11

М. М. Ковцур, В. Е. Дрепа

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

Системы определения местоположения, в частности, основанные на уровнях принимаемого сигнала, являются одними из наиболее популярных систем определения местоположения беспроводных клиентов в Wi-Fi. При разработке или выборе таких систем возникает необходимость в их объективном сравнении, то есть возникает потребность в наличии критериев оценки систем позиционирования.

Wi-Fi, IEEE 802.11, позиционирование, RSSI, сравнение систем

За последние 5 лет было выпущено достаточно большое количество публикаций [1-4], связанных с позиционированием в Wi-Fi сетях. Тем не менее, говоря о разработке и оптимизации подобных систем, необходимо иметь ряд объективных параметров для сравнения систем между собой. Каждый вендор определяет характеристики своих систем самостоятельно, причем публикуя только те, которые не позволяют объективно оценить качество определения местоположения беспроводных клиентов данными системами. Такие системы могут использоваться в том числе в целях информационной безопасности [5, 6], например, для выявления нелегитимных клиентов [7].

Вероятность успешного позиционирования клиента в заданной области для N испытаний (%)

Является одним из самых важных показателей. Данный показатель дает общее представление о точности системы определения местоположения.

На рис. 1 центральная красная точка обозначена как истинное местоположение клиента. Допустим, с помощью некоторой системы было определено местоположение клиента *N* раз. Каждый раз получается какой-то результат, который отклоняется от истинного на определенное значение. Из-

мерив количество точек M, принадлежащих окружности с радиусом R (где R = 5 метров, 8, 10 и так далее), можно определить вероятность успешного позиционирования клиента в заданной области для N испытаний.

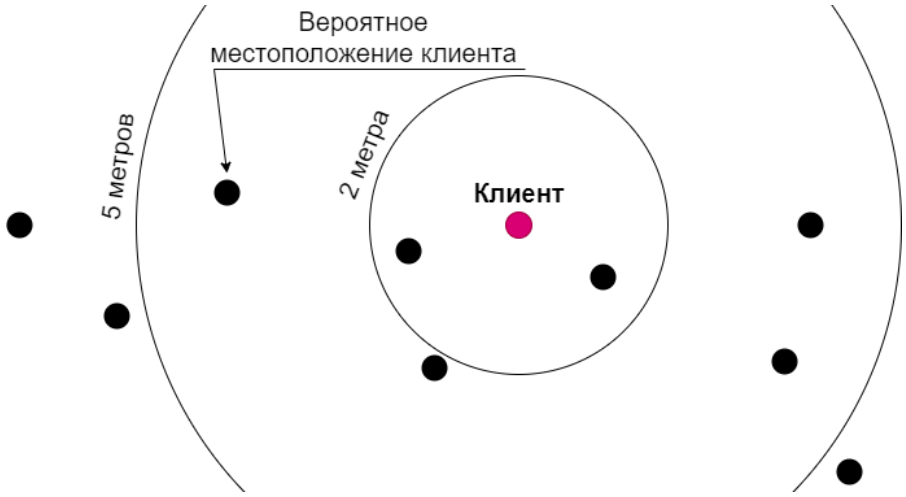


Рис. 1. Демонстрация результатов позиционирования беспроводного клиента

Общая точность позиционирования (м)

Данный показатель определяет номинальную точность позиционирования беспроводных клиентов в идеальных условиях [8]. Например, 10 метров.

Процент отказа в позиционировании для N испытаний

Показывает, как часто система не в состоянии определить местоположение клиента, который находится в зоне покрытия данной системы.

За отказ в позиционировании предлагается принимать отсутствие результата позиционирования либо заведомо неверный результат.

Максимальная скорость движения клиента (м/с)

Определяет максимальную скорость перемещения беспроводного клиента, с которой гарантируется сохранение заданной точности позиционирования. Данный показатель напрямую зависит от частоты сканирования радиоэфира. Демонстрация процесса позиционирования перемещающегося беспроводного клиента представлена на рис. 2.

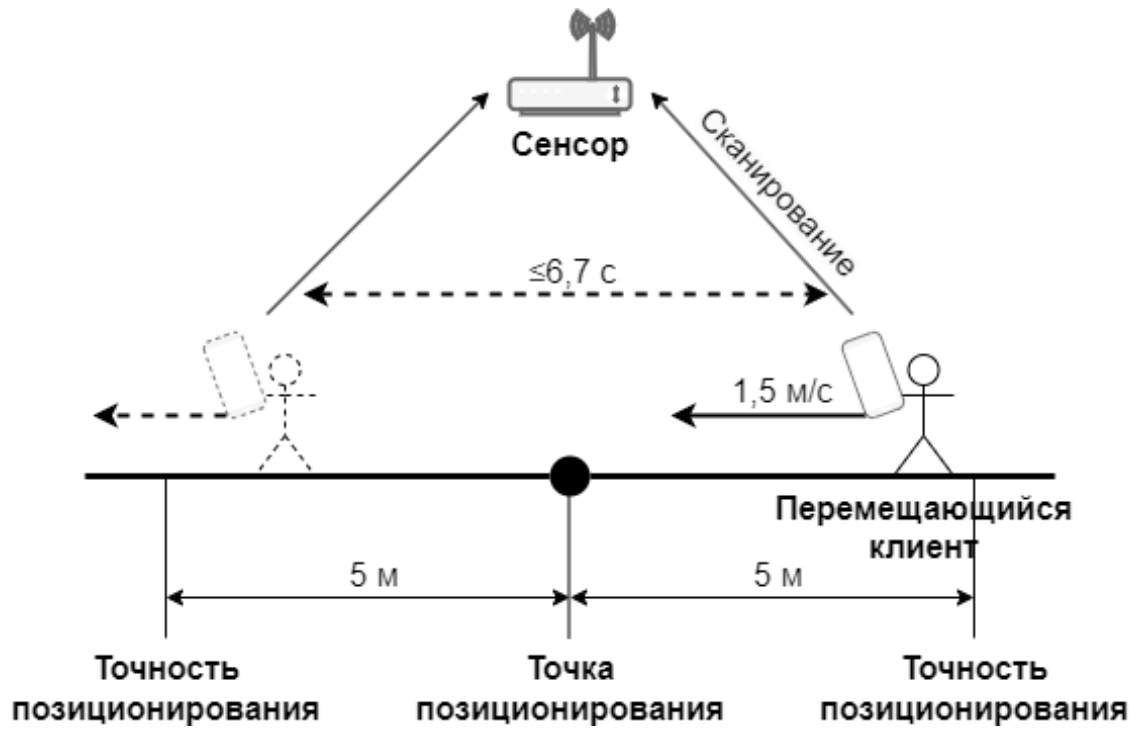


Рис. 2. Демонстрация процесса позиционирования перемещающегося беспроводного клиента

Интервал позиционирования (с)

Показывает, как часто можно запускать позиционирование клиента или как часто система может обновлять его местоположение.

Возможность определения устройств, неподключенных к сети

Определение устройств, неподключенных к сети, может составлять особые трудности, поэтому данная характеристика декларирует возможность или невозможность определение местоположения таких клиентов.

Критерии расстановки датчиков

Совокупность критериев расстановки датчиков как показатель качества [9]. Данные критерии должны включать:

– минимальное необходимое количество датчиков;
– минимальное и максимальное расстояния между датчиками (условия их размещения);
– максимальное расстояние от клиента до датчика;
– и другие.

Данные критерии влияют на экономические показатели системы.

Допустимые параметры неопределенности начальных данных

Данные показатели описывают условия работы системы в неидеальной среде. К ним можно отнести:

– граничные значения уровня принимаемого сигнала RSSI (или, отсечка);
– граничные значения дистанции передачи сигнала от передатчика до приемника для свободного пространства;
– границы значений EIRP (эквивалентная изотропно излучаемая мощность) искомого клиента;
– границы возможных затуханий RSSI между передатчиком и приемником.

Были сформирование показатели качества систем определения местоположения беспроводных устройств семейства стандартов IEEE 802.11.

Список используемых источников

1. Narasimman S. C., Alphones A. Dumbloc: Dumb indoor localization framework using wifi fingerprinting //IEEE Sensors Journal, 2024.

2. Xu Z. et al. Enhancing WiFi Fingerprinting Localization Through a Co-teaching Approach using Crowdsourced Sequential RSS and IMU Data //IEEE Internet of Things Journal, 2023.

3. Du X. et al. CRCLoc: A crowdsourcing-based radio map construction method for WiFi fingerprinting localization //IEEE Internet of Things Journal, 2021.

4. Hemin Ye, Jiansheng Peng. Robot Indoor Positioning and Navigation Based on Improved WiFi Location Fingerprint Positioning Algorithm. 2022. URL: https://www.hindawi.com/journals/wcmc/2022/8274455/ (дата обращения: 20.03.25);

5. Ковцур М. М. Исследование актуального инструментария Kali Linux для проведения тестов на оценку безопасности беспроводных сетей / М. М. Ковцур, А. А. Миняев, В. А. Цыганов // Экономика и качество систем связи. 2023. № 2(28). С. 93-99. EDN MWKAMS.

6. Разработка методики анализа трафика сети WLAN IEEE 802.1X / Е. А. Зебзеев, Е. Ю. Герлинг, А. Ю. Киструга, М. М. Ковцур // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 3. С. 80-85. DOI 10.46418/2079-8199_2024_3_13. EDN OSTBCQ.

7. Определение местоположения беспроводного клиента методом fingerprinting в сети семейства IEEE 802.11. Часть 1. Исследование / М. М. Ковцур, А. А. Миняев, В. Е. Дрепа [и др.] // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 3. С. 54-57. DOI 10.46418/2079-8199_2023_3_8. EDN BROROK.

8. Дрепа В. Е. Оценка точности позиционирования беспроводного IEEE 802.11 клиента в свободном пространстве методами трилатерации с использованием метрики RSSI / В. Е. Дрепа, А. Ю. Киструга, М. М. Ковцур // Региональная информатика и информационная безопасность: Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции, Санкт-Петербург, 26–28 октября 2022 года. Том Выпуск 11. Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2022. С. 578-582. EDN ABKCWL.

9.Безопасность беспроводных локальных сетей: [Электронный ресурс]: учебно-методическое пособие по выполнению курсовой работы / М. М. Ковцур, Д. В. Юркин, Е. Ю. Герлинг; рец. А. А. Гоголь; Министерство цифрового развития, связи и массовых коммуникаций РФ, С.-Петерб. гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича. СПб.: СПбГУТ, 2021. 40 с.: ил. (дата обращения: 01.06.2024).

QUALITY INDICATORS FORMATION FOR POSITIONING SYSTEMS FOR WIRELESS DEVICES OF THE IEEE 802.11 FAMILY OF STANDARDS

Kovtsur M., Drepa V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Positioning systems, in particular those based on received signal strength indicator, are among the most popular systems for determining the wireless clients location in Wi-Fi. Per developing or selecting such systems, there is a need for their objective comparison – need for the criteria for evaluating positioning systems.

Key words: *Wi-Fi, IEEE 802.11, positioning, RSSI, system comparison*

УДК 004.932.2
ГРНТИ 20.19.29

О НЕКОТОРЫХ АСПЕКТАХ ПРИМЕНЕНИЯ МЕТОДОВ МАРКИРОВАНИЯ ВИДЕОДАННЫХ

С. А. Копылов, П. Н. Горбачев, П. Р. Романюк

Академия Федеральной службы охраны Российской Федерации

Современные методы маркирования находят широкое применение в задачах аутентификации видеопотоков, защиты авторских прав, отслеживания происхождения контента, а также в системах автоматического анализа данных. Однако, несмотря на существенный прогресс в данной области, остаются нерешенные проблемы, связанные с устойчивостью маркировки к атакам, влиянием на качество видео, а также сложностью адаптации методов к различным форматам и условиям использования. В данной статье рассматривается применение технологии маркирования видеоданных, включая приведенную классификацию и сравнительный анализ существующих подходов, а также перспективы развития технологий в контексте современных вызовов. Особое внимание уделяется вопросам надежности, вычислительной эффективности и применимости методов в реальных сценариях.

маркирование, видеоданные, защиты авторских прав

Во время стремительного развития цифровых технологий защита информации, которая распространяется с невероятной скоростью, является одним из наиболее актуальных и важных вопросов. Каждый день огромное количество людей и организаций сталкивается с проблемой утечки и искажения данных. Эффективным инструментом решения задачи защиты авторских прав, подтверждения подлинности и отслеживания использования информации стало маркирование данных.

Маркирование данных – это внесение дополнительной информации (маркера, цифрового водяного знака) в исходные данные. Цифровой водяной знак представляет собой метку (например, текст или логотип), внедряемую в цифровой файл для идентификации правообладателя и защиты от несанкционированного использования или распространения. Инновационные решения для защиты конфиденциальных медиа файлов с помощью невидимой маркировки, позволяют отслеживать все действия с ними и проводить экспертизы в случае утечки. Это особенно важно в условиях роста умышленных утечек данных, когда сотрудники часто становятся причиной несанкционированного распространения информации [1].

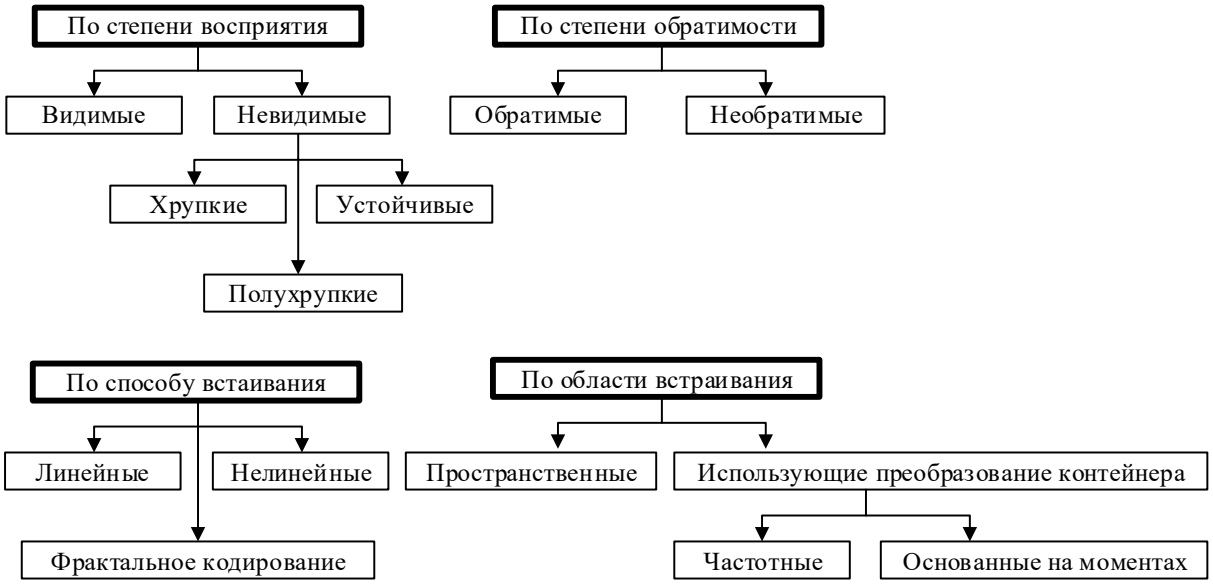


Рис. 1. Классификация цифровых водяных знаков

По способу восприятия цифровые водяные знаки бывают как видимым человеческому глазу, так и невидимым. Современные видимые водяные знаки могут быть визуальными узорами (например, логотип компании или знак авторских прав), наложенными на цифровые изображения [2]. Невидимые цифровые водяные знаки используются сейчас намного чаще и направлены на то, чтобы нарушитель не смог визуально обнаружить и уничтожить их. Такие маркеры при необходимости можно извлечь при необходимости доказательства авторских прав.

Невидимые цифровые водяные знаки бывают хрупкими, полухрупкими и робастными (устойчивыми). Хрупкие цифровые знаки чувствительны к изменениям и разрушаются или искажаются после любого незначительного воздействия на объект. Они применяются для обнаружения несанкционированных изменений, обеспечения целостности данных, а также используются в критических системах. Исчезновение или модификация водяного знака будет свидетельствовать о неправомерном вмешательстве. Полухрупкие цифровые водяные знаки – это особые водяные знаки, которые балансируют между устойчивостью и чувствительностью к изменениям и обладают избирательной стойкостью, то есть выдерживают только определенные изменения предмета маркирования [3]. Сочетая в себе свойства хрупких и робастых цифровых водяных знаков, они, например, могут быть использованы для обнаружения и локализации изменений в изображениях, если эти изменения выходят за пределы допустимых. Робастные же водяные знаки отличаются особой живучестью и стойкостью, способностью противостоять даже преднамеренным попыткам уничтожения или искажения. Они выдерживают любые внешние воздействия, сохраняя при этом возмож-

ность обнаружения после различных преобразований и атак. Устойчивый цифровой водяной знак даже после значительных модификаций контейнера (цифровой носитель, будь то фото-, аудио- или видеофайл, в который встраивается водяной знак, называется контейнером) может быть выведен и использован для дальнейшей идентификации владельца и подтверждения авторства.

В зависимости от использования алгоритма создания и внедрения маркера по степени обратимости цифровые водяные знаки делятся на необратимые и обратимые. Первые при их извлечении вносят изменения в исходный контейнер. Это означает, что после удаления цифрового водяного знака первоначальное состояние документа не может быть полностью восстановлено. В основном они используются в случаях, когда оригинал медиа файла не требуется – важно только сохранить информацию о применении цифрового водяного знака [4]. Примерами служат любые электронные структуры данных (фильмы, музыка, изображения, Интернет-ресурсы), нуждающиеся в защите авторских прав их владельцев и контроля целостности цифрового контента. Применение обратимых водяных знаков является более сложной в реализации по сравнению с необратимыми алгоритмами, но в свою очередь дает возможность полностью достать цифровой водяной знак и восстановить контейнер. Такие методы часто реализуются в медицинской визуализации, юридических документах и военных программах, где любые, даже незначительные, искажения категорически запрещены. Можно выделить два алгоритма их внедрения: модификация гистограмм изображений (изменение распределения яркости и цвета для внедрения цифрового водяного знака) и преднамеренная регулировка разности между соседними парами пикселей.

Цифровые водяные знаки могут быть встроены в цифровые объекты различными методами, которые классифицируются по способу встраивания информации. Различают три метода: линейные, нелинейные и фрактальное кодирование [5].

Линейные подразделяются на алгоритмы встраивания (аддитивные), когда в контейнер добавляется цифровое сообщение, и алгоритмы слияния (методы модификации наименее значащих бит областей изображения), когда, например, в изображение «вплавляется» другое изображение, изменяя при этом наименее значащие биты пикселей. Нелинейные методы встраивания информации включают в себя различные алгоритмы, которые используют более сложные математические операции по сравнению с линейными методами. В основном используется скалярное либо векторное квантование. Процедура квантования обеспечивает изменения значений пикселей изоб-

ражения на значения, соответствующие незначительному изменению градиента или оттенка основного цвета, что, в свою очередь, позволяет увеличить количество (объем) встраиваемой информации. Помимо квантования в процессе встраивания цифровых водяных знаком могут применяться фракталы, обеспечивающие создание самоподобных структур, позволяющих за счет свойства масштабируемости повышать емкость встраиваемой информации (объем цифрового водяного знака). Данная особенность позволяет повышать робастность водяного знаки стеганографическую невидимость встроенных данных.

Помимо способа встраивания цифровые водяные знаки могут быть классифицированы по месту (области) внедрения на пространственные и алгоритмы, осуществляющие модификацию файла-контейнера. Пространственные алгоритмы встраивания осуществляют наложение цифрового водяного знака поверх исходного медиа файла посредством внесения изменений в область пространства при этом частотная область исходного файла-контейнера не подвергается изменениям. В отличие от пространственных алгоритмов внедрения алгоритмы, осуществляющие модификацию файла-контейнера, реализуют модификацию исходного контейнера, позволяя тем самым добиться повышения робастности встроенных данных к осуществлению преобразований и внесению искажений. К основным алгоритмам, осуществляющим модификацию файла-контейнера, относятся алгоритмы встраивания в частотную область, основанные на применении дискретного преобразования Фурье, дискретного косинусного и дискретного вейвлет преобразований. Стоит отметить, что практическая реализация указанных алгоритмов встраивания является более сложной по сравнению с пространственными алгоритмами внедрения ввиду необходимости реализации дополнительных этапов обработки исходных данных [6].

Методы внедрения цифровых водяных знаков, основанные на моментах изображений, реализуют технику встраивания посредством реализации аффинных преобразований, позволяющих обеспечивать робастность встроенных данных к применению геометрических преобразований: поворот, сжатие, масштабирование изображений, а также изменение пропорций изображений. При этом указанная группа методов имеет ограниченное применение, что не позволяет применять методы данной группы для внедрения маркера в видеоданные и видео последовательности.

На основе проведенного обзора существующих подходов к маркированию видеоданных можно сделать вывод о необходимости разработки новых методов и совершенствования существующих ввиду наличия недостатков и ограничений не позволяющих использовать только один из рассмотренных

подходов или его практическую реализацию. Разработка подхода к маркированию видеоданных, позволяющего осуществлять внедрение невидимого маркера, характеризующийся достаточно высокой емкостью встраивания и робастностью к внесению искажений и применению преобразований, а также реализации атак на системы цифровых водяных знаков является направлением дальнейших исследований.

Список используемых источников

1. Osborne C., vsn Schyndel R., Tirkel A. A Digital Watermark // IEEE Intern. Conf. on Image Processing, 1994. P. 86-90

2. Орешкина Е. И. Классификация методов нанесения цифровых водяных знаков: // Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева. URL: https://cyberleninka.ru/article/n/klassifikatsiya-metodov-naneseniya-tsifrovyh-vodyanyh-znakov/viewer. (дата обращения 03.03.2025).

3. Сивограков А. А. Цифровые водяные знаки как метод защиты изображения: // Промышленность. Информационные технологии. URL: https://elib.psu.by/bitstream/123456789/33915/1/255-256.pdf. (дата обращения 10.03.2025).

4. Григорян А. К. Методы внедрения цифровых водяных знаков в потоковое видео. Обзор: // Санкт-Петербургский государственный университет аэрокосмического приборостроения. URL: https://cyberleninka.ru/article/n/metody-vnedreniya-tsifrovyh-vodyanyh-znakov-v-potokovoe-video-obzor/viewer. (дата обращения 10.03.2025).

5. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.

6. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. Киев: «МК-Пресс», 2006. 288 с., ил.

SOME ASPECTS OF VIDEO DATA LABELING METHODS APPLICATION

Kopylov S., Gorbachev P. Romanyuk P.
Russian Federation Security Guard Service Federal Academy

Modern marking methods are widely used in video stream authentication, copyright protection, content origin tracking, and in automatic data analysis systems. However, despite significant progress in this area, there are still unresolved issues related to labeling resistance to attacks, impact on video quality, and the complexity of adapting methods to different formats and conditions of use. This article discusses the application of video data labeling technology, including the classification and comparative analysis of existing approaches, as well as prospects for technology development in the context of modern challenges. Particular attention is paid to issues of reliability, computational efficiency, and applicability of methods in real-world scenario.

Key words: *biometric features, behavioral authentication, access control*

УДК 004.492.3
ГРНТИ 50.41.27

ОБЗОР МЕТОДОВ ПОВЕДЕНЧЕСКОЙ АУТЕНТИФИКАЦИИ

С. А. Копылов, К. Б. Кощенко

Академия Федеральной службы охраны Российской Федерации

Системы управления доступом остаются одним из наиболее широко используемых механизмов обеспечения информационной безопасности. При этом традиционные подходы к аутентификации пользователей, основанные на паролях и одноразовых кодах, подвержены атакам, связанным с компрометацией учетных данных. В связи широкое распространение получили методы поведенческая аутентификации, основаной на анализе индивидуальных характеристик поведения пользователя, таких как почерк, манера набора текста, передвижение курсора мыши, особенности походки и другие параметры. В работе приведен обзор существующих методов поведенческой аутентификации, описаны ключевые характеристики, требования и ограничения, а также возможность применения методов машинного обучения и направления дальнейших исследований.

биометрические признаки, поведенческая аутентификация

Использование биометрических характеристик человека как средства идентификации стало широко распространенным в последнее время. Однако после определенных событий на замену ей пришла более надежная и безопасная альтернатива-биометрия на основе поведенческих особенностей человека.

Статическая биометрия заменила пароли отпечатками пальцев, чертами лица, радужной оболочкой глаза, формой уха или рисунком. Но ожидания не подтвердились, такие системы идентификации не только не безопасны, но и не всегда просты в использовании. В качестве примера, сканирование радужной оболочки глаза оказалось неэффективным при солнечном свете, разблокировать телефон во время тренировки или при выполнения различного рода грязных работ не совсем легко [1].

В том числе пользователи не желают распространять свои данные третьим лицам. Статическая биометрия требует от человека предоставление личной информации, что не гарантирует безопасное хранение и содержание ее в тайне от третьих лиц.

На основе вышеупомянутых проблем рассмотрим многофакторный способ идентификации пользователя. Объединение статических и динами-

ческих способов аутентификации создаст новый безопасный и удобный метод. Достижения в области машинного обучения позволили поглубже разобраться с методом идентификации, анализирующим взаимодействие пользователя с прибором, который используется в качестве считывающего устройства [2].

Применение поведения человека в качестве объекта исследования требует хранение большого объема данных. Сохраненная информация используется для усреднения различных образов поведения пользователя. Так как человек может быть уставшим, торопиться, пьяным, она, в свою очередь, повышает точность аутентификации.

Все ненужные данные после создания образца нормального поведения можно удалить, но большая часть все равно остается для случаев затруднения в определении пользователя. Хотя в процессе разработки будет собираться и храниться много информации, проверка будет выполняться только с одним набором данных.

Компании могут создать надежную многофакторную систему контроля доступа при объединении уникальных идентифицирующих маркеров. Исследования, проведенные компанией "Positive Technologies" (рис. 1), показывают, что в 2023 году злоумышленники активно организуют атаки на государственные, промышленные и медицинские учреждения.

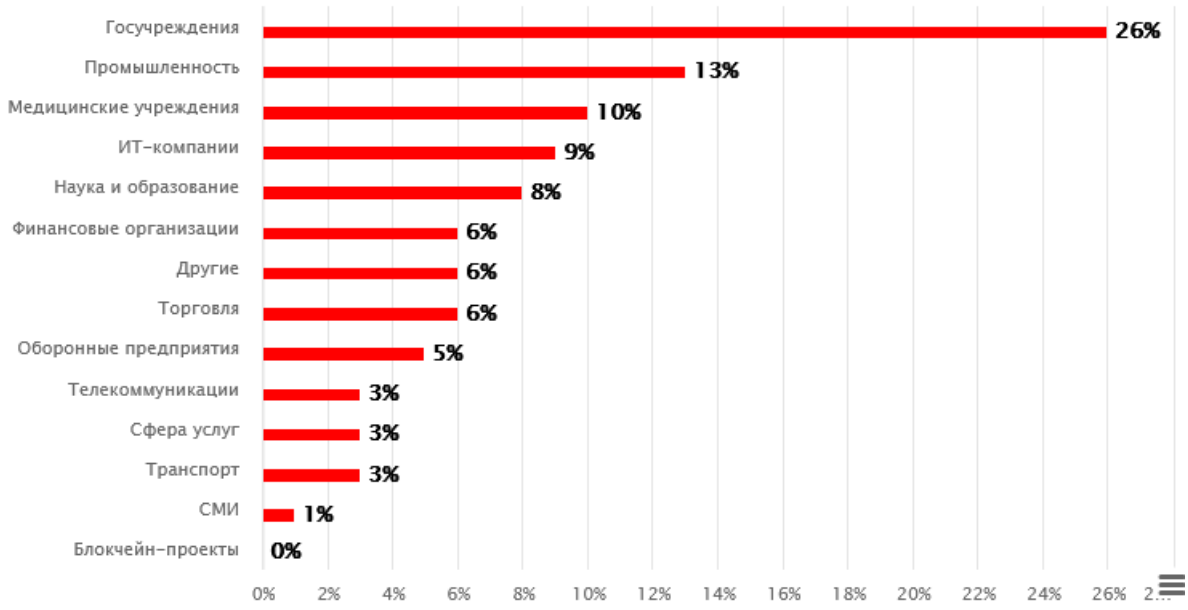


Рис. 1. Используемые злоумышленниками каналы социальной инженерии

В данной работе рассмотрим метод многофакторной аутентификации, который включает анализ поведенческих характеристик пользователя (скорость набора текста, движения мыши, взаимодействие с различными дополнительными устройствами) и биометрических параметров (распознавание лица, голоса) с применением методов машинного обучения. Это позволит повысить точность идентификации, снизить количество возможных атак и их успешность, а также подстроиться под изменяющееся в течение времени поведение человека.

На первом этапе разработанного подхода осуществляется проектирование и реализация системы для сбора, обработки и хранения информации о поведенческих параметрах. Основное внимание уделяется динамике набора текста (интервалы между нажатиями клавиш, скорость печати, типичные ошибки), моделям использования мыши (траектории перемещения, скорость нажатий), а также особенностям работы с другими графическими устройствами [3]. Для сбора данных разрабатывается клиентское приложение, устанавливаемое на ЭВМ пользователей и работающее в фоновом режиме. Для копирования информации с анализируемых устройств будет использована библиотека pynput на языке Python, которая обеспечивает совместимость практически со всеми ОС. Собранные данные передаются на сервер обработки через защищенное соединение с применением протокола TLS 1.3.

На втором этапе происходит предварительная обработка и анализ собранных данных. Обработка включает в себя выделение значимых признаков, фильтрацию и нормализацию информации. Для анализа печати применяются методы временного анализа, включающие вычисление средних значений, дисперсий, автокорреляционных функций, спектральный анализ [4]. Шаблоны использования мыши для выявления характерных траекторий и последовательностей действий обрабатываются с применением алгоритмов кластеризации. Все извлеченные признаки сохраняются в базе данных PostgreSQL. Вся идентификационная информация удаляется и преобразуется так, чтобы по полученным данным нельзя было определить, к какому лицу они относятся.

Для классификации поведенческих качеств на третьем этапе совершается обучение модели машинного обучения. Основной акцент уделяется алгоритмам, способным эффективно работать с временными последовательностями: рекуррентные нейронные сети (LSTM, GRU), временные сверточные сети (TCN) и методы случайного леса (XGBoost, LightGBM) [5]. Чтобы

обучить модели создается размеченный набор данных, содержащий не только поведенческие образы легитимных пользователей, но и попытки их скомпрометировать. Процесс обучения включает оценку устойчивости моделей к изменениям в поведении пользователей со временем. Оптимизация параметров осуществляется с помощью библиотеки Optuna, позволяющей уравновесить точность классификации и вычислительную эффективность.

На четвертом этапе осуществляется интеграция поведенческой аутентификации в общую систему безопасности. Разрабатывается механизм непрерывной аутентификации, который в фоновом режиме анализирует активность пользователя и вычисляет степень доверия. При снижении показателя ниже заданного порога система может запросить дополнительную проверку. Для принятия решений используется адаптивный алгоритм, учитывающий условия работы и автоматически регулирующий точность проверки. Система основана на микросервисной архитектуре с использованием Docker-контейнеров и оркестратора Kubernetes и обеспечивает высокую доступность и способность системы адаптироваться к расширению предъявляемых требований и возрастанию объемов решаемых задач [6].

На пятом этапе проводится тестирование системы. Оно заключается в: оценке точности на различных наборах данных, проверке устойчивости к спуфинг-атакам, тестировании в условиях большой нагрузки для определения максимального количества одновременных покдлючений. По результатам тестирования выполняется калибровка пороговых значений и доработка алгоритмов. Разрабатывается система мониторинга, которая отслеживает качество работы моделей в реальных условиях и автоматически их переобучивает при снижении точности ниже заданного уровня. Конечным результатом является надежная система аутентификации, которая обеспечивает постоянный контроль доступа без участия пользователя.

Список используемых источников

1. OWASP Foundation, the Open Source Foundation for Application Security on the main website for The OWASP Foundation // OWASP [Электронный ресурс]. 2025. URL: https://owasp.org (дата обращения 24.03.2025)

2. ГОСТ Р 52633.5-2022. Защита информации. Техника защиты информации. Требования к средствам биометрической аутентификации. М.: Стандартинформ, 2018. 20 с.

3. Sundararajan K., Woodard D. Deep Learning for Biometrics: A Survey // ACM Computing Surveys. 2018. Vol. 51. № 3. P. 1–34. DOI: 10.1145/3190618

4. Шорманов Т. С., Джомартова Ш. А., Зиятбекова Г. З., Амирханов Б. С., Алиаскар М. С. Алгоритмы машинного обучения для биометрической идентификации лиц //

Вестник казахстанско-британского технического университета. 2019. № 1(48). С. 119–128.

5. Ерошин Р. В. Непрерывная аутентификация пользователя по клавиатурному подчерку // Экономика и социум. 2017. № 6(37). С. 697–699.

6. Галуев Г. А. Нейросетевые методы и технологии в задачах комплексного обеспечения информационной безопасности // Известия ЮФУ. Технические науки. 2003. № 4. С. 1–4.

OVERVIEW OF BEHAVIORAL AUTHENTICATION METHODS.

Kopylov S., Koschenko K.
Russian Federation Security Guard Service Federal Academy

Access control systems remain one of the most widely used mechanisms for ensuring information security. At the same time, traditional approaches to user authentication based on passwords and one-time codes are susceptible to attacks associated with the compromise of credentials. In this regard, behavioral authentication methods based on the analysis of individual characteristics of user behavior, such as handwriting, typing style, mouse cursor movement, gait characteristics and other parameters, have become widespread. The paper provides an overview of existing behavioral authentication methods, describes key characteristics, requirements and limitations, as well as the possibility of using machine learning methods and directions for further research.

Key words: *biometric features, behavioral authentication, access control*

УДК 004.852
ГРНТИ 28.23.25

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

С. А. Копылов, И. А. Чертовских

Академия Федеральной службы охраны Российской Федерации

Современные информационные системы подвержены широкому спектру кибератак, направленных на нарушение конфиденциальности, целостности и доступности защищаемой информации. Традиционные системы обнаружения вторжений, основанные на сигнатурных и эвристических методах, сталкиваются с рядом ограничений, включая высокую вероятность ложных срабатываний и неспособность эффективно выявлять ранее неизвестные атаки. В связи с этим актуальным направлением исследований становится применение методов машинного обучения. Работа посвящена анализу применения методов машинного обучения в системах обнаружения сетевых вторжений. Представлена классификация алгоритмов машинного обучения, их достоинства и недостатки, и направления реализации рассмотренных алгоритмав в средствах защиты информации от кибератак.

системы обнаружения вторжений, классификация, машинное обучение.

Система обнаружения вторжений – это совокупность двух понятий, таких как «Вторжение» и «Система обнаружений». Вторжение [1] относится к несанкционированному доступу к информации в компьютерных или сетевых системах с целью компрометации их целостности, конфиденциальности или доступности. Система обнаружения [1] – это механизм безопасности для выявления такой незаконной деятельности. Таким образом, данная система является инструментом безопасности, которая постоянно следит за хостом и сетевым трафиком для обнаружения любого подозрительного поведения, нарушающего политику безопасности и компрометирующего ее конфиденциальность, целостность и доступность. Система обнаружения вторжений генерирует оповещения о выявленном вредоносном поведении.

Современные системы обнаружения вторжений работают, в основном, на основе сравнения поступающего трафика и имеющихся сигнатур, что дает возможность превосходно отслеживать и блокировать поступающие атаки, имеющиеся в базе. Но с учетом непрерывного развития современных технологий, и способов проведения атак, на помощь приходят методы машинного обучения.

Итак, рассмотрим общую методологию AI-основанного NIDS [1] (Сетевая система обнаружения вторжений) вместе с деталями наиболее часто используемых алгоритмов ML (Методы машинного обучения), применяемых для проектирования эффективного NIDS. ML [2] в широком смысле классифицируются как контролируемые и неконтролируемые алгоритмы. В контролируемых алгоритмах полезная информация извлекается из размеченных данных, в то время как неконтролируемые алгоритмы полагаются на неразмеченные данные для извлечения полезных признаков и информации.

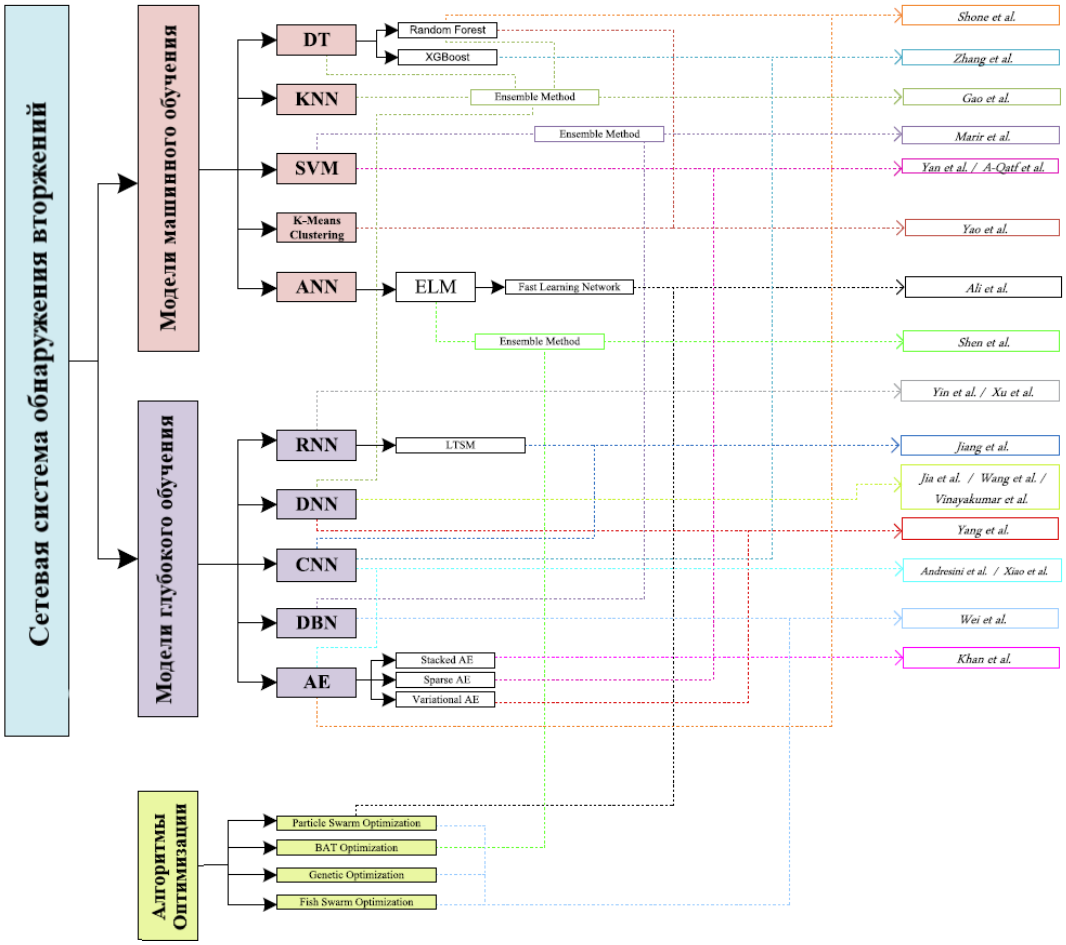


Рис. 1. Таксономия систем обнаружения вторжений на основе машинного и глубокого обучения в сетях

Итак, имеем два основных алгоритма для построения сетевой системы обнаружения вторжений: методы глубинного обучения и методы машинного обучения. Первые требуют больших объемов данных для обучения и время обучения. Что в условиях построения небольших сетей играет важную роль. Рассмотрим же методы машинного обучения, они требуют мень-

шего времени и меньшего объема данных, тем самым делая их перспективными для использования в данной работе.

Кроме того, рассмотрим методы машинного обучения, показанные выше (рис. 1). Дерево решений (DT) [3] – контролируемый алгоритм машинного обучения, используемый для классификации и регрессии, представляющий данные в виде древовидной структуры с узлами, ветвями и листьями, где узлы – это признаки, ветви – решения, а листья – результаты. Алгоритм автоматически выбирает лучшие признаки и обрезает несущественные ветви, чтобы избежать переобучения. Другие алгоритмы включают K-ближайших соседей (KNN), который предсказывает класс на основе расстояний до соседей, метод опорных векторов (SVM), который использует гиперплоскости для разделения классов, и кластеризацию K-средних, делящую данные на кластеры по центроидам. Искусственные нейронные сети (ANN) имитируют работу мозга и способны к нелинейному моделированию, но требуют значительных вычислительных ресурсов. Ансамблевые [3] методы комбинируют несколько классификаторов для повышения точности, используя голосование для формирования более сильного классификатора.

В качестве примера будем рассматривать небольшую сеть, в которой будут находиться 2 защищаемых устройства и сервер обработки приходящих на них пакетов, а также еще одно устройство, с которого будут производить атаки. Соответственно, построение сетевой системы обнаружения атак будет строится из нескольких этапов.

На первом этапе необходимо сконфигурировать сеть, указанную выше. Для ее построения воспользуемся средствами виртуализации, их существует немало: виртуальная машина, контейнер и песочница (Sandbox). Виртуальная машина [4] – это платформа, которая объединяет виртуальные ресурсы для обработки, хранения и передачи данных, включая аппаратное обеспечение и пользовательские данные. Контейнер [5] – это легкая форма виртуализации на уровне операционной системы, использующая общее ядро хоста и обеспечивающая запуск приложений с их зависимостями в различных средах. В отличие от виртуальных машин, контейнеры не сохраняются, а разворачиваются из образов. Песочница – это изолированная среда для запуска программ с целью выявления и предотвращения ошибок или уязвимостей, которая эмулирует рабочую среду и защищает критически важные системы, позволяя анализировать подозрительные программы без риска для основной системы.

Вторым этапом будет развертывание специального программного обеспечения. На защищаемых компьютерах, соответственно, клиентского, а на управляющей машине серверного программного обеспечения. Введение данных для поиска сервера, установление работоспособности и связи с ним. Далее будет необходимо убедиться в правильности получения данных управляющим компьютером. После этого можно переходить к следующему этапу.

Третий этап характеризуется полученных наборов данных, полученных от защищаемых компьютеров, осуществляется обучение используемого алгоритма регрессии методов машинного обучения для формирования функции преобразования и получения разделяющего правила (порогового значения), разделяющего вредоносные и «чистые» пакеты. Полученное пороговое значение представляет собой правило принятия, которое используется в процессе анализа новых пакетов и выявления вредоносных.

Четвертый этап представляет собой мер по предотвращению воздействия атак на охраняемые компьютеры. Будь то отключение их от сети или написание определенных правил на встроенный в операционную систему межсетевой экран. Например, iptables или nftables. Данные меры лишают злоумышленника объекта воздействия. И приведут к бессмысленности атаки, и дальнейшей невозможности ее применения, из-за используемых алгоритмов адаптации.

Предложенные меры и способы организации помогут предотвратить дальнейшие атаки, уже обработанные на сервере, а построение типа клиент-сервер поможет сконцентрировать все в одном месте. В дальнейшем практическая реализация поможет выйти за пределы одной независимой сети, тем самым получив новые предметы для воздействия на сеть, что, в свою очередь, приведет к увеличению обрабатываемого трафика, ну и получаемых данных. Это приведет к необходимости более тонкой и углубленной настройки правил, разделяющих пакеты.

Список используемых источников

1. Ли Дж., Цюй Ю., Чао Ф., Шум Х.П., Хо Э.С., Ян Л. Алгоритмы машинного обучения для обнаружения сетевых вторжений. Искусственный интеллект в кибербезопасности. Нью-Йорк, NY:Springer;2019:151-179.

2. A systematic study of Machine Learning and Deep Learning approaches, Transactions on Emerging Telecommunications Technologies. Vol., e4150. PP. (In-press). https://dx.doi.org/10.1002/ett.4150.

3. Донг Б., Ван Х. Сравнение методов глубокого обучения с традиционными методами, используемыми для обнаружения сетевых вторжений. Доклад представлен на: Ма-

териалы 8-й Международной конференции IEEE по программному обеспечению и сетям связи (ICCSN). Пекин, Китай: IEEE; 2016:581-585.

4. ГОСТ Р 59163-2020 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Руководство по обеспечению безопасности при внедрении серверов виртуализации.

5. Официальный сайт oracle.com. URL: https://www.oracle.com/cis/cloud/cloud-native/container-registry/what-is-docker/ (дата обращения 10.02.2025).

APPLICATION OF MACHINE LEARNING METHODS IN NETWORK INTRUSION DETECTION SYSTEMS

Kopylov S., Chertovskikh I.
Russian Federation Security Guard Service Federal Academy

Modern development systems develop a wide range of cyber-attacks aimed at violating confidentiality, security and ensuring protected information. Traditional intrusion detection systems based on signature and heuristic methods, problems with neighboring limitations, including the main functions of false projects and the inability to effectively detect previously unknown actions. In this regard, the use of machine learning methods becomes an urgent area of research. The work is devoted to the analysis of the application of machine learning methods in the network intrusion detection network. The classification of machine learning algorithms, their advantages and disadvantages, as well as directions for the implementation of progressive algorithms in information security tools from cyber-attacks are presented.

Key words: *intrusion detection systems, classification, machine learning*

УДК 004.056
ГРНТИ 81.93.29

ИСПОЛЬЗОВАНИЕ ОТНОЛОГИЙ И БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ ДЛЯ ИНТЕРПРЕТАЦИЙ СОБЫТИЙ SURICATA

И. В. Котенко[2], Г. Т. Абраменко[1],

[1]Национальный исследовательский университет ИТМО
[2]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В статье описывается прототип системы, предназначенной для автоматизированного обнаружения и анализа кибератак посредством интеграции логов IDS Suricata, графовых нейронных сетей, онтологической модели на базе MITRE ATT&CK и больших языковых моделей с использованием генерации с дополненной выборкой. Экспериментальная система включает сбор и предобработку сетевых событий, онтологическую разметку, построение графа знаний для выявления скрытых взаимосвязей и генерацию пояснительных рекомендаций для оператора.

LLM, GNN, RAG, онтологии, обнаружение аномалий, Suricata.

Современные кибератаки характеризуются возрастанием сложности и многоступенчатостью, что требует применения передовых методов для их обнаружения и анализа. Традиционные подходы зачастую оказываются недостаточными для противодействия многофазным атакам, использующим ранее неизвестные уязвимости и тщательно скрывающим свои следы [1]. В таких условиях необходимо интегрировать инновационные технологии, способные эффективно обрабатывать большие объемы данных и выявлять скрытые зависимости между событиями.

Одним из перспективных направлений является объединение онтологий [2] и графовых нейронных сетей (GNN) [3]. Онтологии позволяют формализовать и структурировать знания о киберугрозах, создавая единый классификатор и описание взаимосвязей между объектами. Такой подход обеспечивает более эффективный обмен информацией и улучшает процессы обнаружения и анализа атак. В отличие от простых знаний, представленных в виде графов, онтологии предоставляют семантическую основу для представления данных, основанную на логике с использованием специализированного словаря и набора утверждений о моделируемых объектах.

Графовые нейронные сети, способные анализировать данные, представленные в виде графов [3], эффективно выявляют скрытые зависимости

и аномалии в сетевых структурах [4], что особенно важно для обнаружения сложных атак. Кроме того, большие языковые модели (LLM) все чаще применяются для улучшения взаимодействия между человеком и системой, а также для автоматизации интерпретации сложных аналитических данных. Интеграция LLM с технологиями, такими как генерация с дополненной выборкой (Retrieval-Augmented Generation, RAG) [5], позволяет обращаться к дополнительным источникам информации и предоставлять более точные и релевантные ответы [6].

Архитектура и ключевые компоненты системы

В данной системе для обнаружения и анализа кибератак предлагается подход, вначале реализующий регистрацию сетевых событий, затем - предобработку данных, сопоставление сетевых событий с конкретными векторами атак на основе онтологии, построение графа знаний, анализ на основе графовой нейронной сети, формирование понятных оператору пояснений и рекомендаций на основе LLM, а в итоге – предоставление оператору понятных рекомендаций через взаимодействие с ассистентом. На рис. 1 показан предлагаемый подход к обнаружению и анализу кибератак на основе GNN и LLM.

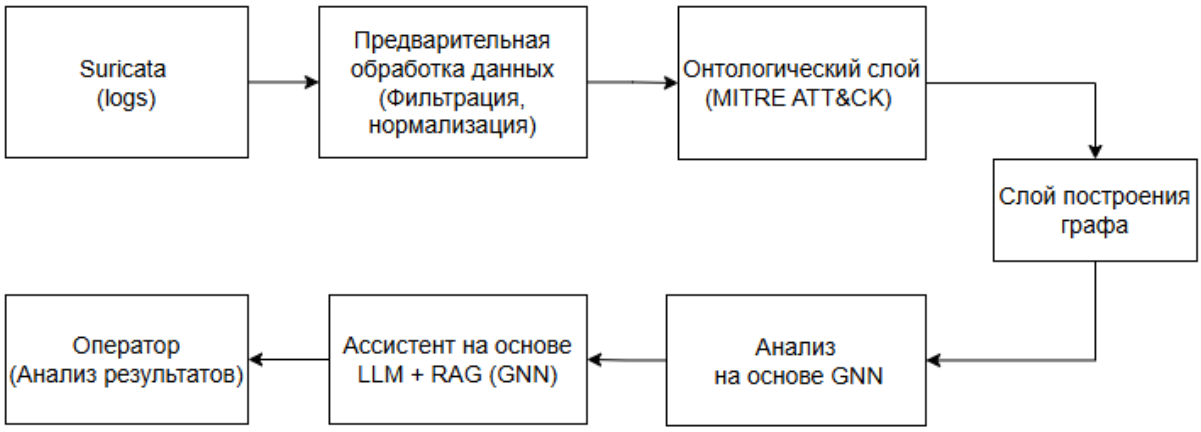


Рис. 1. Схема предлагаемого подхода

Сбор и регистрация событий. На начальном этапе система регистрирует сетевые события с помощью IDS Suricata, которая в режиме реального времени фиксирует IP-адреса, протоколы, порты, временные метки и сигнатуры атак. Собранные логи служат исходным материалом для дальнейшей обработки.

Предобработка данных. Полученные данные проходят фильтрацию и очистку, в результате чего удаляются дубли и нерелевантные поля, а также выполняется нормализация: IP-адреса преобразуются в числовой формат, временные метки приводятся к единому виду, и рассчитываются дополнительные атрибуты, такие как частотные характеристики. Итоговый структурированный набор данных сохраняется во временном хранилище для масштабируемой дальнейшей обработки.

Онтологический уровень. Для сопоставления сетевых событий с конкретными векторами атак интегрируется онтология, основанная на модели MITRE ATT&CK [7]. Каждая запись лога анализируется на предмет соответствия определенным тактикам и техникам, что позволяет перейти от необработанных данных к формализованной модели инцидентов.

Построение графа знаний. Онтологически обогащенные данные переносятся в граф знаний, где узлы представляют события Suricata и элементы MITRE (тактики, техники), а ребра отражают временные и причинно-следственные связи. Каждый элемент дополнительно обогащается атрибутами, полученными на предыдущем этапе, что позволяет гибко выявлять взаимосвязи и паттерны атак.

Анализ на основе графовой нейронной сети. На построенном графе обучается графовая нейронная сеть (GNN), которая итеративно обновляет векторные представления узлов (эмбеддинги). Этот процесс обеспечивает кластеризацию взаимосвязанных событий и позволяет не только классифицировать известные типы атак, но и обнаруживать новые сценарии, схожие по структуре с ранее обнаруженными угрозами.

LLM-ассистент. Результаты работы GNN передаются в модуль на базе LLM, использующей RAG для формирования понятных оператору пояснений и рекомендаций. Ассистент принимает запросы вместе с контекстом, сформированным на основе графа и генерирует развернутый ответ с рекомендациями по реагированию (например, блокировка IP, обновление правил IDS). В реализации прототипа использована модель deepseek:32B [8], развернутая через платформу Ollama [9].

Анализ оператором и принятие решения. На завершающем этапе оператор осуществляет визуальный аудит с помощью интерактивного интерфейса, на котором отображаются ключевые события, диаграммы и графы с отмеченными угрозами. На основании предоставленных пояснений и рекомендаций принимаются меры по реагированию, а система посредством обратной связи совершенствуется для дальнейшего повышения точности анализа.

Эксперимент

В рамках демонстрации работоспособности разработанного прототипа был создан тестовый стенд, демонстрирующий основные функциональные возможности системы. Прототип реализован в виртуализированной среде, где на одном сервере с ОС Linux развернута IDS Suricata для регистрации сетевых событий. Suricata генерирует стандартные журналы, содержащие сигнатуры типичных атак (сканирование портов, ICMP-flood и др.), которые сохраняются в формате JSON и служат исходным материалом для последующей обработки.

Для аналитической обработки и реализации компонентов, основанных на онтологии MITRE ATT&CK, графовой нейронной сети и LLM-ассистенте, выделен отдельный виртуальный сервер с достаточным объемом оперативной памяти и графическим ускорителем. Обмен данными между узлами осуществляется через локальную сеть, что позволяет обеспечить анализ. В модуле LLM-ассистента используется модель Deepseek с 32B параметрами, развернутая через фреймворк Ollama, что позволяет генерировать понятные и подробные пояснения к выявленным угрозам.

Следует отметить, что данная экспериментальная платформа находится на стадии прототипирования. Прототип демонстрирует жизнеспособность предлагаемого подхода и является базой для дальнейшей оптимизации системы в условиях высоконагруженных и распределенных инфраструктур.

Заключение

Представленный прототип интеллектуальной системы для обнаружения и анализа кибератак объединяет графовые нейронные сети, онтологическую разметку и большие языковые модели с применением метода RAG. Среди преимуществ прототипа – способность выявлять скрытые взаимосвязи между сетевыми событиями и формировать понятные рекомендации для оперативного реагирования. Однако система обладает ограничениями, связанными с высокой вычислительной сложностью обработки больших объемов данных.

В будущем планируется оптимизация вычислительных затрат, расширение функциональности за счет интеграции дополнительных источников данных (SIEM, EDR, UEBA) и адаптация системы к различным типам инфраструктур, а также дальнейшая доработка модуля LLM для повышения качества генерации пояснений в условиях динамично изменяющихся атакующих сценариев. Предусматривается также рассмотреть вопросы обеспечения безопасности предложенных решений, в том числе в сетях промышленного Интернета вещей [10, 11].

Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.

Список используемых источников

1. Levshun D., Kotenko I. Intelligent graph-based correlation of security events in cyber-physical systems // International Conference on Intelligent Information Technologies for Industry, Cham, 2023. Cham: Springer Nature Switzerland, 2023. P. 115–124. doi: 10.1007/978-3-031-43792-2_12.

2. Kotenko I., Polubelova O., Saenko I., Doynikova E. The ontology of metrics for security evaluation and decision support in SIEM systems // 2013 International Conference on Availability, Reliability and Security (ARES 2013), 2013. P.638–645. doi: 10.1109/ARES.2013.84.

3. Mao Q., Liu Z., Liu C., Li Z., Sun J. Advancing Graph Representation Learning with Large Language Models: A Comprehensive Survey of Techniques: arXiv preprint arXiv:2402.05952 [электронный ресурс]. 2024. URL: https://arxiv.org/html/2402.05952v1 (дата обращения: 12.03.2025).

4. Zou Z., Wang B., Li F., Ye B. Research on Network Security Threat Analysis Method Based on Knowledge Graph // 2024 IEEE 7th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2024. T. 7. P.668–672. DOI: 10.1109/IAEAC59436.2024.10504024.

5. Pan S., Luo L., Wang Y., Chen C., Wang J., Wu X. Unifying Large Language Models and Knowledge Graphs: A Roadmap // IEEE Transactions on Knowledge and Data Engineering. 2024. Vol. 36. № 7. C. 3580–3599. DOI: 10.1109/TKDE.2024.3352100.

6. Mavromatis F., Karypis G. Gnn-Rag: Graph Neural Retrieval for Large Language Model Reasoning: arXiv preprint arXiv:2405.20139 [электронный ресурс]. 2024. URL: https://arxiv.org/html/2405.20139v1 (дата обращения: 25.03.2025).

7. MITRE [электронный ресурс]. URL: https://www.mitre.org/ (дата обращения: 15.03.2025).

8. Deepseek [электронный ресурс]. URL: https://deepseek.io/ (дата обращения: 20.03.2025).

9. Ollama [электронный ресурс]. URL: https://ollama.ai/ (дата обращения: 27.03.2025).

10. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5-31.

11. Desnitsky V., Levshun D., Chechulin A., Kotenko I. Design technique for secure embedded devices: application for creation of integrated cyber-physical security system // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. Vol. 7. № 2, June 2016. P.60-80.

THE USE OF OTHNOLOGIES AND LARGE LANGUAGE MODELS FOR THE INTERPRETATION OF SURICATA EVENTS

Kotenko I., Abramenko G.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper describes a prototype system designed for automated detection and analysis of cyber-attacks by integrating IDS Suricata logs, graph neural networks, MITRE ATT&CK-based ontology model and large language models using retrieval-augmented generation. The experimental system includes collection and pre-processing of network events, ontology partitioning, knowledge graph construction to identify hidden relationships and generation of explanatory recommendations for the operator.

Key words: *LLM, GNN, RAG, ontologies, anomaly detection, Suricata*

УДК 004.056
ГРНТИ 81.98

МЕТОДЫ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ И ИХ ВЛИЯНИЕ НА ВЫЯВЛЕНИЕ МНОГОШАГОВЫХ АТАК

И. В. Котенко, И. Ю. Зеличенок

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (ФИЦ РАН)

В современных сетях растет число сложных многошаговых атак, которые характеризуются низкой заметностью и могут оставаться нераскрытыми в течение длительного времени. Традиционные системы обнаружения вторжений испытывают трудности при выявлении сложных атак. Многие подходы на основе интеллектуального анализа данных, предлагаемые исследователями, не учитывают поведение моделей при эксплуатации на реальных объемах данных. В статье рассмотрены основные методы обработки больших данных и их влияние в условиях выявления многошаговых атак при помощи нейронных сетей с долгой краткосрочной памятью в задаче анализа временных рядов. Предложен подход, который сочетает потоковую обработку, буферизацию входящих данных и использование распределенных баз данных. Представленные результаты экспериментов демонстрируют сокращение задержки обнаружения атак и рост пропускной способности системы.

информационная безопасность, кибератаки, многошаговые атаки, большие данные

Современные кибератаки все чаще представляют собой многошаговые сценарии, которые охватывают разные сегменты сети и используют несколько уязвимостей. Это усложняет их своевременное выявление и требует от систем обнаружения вторжений (intrusion detection system, IDS) умения быстро анализировать большие объемы данных. Традиционные методы нередко «тормозят» из-за больших потоков входящей информации и ограниченных вычислительных ресурсов.

Задача автоматизации выявления сложных атак зачастую решается путем использования методик интеллектуального анализа данных [1], в том числе при помощи машинного и глубокого обучения. Однако, многие исследования, при тестировании предлагаемых подходов, не учитывают реальные объемы трафика и особенностей поведения моделей машинного обучения в связке с технологиями, обрабатывающих потоки данных.

Применение технологий Big Data помогает ускорить процесс обработки поступающих сетевых пакетов и выявлять цепочки событий, указывающие на развивающуюся атаку. К таким технологиям относятся потоко-

вый анализ трафика, распределенное хранение логов, а также многопоточность при обработке и анализе данных. Дополнительно важную роль играет использование глубоких нейронных сетей, особенно рекуррентных архитектур LSTM [2] (long-short-term memory), которые позволяют учитывать временные зависимости между событиями.

Разработанный экспериментальный стенд, основанный на системе L/STIM [3], предназначен для обнаружения многоэтапных атак с помощью методов машинного обучения, включая анализ временных рядов. Он выполняет несколько шагов обработки данных: от их сбора и разбиения на пакеты до предварительной обработки, анализа с помощью нейронных сетей и сохранения результатов в базах данных для долгосрочного анализа.

Для сокращения задержки между появлением события до его обнаружения были использованы следующие подходы:

– гибридная пакетно-потоковая обработка;
– обработчик потоков;
– каскад баз данных.

Далее каждый подход описан более подробно.

Гибридная пакетно-потоковая обработка (ГПО). На первом этапе принимается входящий поток данных, представляющий логи сетевого трафика или активности пользователей за 30 секунд. Этот поток делится на временные пакеты [4], что помогает оптимизировать нагрузку на систему и анализировать атаки в контексте временных зависимостей. В зависимости от интенсивности поступающих событий принимается решение, буферизовать ли их в стеке. перед анализом, чтобы сгладить всплески нагрузки и обеспечить равномерную обработку.

Когда в стеке накапливается несколько пакетов, система определяет разницу во времени между последним и первым. Если она меньше или равна пороговому значению для краткосрочного анализа, запускается анализ данных в однопоточном режиме. Если же система не успевает обработать их вовремя, создаются дополнительные потоки для своевременного выявления возможной угрозы и уменьшения накопленных данных в стеке.

Обработчик потоков (ОП). При повышенной нагрузке события передаются в Thread-handler, который распределяет их по нескольким модулям машинного обучения [5]. Это ускоряет анализ и сокращает время ожидания результатов.

Предлагаемый подход объединяет пакетную и потоковую обработку данных, что помогает снизить вероятность переполнения буфера благодаря

многопоточному запуску обработчиков и детекторов. Техники пакетно/потоковой и многопоточной обработки работают в паре. Сначала сборщики (агенты) получают сетевые пакеты от клиентских устройств и передают их на сервер, где пакеты складываются в стек в порядке поступления.

Каскад баз данных (КБД). Результаты анализа записываются в нереляционную (NoSQL) [6] базу данных для дальнейшей обработки. Параллельно с основным конвейером работает модуль, который ищет в уже классифицированных данных связь между событиями и формирует из них отдельный пакет, включая события за период до 7 дней. Затем модуль долгосрочного анализа определяет сценарий и возможные направления атаки, после чего отправляет эти данные в историческую реляционную базу (SQL).

Эксперименты проводились на наборе данных Edge IIoT [7]. Главная его особенность заключается в предоставлении высоконагруженного IoT трафика с использованием pcap файлов, что дало возможность смоделировать реальные потоки данных с разным числом клиентских устройств, что позволило получить результаты обнаружения в условиях, приближенных к реальным.

Таблица 1 содержит информацию о влиянии каждой из представленных методик на задержку между событием и его обнаружением.

ТАБЛИЦА 1. Результаты экспериментов.

Число устройств	Без техник (сек.)	ГПО (сек.)	ОП (сек.)	КБД (сек.)	Все техники (сек.)
1	0.87	1.02	0.62	0.89	0.52
25	2.69	2.52	1.84	2.34	1.51
50	4.54	5.43	3.29	4.05	2.94
75	6.88	9.05	4.85	5.91	4.51
100	8.88	11.13	6.33	8.35	5.74

Анализируя результаты экспериментов, можно сделать вывод, что система работает стабильно, хотя время обработки растет линейно с увеличением числа эмулированных устройств. Это видно по плавному росту задержки при масштабировании. Важно отметить, что поведение системы предсказуемо при увеличении нагрузки, что делает ее подходящей для мониторинга и обнаружения атак в реальных условиях.

Рассматривая влияние различных способов обработки данных, видно, что метод ГПО несколько ухудшает результаты по сравнению с базовой моделью. Это связано с дополнительными вычислительными затратами, возникающими при предварительной буферизации событий перед их анализом. Однако этот метод дает более гибкий контроль за загрузкой системы и своевременностью обнаружения атак.

Метод ОП показывает лучший прирост производительности за счет оптимизации потоковой обработки, которая снижает нагрузку на систему. Метод КБД отличается наилучшей скоростью обработки, поскольку учитывает накопленные исторические данные и эффективно выявляет многошаговые атаки при помощи модуля долгосрочного анализа.

В целом, результат при использовании всех методик вместе обеспечивает практически двухкратный прирост производительности, что дает возможность использовать протестированные подходы в реальных системах.

В работе были представлены используемые в L/STIM методики обработки больших данных и машинного обучения, а также проведена демонстрация их работы. В будущих работах предполагается тестирование представленного подхода в реальной инфраструктуре и рассмотрение аспектов обеспечения безопасности предложенных решений, в том числе в сетях промышленного Интернета вещей [8, 9].

Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 23-РБ-01-09.

Список используемых источников

1. Branitskiy A., Kotenko I. Hybridization of computational intelligence methods for attack detection in computer networks // Journal of Computational Science. 2017. T. 23. P.145-156. doi: 10.1016/j.jocs.2016.07.010.

2. Hochreiter S., Schmidhuber J. Long short-term memory // in Neural computation. 1997. Vol. 9. № 8. P. 1735-1780.

3. Zelichenok I., Kotenko I. L/STIM: A Framework for Detecting Multi-Stage Cyber Attacks // 2024 International Russian Smart Industry Conference (SmartIndustryCon). 2024. P. 208-213. doi: 10.1109/SmartIndustryCon61328.2024.10516137.

4. Nie P. et al. Sparse Trust Data Mining // IEEE Transactions on Information Forensics and Security. 2021. Vol. 16. P. 4559-4573. doi: 10.1109/TIFS.2021.3109412

5. Shu J., Fang K., Chen Y., Wang S. TH-iSSD: Design and Implementation of a Generic and Reconfigurable Near-Data Processing Framework // ACM Trans. Embed. Comput. Syst. 2023. doi: https://doi.org/10.1145/3563456

6. Zhang G., Mariano B., Shen X., Dillig I. Automated Translation of Functional Big Data Queries to SQL // Proc. ACM Program. Lang. 2023. Vol. 7. № 95. 29 p. doi: https://doi.org/10.1145/3586047

7. Ferrag M. A., Friha O., Hamouda D., Maglaras L., Janicke H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications: Centralized and Federated Learning // IEEE Dataport. 2022. DOI: https://dx.doi.org/10.21227/mbc1-1h68.

8. Десницкий В. А., Чечулин А. А., Котенко И. В., Левшун Д. С., Коломеец М. В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. № 5 (48). С. 5-31.

9. Desnitsky V., Levshun D., Chechulin A., Kotenko I. Design technique for secure embedded devices: application for creation of integrated cyber-physical security system // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. Vol. 7. № 2. June 2016. P. 60-80.

BIG DATA PROCESSING METHODS AND THEIR IMPACT ON DETECTING MULTI-STEP ATTACKS

Kotenko I., Zelichenok I.
Saint Petersburg Federal Research Center of the Russian Academy of Sciences

Modern networks are experiencing an increasing number of complex multi-step attacks that are characterized by low visibility and can remain undetected for a long time. Traditional intrusion detection systems have difficulty detecting complex attacks. Many data mining approaches proposed by researchers do not take into account the behavior of models when operating on real data volumes. The article discusses the main methods of big data processing and their impact in terms of detecting multi-step attacks using neural networks with long short-term memory in the problem of time series analysis. An approach is proposed that combines stream processing, buffering of incoming data, and the use of distributed databases. The presented experimental results demonstrate a reduction in attack detection latency and an increase in system throughput.

Key words: *information security, cyber-attacks, multi-step attacks, big data.*

УДК 004.056
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ АНСАМБЛЕВОГО МЕТОДА АВТОМАТИЗИРОВАННОГО ПЕНТЕСТА НА БАЗЕ ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

И. В. Котенко[1], М. А. Слётов[2]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Национальный исследовательский университет ИТМО

Современные киберугрозы требуют эффективных методов проверки безопасности информационных систем. Традиционные подходы к тестированию на проникновение (пентесту), основанные на ручном тестировании или использовании автоматизированных инструментов, имеют ограниченную гибкость и масштабируемость. Данный доклад посвящен разработке системы автоматизированного пентеста, использующей алгоритмы обучения с подкреплением в сочетании с методами ансамблевого обучения. Благодаря такому комбинированию методов предполагается повысить точность и устойчивость принимаемых решений. В работе показано, что использование множества моделей для принятия решений благоприятно сказывается на эффективности тестирования на проникновение.

пентест, искусственный интеллект, обучение с подкреплением, ансамбль

С ростом сложности компьютерных систем и усложнением процесса обработки информации проблемы кибербезопасности становятся все более актуальными [1-4]. Современные системы часто содержат уязвимости, которые могут привести к утечке данных или сбоям в работе системы, создавая значительные риски. Для эффективного тестирования на проникновение (пентеста) традиционно требуются высококвалифицированные специалисты, которые выявляют, используют и устраняют уязвимости. Несмотря на частичную автоматизацию, человеческий опыт остается важнейшим компонентом процесса. Однако последние достижения в области машинного обучения, в частности обучения с подкреплением, открыли новые возможности для автоматизации пентеста [5-8]. Используя методы ансамблей, можно повысить эффективность обнаружения уязвимостей и генерировать разнообразные сценарии атак, адаптированные к конкретным системам. В статье рассматривается применение ансамблевых методов при реализации пентеста с упором на обучение с подкреплением, как основу для улучшения стратегий оценки безопасности и эксплуатации.

Одним из возможных направлений исследований является изучение того, как можно комбинировать различные модели обучения с подкреплением для повышения общей производительности. Например, для объединения агентов с разным уровнем специализации можно использовать методы ансамблевого обучения, например bagging или boosting. Это поможет устранить недостатки отдельных агентов и создать более надежную автоматизированную систему тестирования на проникновение. Один из таких методов уже применяется при работе с существующими инструментами для пентеста. Данный подход позволяет обнаружить больше уязвимостей за счет комбинирования нескольких инструментов [5]. В конечном итоге интеграция таких методов для автоматизированного тестирования на проникновение способна повысить эффективность принятия решений, адаптивность и масштабируемость.

Ансамблирование в автоматизированном тестировании на проникновение подразумевает объединение нескольких моделей или стратегий для повышения успешности атак, охвата и адаптивности. Принцип работы ансамбля можно представить в виде набора моделей, результат работы которых суммируется для более устойчивого поведения (рис. 1).

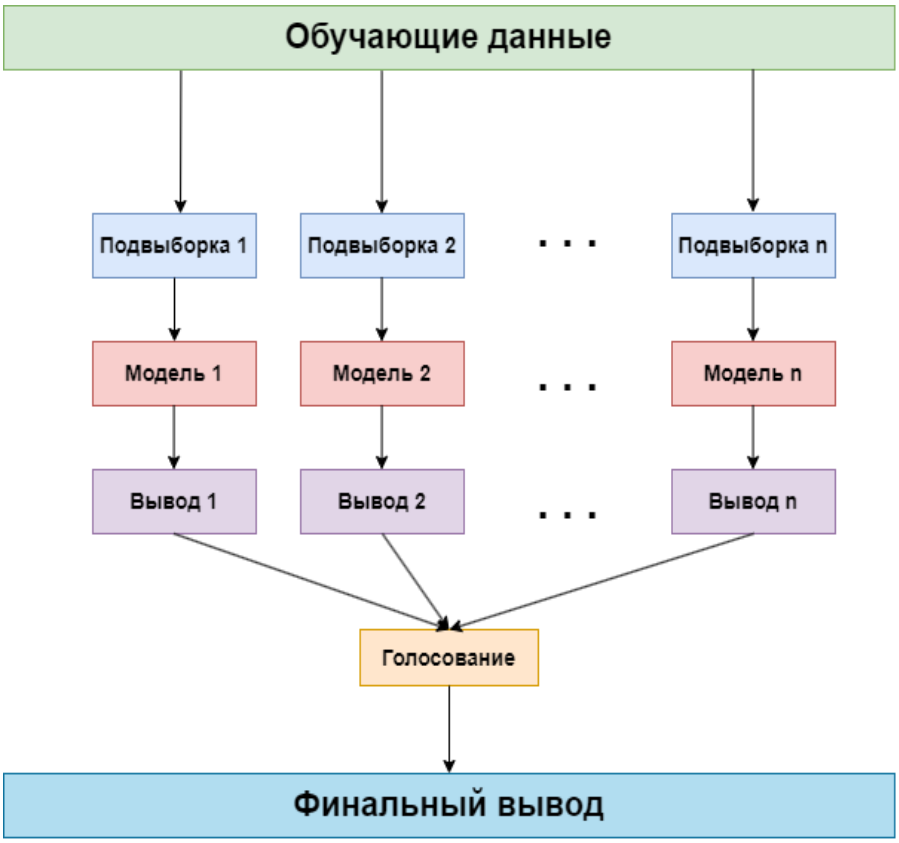


Рис. 1. Диаграмма ансамблевого метода (на основе голосования)

Базой для возможного использования данного метода является иерархический подход к обучению с подкреплением, предложенный Тран К. [6]. Этот подход был назван Hierarchical Agent Deep Reinforcement Learning (HA-DRL). В его работе была разработана модель обучения с подкреплением, в которой агенты представляют собой иерархическую структуру. Данные агенты разделены на высокоуровневые и низкоуровневые. Высокоуровневые агенты определяют общую стратегию и цели, в то время как низкоуровневые выбирают конкретные действия для достижения поставленных целей. Данное решение обусловлено стремлением снизить пространство действий для каждого отдельно взятого агента за счет параметризации пространства действий. Такое разделение агентов имеет минус в виде необходимости изучения ими нескольких политик, однако даже так плоское пространство действий в значительно большей степени замедляет процесс обучения [6]. На рис. 2 представлена схема работы предложенной системы.

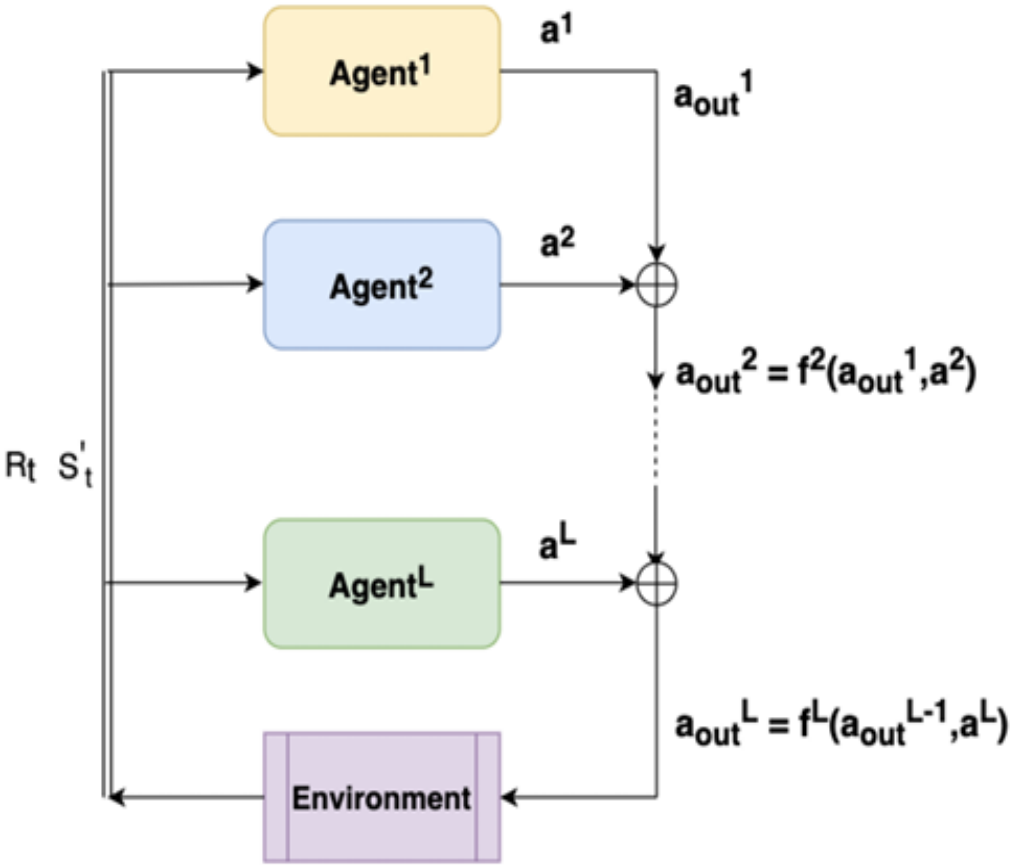


Рис. 2. Схема работы мультиагентной системы

Данный подход позволил улучшить скорость обучения и качество итоговой модели по сравнению с другой моделью – дуэльной глубокой Q сетью

(DDQN). DDQN, в отличие от классической глубокой Q сети, имеет разложенную на две части функцию ценности. Разложена она на функцию ценности состояния и функцию преимущества. Благодаря данному изменению агент способен лучше принимать решения в средах, где некоторые действия мало влияют на результат [7].

Указанная мультиагентная система имеет заметные улучшения по сравнению с традиционными методами автоматизированного пентеста, однако необходимо провести дальнейшие исследования с другими ансамблевыми методами для определения наиболее перспективного решения. Такой подход в настоящее время используется авторами настоящей работы.

Используя несколько агентов усиленного обучения, каждый из которых специализируется на различных векторах атак или конфигурациях сети, предлагается создать ансамбль, который сбалансирует процедуры исследования и эксплуатации уязвимостей, что приведет к более эффективному и результативному тестированию на проникновение.

Это наиболее заметно на примере описанного ранее иерархического подхода [6]. Основными проблемами в автоматизированном пентесте являются скорость обучения и масштабируемость моделей. Исследованиям, не использующим ансамблевые методы, на данный момент присущ значительный недостаток, а именно потеря качества модели при попытке применить ее на более крупных сетевых инфраструктурах. Как правило, предлагаемые модели способны обнаруживать уязвимости в сетях, включающих в себя не более 25-50 хостов. Среди таких моделей можно перечислить упомянутый ранее DQN, CLAP, ND3RQN, The MulVAL double deep Qnetwork (MDDQN). При попытке превысить данный порог хостов возникает проблема в стабильности работы этих моделей [8-12].

Однако, использование иерархического метода позволило увеличить количество хостов, проверяемых за раз, без ухудшения скорости выработки стратегий и стабильности работы системы. На рис. 3 представлены графики количества шагов и общей награды в ходе обучения иерархической модели (HA-DRL) и дуэльной глубокой Q-сети (DDQN) в сетевой инфраструктуре, состоящей из 70 и 100 хостов соответственно [6]. Иерархическая модель быстрее достигает максимума наград и делает это за меньшее количество эпизодов обучения. Однако, на графике со 100 хостами можно заметить колебания графика на его конце, что может свидетельствовать о возможной нестабильности, которую необходимо исследовать в дальнейшем.

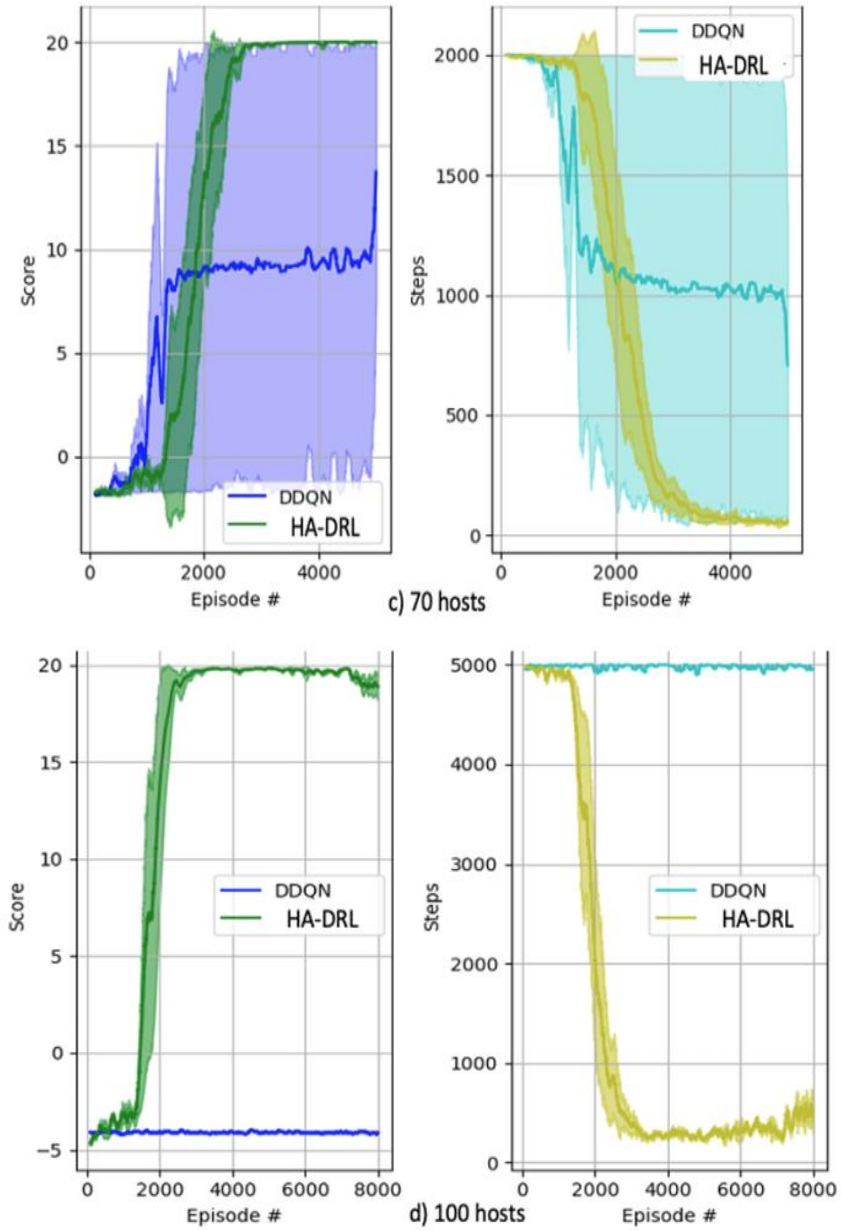


Рис. 3. Графики результатов работы HA-DRL и DDQN

Продолжая исследования иерархических агентов для автоматизированного тестирования на проникновение, планируется исследовать возможности ансамблевых методов для увеличения устойчивости работы всей системы на сетях с большим количеством хостов.

Предлагается разделить имеющуюся иерархическую модель на множество более специализированных, объединенных в одну систему с помощью ансамбля. В первую очередь исследования будут направлены на применение различных ансамблевых методов, таких как bagging, boosting и взвешенное усреднение, для объединения нескольких мультиагетных моделей, обученных на различных наборах данных или сценариях атак. Конечной целью

является развитие иерархической модели и создание ансамблевой системы, в которой специализированные модели будут заниматься конкретными действиями для достижения цели, в то время как мета-агент будет учиться выбирать наиболее эффективную модель для каждой ситуации. Для первого этапа исследования планируется использовать наборы данных для сетевых вторжений ввиду обширности доступных данных. Это позволит лучше обучить исследуемые модели и более контролируемо провести тестирование на сетях с большим количеством хостов.

Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.

Список использованных источников

1. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. 2005. T. 3685 LNCS. PP. 311-324.

2. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // Proceedings. International Conference on Security and Cryptography, SECRYPT 2006. Polytechnic Institute of Setubal. Setubal, 2006. PP. 339-344.

3. Kotenko I., Chechulin A., Novikova E. Attack Modelling and Security Evaluation for Security Information and Event Management // SECRYPT 2012. International Conference on Security and Cryptography // Proceedings. Rome, Italy. 24-27 July 2012. PP. 391-394. ISBN 978-989-8565-24-2.

4. Kotenko I., Chechulin A. Computer attack modeling and security evaluation based on attack graphs // Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems, IDAACS 2013, 2013, 2, PP. 614–619.

5. Goel J. N. et al. Ensemble based approach to increase vulnerability assessment and penetration testing accuracy // 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). IEEE, 2016. C. 330-335.

6. Tran K. et al. Deep hierarchical reinforcement agents for automated penetration testing // arXiv preprint arXiv:2109.06449. 2021.

7. Wang Z. et al. Dueling network architectures for deep reinforcement learning // International conference on machine learning. PMLR, 2016. C. 1995-2003.

8. Yang Y., Liu X. Behaviour-diverse automatic penetration testing: A curiosity-driven multi-objective deep reinforcement learning approach // arXiv preprint arXiv:2202.10630. 2022.

9. Chowdhary A. et al. Autonomous security analysis and penetration testing //2020 16th International Conference on Mobility, Sensing and Networking (MSN). IEEE, 2020. PP. 508-515.

10. Hu Z., Beuran R., Tan Y. Automated penetration testing using deep reinforcement learning // 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2020. PP. 2-10.

11. Yi J., Liu X. Deep reinforcement learning for intelligent penetration testing path design // Applied Sciences. 2023. Vol. 13. № 16. PP. 9467.

12. Zhang Y. et al. Improved deep recurrent q-network of POMDPs for automated penetration testing // Applied Sciences. 2022. Vol.12. № 20. PP. 10339.

RESEARCH ON THE ENSEMBLE METHOD OF AUTOMATED PENTEST BASED ON REINFORCEMENT LEARNING

Kotenko I., Slyotov M.
Saint Petersburg Federal Research Center of the Russian Academy of Sciences
ITMO University

Modern cyber threats require effective methods to test the security of information systems. Traditional penetration testing (pentest) approaches based on manual testing or automated tools have limited flexibility and scalability. This paper focuses on the development of an automated pentest system that utilizes reinforcement learning algorithms combined with ensemble learning methods. Through this combination of methods, it is expected to improve the accuracy and robustness of the decisions. The paper shows that the use of multiple models for decision making has a favorable effect on the efficiency of penetration testing.

Key words: *pentest, artificial intelligence, reinforcement learning, ensemble*

УДК 004.056.55
ГРНТИ 81.93.29

ЗАЩИТЫ ДИССЕРТАЦИЙ В РОССИИ В ОБЛАСТИ СТЕГАНОГРАФИИ

А. В. Красов

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

Цифровая стеганография – новое и перспективное направление в защите информации, активное развитее которого связано с широким распространением компьютерной техники. Научный интерес к этому направлению подтверждается более 60 диссертациями на соискание ученых степеней кандидатов наук, в том числе 5 на соискание ученых степеней докторов наук.

стеганография, скрытые каналы, цифровые водяные знаки

По данным РИНЦ с 2000 года (более ранних сведения сведений РИНЦ не содержит), в России были защищены 63 диссертации на тему применения стеганографии, из них 5 диссертаций на соискание ученых степеней д.т.н. (рис. 1, 2). Большинство из них, в том числе 5 диссертаций на соискание ученых степеней доктора наук, относятся к техническим наукам, так же 5 диссертаций защищены на соискание ученой степени к.ф.-м.н., есть одна диссертация на соискание ученой степени к.фил.н.

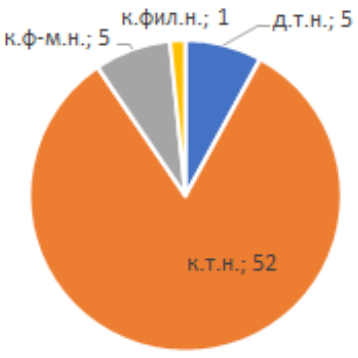


Рис. 1. Статистика защит диссертаций

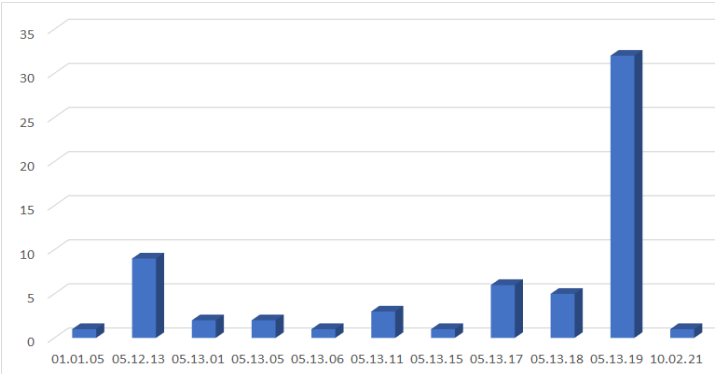


Рис. 2. Распределение диссертаций в области стеганографии по научным специальностям

Половина из этих диссертаций защищена по научной специальности 2.3.6 (05.13.19) «Методы и системы защиты информации, информация безопасность» и соответствует паспорту научной специальности п. 17 «Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях», и близко другим пунктам, таким как п. 15, п. 19. Но только одна из пяти диссертаций на соискание ученой степени д.т.н. была защищена по этой научной специальности.

Второй по числу защищенных диссертаций в области стеганографии – 9 – является научная специальность 2.2.15 (05.12.13) «Системы, сети и устройства телекоммуникаций». В паспорте данной специальности есть п. 17 «Исследование и разработка новых методов защиты информации и обеспечение информационной безопасности в сетях, системах и устройствах телекоммуникаций», но только 3 из 9 защищенных диссертаций можно отнести к данному пункту, остальные 6 диссертаций посвящены вопросам стеганографии в изображениях, что бесспорно имеет отношение к вопросам информационной безопасности, но не в сетях, системах и устройствах телекоммуникаций.

Еще три диссертации защищены по научной специальности 2.3.5 (05.13.11) «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей», в том числе одна диссертация д.т.н. В паспорте этой научной специальности есть п. 1. «Модели, методы и алгоритмы проектирования, анализа, трансформации, верификации и тестирования программ и программных систем» и представленные диссертации, посвященные вопросам разработки программных средств для решения вопросов защиты информации методами стеганографии и защиты самого программного обеспечения на основе методов близким к стеганографии (обфускации кода).

Остальные 19 диссертаций, в т.ч. 3 из 5 диссертаций д.т.н., защищены по научным специальностям, в паспортах которых отсутствуют не только вопросы стеганографии, но и защиты информации.

Если рассматривать статистику защит диссертаций по годам, приведенную на рис. 3, видно, что, начавшись с первых работ в 2000 г., посвященных применению стеганографии в устройствах маскировки информации, производственных процессах, распределенных автоматизированных систем и систем связи, интерес в диссертациях по стеганографии сместился к более

простым задачам – стеганографии в мультимедийных файлах (41 диссертация – 65%). При этом в основном использовался самый простой метод вложения в наименьшие значащие биты (НЗБ). Даже если отдельные авторы переходили на использование более сложных графических форматов со сжатием типа jpeg, большинство из них сводили все вопросы к распаковке сжатого файла и вложению в НЗБ, не анализируя, что при изменении коэффициентов сжатия вложенная информация может быть утрачена. Аналогичным образом обстояло дело с вложением в видео последовательности, когда использовались только I кадры, содержащие полное изображение, без анализа как сложение в него, методами НЗБ повлияет на всю видеопоследовательность следующих кадров содержащих изменения кадров I (кадры P, B, D форматов).

Таким образом, фактически все эти диссертации описывали один и тот же метод с минимальными изменениями, которые и составляли новизну этих работ.

К вопросам применения сетевых методов стеганографии приходится только 7 работ (11 %), стеганографии в программном обеспечении посещено еще меньше, всего 4 работы (6 %). На все оставшиеся направления приходится 10 работ (15 %).

Таким образом, для большинства научных руководителей тема стеганографии была проходящей, сделав одну успешную защиту аспиранта, возможностей продолжения они для себя не видели 30 научных руководителей из 39, имеющих опыт защит диссертаций в области стеганографии это, т.е. 77 %, кроме того часть руководителей защитивших по 2 аспиранта в этой области, фактически повторяли туже самую работу спустя 4-7 лет, это еще 3 научных руководителя. Фактически опыт защит аспирантов различных областях стеганографии есть только у 6 научных руководителей в этой области, только 15 %!

Пик интереса к стеганографии приходится на 2009-2014 гг., анализируя вклад каждого вуза, фактически успешный интервал защит в большинстве вузов по данной теме составлял от 2 до 6 лет.

Лидером по числу защит диссертаций в области стеганографии можно назвать ИТМО, где было защищено 10 диссертаций на тему стеганографии, однако фактически работы за последние 6 лет защит диссертаций на эту тему у преподавателей данного вуза не было.

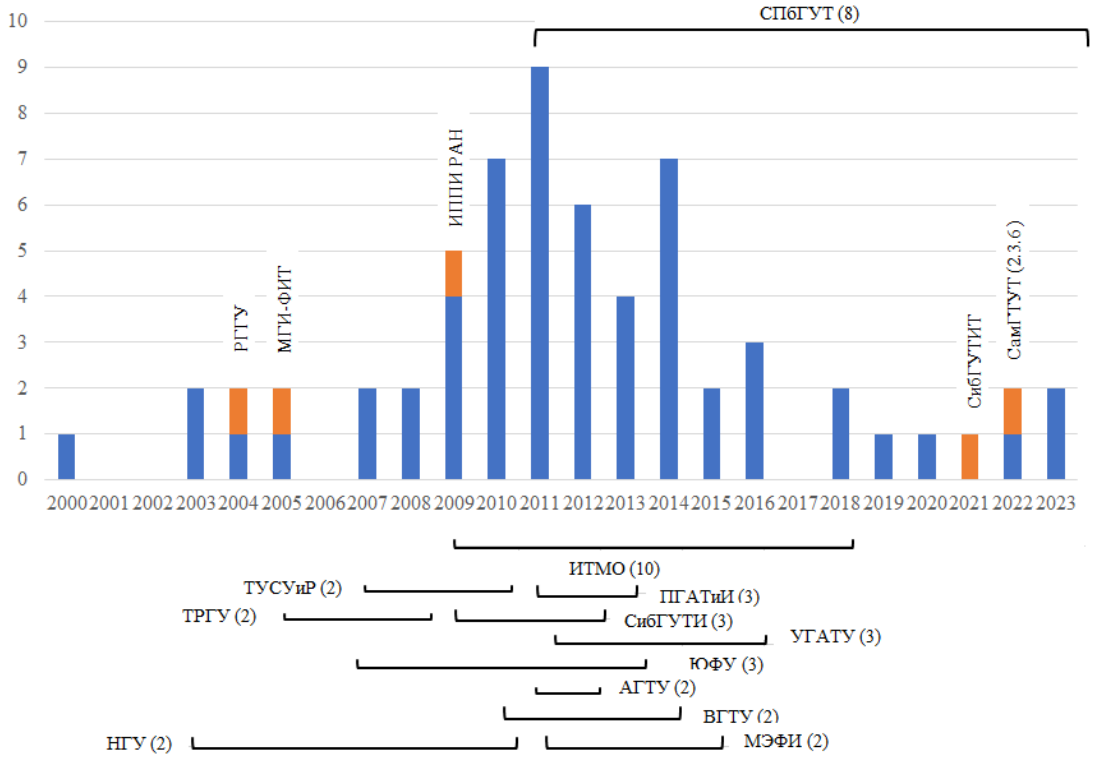


Рис. 3. Статистика защит диссертаций по стеганографии по годам

Единственным вузом, в котором уже на протяжении последних 12 лет продолжаются успешные защиты диссертаций это – СПбГУТ, где за эти годы защищены 8 диссертаций. Важно отметить, что эти работы выполняются в рамках одной кафедры – Защищенных систем связи, несколько аспирантов, защитивших диссертации на тему стеганографии, остались работать на кафедре и так же уже руководят новыми аспирантам и дипломниками в этой области.

Кроме СПбГУТ, защиты диссертаций в области стеганогрфии за последние 5 лет имеют научные руководители еще только 2 вузов: МТУСИ и МЭИ (по одной, единственной, защите в этой области). Статистика по числу защит научных руководителей приведена на рис. 4.

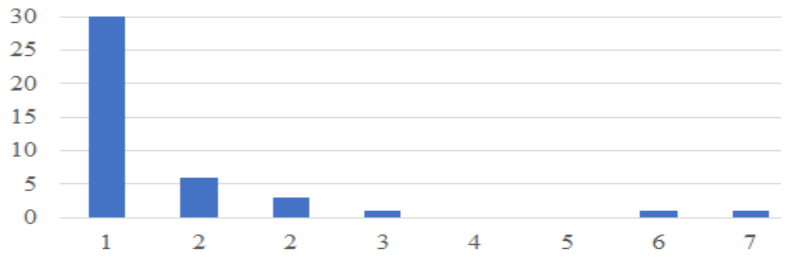


Рис. 4. Статистика научных руководителей (по вертикале) по числу защит

Лидерами по числу защит аспирантов в области стеганографии являются д.т.н., проф. Коржик В. И. (СПбГУТ) – 7 защит и д.т.н., проф. Коробейников А. Г. (ИТМО) – 7 защит.

Профессор Коробейников А.Г. (ИТМО) активно работает с аспирантами на протяжении 10 лет, основные научные интересы связанны с комплексной защитой объектов информатизации, криптографическими методами, стеганография не является основным научным интересом этого уважаемого автора, тематика исследований связанна только с одним из направлений стеганографии – возложениями в неподвижные изображения. Новых публикаций и защит аспирантов после 2018 года у него нет.

Единственным ученым России активно занимающимся вопросам стеганографии является проф. Коржик В. И., кафедра ЗСС СПбГУТ. По материалам защищенных диссертаций его аспирантов и в соавторстве с ними, проф. В. И. Коржиком написаны три монографии [4, 5, 6].

Среди наиболее значимых монографий, изданных в России в области стеганографии, так же необходимо отметить:

– Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография [1]. Ранее, в 2006 г., И. Н. Оковым была так же опубликована монография «Аутентификация речевых сообщений и изображений в каналах связи» [2]. Необходимо отметить, что он так же является учеником проф. В. И. Коржика.
– Шелухин О. И., Канаев С. Д., Стеганография. Алгоритмы и программная реализация [3]. Под научным руководством проф. Шелухина О. И. защищена одна кандидатская диссертация по стеганографии.

Несмотря на все достоинства представленных выше работ, единственным официальным учебником с грифом «Рекомендовано ФУМО в области Информационной безопасности» является учебник, изданный проф. В. И. Коржиком и А. В. Красовым [7]. Чтение дисциплин по стеганографии в СПбГУТ началось в 2004 году, они читаются всем нашим направлениям подготовки бакалавров, магистров и специалистов по направлениям «Информационная безопасность» «Инфокоммуникационные технологии и системы связи», ежегодно через них обучалось более 300 студентов.

Научное руководство аспирантами в этой области, кроме проф. В. И. Коржика осуществляют еще 5 сотрудников кафедры. Очень важно отметить, что все они ориентируются на сложившиеся работы проф. В. И. Коржика, единые для кафедры подходов к стеганографии, исследования охватывают широкий спектр направления применений технологий стеганографии: защита авторских прав, стеганография и ЦВЗ в изображениях, видео- и аудиосигналах, бумажных носителях и других физических носите-

лях, стеганографии в программном обеспечении на уровне машинного и байт кода, стеганографии в компьютерных сетях, вопросах стегоанализа и выявления стегаинсайдера.

Таким образом, можно констатировать, что СПбГУТ является единственным вузом России, в котором еже в течение более 20 лет под руководством проф. В. И. Коржика идут исследования в области применения технологий стеганографии для защиты информации, успешно защищаются диссертации аспирантов, пишутся научные статьи, монографии, вопросы стеганографии внедрены во все уровни подготовки специалистов. Данная работа активно продолжается в нестоящее время.

Список используемых источников

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. Москва: СОЛОН-ПРЕСС, 2009. 264 с.

2. Оков И. Н. Аутентификация речевых сообщений и изображений в каналах связи: монография; Военная акад. связи. Санкт-Петербург: Изд-во Политехнического ун-та, 2006. 391 с.

3. Шелухин О. И., Канаев С. Д., Стеганография. Алгоритмы и программная реализация. М.: Горячая линия–Телеком». 2018. 592 с.

4. Коржик В. И., Небаева К. А., Герлинг Е. Ю. и др.] Цифровая стеганография и цифровые водяные знаки. Том Часть 1. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. 226 с.

5. Коржик В. И., Анфиногенов С. О., Кочкарев А. И. Цифровая стеганография и цифровые водяные знаки / Том 2. СПб: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2017. 198 с.

6. Красов А. В., Гельфанд А. М., Коржик В. И. [и др.]. Построение доверенной вычислительной среды / СПб.: 2019. 108 с.

7. Коржик В. И., Красов А. В. Цифровая стеганография: учебник. Москва: Издательство «КноРус», 2023. 324 с.

DEFENSE OF DISSERTATIONS IN RUSSIA IN THE FIELD OF STEGANOGRAPHY

Krasov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Digital steganography is a new and promising direction in information security, the active development of which is associated with the widespread use of computer technology. Scientific interest in this area is confirmed by more than 60 dissertations for the degrees of candidates of science, including 5 for the degrees of doctors of science.

Key words: *steganography, hidden channels, digital watermarks.*

УДК 004.772
ГРНТИ 49.38.49

ОБНАРУЖЕНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ ПРИ ПОМОЩИ СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ SNORT

А. В. Красов

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

В данной работе рассматривается возможность детектирования сетевой стеганографии при помощи системы обнаружения вторжений, со стандартными правилами. В качестве системы обнаружения вторжений была взята система обнаружения вторжений Snort, распространяемая свободно. Для построения стеганографических каналов использовалась программная утилита Scapy, при помощи которой возможно собирать и отправлять сетевые пакеты.

сетевые протоколы, транспортные протоколы, сетевой анализ, сетевая безопасность, стеганография

Во время проведения кибер-войн и промышленного шпионажа, агенты некоторых стран не редко прибегают к использованию стеганографии. Стеганография – это наука о сокрытии самого факта передачи информации. Другими словами, это совокупность методов для передачи одной информации под видом другой [1-2].

Сетевая стеганография изменяет структуру передачи или же содержимое сетевых пакетов для передачи информации. В современном интернете существует огромное количество пакетов, в которых возможно скрыть информацию. Вложения можно осуществить даже в самые популярные протоколы стека TCP\IP в такие как TCP, IPv4, ICMP. К сожалению, использования данных методов невозможно полностью заблокировать при помощи обычного межсетевого экрана, а также отследить при помощи систем предотвращения утечек информации, поскольку некоторые методы не требуют прав суперпользователя и могут не логироваться вообще.

Все методы сетевой стеганографии возможно разделить на три подхода: модификация пакетов, изменение структуры передачи пакетов и гибридные методы. Модификация пакетов представляет собой метод изменения содержимого полей заголовков сетевых пакетов. Изменение структуры передачи пакетов может изменять время отправки пакетов или вовсе преднамеренно отбрасывать какие-либо пакеты, тем самым передавая информацию. Гибридный метод – это одновременное использование метода измене-

ния структуры передачи пакетов и модификации пакетов. Подробнее про реализацию методов можно прочитать в [3-4].

Вложения можно осуществлять разными способами, например: перехватывать пакет, осуществлять вложение и передавать его далее, генерировать пакет и осуществлять вложение во время создания пакета и т.п. Каждый из способов имеет свои достоинства и недостатки. Например, перехват пакетов и создание из них стегаконтейнеров усложняет поиск отправителя, однако пакеты приходят с задержкой и при использовании некоторых полей нарушается корректность работы протоколов вышестоящих уровней модели OSI, что препятствует нормальной работе пользователя того конечного устройства, куда передается стеганограмма. С другой стороны, генерация пакетов позволяет создавать пакеты, в которых работоспособность вышестоящих протоколов не требуется.

Современные хакеры, также используют стеганографию для пересылки вирусов и другого вредоносного программного обеспечения, а также для воровства информации. Все это делает уязвимыми компании перед лицом инсайдеров и атакующих, владеющих методами стеганографии. В данной статье рассматривается возможность защиты методов стеганографии, стандартными средствами, а именно при помощи системы обнаружения вторжений с набором стандартных правил. Системы предотвращения вторжений используются для отслеживания и предотвращения аномальной сетевой активности. Система просматривает трафик и сравнивает его с заранее заданными паттернами или правилами. Данная система призвана защитить пользователей от некоторых типов сетевых атак, а также атак на информационные системы. В данной статье поднимается вопрос о возможности защиты от сетевой стеганографии при помощи стандартных средств и готовых решений, поскольку в мире в широком доступе не существует решений, направленных на защиту от сетевой стеганографии.

Поскольку в список стандартных средств защиты входят еще и системы предотвращения утечек было решено выявить возможность детектирования и блокирования современной системой предотвращения вторжений, использующей стандартные правила, трафика со стегавложениями.

В данном эксперименте было рассмотрено несколько методов путем вложения в сетевые пакеты. Вложение осуществлялось при помощи программы Scapy [5-6]. Scapy – интерактивная оболочка и программная библиотека для манипулирования сетевыми пакетами на языке программирования Python, позволяющая генерировать большинство известных кадров, пакетов и блоков данных. Scapy использует библиотеку libpcap поэтому может

использоваться как конструктор пакетов, так и как снифер для перехвата или анализа сетевого трафика.

В качестве системы предотвращения вторжений использовалась система Snort, которая была установлена как компонент межсетевого экрана PfSense. Snort community edition (далее просто Snort) является открытой системой и доступна каждому бесплатно, также существует несколько репозиториев с постоянно обновляющимися правилами, которые доступны бесплатно для пользователей Snort.

Изначально был собран виртуальный полигон, состоящий из трех виртуальных машин и виртуальных роутеров. Виртуальные роутеры не указаны на схеме (рис. 1). Как видно из схемы, трафик с виртуальной машины с IP адресом 192.168.110.4 отправлялся на межсетевой экран, где была установлена система предотвращения вторжений. Для того, чтобы попасть на систему предотвращения вторжений трафику необходимо было пройти через виртуальный роутер (с IP адресом 192.168.110.1, на рисунке данный роутер не отражен). После прохождения системы обнаружения вторжений трафик перенаправлялся на виртуальный роутер с IP адресом 192.168.111.1 откуда шел на хост с IP адресом 192.168.111.2, где принимался и обрабатывался. На принимающем хосте была установлена программа Wireshark, при помощи которой и отслеживалась успешность прохождения трафика.

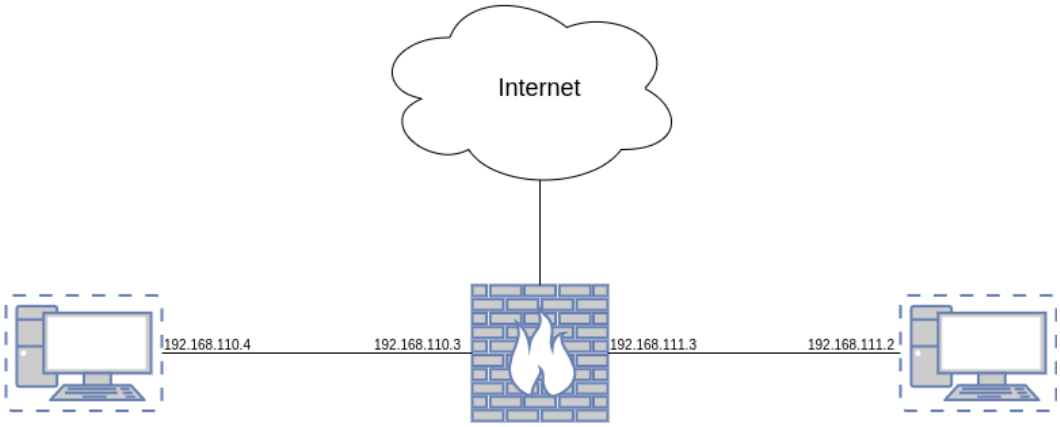


Рис. 1. Схема виртуального полигона

Правила для системы предотвращения вторжений не писались вручную, а были взяты из бесплатных репозиториев, возможность защиты при помощи самостоятельно написанных правил будет рассмотрена в следующих статьях. На момент проведения эксперимента базы обновлялись 20.12.2024. В результате вложений в поля протокола IPv4 была построена следующая таблица. Стоит отметить, что поскольку трафик проходил через сетевое оборудование, до момента попадания на систему предотвращения вторжений Snort, часть па-

кетов была отброшена потому, что сетевое оборудование считает пакет искаженным и отбрасывает его, следовательно такие поля не пригодны для стеганографических вложений и помечены в таблице, как «не пригодные». Подробное описание полей протокола IPv4 и пригодность их для использования в качестве стегоконтейнера можно найти в [7-8].

Как видно из таблицы, система предотвращения вторжений со стандартным набором правил не может детектировать и предотвратить большинство методов передачи сетевой стеганографии, что говорит нам о том, что необходима разработка собственных методов для обнаружения сетевой стеганографии, что требует большое количество человеко-часов, поскольку в современной сети интернет используются сотни сетевых протоколов, со своими полями, а это в свою очередь тысячи разных полей.

Однако, можно отметить, что при необходимости часть методов возможно заблокировать при помощи написаний собственных правил для работы IPS системы. К примеру, мы можем написать правило для пропуска только ICMP, TCP и UDP пакетов, тем самым сделав невозможным передачу информации в поле protocol, но это все еще оставляет злоумышленникам огромное пространство для использования других полей и методов.

ТАБЛИЦА 1. Обнаружение полей протокола IPv4 системой обнаружения вторжений

Название поля	Обнаружение системой предотвращения вторжений	Комментарии
Version (Версия)	-	Отбрасывается до начала проверки, следовательно не пригодно для передачи
IHL (длинна заголовка)	-	Отбрасывается до начала проверки, следовательно не пригодно для передачи
DSCP	Не обнаруживается	Пригодно к использованию
ECN	Не обнаруживается	Может быть изменено на пути следования, если ус-во работает с данным полем. Пригодно к использованию в сетях, в которых известны все сетевые устройства, через которые будет проходить трафик с вложениями
LEN	Не обнаруживается	Не обнаруживается, если помещать в поле Data столько бит, сколько прописано в поле LEN – длинна заголовка
Identification	Не обнаруживается	-

Название поля	Обнаружение системой предотвращения вторжений	Комментарии
flags	Не обнаруживается	-
Fragment Offset	Обнаруживается	Обнаруживается в случае, если не стоит флаг фрагментации
TTL	Не обнаруживается	Использование возможно только при знании всех маршрутов и топологии сети, высокая сложность реализации в крупных сетях.
Protocol	Не обнаруживается	-
Header Checksum	-	Отбрасывается до начала проверки, следовательно не пригодно для передачи
Source Address	Не обнаруживается	-
Dest address	Не обнаруживается	При изменении данного поля возможна передача только через пассивные устройства по прямому каналу
Options	-	Отбрасывается до начала проверки, следовательно не пригодно для передачи

Системы обнаружения и предотвращения вторжений, со стандартным набором правил, не способны детектировать сетевую стеганографию в пакетах протокола *IPv4*, который является самым распространенным протоколом в сети интернет, поэтому дальнейшие исследование не имеет смысла. Также существует возможность написания собственных правил, что может позволить детектировать стеганографию в некоторых полях, поэтому необходимо провести дополнительные исследования, с целью возможности защиты сети от сетевой стеганографии при помощи написанных правил. Для детектирования и предотвращения стеганографии в сетях необходима разработка собственных механизмов и программ. Например, можно использовать искусственный интеллект и машинное обучение, как описано в [9,10,11,12].

Список используемых источников

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

2. Коржик В. И., Красов А. В. Цифровая стеганография: учебник М.: КноРус, 2023. 324 с.

3. Волкогонов В. Н., Гетьман Е. М., Салита А. С. Сокрытие информации в протоколах RTP, RTCP // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021, С. 183-188.

4. Волкогонов В. Н., Гетьман Е. М., Салита А. С. Методы и способы создания стеганографических вложений в сетевых пакетах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2021, С. 178-183.

5. Бражук А. Утилита scapy. Основы конструирования сетевых пакетов |// Системный администратор. 2011. № 10. С. 66-69.

6. Власенко В. Р., Рубин В. А. Тестирование компьютерных сетей при помощи утилиты scapy. // Международный научный журнал № 10-1, 2016, С. 105-107.

7. Салита А. С., Красов А. В. Выявление полей заголовка протокола IPv4 пригодных для стеганографических вложений. // Региональная информатика-2020 РИ-2020 Материалы XXII Санкт-Петербургской Международной конференции, 2020, С. 304-3056.

8. Smolarczyk M., Szczypiorski K., Pawluk J. Multilayer detection of network steganography // Electronics. vol. 9. № 12, 2020 pp. 1–14. DOI: 10.3390/electronics9122128.

9. Красов А. В., Паскидов Н. В., Салита А. С. Использование методов машинного обучения при выявлении сетевой стеганографии // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки, 2022, С. 50-53

10. An approach for stego-insider detection based on a hybrid nosql database / I. Kotenko, K. Izrailov, A. Krasov, I. Ushakov // Journal of Sensor and Actuator Networks. 2021. Vol. 10, № 2. DOI 10.3390/jsan10020025.

11. Detection of stego-insiders in corporate networks based on a hybrid NoSQL database model / I. Kotenko, A. Krasov, I. Ushakov, K. Izrailov // ACM International Conference Proceeding Series: 4, St. Petersburg, 26–27 ноября 2020 года. St. Petersburg, 2020. P. 3442612. DOI 10.1145/3440749.3442612.

12. Красов А. В. Метод обнаружения сетевой стеганографии на основе машинного обучения / А. В. Красов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 3. С. 100-108. DOI: 10.37882/2223-2966.2022.03.17

NETWORK STEGANOGRAPHY DETECTION WITH SNORT INTRUSION PREVENTION SYSTEM

Krasov A.V.,
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper considers the possibility of detecting network steganography using an intrusion detection system, with standard rules. As an intrusion detection system was taken Snort intrusion detection system, distributed freely. For the construction of steganographic channels was used software utility Scapy, with which it is possible to collect and send network packets.

Key words: *Network protocols, transport protocols, network analysis, network security, steganography*

УДК 004.75
ГРНТИ 20.53.15

АНАЛИЗ ВОЗМОЖНОСТИ ВСТРАИВАНИЯ СООБЩЕНИЙ В СТРУКТУРЫ ДАННЫХ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ

Д. В. Кушнир

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

Появление и стремительное развитие систем, основанных на блокчейнах и других технологиях распределенного реестра, привели к изменениям во многих сферах и возникновению новых направлений в обработке, распространении и хранении данных. Основным востребованным свойством является возможность обеспечение доверия к данным, которые размещены в реестрах. Важным является обеспечение доверия, опирающегося на свойства криптографических преобразований и реализованном методе обеспечения консенсуса в соответствующем реестре. Одно из востребованных направлений применения распределенных реестров является возможность сохранения в них произвольной информации открытой или зашифрованной. В некоторых случаях эта информация может быть встроена в структуры данных блокчейнов скрытно и неявно.

встраивание сообщений; блокчейн; распределенный реестр; хеш; coinbase; транзакции

С самого возникновения распределенных реестров на основе блокчейна они стали использоваться для хранения произвольной информации. Если сама идея блокчейна первой криптовалюты заключалась в записи в распределенный реестр информации о совершаемых транзакциях, то практическое использование оказалось значительно шире. Биткоин, и связанный с ним блокчейн, стал использоваться в качестве свободной платформы, не подверженной внешнему регулированию [1, 2]. Помимо обмена цифровой валюты в глобальном масштабе, биткоин также предоставляет возможность размещать информацию, которая не может быть подвергнута цензуре или отзыву и будет постоянно доступна (до тех пор, пока существует биткоин и к нему существует доступ). Методы размещения информации в блокчейне освещены в целом ряде работ, как научно-популярных [3, 4], так и исследовательских [2, 5]. Так, в работе [7] выполнен весьма подробный анализ некоторых подходов к размещению данных, но обширность темы и активное развитие наиболее успешных распределенных реестров требует дальнейшего исследования в данной области.

Причины, по которой существует интерес к размещению информации в блокчейне, связаны с теми свойствами, которые предоставляют реестры

криптовалют. Основными особенностями являются следующие свойства блокчейна:

– репликация и синхронизация данных у всех участников;
– совместное использование данных;
– отсутствие центрального администрирования;
– использование одноранговой, децентрализованной сети;
– отработанные алгоритмы консенсуса для обеспечения доверия к данным;
– запись данных требует затраты значительного количества каких-либо ресурсов, например, вычислительных;
– записанную в реестр информацию никто из участников не может изменить или удалить.

Блокчейн криптовалют, например, биткоина или эфириума, не предназначен для хранения большого объема данных. Прямых инструментов для этого не предусмотрено. Обычно рассматривается размещение самой информации в собственных базах владельца информации или в каком-либо облачном сервисе, а уже хеш этих данных сохраняется в распределенном реестре. Однако такой подход приводит к потере части преимуществ блокчейна. Если необходимо децентрализованное решение для хранения данных, то непосредственно данные могут быть размещены на других децентрализованных решениях, например, IPFS (InterPlanetary File System), Swarm или Arweave с аналогичным помещением в блокчейн только хеша хранимых данных [7].

В реестре криптовалют могут быть записаны любые данные, но это требует больших накладных расходов. Большой набор данных будет рассылаться по всей пиринговой, одноранговой сети на этапе подготовки данных для включения в блоки, затем, уже сформированные блоки, будут передаваться всем участникам сети и записываться в локальные копии реестра на узлах сети. Однако, хранение в доверенном реестре только хеша данных приводит к потере ряда свойств, которые привели к размещению хеша данных в реестре, а именно, доверие к решению и его доступность. Переход на другие децентрализованные решения пока не может обеспечить такого же уровня надежности этих характеристик.

Требование надежности и доступности приводит к необходимости встраивания сообщений в сам блокчейн. Некоторый объем информации может быть встроен штатным образом в те или иные распределенные реестры. Однако, для размещения больших объемов данных непосредственно в блокчейне распределенные реестры не предназначены, так что встраивание происходит в служебную информацию распределенных реестров. Наиболее до-

веренным реестром в настоящее время является реестр биткоина, вероятность подмены данных в нем или его исчезновение практически невероятны, в отличии от многих других существующих реестров.

Необходимо обратить внимание, что те свойства, которые предоставляет хранение информации в блокчейне, например, такие как сложность определения отправителя сообщения, невозможность определения получателя сообщения, невозможность внесения изменений или удаления размещенной информации имеет некоторые общие черты со стеганографией [8, 9].

Существуют некоторые негативные аспекты вставки данных непосредственно в блокчейн. Одна из главных проблем связана с огромным размером реестра, копии которого хранятся каждым узлом сети, что создает определенные трудности доступности данных, масштабируемости и удобства использования рассматриваемых распределенных реестров. Кроме того, добавление данных блоками в блокчейн создает дополнительные сложности при встраивании сообщений, из-за ограничений на размер блоков и транзакций напрямую или опосредованно [10].

Одним из методов размещения данных, который можно наблюдать в самом первом блоке биткоина, предполагает использование первой транзакции в блоке – coinbase транзакции, переводящей средства создателю блока. Coinbase транзакция не имеет входа (средства переводятся из ниоткуда), но синтаксически ничем не отличается от обычной и поле входа может произвольно заполняться (100 байт). Данная позиция традиционная для записи данных создателями блоков. Самый первый пример размещения сообщения в coinbase транзакции выполнен создателем криптовалюты bitcoin [2] см. рис. 1.

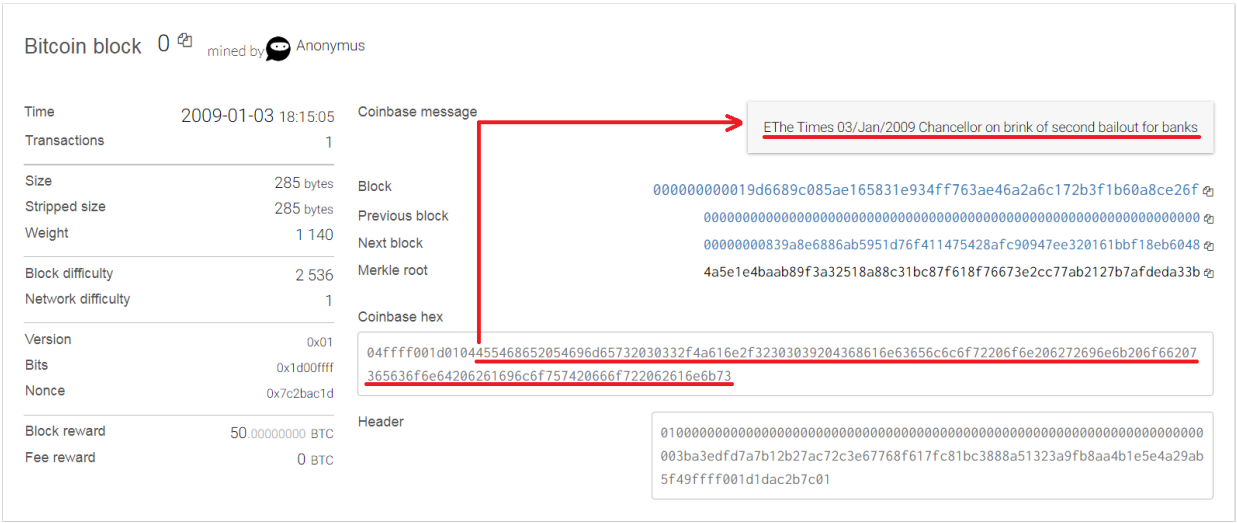


Рис. 1. Информация в coinbase транзакциях. Пример сообщения в генезис блоке биткоина (EThe Times 03/Jan/2009 Chancellor on brink of second bailout for banks)

Просмотреть созданные сообщения могут помочь как некоторые эксплореры блокчейна, один из которых представлен по ссылке выше, так и отдельные решения, например, ресурсы перевода ASCII набора символов в шестнадцатеричные последовательности [11]. Кроме того, так как coinbase транзакция может содержать и множество выходов, каждый адрес такого выхода может быть не реальным адресом, а преобразованным сообщением.

Необходимо иметь в виду, что создавать coinbase транзакции могут только создатели блоков (майнеры), т.е. ограниченное число участников. Майнеры также имеют и другие дополнительные возможности по встраиванию сообщений, по сравнению с обычными участниками. Так майнер может скрывать сообщения, варьируя порядок расположения транзакций в блоке или метку времени создания блока (хотя и в очень ограниченных пределах). Другим подходом для майнера является использование перебираемого параметра nonce (number that can only be used once). Это значение перебирается при формировании блока и будет записано в результирующий блок. Обычно значения перебирается с «0» приращением на единицу, однако нет ограничений на порядок перебора. Можно перебирать сообщения в шестнадцатеричной форме и потенциально обеспечивать вложение сообщения длиной до 32 бит. Важно отметить, что для формирования блока перебирается не только параметр nonce, но и некоторые биты в поле заголовка блока version.

Существуют отдельные исследования значений nonce на поиск отклонений от ожидаемого закона распределения результирующих значений данного параметра [12].

Рассмотрим методы встраивания, которыми могут воспользоваться любые участники, эксплуатирующие особенности формирования адресов в блокчейне и методов формирования транзакций и соответствующих скриптов [2, 13, 14].

Метод на основе P2PKH (Pay-to-Public-Key-Hash). Транзакция производится с указанием биткоин-адреса получателя, но вместо реального адреса используется преобразованный алгоритмом base58 открытый или предварительно зашифрованный текст. Таким образом, возможно размещение до 20 байт на вывод транзакции. В одной транзакции возможно несколько выходов. Для майнера транзакции с такими выходами ничем не отличаются от обычных. Так как невозможно выполнять транзакции с нулевыми переводами, то средства, переводимые на такие «адреса», будут безвозвратно потеряны.

Метод P2PK (Pay To Public Key). Транзакция производится с указанием открытого ключа, а не адреса. Возможно встраивание до 65 байт на один выход транзакции, возможность таких транзакций присутствует в ПО биткоина изначально и поддерживается до сих пор. В начальных блоках биткоина даже присутствуют транзакции данного типа. Однако важным недостатком метода является возможный отказ от поддержки такого типа транзакций в будущих версиях блокчейна. Кроме того, такие транзакции привлекают внимание и их могут отказаться включать в блоки.

Метод P2MS (Pay To Multisig). Транзакция производится с указанием нескольких открытых ключей. Для последующей траты средств требуется предъявить один или несколько из них. Метод предоставляет возможность встраивания до 20 байт на ключ. Существуют определенные требования к таким транзакциям, что приводит к большим финансовым затратам на их проведение.

Метод P2SH (Pay-to-Script-Hash). Транзакция производится с указанием хеша скрипта. Для возможности потратить данные средства необходимо предъявлять ключи для управления скриптом выкупа (redeem script). Вместо самого скрипта входа/предшествующего выхода или его части записываем встраиваемое сообщение. Потенциально можно встроить до 1529 байт или объединить несколько транзакций с итоговой возможностью встроить до 100Кб при отказе от полного подписывания, что создает возможность подделки.

Востребованность биткоина и необходимость расширения масштабируемости и функционала привели к новым видам транзакций и скриптам в блокчейне, которые предлагают и свои особенности добавления сообщений, такие как: P2WPKH, P2WSH и P2TR.

Метод OP_RETURN. Специальный способ пометки выхода транзакции, как не валидного. Позволяет разместить 80 байт. Очевидным образом воспринимается как место для вставки сообщения. Данный выход транзакции может игнорироваться (не сохраняться) некоторыми узлами, после использования реальных выходов. Блокчейн сообщество считает безответственным использовать данную опцию для сохранения произвольных данных, однако это значительно лучше, с точки зрения производительности биткоина, чем задействование выходов, которые неотличимы от настоящих.

Менее очевидным способом записи информации в блокчейн является ее размещение в виде суммы транзакции [6]. Сумма транзакции может принимать значение с точностью до 0.00000001 BTC. Используя код Фано,

можно разместить некоторое количество символов в сумме транзакции. В настоящее время для блокчейна сети биткоин метод экзотический, так как для размещения даже нескольких символов придется использовать значительную сумму для перевода, что мало кто сможет себе позволить, так как мало кто будет обладать необходимой суммой для размещения значительного по количеству символов сообщения. Создание фиктивных переводов, самому себе, возможно, но в настоящее время и они приведут к потерям средств из-за необходимости платить комиссию за включение необходимой транзакции в блокчейн. Кроме того, необходимо учитывать, что в некоторых случаях могут быть установлены ограничения на минимальную сумму транзакции, например, в размере 0,0000546 BTC для защиты от мошеннических транзакций [15].

Более сложным, и несколько менее очевидным способом размещения сообщения, является встраивание сообщения в часть адреса отправителя/получателя. Речь идет о сообщениях в адресах, с которых и на которые переводятся средства (даже если они используются впоследствии). Пользователь может создавать ключи, перебирая адреса, пока не будет сформирован адрес с нужным набором шестнадцатеричных символов на нужных местах. Эти позиции не обязательно должны быть начальными символами в адресе. Очевидно, что составить нужный адрес полный длины не представляется возможным, но некоторое количество, 6-8, шестнадцатеричных символов вполне может быть подобрано пользователем без значительных вычислительных затрат. Так как адрес в данном случае является реальным, то инициатор (или получатель) транзакции не теряет дополнительных средств на выполнение такого способа записи сообщения. Одним из примеров использования такого метода размещения сообщения с рекламными целями компанией Laxo Trade является транзакция в блоке биткоина с номером 319464. В транзакции 149 имеется один вход с адресом 1LaxoTrQy51LnB289VmoSAgN6J6UrJbfL9 и 56 выходов, существуют и другие аналогичные случаи использования адреса в рекламных целях. Кроме уже упомянутой фирмы, данную идею использовала фирма BestMixer, создав адрес 1BestMixVhna91Mk… [13]

Сообщения в открытом ключе. При создании транзакции в скрипте подписи [2] указывается открытый ключ, связанный с адресом, с которого производится перевод средств. Данный ключ, также может содержать сообщение из нескольких символов, составляющих часть ключа, полученных перебором при формировании ключевой пары.

Другими возможными, хотя и довольно неочевидными способами встраивания данных может быть варьирование количества входов и выходов транзакции, а также подбор необходимого порядка расположения адресов входов и/или выходов в транзакции.

Как следует из ранее рассмотренных методов, наибольшие возможности предоставляет размещение данных через запись в скрипт без использования подписи, хотя он и не обеспечивает невозможность подмены данных. Из современных форматов транзакций наибольшие возможности у скриптов типа P2WSH и P2TR. Если требуется полная аутентификация данных, то может быть использован метод записи в скрипт уже с подписью, хотя и чуть менее эффективный по объему встраивания на размер транзакции. Вместе с тем, наиболее очевидным и штатным методом является размещение данных в блокчейн на основе опции OP_RETURN, однако он может не подходить для срытого размещения информации. В любом случае необходимо учитывать и другие методы встраивания, и возможность одновременного задействования нескольких методов, особенно при необходимости скрытного сохранения данных.

Анализ методов встраивания сообщений в блокчейн, на примере блокчейна биткоина, показывает некоторые общие закономерности и особенности хранения данных в распределенных реестрах. С одной стороны, непосредственное хранение больших объемов информации в самом блокчейне сопряжено со значительными трудностями и, кроме того, вызывает нарекания со стороны блокчейн сообщества. С другой стороны, технически такая возможность существует, но требует определенных затрат средств, что, судя по всему, оправдано для тех, кто считает необходимым разместить информацию в конкретном распределенном реестре. Исследование формулирует те свойства, которыми обладает размещение данных в блокчейне и предлагает обратить внимание на относительно экзотические методы встраивания сообщений, которые обычно не упоминаются в литературе, например, такой как порядок перечисления входов и/или выходов транзакций или порядок самих транзакций при их размещении в блоках. Для размещенной информации невозможно определить получателя сообщения. В большинстве случаев трудно определить отправителя сообщения. После размещения информация не может быть удалена без взлома самого реестра. Ряд методов встраивания данных предполагает возможные подозрения в попытках разместить информацию (возможна «цензура» со стороны создателя блоков), например, при использовании опции OP_RETURN. Необходимо добавить, что. хотя в не-

которых случаях добавляемые в блокчейн данные размещаются в открытом виде и могут быть легко обнаружены, существуют методы, в которых встраивание информации не может быть обнаружено при использовании соответствующих криптографических преобразованиях и способах размещения информации. Дальнейшие исследования в этом направлении также необходимы для обнаружения дополнительных методов размещения информации в распределенных реестрах и постоянного внесения изменений в алгоритмы работы конкретных блокчейнов.

Список используемых источников

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system //Decentralized Business Review. 2008. С. 21260.

2. Greg Walker. Learn me a bitcoin URL: https://learnmeabitcoin.com/ (дата обращения: 20.01.2025)

3. Скрытые сюрпризы в блокчейне Биткоин и то, как они хранятся: Нельсон Мандела, Wikileaks, фотографии и программное обеспечение Python. URL: http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html (дата обращения: 21.12.2024).

4. Биткоин вместо эмодзи: как оставить сообщение в блокчейне первой криптовалюты URL: https://data-to-data.ru/novosti-kriptovalyuty/bitkoin-vmesto-emodzi-kak-ostavit-soobshhenie-v-blokchejne-pervoj-kriptovalyuty.html (дата обращения: 26.11.2024)

5. Sleiman M. D. Bitcoin message: Data insertion on a proof-of-work cryptocurrency system/ M. D. Sleiman, A. P. Lauf, R. Yampolskiy //2015 International Conference on Cyberworlds (CW). IEEE, 2015. С. 332-336.

6. Sward A. Data insertion in bitcoin's blockchain/A. Sward, I. Vecna, F. Stonedahl//Ledger. 2018. Т. 3.

7. Konashevych O. Data Insertion in Blockchain For Legal Purposes. How to Sign Contracts Using Blockchain //Electronic Modeling. 2019. С. 103-120.

8. Цифровая стеганография и цифровые водяные знаки. В. И. Коржик, К. А. Небаева, Е. Ю. Герлинг [и др.]; под ред. В. И. Коржика, Часть 1. Цифровая стеганография. Санкт-Петербург. 2016.

9. Цифровая стеганография и цифровые водяные знаки / [В. И. Коржик и др.]; под ред. В. И. Коржика. Часть 2. Цифровые водяные знаки. Санкт-Петербург. 2017.

10. Blockchain Size (MB). The total size of the blockchain minus database indexes in megabytes. URL: https://www.blockchain.com/en/charts/blocks-size/ (дата обращения: 30.05.2024).

11. Hex to ASCII Text Converter. URL: https://www.rapidtables.com/ convert/number/hex-to-ascii.html (дата обращения: 20.01.2025)

12. Giron A. A. Steganographic Analysis of Blockchains/ A. A. Giron, J. E. Martina, R. Custódio //Sensors. 2021. Т. 21. №. 12. С. 4078.

13. Bitcoin address Programming The Blockchain in C#. URL: https://programmingblockchain.gitbook.io/programmingblockchain/bitcoin_transfer/bitcoin_address (дата обращения: 20.01.2025).

14. Singhal B. Beginning Blockchain: A Beginner's guide to building Blockchain solutions/ B. Singhal, G. Dhameja, P.S. Panda Apress, 2018.

15. Prusty N. Building blockchain projects. Packt Publishing Ltd, 2017.

ANALYSIS OF THE POSSIBILITY OF EMBEDDING MESSAGES INTO DISTRIBUTED LEDGER DATA STRUCTURES

Kushnir D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The emergence and rapid development of systems based on blockchains and other distributed ledger technologies have led to changes in many areas and the emergence of new directions in the processing, distribution and storage of data. A key property in demand is the ability to provide trust in the data that is hosted in registries. It is important to ensure trust based on the properties of cryptographic transformations and the implemented method of ensuring consensus in the corresponding registry. One of the demanded applications of distributed registries is the possibility to store in them arbitrary information open or encrypted. In some cases, this information can be embedded in blockchain data structures implicitly and covertly.

Key words: *message embedding; blockchain; distributed ledger; hash; coinbase; transactions*

УДК 004.056
ГРНТИ 20.53.23

СЕРВИС ДЛЯ ГЕНЕРАЦИИ НАДЕЖНЫХ И ЗАПОМИНАЕМЫХ ПАРОЛЕЙ

О. С. Лаута, Н. А. Васильев, М. Д. Беседин, А. Ю. Копачев

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

Статья посвящена разработке сервиса для генерации надежных паролей на основе ключевых слов. Представлен анализ существующих решений и разработан собственный алгоритм, позволяющий генерировать сложные, но запоминаемые пароли.

генерация паролей, информационная безопасность, управление паролями, инновации, надежность, конфиденциальность

В современном цифровом мире защита персональных данных и конфиденциальной информации является критически важной задачей. С ростом числа онлайн-сервисов управление надежными паролями становится сложнее. Традиционные методы генерации и хранения паролей, такие как использование простых слов или ручное сохранение, больше не обеспечивают достаточный уровень безопасности.

Существующие менеджеры паролей, хотя и облегчают управление, имеют недостатки, такие как необходимость запоминания мастер-пароля и риски синхронизации. Егоров и др. [1] подчеркивают важность криптографической защиты данных, а Черников [2] рассматривает безопасность менеджеров паролей для мобильных устройств.

Разработка инновационных подходов к созданию и управлению паролями является актуальной задачей для повышения информационной безопасности и удобства пользователей. Целью данной работы является создание веб-сервиса “RYP”, который генерирует надежные и запоминаемые пароли на основе ключевых слов, обеспечивая простоту использования, высокий уровень безопасности и доступность с любого устройства.

Для достижения этой цели были решены следующие задачи:

– проанализированы существующие методы генерации и хранения паролей;

– разработан алгоритм генерации паролей на основе ключевых слов;
– реализован алгоритм в виде программы;
– проведен анализ преимуществ и недостатков разработанного решения по сравнению с существующими аналогами.

Исследование конкурентных решений

Проблема создания и управления паролями является ключевой в области информационной безопасности. Существующие подходы и их недостатки рассмотрены в таблице 1.

ТАБЛИЦА 1. Сравнение подходов хранения и создания паролей.

Метод	Описание	Достоинства	Недостатки
Словарный подход	Пароли создаются на основе запоминающихся слов или фраз	Легкость запоминания	Уязвимость для атак перебором или по словарю, если пароль недостаточно сложен
Аббревиатурный подход	Пароль формируется из первых букв слов запоминающейся фразы	Легкость запоминания	Ограниченное количество комбинаций, недостаточная уникальность
Генераторы случайных паролей	Используют сложные алгоритмы для создания случайных последовательностей символов	Надежность паролей	Трудность запоминания, необходимость использования менеджеров паролей
Ручное хранение	Запись паролей в блокнот, текстовый файл или на электронном носителе без шифрования	-	Крайне небезопасный метод, подвергающий пароли риску утечки
Менеджеры паролей	Специализированное ПО, позволяющее создавать, хранить и синхронизировать пароли	Надежность паролей, удобство управления паролями	Зависимость от мастер-пароля, необходимость установки ПО, риски синхронизации, уязвимость при использовании на общедоступных устройствах

На основании анализа вопросов безопасности менеджеров паролей были сформированы критерии к исправлению недостатков программного обеспечения [3].

Хотя менеджеры паролей обеспечивают более высокую безопасность, они также не лишены недостатков. В результате анализ существующих подходов показывает необходимость создания нового метода генерации и управления паролями, сочетающего высокую надежность, удобство запоминания и доступность с различных устройств.

Разработка сервиса “RYP”

Разработанный веб-сервис “RYP” представляет собой инновационный подход к генерации надежных паролей на основе ключевых слов, предоставляя пользователю возможность создавать уникальные и запоминаемые пароли, не требующие хранения.

Архитектура сервиса

Сервис “RYP” представляет собой веб-приложение, доступное с любого устройства, имеющего интернет-соединение, без необходимости установки дополнительного ПО. Архитектура приложения создана на основе современных стандартов [4].

Основные компоненты сервиса:

– интерфейс пользователя: веб-страница с полями для ввода ключевых слов (идентификатор, ключевое слово, специальная часть) и отображения сгенерированного пароля;
– алгоритм генерации ключа: компонент, преобразующий введенные пользователем ключевые слова в ключ для генерации пароля с использованием необратимых хеш-функций;
– алгоритм генерации пароля: компонент, генерирующий пароль на основе созданного ключа, обеспечивая его уникальность, надежность и соответствие заданным параметрам (длина, типы символов);
– защита от фишинга: логика, которая при включении доменного имени сайта в список ключевых слов, будет генерировать уникальный пароль для каждого доменного имени.

Архитектура сервиса представлена на рисунке 1.

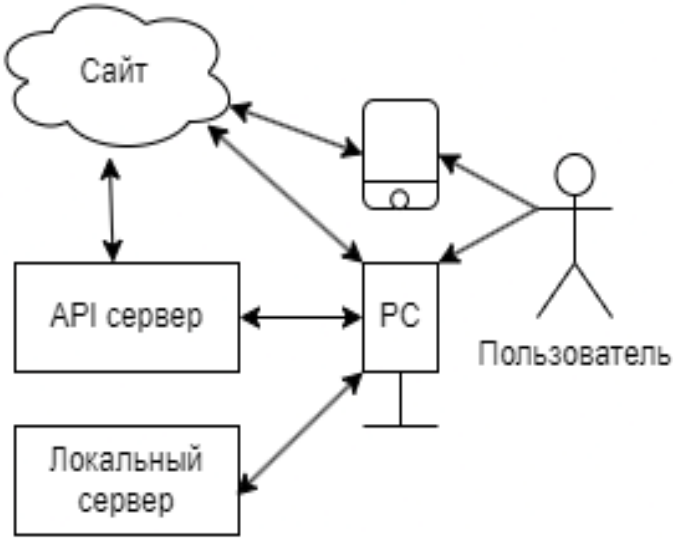


Рис. 1. Архитектура сервиса

Алгоритм генерации пароля

Алгоритм генерации пароля в сервисе “RYP” включает в себя следующие шаги:

– ввод данных: пользователь вводит три ключевых слова;
– идентификатор: постоянное значение, выбранное пользователем;
– ключевое слово: изменяемое значение, позволяющее менять набор паролей;
– специальная часть: ассоциация между пользователем и конкретным сайтом;
– создание ключа: введенные пользователем значения хэшируются (SHA-512), ключевые слова суммируются попарно, хэши объединяются и повторно хэшируются;
– генерация пароля: на основе ключа создается пароль с символами разных регистров, цифрами и специальными символами; используются два типа ключей: type_key (определяет тип символа) и password_key (определяет конкретный символ); эти ключи получаются из основного ключа путем хэширования и разделения на массивы;
– корректировка длины пароля: пароль приводится к требуемой длине путем деления ключей, применения операции XOR и преобразования массивов в символы. Были проанализированы алгоритмы хеширования и шифрования и на основе критериев к ним был создан алгоритм преобразования ключевых слов с помощью хеширования [5, 6]. Алгоритм создания пароля представлен на рисунке 2.

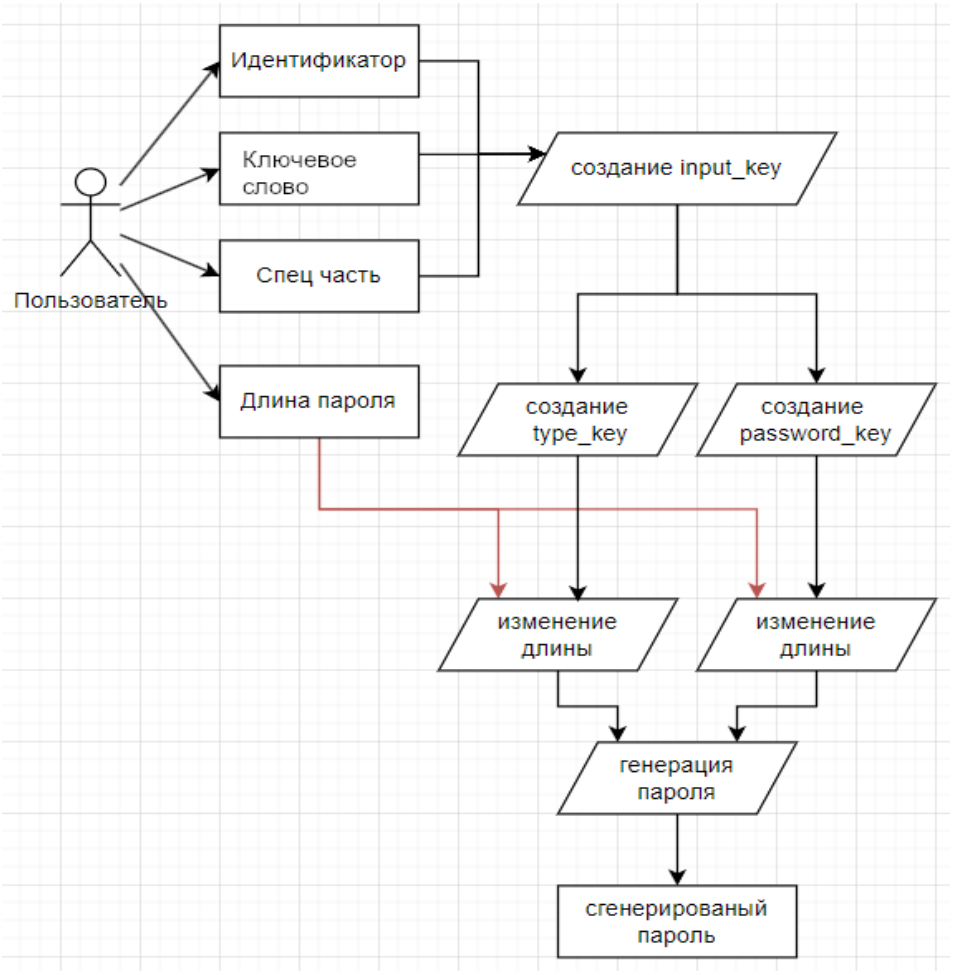


Рис. 2. Алгоритм преобразования ключевых слов в пароль

Конкурентные преимущества созданного сервиса “RYP”

– отсутствие хранения паролей: пароли не хранятся в базе данных или на устройстве пользователя, что исключает риск утечки;
– генерация запоминающихся паролей: пароли генерируются на основе ключевых слов, которые легко запомнить;
– высокая надежность: использование сложных криптографических алгоритмов обеспечивает высокую стойкость паролей к взлому;
– доступность с любого устройства: веб-интерфейс позволяет пользоваться сервисом с любого устройства, не зависимо от установленного ПО;
– кроссплатформенность: сервис работает в любом современном браузере;
– защита от фишинга: при включении доменного имени сайта в список ключевых слов, сервис будет генерировать уникальный пароль для каждого домена;
– возможность генерации мастер-пароля: пользователь может сгенерировать мастер-пароль на основе ключевых слов и использовать его в качестве идентификатора.

Потенциальные проблемы, с которыми может столкнутся сервис при развитии

– конкуренция: на рынке существуют другие решения для генерации и хранения паролей;
– переход на другие методы аутентификации: развитие технологий может привести к снижению актуальности паролей. Необходимость постоянного развития и адаптации к новым тенденциям.

Заключение

Сервис “RYP” предлагает инновационный подход к генерации и управлению паролями, сочетая словарный и аббревиатурный методы с криптографией, и не требует хранения паролей. Это делает его конкурентоспособным на рынке информационной безопасности. Веб-сервис “RYP” обеспечивает безопасное и удобное управление паролями, повышая защищенность от кибератак и способствуя созданию более безопасного цифрового мира.

Список используемых источников

1. Егоров Н. В., Сенько К. А., Сафарьян О. А. Программная разработка менеджера паролей с использованием криптографических алгоритмов защиты данных // Молодой исследователь Дона. 2022. № 5. С. 39–42.

2. Черников А. В. Рекомендации по разработке менеджеров паролей для ОС Андроид // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2021. № 4. С. 49–57.

3. Черников А. В. Одна из возможных реализаций модели менеджера паролей для ОС Андроид // Вестник Пермского университета. Серия: Математика. Механика. Информатика. 2022. № 1. С. 38–46.

4. Двуреченский И. О., Симонов И. Н., Гаев Л. В. Веб-приложения: основы, технологии и разработка // Инновационная наука. 2023. № 6. С. 35–37.

5. Зацепа А. И. Шифрование данных // StudNet. 2022. № 1. С. 344–350.

6. Москвин А. Д., Петросян Л. Э. Анализ современных алгоритмов шифрования данных // Инженерный вестник Дона. 2023. № 4. С. 1–14.

SERVICE FOR GENERATING RELIABLE AND MEMORABLE PASSWORDS

Lauta O., Vasiliev N., Besedin M., Kopachev A.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is dedicated to the development of a service for generating reliable passwords based on keywords. An analysis of existing solutions is presented, and a proprietary algorithm is developed, allowing for the generation of complex, yet memorable passwords.

Key words: *password generation, information security, password management, innovation, reliability, confidentiality*

УДК 004.056.5
ГРНТИ 81.93.29

АРХИТЕКТУРА СИСТЕМЫ НА ОСНОВЕ LLM-АГЕНТОВ ДЛЯ ЗАЩИТЫ УМНОГО ЗАВОДА

Д. С. Левшун, В. В. Лаврентьев

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Бурное развитие генеративных алгоритмов, включая большие языковые модели, повышает требования к безопасности и защите данных. Угрозы, связанные с созданием недостоверной информации, могут стать серьезной проблемой, приводя к дезинформации и распространению непроверенных новостей. В статье рассматривается архитектура системы на основе больших языковых моделей (LLM-агентов) для обеспечения безопасности Умного завода. Основное внимание уделяется применению LLM-агентов для мониторинга, анализа данных и выявления аномалий в реальном времени. Описаны ключевые компоненты системы, включая интеграцию с устройствами Интернета вещей и взаимодействие с операторами. Кроме того, авторы рассматривают возможность использования технологии "генерации с дополненной выборкой" (Retrieval-Augmented Generation, RAG) с целью реализации систем умного поиска в документации предприятия для создания помощника по настройке и отладке оборудования, а также обучения персонала. Авторы подробно описывают архитектуру решения по повышению защищенности Умного завода, а также представляют предварительные результаты экспериментов, которые подтверждают эффективность предложенного решения.

Интернет вещей, Умный завод, искусственный интеллект, уязвимости информационных систем, большие языковые модели, автоматизация тестирования

В современном мире приобретают все большую популярность решения, основанные на технологиях искусственного интеллекта: крупные компании используют программные продукты для подведения итогов встреч и анализа документов, а рядовые пользователи используют чат-ботов и голосовых ассистентов для анализа веб-страниц и генерации ответов на электронные письма. В качестве примера систем, реализующих искусственный интеллект, можно привести ChatGPT, разработанный компанией Open AI, и ее отечественные аналоги YandexGPT и GigaChat.

Однако за последнее время стало понятно, что индустрии недостаточно только больших языковых моделей. Для реализации по-настоящему сложных кейсов необходимо использовать более сложные архитектуры, такие, как мультиагентные системы [1] или RAG-пайплайны [2] (Retrieval-Augmented Generation).

Кроме того, не перестают развиваться и другие технологические сферы, такие как Интернет Вещей в целом и Умные дома, города, и заводы в частности [3]. Каждое из этих решений включает работу с огромным количеством информации: например, на Умном заводе есть необходимость ремонтировать оборудование, проводить обучение персонала – выполнять быстрый поиск по большому объему данных. Кроме того, внедрение большой языковой модели в работу Умного предприятия позволит существенно автоматизировать рутинные процессы, сократить трудозатраты и, как следствие, расходы на содержание предприятия [4].

В данной работе предлагаются следующие примеры внедрения решений на основе больших языковых моделей:

– управление оборудованием: голосовой помощник для включения, отключения и изменения параметров работы оборудования;
– обучение персонала: система поиска информации в технической документации оборудования и регламентах работ на основе RAG-пайплайна;
– ремонт и отладка оборудования: голосовой помощник для помощи техническому персоналу на основе RAG-пайплайна.

Ожидается, что внедрение больших языковых моделей позволит существенно оптимизировать существующие процессы и достичь следующих целей:

1. Снижение трудозатрат предприятия на рутинные операции:
   – поиск информации о работе оборудования;
   – устранение базовых неисправностей оборудования;
   – автоматизация рутинных процессов подготовки или отключения оборудования.
2. Создание интерфейса управления предприятием нового типа:
   – система контроля семантики запросов для оценки полномочий сотрудников выполнять различные операции;
   – защита от утечки чувствительных данных.

Принципиальная схема внедрения решений на базе больших языковых моделей в архитектуру Умного завода предполагает разработку мультиагентной системы. Это означает, что конечный пользователь не будет взаимодействовать непосредственно с большой языковой моделью, а будет выполнять запросы и общаться с так называемыми агентами [5].

Агенты, в свою очередь, будут воспринимать пользовательский запрос, будут способны взаимодействовать с окружающей средой для получения какой-либо информации, будут генерировать ответы на пользовательские

запросы с помощью большой языковой модели с учетом всех собранных данных. Такой подход позволит работать с большой языковой моделью в более сложном, чем “запрос-ответ” формате, например, получать от нее несколько вариантов ответа на один и тот же пользовательский запрос и выбирать лучший ответ (также при помощи большой языковой модели).

Важно, что предоставление пользователям новых интерфейсов для взаимодействия с системами предприятия с точки зрения информационной безопасности порождает потенциальные уязвимости [6]. Так, например, голосовой интерфейс для управления оборудованием может быть использован злоумышленником для выведения предприятия из строя, преднамеренного выпуска бракованной продукции, выполнения несанкционированных действий, в том числе краж.

Именно поэтому является актуальной задача фильтрации пользовательских запросов, поступающих в систему управления Умным заводом. Важно, что система фильтрации должна не просто запрещать определенные категории запросов, но и анализировать семантику входящих текстов, принимать решения, учитывая параметры окружения (например, текущее состояние оборудования или температуру в помещении). В частности, голосовой помощник по управлению предприятием не должен позволить отключить камеры наружного наблюдения и позволить одновременно открыть входную дверь, однако сама команда “открыть входную дверь” при включенных камерах и прочих корректных условиях должна быть выполнена.

Разработанная система фильтрации запросов называется LLM Security Proxy (см. рис. 1) и включает два основных модуля:

1. Модуль обфускации пользовательских запросов: программный код, маскирующий чувствительные данные в запросах.

2. Модуль фильтрации пользовательских запросов: программный код, анализирующий пользовательский запрос с помощью LLM и запрещающий выполнение действий на предприятии в случае, если запрос вредоносный.

Для разработки тестирующей системы был выбран технологический стек: Kotlin [7], SpringBoot [8], PostgreSQL [9].

Была проведена серия предварительных экспериментов с использованием предложенного прототипа и самостоятельно разработанного инструмента для тестирования больших языковых моделей [10], которые показали, что рассматриваемая архитектура позволяет действительно сократить количество вредоносных запросов, поступающих в систему управления Умным предприятием (см. рис. 2). Однако были выявленные ограничения в каче-

стве работы системы в условиях Интернета вещей: использование облачных больших языковых моделей зачастую недоступно, а для локальных моделей есть лишь ограниченные вычислительные ресурсы.

В качестве направления дальнейшей работы выбрано исследование языковых моделей с малым (до 2-ух миллиардов) числом параметров [11], которые можно запустить без использования видеокарт на ограниченных вычислительных ресурсах. Такие языковые модели могут позволить автоматизировать процессы Умного предприятия без существенного удорожания инфраструктуры. Авторы планируют затронуть вопрос дообучения [12] языковых моделей малых размерностей для работы с запросами, связанными с информационной безопасностью.

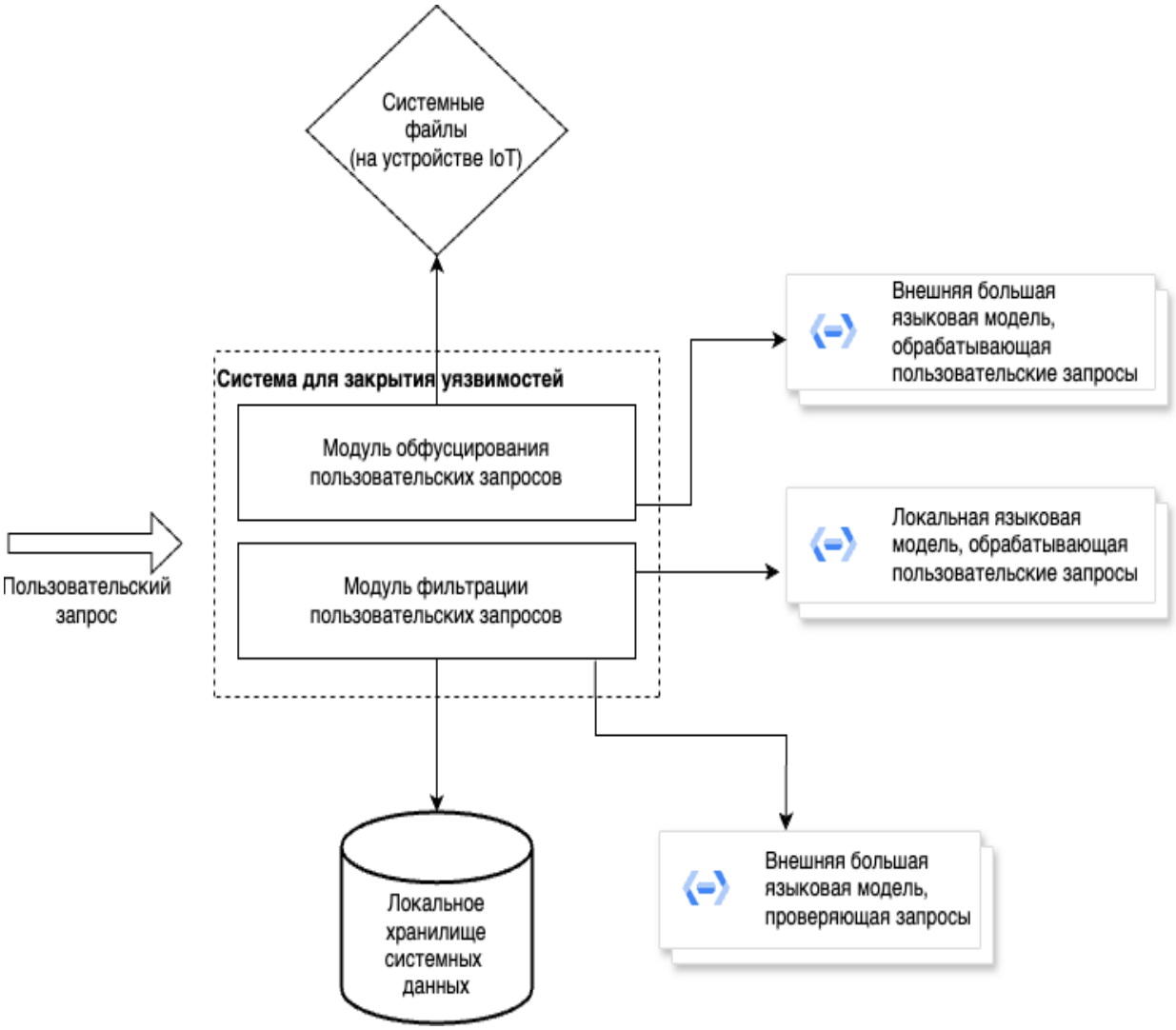


Рис. 1. Архитектура прототипа системы для защиты системы управления Умным заводом

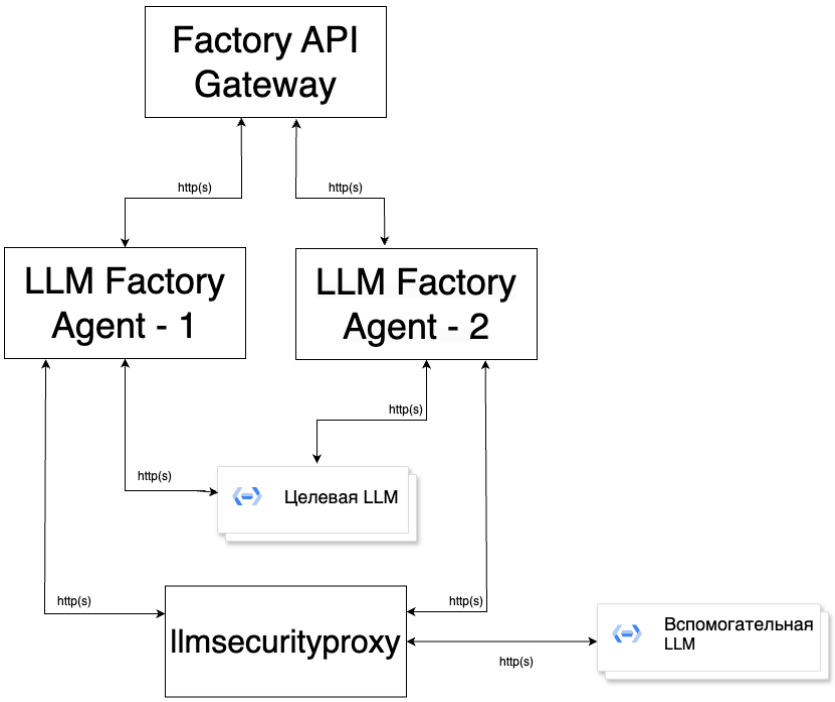


Рис. 2. Архитектура прототипа системы автоматизации управления предприятием с помощью больших языковых моделей

Ожидается, что внедрение дообученных языковых моделей позволит реализовать проверку запросов к системе Умного предприятия на потенциальную вредоносность быстро и при этом без существенных затрат на вычислительные ресурсы. В свою очередь, это позволит повысить защищенность решений на основе Интернета вещей на основе решения, которое будет доступным для внедрения на уровне предприятий.

Список использованных источников

1. Li X., Wang S., Zeng S., Wu Y., Yang Y. A survey on LLM-based multi-agent systems: workflow, infrastructure, and challenges // Vicinagearth. 2024. Vol. 1. № 1. P. 9.

2. What is RAG (Retrieval-Augmented Generation)? // [Электронный ресурс]. Режим доступа: https://aws.amazon.com/what-is/retrieval-augmented-generation/ (дата обращения: 29.03.2024).

3. Levshun D., Chechulin A., Kotenko I., Chevalier Y. Design and verification methodology for secure and distributed cyber-physical systems // Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2019. P. 1-5.

4. Старостина Т. Г., Щукин В. С. Состав и структура расходов предприятия // Теория и практика современной науки. 2017. №. 1 (19). С. 888–891.

5. Лаврентьев В. В., Левшун Д. С. Архитектура системы для автоматизации выявления уязвимостей больших языковых моделей // XIII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2024). Санкт-Петербург, Россия, 27–28 февраля, 2024. Т. 1. С. 539–543.

6. Xi Z., Chen W., Guo X., He W., Ding Y., Hong B., Gui T. The rise and potential of large language model-based agents: A survey // Science China Information Sciences. 2025. Vol. 68. № 2. P. 121101.

7. Официальный сайт Kotlin – языка программирования, разработанного компанией JetBrains // [Электронный ресурс]. Режим доступа: https://kotlinlang.org/ (дата обращения: 29.03.2024).

8. Официальная документация фреймворка Spring // [Электронный ресурс]. Режим доступа: https://spring.io/projects/spring-boot (дата обращения: 29.03.2024).

9. Официальный сайт проекта PostgreSQL // [Электронный ресурс]. Режим доступа: https://www.postgresql.org/ (дата обращения: 29.03.2024).

10. Vladimir Lavrentiev, Dmitry Levshun. LLMSecurityTester: A Tool for Detection of Vulnerabilities in LLM-based Chatbots. Proceedings of the 33rd Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2025). P. 608–615. DOI: 10.1109/PDP66500.2025.00091.

11. Allal L. B., Lozhkov A., Bakouch E., Blazquez G. M., Penedo G., Tunstall L., Wolf T. SmolLM2: When Smol Goes Big Data-Centric Training of a Small Language Model // arXiv preprint. 2025. DOI: arXiv:2502.02737.

12. Xia Y., Kim J., Chen Y., Ye H., Kundu S., Hao C. C., Talati N. Understanding the performance and estimating the cost of LLM fine-tuning // Proceedings of the IEEE International Symposium on Workload Characterization (IISWC). IEEE, 2024. P. 210-223.

ARCHITECTURE OF A SYSTEM BASED ON LLM-AGENTS TO PROTECT A SMART FACTORY

Levshun D., Lavrentyev V.
St. Petersburg Federal Research Center of the Russian Academy of Sciences

The rapid development of generative algorithms, including large language models, increases the requirements for data security and protection. Threats associated with the creation of unreliable information can become a serious problem, leading to disinformation and the spread of unverified news. The report considers the architecture of a system based on large language models (LLM agents) to ensure the security of a Smart Factory. The main focus is on the use of LLM agents for monitoring, data analysis and anomaly detection in real time. The key components of the system are described, including integration with Internet of Things devices and interaction with operators. In addition, the authors consider the possibility of using the "generation with augmented selection" (Retrieval-Augmented Generation, RAG) technology to implement smart search systems in enterprise documentation to create an assistant for setting up and debugging equipment, as well as training personnel. The authors describe in detail the architecture of the solution to improve the security of the Smart Factory, and also present preliminary results of experiments that confirm the effectiveness of the proposed solution.

Key words: *Internet of Things, Smart Factory, artificial intelligence, vulnerabilities of information systems, large language models, automation of testing*

УДК 004.056.5
ГРНТИ 81.93.29

МЕТОДЫ ОТРАВЛЕНИЯ ДАННЫХ НА ОСНОВЕ ИЗОБРАЖЕНИЙ В ФЕДЕРАТИВНОМ ОБУЧЕНИИ: АНАЛИЗ И ПОДХОДЫ К ЗАЩИТЕ

Д. С. Левшун, К. И. Хушея

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

В данной работе рассматриваются методы отравления данных для федеративного обучения в задачах, связанных с обработкой изображений. Федеративное обучение позволяет обучать модели, используя данные, хранящиеся на устройствах пользователей, что создает уникальные вызовы для безопасности и конфиденциальности. В работе анализируются различные методы отравления данных, которые могут использовать злоумышленники для манипуляции обучением моделей, ухудшая их производительность или внедряя предвзятости. Обсуждаются существующие подходы к защите от таких атак. Подчеркивается важность разработки устойчивых к атакам систем и необходимость дальнейших исследований в данной области для обеспечения безопасности федеративного обучения.

информационная безопасность, федеративное обучение, отравление данных, защита данных, машинное обучение, генеративный и базовый триггеры

В настоящее время федеративное обучение (ФО) является современным подходом к машинному обучению, позволяющий моделям обучаться на распределенных данных, не передавая их на центральный сервер [1]. Данный метод обеспечивает конфиденциальность и безопасность данных, что особенно важно в условиях строгих требований к защите персональной информации [2].

ФО применяется в различных областях, например, для улучшения персонализированных рекомендаций, распознавания речи и улучшения качества сервисов без передачи личных данных на центральные серверы. В области медицинских исследований и диагностики, где важна конфиденциальность данных пациентов, ФО позволяет обучать модели на медицинских изображениях и других данных без необходимости передавать их в централизованные хранилища. В банках и финансовых учреждениях ФО используется для улучшения алгоритмов кредитных рейтингов, обнаружения мошенничества и прогнозирования финансовых трендов, сохраняя при этом безопасность пользовательских данных [3]. Также ФО применяют в Умных городах для анализа данных о движении, энергопотреблении и других аспектах городской жизни, обеспечивая защиту конфиденциальности граждан [4].

Однако, несмотря на преимущества, ФО подвержено ряду угроз, одной из которых является атака с отравлением данных (Data Poisoning Attack) [5]. В частности, манипуляции с изображениями в рамках ФО представляют серьезную проблему, так как отравление данных может привести к искажению результатов модели, снижению ее точности и повышению уязвимости [6]. Один из методов реализации таких атак – внедрение вредоносных данных с использованием файлов изображений. Злоумышленники могут применять различные техники, включая стеганографию, манипуляцию метаданными или встраивание скрытых скриптов, чтобы обходить механизмы безопасности. Такие атаки способны существенно снизить точность модели или внести критические ошибки, особенно в системах компьютерного зрения, используемых в автономных автомобилях и медицинской диагностике [7].

На сегодняшний день основными направлениями исследований в области отравления данных в ФО являются процессы по обнаружению атак (разработка алгоритмов для выявления отравленных данных на этапе обучения), по повышению устойчивости моделей к атакам, по учету аномальных патернов в моделях, по разработке кросс-обучений (совместная работа участников для улучшения безопасности и защиты данных) [8]. Существуют трудности в области отравления данных в ФО, которые заключаются в сложности выявления признаков отравленных данных на распределенных устройствах и в разработке методов защиты без потери производительности. Также затруднением является сохранение баланса между безопасностью моделей и защитой данных пользователей, т. к. отсутствуют унифицированные решения для защиты от атак, и наличие высоких вычислительных затрат на защиту и масштабирование. Перечисленные проблемы требуют дальнейших исследований для повышения безопасности ФО.

В работе [9] представлен сравнительный анализ триггеров в контексте атак на модели машинного обучения. Авторы исследуют влияние различных типов триггеров на модель, оценивая их эффективность с точки зрения успешности атаки (ASR – Attack Success Rate).

В частности, в исследовании анализируются два типа триггеров: генеративный и базовый. Генеративный триггер, разработанный на основе обучения генеративной модели с использованием данных целевого класса, демонстрирует высокий ASR (70.85 %), что свидетельствует о его способности эффективно манипулировать классификацией модели и вызывать сбои в ее работе. В отличие от него, базовые триггеры (например, случайные изображения или шум) показали ASR 0.0 %, что указывает на их полную неэффективность в данном типе атак.

Основным результатом исследования является подтверждение того, что сложная структура генеративного триггера делает его более эффективным инструментом для атак, тогда как простые базовые триггеры не оказывают значимого влияния на модель. Такой вывод подкреплен экспериментальными данными, представленными в работе, что подчеркивает важность выбора подходящих триггеров при проведении атак на модели машинного обучения.

Применение данных целевого класса, а также сравнительный анализ таблицы 1 подтверждает, что генеративный триггер значительно более эффективен для атак на модели, чем базовые триггеры, которые не имеют никакого воздействия на их работу. Это подчеркивает важность использования более сложных и специально разработанных триггеров для успешных атак в федеративном обучении.

ТАБЛИЦА 1. Сравнительный анализ методов атак и защиты

Метод атаки	Описание	Методы защиты	Оценка эффективности атаки
Добавление триггеров [9]	Встраивание визуальных изменений	Фильтрация аномалий, детекторы.	Высокая
Изменение цветовой палитры [10]	Незаметные изменения цвета, влияющие на классификацию.	Нормализация, регуляризация	Средняя
Глубокая манипуляция [11]	Изменение скрытых признаков изображения	Защита на уровне модели	Очень высокая
Пиксельные атаки [12]	Изменение небольшого числа пикселей для искажения вывода.	Анализ градиентов , устойчивые модели	Средняя

Таким образом, следует сделать вывод, что отравление изображений в федеративном обучении представляет серьезную угрозу для безопасности данных. Современные методы защиты не обеспечивают полной безопасности, а потому требуются дальнейшие исследования по повышению их эффективности.

Список используемых источников

1. Намиот Д. Е., Ильюшин М. А., Федеративное обучение для интеллектуального анализа конфиденциальной информации // International Journal of Open Information Technologies. 2021. Т. 9. № 10. С. 35-46.
2. Levshun D., Chechulin A., Kotenko I., Chevalier Y. Design and verification methodology for secure and distributed cyber-physical systems // Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2019. С. 1-5.
3. Холод И. И., Ефремова Е. А., Чижов И. В. Текущие академические и индустриальные проекты, посвященные устойчивому машинному обучению // International Journal of St. Petersburg International Conference «Regional Informatics». 2022. Т. 9. С. 352-356.
4. Zelle D., Rieke R., Plappert C., Krauß C., Levshun D., Chechulin, A. SEPAD – security evaluation platform for autonomous driving // Proceedings of the 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). IEEE, 2020. С. 413-420.
5. Sun G., Cong Ya., Dong J., Wang Q., Lyu L., Liu Ji. Data poisoning attacks on federated machine learning // IEEE Internet of Things Journal. 2022. Т. 9. № 13. С. 11365-11375.
6. Fan J., Yan Q., Li M., Qu G., Xiao Y. A survey on data poisoning attacks and defenses // Proceedings of the 7th IEEE International Conference on Data Science in Cyberspace (DSC). IEEE, 2022. С. 48-55.
7. Намиот Д. Е., Ильюшин Е. А., Чижов И. В. Основания для работ по устойчивому машинному обучению // International Journal of Open Information Technologies. 2021. Т. 9. № 11. С. 68-74.
8. Макгроу Г. Обеспечение безопасности систем машинного обучения / Г. Макгроу, Р. Бонетт, Х. Фигероа, В. Шепардсон // Открытые системы. СУБД. 2019. № 4. С. 22.
9. Wang Q., Wu Y., Xuan H., Wu H. FLARE: A Backdoor Attack to Federated Learning with Refined Evasion // Mathematics. 2024. Т. 12. № 23. С. 3751 3765.
10. Jiang W., Li H., Xu G., Zhang T. Color backdoor: A robust poisoning attack in color space // Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2023. С. 8133-8142.
11. Huang H., Mu J., Gong N. Z., Li Q., Liu B., Xu M. Data poisoning attacks to deep learning-based recommender systems // arXiv preprint arXiv:2101.02644. 2021.
12. Есипов Д. А., Бучаев А. Я., Керимбай А., Пузикова Я. В., Сайдумаров С. К., Сулименко Н.., Попов И. Ю., Кармановский Н. Атаки на основе вредоносных возмущений на системы обработки изображений и методы защиты от них // Научно-технический вестник информационных технологий, механики и оптики. 2023. Т. 23. № 4. С. 720-733.

IMAGE-BASED DATA POISONING METHODS IN FEDERATED LEARNING: ANALYSIS AND DEFENSE APPROACHES

Levshun D., Housheya K.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper discusses data poisoning techniques for federated learning in image processing tasks. Federated learning enables training models using data stored on users' devices, which poses unique security and privacy challenges. The paper analyzes various data poisoning techniques that attackers can use to manipulate model training, degrading their performance or introducing biases. Existing approaches to defend against such attacks are discussed. The importance of developing attack-resistant systems and the need for further research in this area to ensure the security of federated learning are highlighted.

Key words: *information security, federated learning, data poisoning, data protection, machine learning, generative and basic triggers*

УДК 004.056.5
ГРНТИ 21.35.19

МОДЕЛИРОВАНИЕ АТАКИ ТИПА «СКАНИРОВАНИЕ СЕТИ»

В. А. Липатников, И. С. Гущин, Я.Г. Солдатенко

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

В статье рассматриваются подходы к моделированию атак типа «сканирование сети» с использованием инструмента Nmap. Подробно описаны этапы сканирования, такие как определение активных устройств, анализ портов, исследование версий служб и операционных систем, а также выявление уязвимостей. Представлен алгоритм сканирования, включающий структурированный подход к анализу сетевой инфраструктуры. Указаны рекомендации по защите от подобных атак и повышению информационной безопасности.

Сканирование сети, Nmap, информационная безопасность, уязвимости, активные устройства, алгоритмы защиты.

Актуальность. Современные сети передачи данных (СПД) подвержены множеству угроз, включая многоэтапные кибератаки, направленные на получение несанкционированного доступа к системам. Сканирование является основным способом сбора данных в СПД и позволяет без знания топологии собрать актуальные данные, а также произвести поиск сервисов, работающий на хостах. Оно базируется на знании особенностей поведения хостов и протоколов при нарушении стандартных алгоритмов взаимодействия [1, 2]. Разработка моделей, способных имитировать атаки, актуальна для обеспечения защиты инфраструктуры СПД и своевременного реагирования на угрозы.

Цель исследования – создание детализированной модели атаки типа «сканирования сети» с учетом современных угроз и требований к безопасности.

Объект исследования: СПД, включающая рабочие станции, серверы и сетевое оборудование.

Предмет исследования: способы и алгоритмы моделирования атаки типа «сканирование сети».

Задача: разработать модель атаки типа «сканирования сети», включающую этапы анализа и прогнозирования угроз.

Сканирование сети – это важный процесс в области информационной безопасности, который позволяет выявить активные устройства, открытые порты и уязвимости в сети. Nmap (Network Mapper) – это мощный инструмент для сканирования и анализа сетей, который позволяет администраторам и специалистам по безопасности оценить состояние сетевой инфраструктуры.

Для моделирования атаки типа сканирование сети используем графический метод. Этот подход позволяет строить структурированные представления сетевых атак и визуализировать их и выполнят задачи от определения активных устройств до анализа уязвимостей и сохранения результатов. Алгоритм сканирования сети представлен на рис 1.

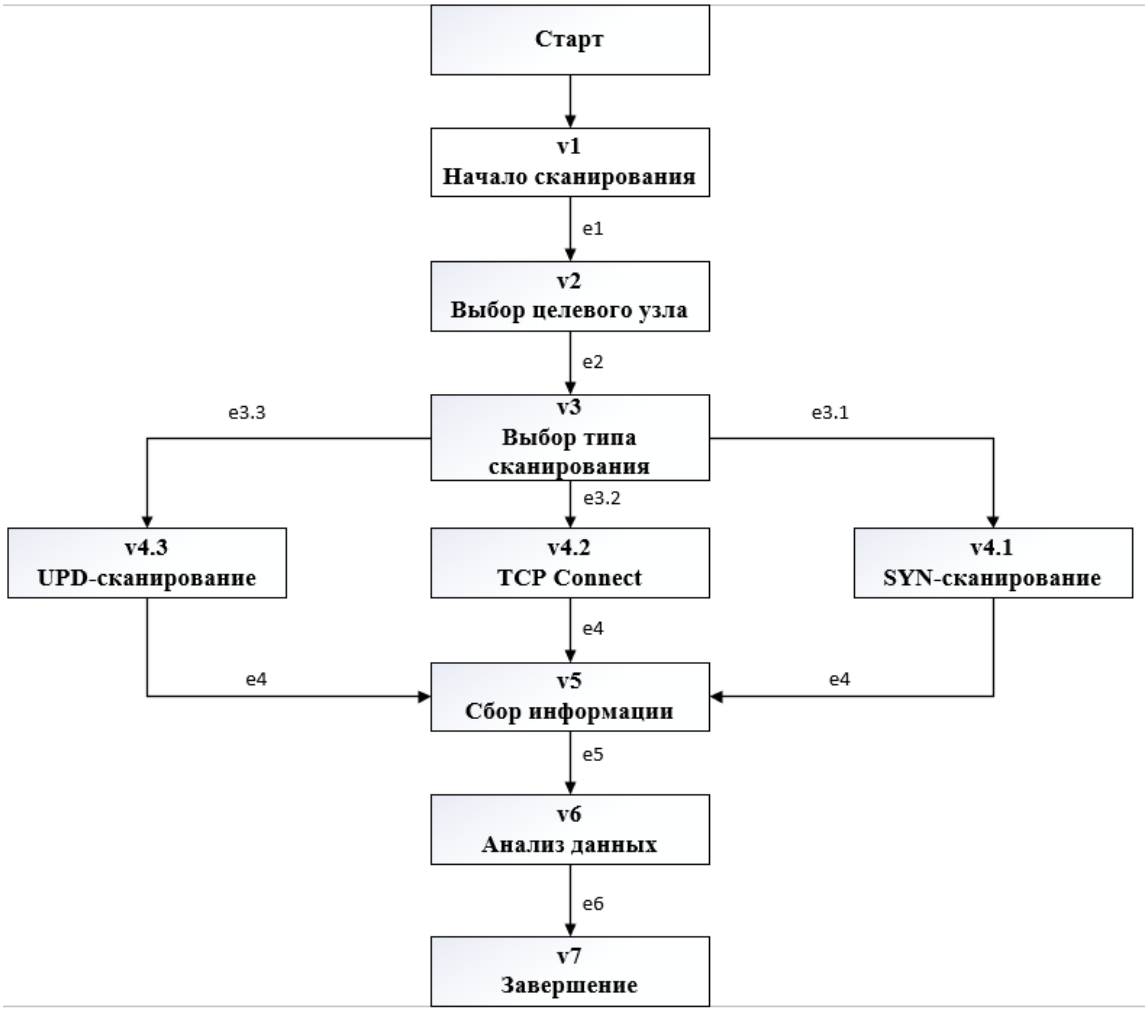


Рис. 1. Алгоритм описательной модели атаки «сканирования сети»

Для алгоритма, представленного на рис. 1, была создана таблица 1, описывающая процесс сканирования сети.

ТАБЛИЦА 1. Описание алгоритма сканирования

№ Состояния	Название состояния	Выполняемые действия	Обозначение перехода	Следующее состояние
1	Начало процесса	Запуск сканирования	e_1	v_2
2	Выбор целевого узла	Определение IP-адреса и порта целевого узла	e_2	v_3
3	Выбор типа сканирования	Определение метода (SYN, TCP Connect, UDP)	$e_{3.1}$, $e_{3.2}$, $e_{3.3}$	v_4_SYN, v_4_TCP, v_4_UDP
4.1	SYN-сканирование	Отправка SYN-пакета и ожидание ответа	e_4	v_5
4.2	TCP Connect	Установление полного TCP-соединения и анализ ответа	e_4	v_5
4.3	UDP-сканирование	Отправка UDP-пакета и ожидание ICMP-ответа	e_4	v_5
5	Сбор информации	Получение и сохранение данных из ответов целевого узла	e_5	v_6
6	Анализ данных	Обработка собранной информации для выявления открытых портов	e_6	v_7
7	Завершение	Фиксация результата и завершение процесса	-	Конец

Этап 1: Определение активных устройств.

Активные устройства – это хосты в сети, которые отвечают на запросы. Они могут быть компьютерами, серверами, маршрутизаторами или IoT-устройствами. Если на данном этапе нет активных устройств, то дальнейшее сканирование сети невозможно.

Этап 2: Сканирование портов. Рассмотрены три основных типа сканирования сети. SYN-сканирование (полуоткрытое сканирование) реализуется через отправку пакетов с флагом SYN (synchronize) целевому устройству. Этот флаг инициирует процесс установления соединения. Если порт открыт, сервер отвечает пакетом SYN-ACK (synchronize-acknowledge), подтверждая готовность к установлению соединения. На этом этапе злоумышленник отправляет пакет RST («reset» – это флаг а заголовке TCP-сегмента, который

используется для немедленного завершения соединения или сброса текущего состояния сессии между двумя узлами сети), чтобы прервать процесс соединения, избегая завершения полного TCP Handshake. Это позволяет сократить вероятность обнаружения сканирования системами IDS/IPS.

TCP Connect – это метод, в котором сканирующий инструмент устанавливает полноценное соединение с целевой системой. Он использует стандартный трехсторонний процесс TCP Handshake. После установления соединения может быть отправлен запрос для взаимодействия с портом или его тестирования. Если порт закрыт, целевая система отправляет RST.

UDP-сканирование направлено на выявление открытых портов, работающих на протоколе UDP, который не требует установления соединения. Сканирующее устройство отправляет UDP-пакет на целевой порт и анализирует ответ. Если порт открыт, ответ может содержать данные сервиса (например, ответ DNS-сервера). Если порт закрыт, система может отправить ICMP-сообщение «порт недоступен». Если ответа нет, порт считается открытым или фильтруемым. Этот метод менее надежен, чем TCP-сканирование, так как отсутствие ответа может интерпретироваться по-разному [2]. Кроме того, UDP-сканирование медленнее из-за необходимости ожидания, в таблице 2 представлено сравнение этих методов.

ТАБЛИЦА 2. Сравнительный анализ

Тип сканирования	Скрытность	Скорость	Точность	Применение
SYN-сканирование	Высокая	Быстрая	Точная	Первичный анализ сети
TCP Connect	Низкая	Медленная	Точная	Тестирование полной доступности портов
UDP-сканирование	Средняя	Медленная	Ограниченная	Анализ UPD-сервисов

Этап 3: Сбор данных. После выполнения сканирования сети с помощью Nmap, можно собрать различные данные, которые помогут анализировать состояние сети, обнаружить открытые порты, выявить уязвимости и получить информацию о сервисах.

Определение версий служб позволяет идентифицировать, есть ли уязвимости в конкретной версии приложения. Например, устаревшая версия Apache может быть подвержена *DoS*-атаке или исполнению произвольного кода. Также важно определить операционную систему, потому что, каждая

операционная система имеет свои особенности безопасности. Устаревшие версии ОС часто имеют незащищенные компоненты.

Этап 4: Анализ данных. Анализ данных, полученных в ходе сбора сведений, является важным этапом в обеспечении безопасности сети и систем. Этот процесс позволяет не только выявить уязвимости, но и создать полное представление о текущем состоянии инфраструктуры, что важно для выработки стратегии атаки. Nmap позволяет запускать скрипты для обнаружения уязвимостей и выполнения более глубокого анализа. Это называется Nmap Scripting Engine (NSE). Мы можем запустить скрипт, который проверяет, например, наличие известных уязвимостей или неправильных конфигураций на сервисах. После того как были обнаружены сервисы и их версии, важно проверить их на наличие уязвимостей. Каждая уязвимость в CVE (Common Vulnerabilities and Exposures) имеет уникальный идентификатор, который помогает искать информацию о ней. Некоторые уязвимости могут быть связаны не с устаревшим ПО, а с неправильными настройками безопасности сервисов, например:

– SSH может использовать слабые ключи.
– Apache может быть настроен с ошибочными правами доступа.
– SMTP может быть открыт для отправки спама.

Этап 5: Завершение и сохранение результатов.

Разработка модели атаки типа «сканирования сети» с использованием Nmap позволяет эффективно выявлять активные устройства и уязвимости в сети. Регулярное сканирование и анализ результатов помогут поддерживать высокий уровень безопасности и защищенности информационной инфраструктуры. Для повышения защищенности сети рекомендуется: закрывать неиспользуемые порты; устанавливать межсетевые экраны для фильтрации подозрительного трафика; регулярно обновлять операционные системы и приложения; проводить регулярные аудиты безопасности и сканирование сети [3].

Прерывание атаки возможно на различных этапах [4,5]. На этапе определения активных устройств этого можно достичь с помощью настройки фильтрации ICMP-запросов или закрытия неиспользуемых адресов. Во время сканирования портов предотвращение обеспечивают межсетевые экраны и системы предотвращения вторжений (IDS/IPS), блокирующие подозрительный трафик. На этапе сбора данных ограничение доступа к информации о версиях служб и настройка безопасных конфигураций минимизируют успех атакующих. Завершающий этап анализа данных может быть сорван регулярным обновлением операционных систем и приложений, что закрывает обнаруженные уязвимости и снижает ценность собранных данных.

Заключение. Цель исследования – создание детализированной модели атаки типа «сканирования сети» с учетом современных угроз и требований к безопасности – достигнута. Разработанная модель позволяет проводить структурный анализ сетевой инфраструктуры, выявлять активные устройства, открытые порты и уязвимости, что делает ее эффективным инструментом для повышения уровня ИБ. Предложенная модель превосходит подход, описанный в источнике [4], благодаря улучшенной детализации этапов анализа и более широкому спектру применяемых методов. В отличие от известных моделей, новый подход фокусируется на проактивном управлении и адаптации к динамично меняющимся киберугрозам. Это делает разработанную модель более универсальной и эффективной для применения в условиях повышенных требований к безопасности. Возможность оперативного выявления и нейтрализации киберугроз повышает защищенность критически важных систем связи, что особенно важно в современных условиях.

Список использованных источников

1. Федоров И. С. Инструменты сканирования сети и обнаружения уязвимостей: Практическое руководство. М.: Горячая Линия-Телеком, 2023. 288 с.

2. Fyodor. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.org, 2015.

3. Глушков А. В., Мартынов В. В. Основы информационной безопасности. М.: Наука, 2021. 256 с.

4. Липатников В. А., Мелехов К. В., Робак В. А. Моделирование процесса проактивного управления СПД в условиях киберугроз // Военная связь будущего. Квантовый скачок как неизбежность. 2023. С. 90-95.

5. Липатников В. А., Мелехов К. В. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации // Актуальные проблемы защиты и безопасности. 2024. С. 306-310.

SIMULATION OF A NETWORK SCAN ATTACK

Lipatnikov V., Guschin I., Soldatenko Ya.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article discusses approaches to modeling attacks such as "network scanning" using the Nmap tool. The scanning steps are described in detail, such as identifying active devices, analyzing ports, examining versions of services and operating systems, and identifying vulnerabilities. A scanning algorithm is presented that includes a structured approach to network infrastructure analysis. Recommendations are given on how to protect against such attacks and improve information security.

Key words: *Network scanning, Nmap, information security, vulnerabilities, active devices, protection algorithms*

УДК 004.056.
ГРНТИ 81.93.29

МОДЕЛЬ АТАКИ «ДОВЕРЕННЫЙ ОБЪЕКТ СЕТИ» В СЕТИ ПЕРЕДАЧИ ДАННЫХ

В. А. Липатников, И. С. Гущин, Я. Г. Солдатенко

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

Атака «доверенный объект сети» является одной из самых часто реализуемых. Данная атака предполагает получение злоумышленником доступа к сети передачи данных информационной системы под видом различного сетевого устройства. Данный вид атак опасен в первую очередь тем, что злоумышленник может перехватывать пакеты данных и отправлять ложную информацию тем самым дестабилизируя работу сети передачи данных.

сети передачи данных, безопасность сетей передачи данных, атаки на сети передачи данных, доверенный объект сети

В современных условиях, где информационные технологии играют ключевую роль в обеспечении безопасности, управление информационной безопасностью (ИБ) становится одной из приоритетных задач. Сети передачи данных (СПД) подвергаются постоянным угрозам со стороны противника, который использует разнообразные программно-аппаратные воздействия для достижения своих целей. Цель: разработать модель атаки «доверенный объект сети» в (СПД) с учетом полученных теоретических знаний, для дальнейшего планирования программного комплекса с учетом параметров, влияющих на ход защиты.

Под доверенным объектом понимается элемент сети (компьютер, межсетевой экран, маршрутизатор и т.п.), имеющий легальное подключение, и которому присвоены права для доступа к сетевым ресурсам информационной системы.

Осуществление атаки «подмена доверенного объекта сети» и передача по каналам связи сообщений от его имени с присвоением его прав доступа возможна в системах, где используются нестойкие алгоритмы идентификации и аутентификации хостов. Типичным примером является перехват TCP-сессии. Рассмотрены две разновидности процесса осуществления удаленной атаки типа «подмена доверенного объекта сети»: атака с установлением виртуального канала; атака без установления виртуального канала. Процесс реализации атаки с установлением виртуального канала состоит в присвоении прав доверенного пользователя, что позволяет злоумышленнику вести сеанс работы с объектами системы от имени доверенного пользователя. Для форми-

рования ложного TCP-пакета атакующему достаточно подобрать соответствующие текущие значения идентификаторов TCP-пакета (ISSa и ISSb) для данного TCP-соединения (например, FTP- или TELNET-подключение) [1].

В зависимости от условий, начала атаки может быть начато с трех разных этапов. Учитывается, как влияют методы построения системы ИБ, в частности, системы аутентификации [1, 2]. На рисунке 1 представлен подробный алгоритм данной атаки, где показаны основные варианты реализации в зависимости от структуры защиты объекта.

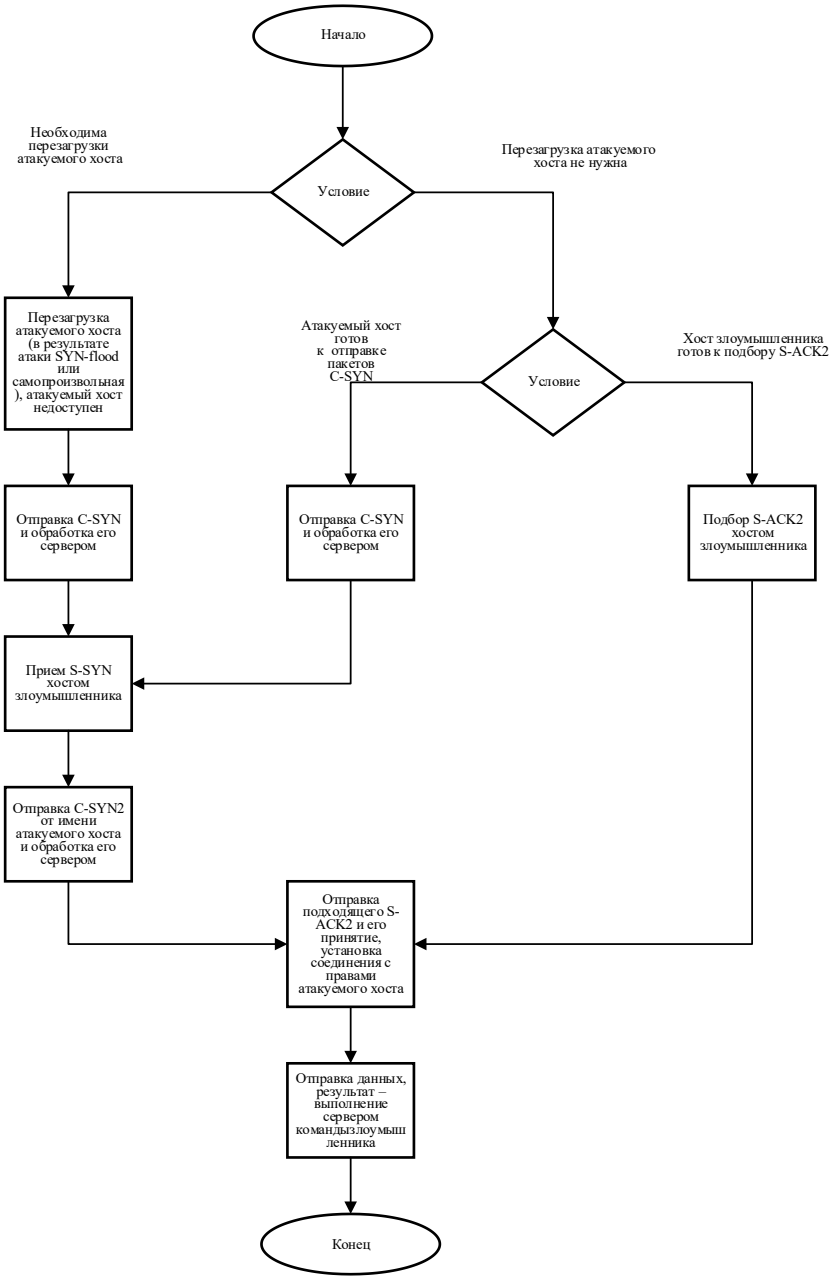


Рис. 1. Алгоритм описательной модели атаки «доверенный объект сети»

На основе данного алгоритма построена дискретная система одноканального многофазового массового обслуживания с ожиданием.

Моделирование атак в (СПД) рассмотрено в [6-8]. Алгоритм атаки «доверенный объект сети» представлен в виде графа, состоящего из конечного числа возможных состояний и переходов системы из одного состояния в другое [1, 2]. В виду маловероятного возникновения очереди данную модель можно представить в виде схемы на рисунке 2.

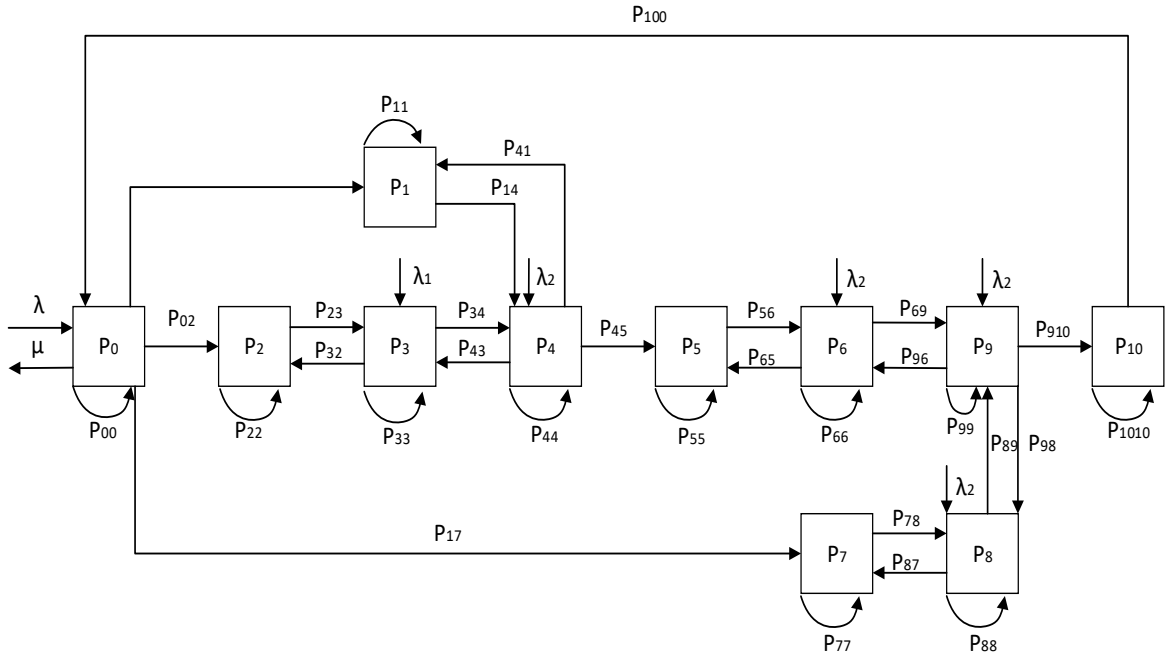


Рис. 2. Граф, описывающий механизм реализации сетевой атаки «Доверенный объект сети»

На данном графе изображен алгоритм атаки ожиданием, а также влияние средств защиты, где:

P_k – вероятность реализации этапа.

P_{kn}– интенсивность перехода от этапа к этапу.

P_{kk} – ожидание.

λ_k – влияние средств защиты.

Так как в данном алгоритме учитывается влияние средств защиты, необходимо доказать их весомость. На этапе P_3 происходит перезагрузка атакуемого хоста, реализуемая через атаку SYN-flood, в данном случае при наличии средств межсетевой маршрутизации и *DoS* защиты имеется вероятность отсутствия положительного результата каковым является переход на следующий этап [3]. На этапах P_4, P_6, P_8, P_9 реализуется отправка пакетов на атакуемый объект сети, на что в свою очередь может повлиять средства обнаружения вторжений [4].

В таблице 1 представлены расшифровки всех этапов данной модели.

ТАБЛИЦА 1. Описание этапов модели атаки

№	Вредоносные функции, выполняемые сетевой атакой	P_k
0	Ожидание начала атаки	P_0
1	Атакуемый хост готов	P_1
2	Хост злоумышленника готов к проведению атаки SYN-flood и ожидает перезагрузки атакуемого хоста	P_2
3	Перезагрузка атакуемого хоста (в результате атаки SYN-flood или самопроизвольная), атакуемый хост недоступен	P_3
4	Отправка *C-SYN* и обработка его сервером	P_4
5	Прием *S-SYN* хостом злоумышленника	P_5
6	Отправка *C-SYN2* от имени атакуемого хоста и обработка его сервером	P_6
7	Хост злоумышленника готов к подбору *S-ACK2*	P_7
8	Подбор *S-ACK2* хостом злоумышленника	P_8
9	Отправка подходящего *S-ACK2* и его принятие, установка соединения с правами атакуемого хоста	P_9
10	Отправка данных, результат – выполнение сервером команды злоумышленника	P_{10}

Заключение

Предложена модель атаки «доверенный объект сети» СПД в виде дискретной системы одноканального многофазового массового обслуживания с ожиданием. Учитываются две разновидности процесса осуществления удаленной атаки: атака с установлением виртуального канала; атака без установления виртуального канала.

Предложенная модель позволяет решать задачи оценки ИБ и выбора способов защиты СПД.

Новизна модели заключается тем, что в отличие от известных в ней учитываются так же фактор влияние средств защиты на ход атаки. Так при учете этих факторов модель имеет более реальное представление ата6ки.

Список используемых источников

1. Введение в общие цепи Маркова. Авторы: Зорин А. В., Зорин В. А., Пройдакова Е. В., Федоткин М. А.: Учебно-методическое пособие. Нижний Новгород: Нижегородский госуниверситет, 2013. 51 с.

2. Химмельблау Д. Прикладное нелинейное программирование: пер. с англ. М.: Мир, 1976. 256 с. ISBN 5-7854-9807-4.

3. Масоедова А. А. Киберпространство как среда совершения преступлений / А. А. Мясоедова. Текст: электронный // Исторические, философские, методологические проблемы современной науки. 2022. 377-381 с. URL: https://www.elibrary.ru/item.asp?id=49336012 (дата обращения: 12.12.2024).

4. Болдырихин Н. В. Исследование систем обнаружения вторжений / Н. В. Болдырихин, Р. И. Комоцкий, Д. И. Лян. – Текст: непосредственный // Молодой ученый. 2023. № 2 (449). 6-9 с.

5. Vuletic Dejan V., Nojkovic Nemanja D.REALIZATION OF A TCP SYN FLOOD ATTACK USING KALI LINUX / University of Defence in Belgrade, Strategic Research Institute, Belgrade, Republic of Serbia, 2013. 640-649 с. URL: https://cyberleninka.ru/article/n/realization-of-a-tcp-syn-flood-attack-using-kali-linux/viewer(дата обращения: 15.12.2024).

6. Липатников В. А., Мелехов К. В. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации. // Актуальные проблемы защиты и безопасности. 2024. С. 306-310.

7. Липатников В. А., Мелехов К. В., Робак В. А. Моделирование процесса проактивного управления СПД в условиях киберугроз. // Военная связь будущего. Квантовый скачок как неизбежность. 2023. С. 90-95.

8. Липатников В. А., Тихонов В. А. Распознавание вторжений нарушителя при управлении кибербезопасностью инфраструктуры интегрированной организации на основе нейро-нечетких сетей и когнитивного моделирования. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ? 2019. С. 659-664.

THE "TRUSTED NETWORK OBJECT" ATTACK MODEL IN A DATA TRANSMISSION NETWORK

Lipatnikov V., Gushchin I., Soldatenko Ya.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The "trusted network object" attack is one of the most frequently implemented. This attack involves an attacker gaining access to the information system's data transmission network under the guise of a different network device. This type of attack is dangerous primarily because an attacker can intercept data packets and send false information, thereby destabilizing the data transmission network.

Key words: *data transmission networks, security of data transmission networks, attacks on data transmission networks, trusted network object*

УДК 004.852
ГРНТИ 28.23.25

ОБУЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ОСНОВЕ МОДЕЛИРОВАНИЯ АТАК В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

В. А. Липатников, В. А. Задбоев

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

Статья посвящена повышению уровня информационной безопасности сетей передачи данных (СПД) с использованием методов искусственного интеллекта на основе динамических байесовских сетей. Обоснована актуальность применения искусственного интеллекта для защиты СПД от кибератак в условиях усложняющихся угроз. Описана методика моделирования кибератак с использованием байесовских графов, которые учитывают неопределенность данных, моделируют зависимости и прогнозируют развитие атак. Рассмотрены этапы формирования графов, вычисления вероятностей компрометации узлов и прогнозирования рисков.

искусственный интеллект, динамические байесовские сети, кибератаки, сети передачи данных, информационная безопасность, моделирование угроз, прогнозирование рисков, байесовские графы

Актуальность: современные (СПД) подвержены множеству постоянно развивающихся угроз. Применение искусственного интеллекта является важным направлением для защиты СПД от кибератак. Искусственный интеллект, как комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе, в котором используются методы машинного обучения), процессы и сервисы по обработке данных, анализу и синтезу решений». С увеличением сложности атак и их объемов возрастает необходимость в эффективных методах защиты и предсказания потенциальных угроз [1, 2, 3]. Одним из таких методов является использование байесовских графов, являющийся крайне актуальным в условиях постоянных сетевых угроз и увеличения объемов обрабатываемых данных.

В рамках научного исследования рассматривается применение моделей для информационной безопасности СПД за счет использования динамических байесовских сетей (ДБС) при моделировании кибератак [4]. Благодаря своей способности обрабатывать неопределенность, моделировать сложные зависимости и адаптироваться к изменениям в реальном времени, этот метод является мощным инструментом для активной защиты СПД.

Целью статьи является повышение информационной безопасности СПД с применением технологий искусственного интеллекта на основе теоремы Байеса.

Задачей является разработка системы обучения искусственного интеллекта с применением теоремы Байеса в виде графов атак.

Байесовские модели в виде графа кибератак, построенные на основе статистического обучения, позволяют определить временные связи для каждого из параметров вторжений, определяемых в процессе управления защитой, и предоставляют возможность прогнозировать результаты анализа путем выполнения процедуры имитационного моделирования, они представляют собой направленные ациклические графы, где вершины ассоциируются с инцидентами, рассматриваемыми также как элементарные условия, а ребра моделируют конъюнкцию (логическую операцию, по смыслу максимально приближенная к союзу «и») или дизъюнкцию (логическое «или» или логическое дополнение или инклюзивная дизъюнкция, представляет собой логическую связку, обычно обозначаемую «или») элементарных условий. Направление каждого ребра указывает на тот инцидент, который может возникнуть, если будет выполнена конъюнкция или дизъюнкция предшествующих ему условий.

Байесовский граф атак имеет одну целевую вершину, которую можно ассоциировать с конкретной атакой. Значения вероятности, которые задаются для каждой вершины, кроме целевой, отражают возможную вероятность возникновения инцидента. Для расчета вероятности возникновения атаки или инцидента при условии возникновения предшествующих инцидентов можно использовать формулу условной вероятности.

Байесовские графы атак представляют собой вероятностные модели, которые позволяют учитывать случаи неопределенности исходных данных о моделируемых атаках.

Существующая методика определения потенциальной атаки для узлов графа использует и развивает работы, применяющие байесовские графы атак. Отличиями являются метод формирования графа атак и метод вычисления локальных вероятностей компрометации узлов.

Для того, чтобы иметь возможность применять искусственный интеллект для анализа СПД с последующим использованием их для работы в условиях неопределенности, необходимо его обучить, для чего прекрасно подходит метод байесовских графов, однако для этого необходимо собрать нужную информацию и на ее основе построить эти графы.

В случае инцидентов безопасности на СПД для всех уровней с учетом особенностей теоремы Байеса учитываются следующие характеристики:
– целевой IP-адрес;
– сигнатуры, соответствующие атакам (рост трафика, попытки авторизации);
– типы проведенных атак (DDoS, SSH-Patator);
– типы событий, соответствующие атакам (отказ в обслуживании, кража записей);
– статус атаки (обнаружена, проведена, устранена и т.д.).

После обнаружения и сопоставления новой атаки с последовательностью атак на графе Байеса риски безопасности пересчитываются.

Байесовский граф атак был выбран для интеграции с динамической методикой, так как позволяет учитывать влияние событий на состояние системы и прогнозировать развитие атаки, а также определять предыдущие шаги атаки.

Алгоритм определения потенциальной атаки включает три шага:
– определение локальных вероятностей узлов;
– определение дискретных условных распределений вероятностей;
– определение полных вероятностей.

Безусловные вероятности компрометации узлов графа (вероятности атаки) определяются на основе локальных вероятностей и распределений условных вероятностей по формуле полной вероятности путем маргинализации по известным вероятностям.

Различные свойства сети позволяют злоумышленнику по-разному скомпрометировать СПД. Сначала мы определяем шаблон-атрибут, который позволяет нам классифицировать эти свойства сети для дальнейшего анализа.

Пусть S – набор атрибутов, а A – набор атомарных атак, определенных на S. Байесовский граф атак – это набор кортежей = (S, τ, ε, P), где:

1) S = Ninternal ∪ Nexternal ∪ Nterminal. Nexternal обозначает набор атрибутов Si, для которых !a ∈ A|Si = post(a). Ninternal обозначает набор атрибутов Sj, для которых ∃a1, a2 ∈ A|[Sj = до(a1) и Sj = после(a2)]. Nterminal обозначает набор атрибутов Sk, для которых !a ∈ A|Sk = pre(a).

2) τ ∈ S×S. Упорядоченная пара (Spre, Spost) ∈ τ, если Spre %⟶ Spost ∈ A. Далее, для Si ∈ S множество Pa[Si] = {Sj ∈ S|(Sj,Si) ∈ τ} называется родительским множеством Si.

3) ε – это набор кортежей декомпозиции вида *Sj,dj+ , определенных для всех Sj ∈ Ninternal ∪ Nterminal и dj ∈ {И,ИЛИ}. dj равно И, если Sj = 1 ⇒ ∀Si ∈ Pa[Sj],Si = 1. dj равно ИЛИ, если Sj = 1 ⇒ ∃Si ∈ Pa[Sj],Si = 1.

4) P – это набор дискретных функций распределения условных вероятностей. Каждый атрибут Sjninternal ∪ Nterminal имеет дискретное локальное распределение условных вероятностей.

Существование этой вероятности – это то, что в первую очередь отличает байесовский граф от классического графа атак. Вероятности отражаются в локальном условном распределении вероятностей узла. По итогу получается набор значений вероятности, определяющих вероятность того, что узел будет взломан, учитывая различную комбинацию состояний его родительских узлов, пример реализации графа представлен на рис. 1.

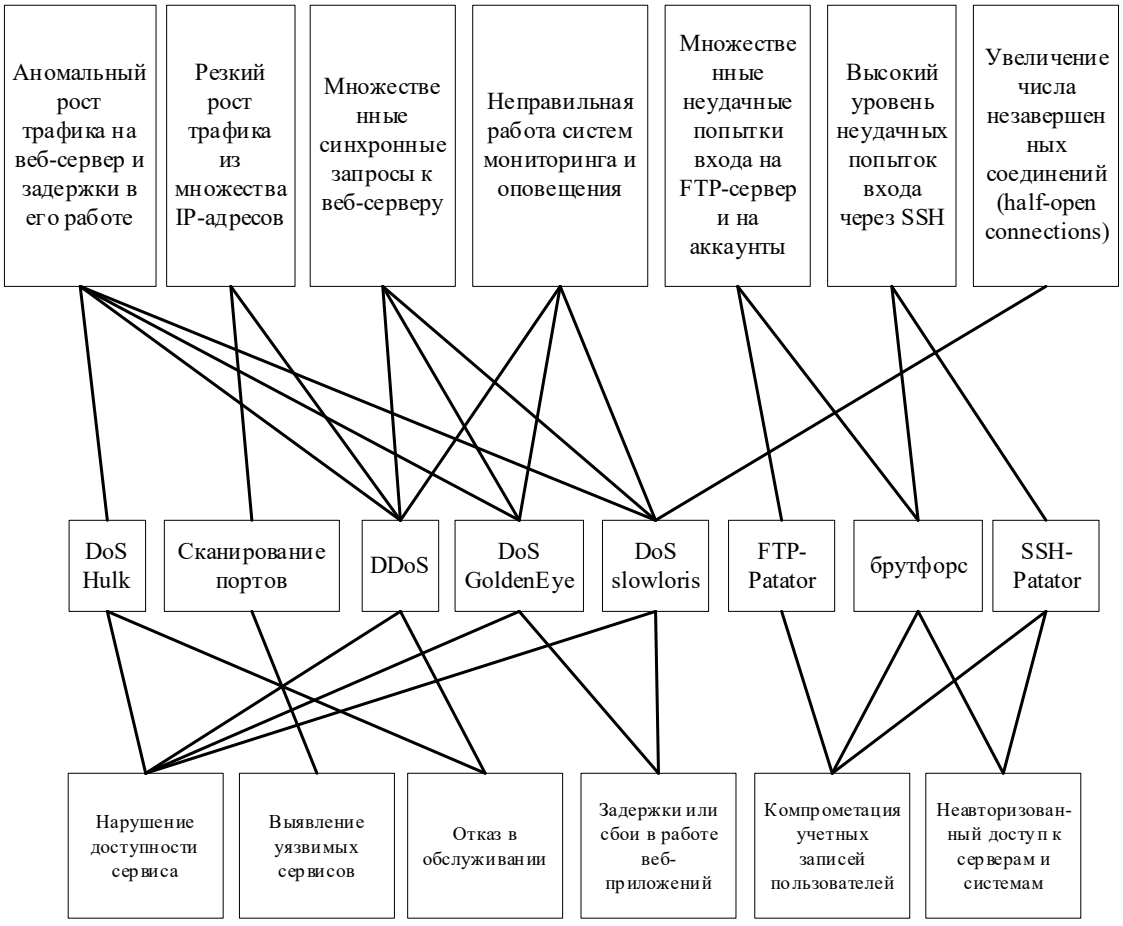


Рис. 1. Реализация байесовского графа

Суть в построении графа заключается в последовательном определении всех возможных последствий реализации угроз в СПД, начиная от обнаруженных в ней факторов уязвимостей.

Таким образом схема имеет вид:

– первоначально описываются факторы реализации уязвимости в СПД, например. высокий уровень неудачных попыток входа через протокол SSH;
– далее описываются все возможные известные атаки на СПД, например, DDoS атака или брутфорс;
– в конце графа уточняются все возможные последствия реализации угрозы в СПД, например, отказ в обслуживание или хищение данных.

Схема может прочитаться следующим образом: в сети обнаружен высокий уровень неудачных попыток входа через протокол SSH, значит проводится попытка реализации атаки брутфорс или SSH-Patator, которые могут привести к угрозе в СПД в виде компрометации учетных записей пользователей или неавторизованному доступу к серверам или системам.

Заключение. Использование байесовских графов при обучении искусственного интеллекта для активной защиты СПД подтверждает свою эффективность в условиях возрастающей сложности кибератак и необходимости оперативного реагирования. Этот метод позволяет более точно оценивать и предсказывать угрозы на основе вероятностных данных, улучшая тем самым управление рисками и оптимизацию защиты. Байесовские сети предоставляют возможность обнаружения аномалий и анализа взаимосвязей между атаками, что значительно повышает уровень защищенности сети. Применение этих графов важно для повышения отказоустойчивости СПД и минимизации рисков компрометации данных и отказа в обслуживании.

Список используемых источников

1. Котенко И. В. Искусственный интеллект для кибербезопасности: новая стадия противоборства в киберпространстве. // Искусственный интеллект и принятие решений. 2024. № 1. С. 3-19.

2. Velankar M. R., Mahalle P. N., Shinde G. R. Machine Thinking: New Paradigm Shift. In: Cognitive Computing for Machine Thinking. // Innovations in Sustainable Technologies and Computing. 2024. pp. 43–53.

3. Takano S. Thinking Machines. // Machine Learning and Its Hardware Implementation. Academic Press, 2021. 306 p.

4. Азарнова Т. В., Полухин П. В. Разработка концепции и инструментария моделирования процессов тестирования веб-приложений методом фаззинга с помощью динамических байесовских сетей. // Моделирование, оптимизация и информационные технологии. 2023.

5. Задбоев В. А., Липатников В. А., Мелехов К. В. Активная защита информационно-вычислительной сети от атак типа ADVANCED PERSISTENT. THREAT. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. 2024. С. 347-351.

6. Липатников В. А., Мелехов К. В., Робак В. А. Моделирование процесса проактивного управления СПД в условиях киберугроз // Военная связь будущего. Квантовый скачок как неизбежность. 2023. С. 90-95.

7. Котенко И. В., Саенко И. Б., Захарченко Р. И., Величко Д. В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации // Вопросы кибербезопасности. 2023. № 1 (53). С. 13-27.

8. Липатников В. А., Мелехов К. В. Способ обработки результатов сетевого контроля при поддержке принятия решения администратора безопасности информации // Актуальные проблемы защиты и безопасности. 2024. С. 306-310.

9. Липатников В. А., Парфиров В. А., Шевченко А. А., Мелехов К. В. Модель процесса обеспечения безопасности сети передачи данных в условиях информационного противоборства // Актуальные проблемы защиты и безопасности. 2023. С. 569-572.

TRAINING ARTIFICIAL INTELLIGENCE BASED ON MODELING ATTACKS IN DATA TRANSMISSION NETWORKS

Lipatnikov V., Zadboev V.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is devoted to increasing the level of information security of data transmission networks (DTN) using artificial intelligence methods based on Bayesian network algorithms. The relevance of using artificial intelligence to protect DTNs from cyberattacks in the face of increasingly complex threats is substantiated. A methodology for modeling cyberattacks using Bayesian graphs is described, which take into account the uncertainty of data, model and predict the development of an attack. The stages of graph formation, calculation of node compromise probabilities and risk forecasting are considered.

Key words: *Artificial intelligence, Bayesian driving networks, cyber-attacks, network data transmission, information security, threat modeling, risk forecasting, Bayesian graphs*

УДК 004.056
ГРНТИ 50.37.23

ЗАЩИЩЕННОСТЬ ВЕБ-ПРИЛОЖЕНИЙ: МОДЕЛИРОВАНИЕ СЕТЕВЫХ АТАК В СТРУКТУРЕ КИБЕРПОЛИГОНА

В. П. Макогон, А. А. Негурица, И. Р. Трухманов

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

В условиях стремительного роста числа веб-приложений и их использования в различных сферах жизнедеятельности, вопрос защищенности этих систем становится особенно актуальным. Данная работа посвящена исследованию методов моделирования сетевых атак на веб-приложения в рамках киберполигона – специализированной платформы для тестирования и анализа безопасности информационных систем.

веб-приложения, моделирование, киберполигон, защищенность.

Современные военные системы связи и управления требуют высокой степени защищенности от кибератак. Создание специализированных полигонов для моделирования таких атак представляет собой эффективный метод оценки устойчивости этих систем [1-4]. Данные полигоны должны быть изолированы от внешних сетей и воспроизводить реальные условия эксплуатации, что позволяет проводить тестирование в безопасной среде.

Структурные компоненты киберполигона в себя следующие ключевые компоненты:

1. Техническая инфраструктура:

– изолированная вычислительная среда, обеспечивающая защиту от внешних угроз;
– модели военных информационных систем, позволяющие имитировать реальные сценарии эксплуатации;
– средства имитации атакующих действий, которые позволяют воспроизводить различные типы кибератак;
– системы мониторинга и анализа, предназначенные для оценки состояния защищенности.

2. Функциональные возможности:

– моделирование различных сценариев кибератак, включая как известные, так и новые угрозы;

– тестирование эффективности защитных мер, направленных на предотвращение атак;
– анализ поведения системы под воздействием угроз, что позволяет выявить уязвимости;
– оценка последствий успешного проникновения, что способствует разработке стратегий защиты.

Преимущества использования киберполигона:

1. Возможность безопасного исследования критических угроз.
2. Экономия ресурсов за счет виртуализации.
3. Гибкость настройки тестовых сценариев.
4. Получение достоверных данных о надежности защиты.

Применение военных веб-приложений

Военные веб-приложения служат для решения множества задач, включая:

1. Обучение персонала через онлайн-платформы для дистанционного обучения военнослужащих.
2. Поддержка принятия решений в рамках межвидовой системы информационного обмена.
3. Управление личными кабинетами военнослужащих Министерства обороны.
4. Обеспечение веб-интерфейсов для средств связи, таких как БШПД, тактический радиоконцентратор (ТРК) и др.

Анализ и примеры успешных атак на военные веб-приложения

Несколько примеров успешных атак на военные веб-приложения демонстрируют важность защиты:

1. Атака на базу данных Министерства обороны США (2008):

Описание: несанкционированный доступ к базам данных через веб-портал управления логистикой.

Метод: SQL-инъекция через незащищенные поля ввода.

Последствия: Доступ к информации о перемещении войск и техники.

Урок: необходимость регулярного аудита безопасности и применения параметризированных запросов.

2. Кибератака на систему управления НАТО (2016):

Описание: внедрение вредоносного ПО через XSS-атаку на внутренний портал коммуникаций.

Метод: использование непроверенных пользовательских данных для внедрения скрипта.

Последствия: кража учетных данных сотрудников и доступ к внутренней переписке.

Урок: важность фильтрации входящих данных и применения современных методов кодирования.

3. APT-атака на оборонного подрядчика США (2017):

Описание: группировка APT28 (Fancy Bear) атаковала веб-приложение для обмена документацией.

Метод: целевые фишинговые атаки и эксплуатация уязвимостей в сторонних компонентах.

Последствия: похищение конфиденциальных проектных данных.

Урок: необходимость регулярного обновления всех используемых библиотек и компонентов.

4. Атака на систему связи Вооруженных сил Российской Федерации (2019):

Описание: кибератака на тестовую версию веб-интерфейса системы связи во время регламентных испытаний новой платформы.

Методы проникновения: эксплуатация уязвимости в конфигурации сервера, обнаружение незащищенной точки входа в тестовом окружении, недостаточно изолированном от внешней сети.

5. DDoS-атака на систему управления боевыми действиями (2020):

Описание: в ходе учений была зафиксирована попытка выведения из строя веб-приложения управления подразделениями.

Метод: организация большого числа одновременных запросов через ботнет.

Последствия: временная недоступность системы, замедление принятия решений.

Урок: необходимость внедрения эффективных систем защиты от DDoS-атак и резервирования ресурсов.

6. Атака на систему разведданных (2021):

Описание: через веб-портал для анализа спутниковых данных был осуществлен несанкционированный доступ.

Метод: использование уязвимости в стороннем плагине и социальной инженерии.

Последствия: кража части архивных данных и временная потеря функциональности системы.

Урок: важность регулярного мониторинга используемых сторонних компонентов и обучения персонала.

Меры реагирования и профилактики

1. Немедленные действия:

– полная блокировка доступа к текстовым серверам из внешних сетей;
– изменение всех паролей и внедрение двухфакторной аутентификации;
– проведение экстренного аудита безопасности всей системы связи.

2. Долгосрочные решения:

– внедрение строгих правил изоляции тестовых сред;
– регулярное обновление и патчирование всех используемых компонентов;
– обучение персонала основам информационной безопасности и методам защиты от социальной инженерии;
– разработка комплексных политик управления паролями, включающих использование сложных комбинаций и регулярную их смену.

3. Технологические улучшения:

– установка современных систем обнаружения вторжений (IDS/IPS);
– внедрение SIEM-решений для централизованного мониторинга событий безопасности;
– использование технологий шифрования для защиты передаваемых данных.

Инструменты анализа уязвимостей

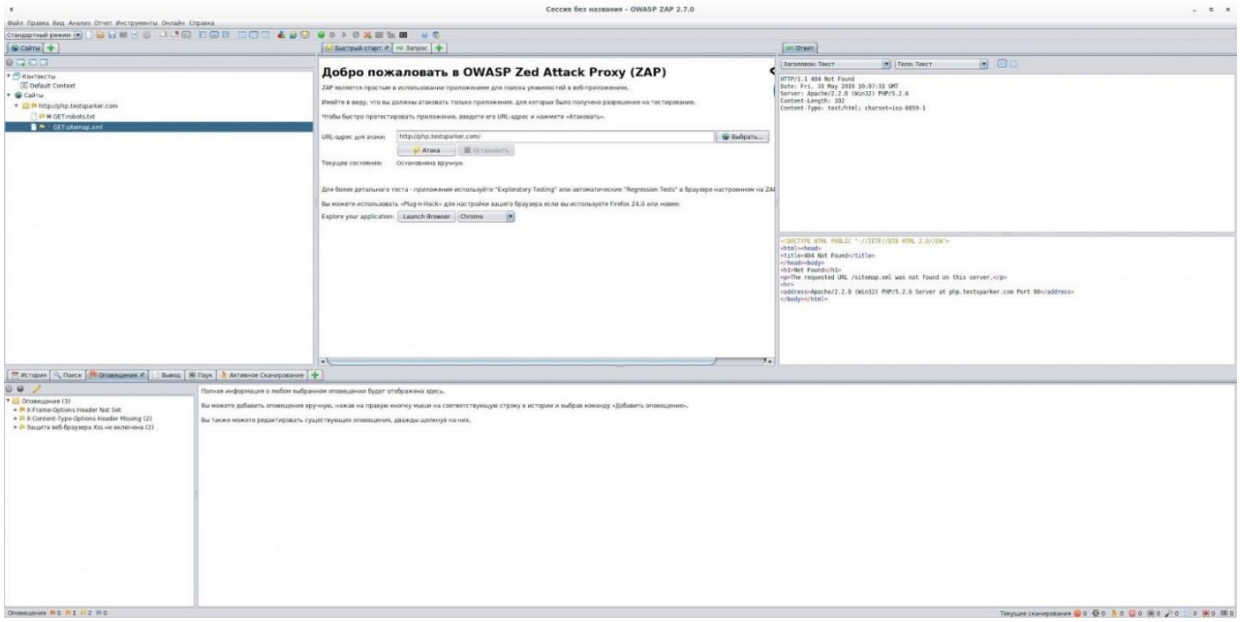


Рис. 1. Интерфейс программы OWASP ZAP

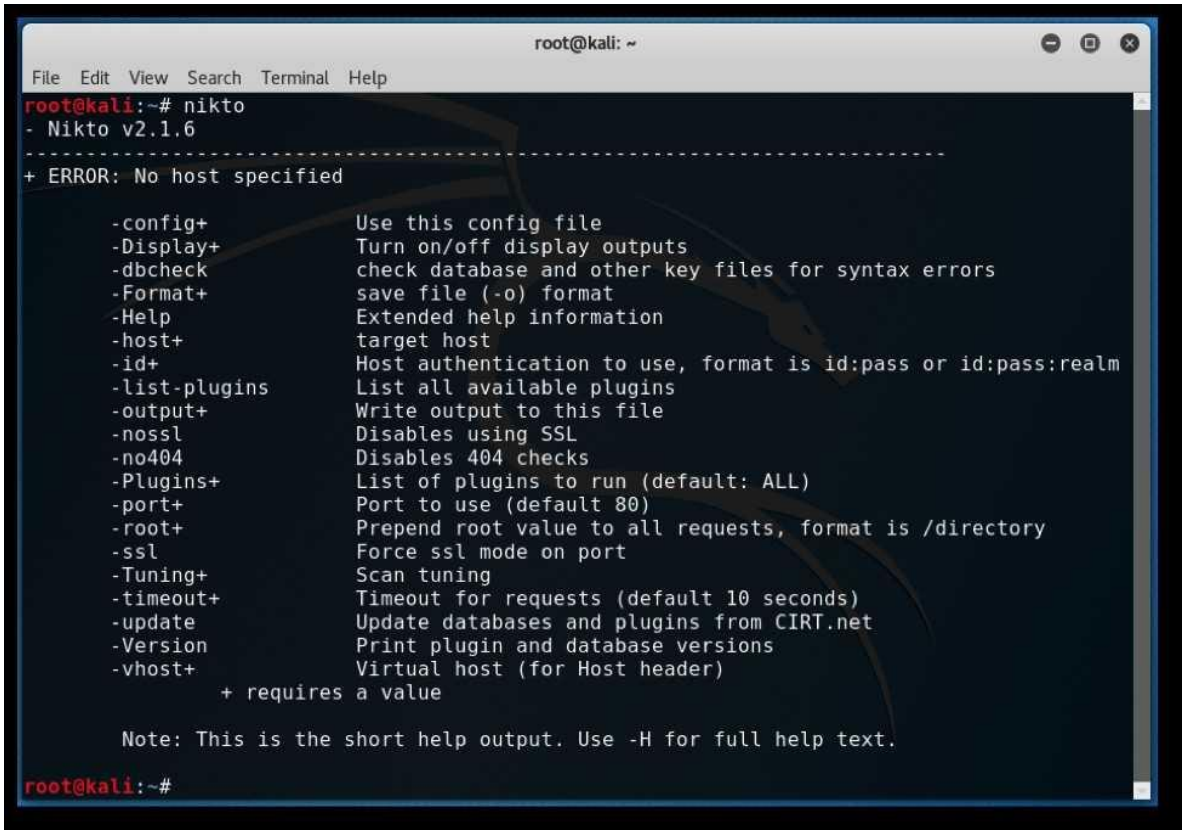


Рис. 2. Интерфейс программы OWASP ZAP

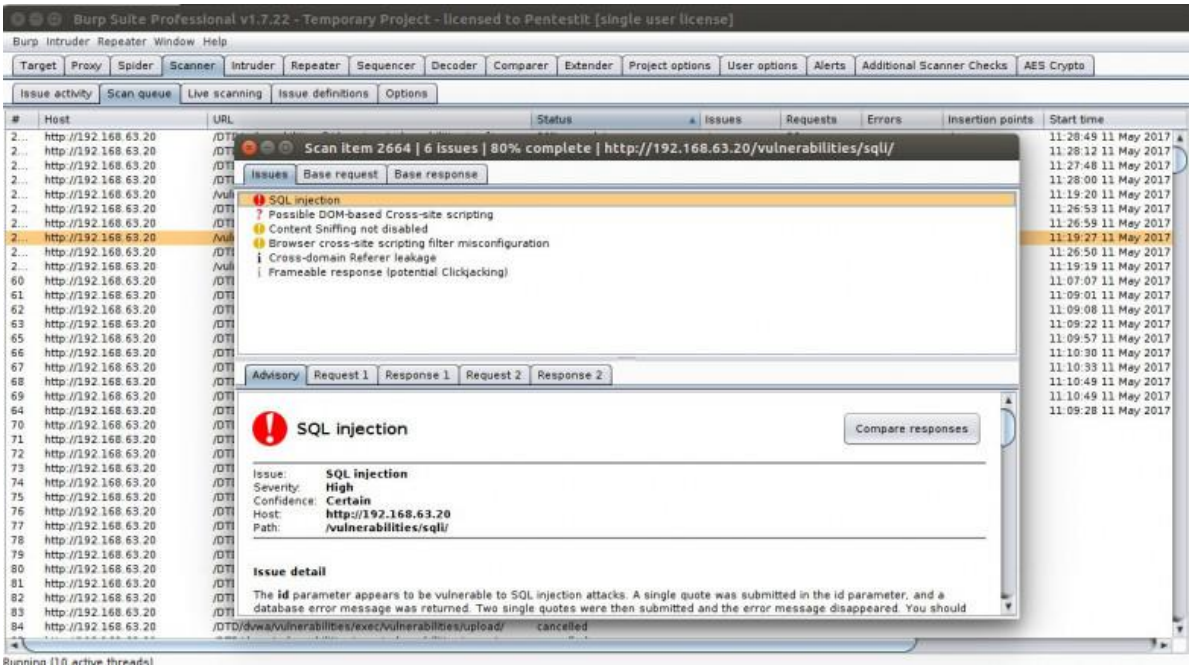


Рис. 3. Интерфейс программы OWASP ZAP

Заключение

Защищенность веб-приложений, используемых в военной сфере, требует комплексного подхода, включая создание специализированных полигонов для моделирования кибератак. Это позволит не только оценить текущую защищенность систем, но и разработать эффективные меры по предотвращению потенциальных угроз. Регулярный аудит, обновление программного обеспечения и обучение персонала являются ключевыми аспектами в обеспечении безопасности военных информационных систем.

Список используемых источников

1. Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. и др. Технические средства и методы защиты информации: Учебник для вузов / под ред. А. П. Зайцева и А. А. Шелупанова. ООО «Издательство Машиностроение», 2009. 255 с.

2. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Утв. приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 № 532-ст.

3. Типы сетевых атак и способы борьбы с ними [Электронный ресурс] URL: https://www.smart-soft.ru/blog/tipy_setevyh_atak_i_sposoby_borjby_s_nimi/ (дата обращения 22.01.2025).

4. OWASP Top 10 [Электронный ресурс] URL: https://owasp.org/www-project-top-ten/ (дата обращения 22.01.2025).

WEB APPLICATION SECURITY: MODELING NETWORK ATTACKS IN THE CYBERPOLYGON STRUCTURE

Makogon V., Neguritsa A., Trukhmanov I.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

With the rapid growth in the number of web applications and their use in various spheres of life, the issue of the security of these systems is becoming particularly relevant. This work is devoted to the study of methods for modeling network attacks on web applications within the framework of cyberpolygon, a specialized platform for testing and analyzing the security of information systems.

Key words: *web applications, modeling, cyberpolygon, security*

УДК 004.056.55
ГРНТИ 28.21.19

ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ, НЕ ПОРА ЛИ НАЧИНАТЬ БЕСПОКОИТЬСЯ

Ю. Я. Перевозник, И. В. Гвоздков, А. И. Ликарь

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

Последние сообщения от разработчиков квантовых компьютеров наталкивают на определенные мысли в плане будущего ассиметричной криптографии, основанной на «односторонних» функциях. Такие организации, как NIST и NSA, уже объявили конкурс на создание ассиметричных алгоритмов, устойчивых к атакам, с применением квантовых компьютеров. В статье будет рассмотрена одна из «односторонних» функций, способной обеспечить безопасность информационных систем в постквантовую эру.

криптография, эллиптические кривые, изогении, квантовый компьютер, постквантовая криптография

Существующее положение в криптографии

В современный криптографии широко используются симметричные алгоритмы (например, AES, «Кузнечик» и др.). При их реализации один ключ легко может быть вычислен из другого, а чаще всего они просто совпадают. Симметричные алгоритмы легко реализуемы на разных платформах и обладают высокой скоростью работы. Но проблема рассылки ключей при всеобщих коммуникациях остается практически не разрешимой без ассиметричной криптографии.

Ассиметричная криптография, основанная на «односторонних» функциях, успешно решает проблему рассылки ключей. Вычислить секретный ключ, зная открытый очень затруднительно в полиноминальное время, если ваш компьютер не обладает огромным быстродействием. Реализация алгоритмов ассиметричного шифрования, требует большой объем оперативной памяти и предполагает применение трудоемких операций.

Быстродействие современных процессоров, позволяющее решить задачу вычисления секретного ключа для симметричных криптосистем, и вычисления «закрытого» ключа для ассиметричных криптосистем, на основе существующих технологий растет приблизительно на 10 % при выходе на рынок следующего поколения процессоров. Темпы роста производительности процессоров успешно компенсируются увеличение длины ключа.

Так в криптосистеме RSA, основанной на одной из «односторонних» функций (факторизации числа), рекомендованная длина ключа не менее 1024 бита, что соответствует 309 знакам десятеричного числа. На сегодняшний день известно о факторизации числа, состоящего из 260 десятичных знаков, которое было реализовано в 2020 году.

Однако отцы-основатели RSA не сильно беспокоятся за свое «детище», так как эту проблему легко решить применение 2048-битного ключа (617 десятичных знака).

Расчеты исследователей, которые факторизовали 663-битное число (200 десятичных знака) показывают, что для этого потребуется 75 лет с применением одного компьютера с тактовой частотой 2,2 ГГц «Общим методом решетки числового поля» (по мнению исследователей – наиболее эффективный из известных методов факторизации большого числа).

Еще одна, применяемая в криптографии «односторонняя» функция – это дискретное логарифмирование. Применяется в схеме обмена ключей Диффи-Хэллмана. В основе этого алгоритма лежит функции $y^x (\mathrm{mod}\ P)$. Задача сводится к решению уравнения $a^x (\mathrm{mod}\ N) = b^y (\mathrm{mod}\ N)$. Для обеспечения достаточной стойкости алгоритма (например, сопоставимой с AES 128) размер «открытого» ключа должен составлять 3072 бит [2].

Проблему «рассылки» ключей без применения алгоритмов ассиметричного шифрования решить практически невозможно. Но применения в этих целях 1000-битных (и более) ключей значительно усложняет эту задачу. Увеличение размера ключа усложняет практическую реализацию этих алгоритмов, особенно с применением в устройствах с ограниченными вычислительными ресурсами и ограничениями на объем памяти.

Алгоритмы с применением эллиптических кривых позволяют значительно сократить размер ключа при одном и том же уровне безопасности (рис. 1) [2].

Security Strength	Symmetric Key Algorithms	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
≤ 80	2TDEA	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA[68]	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Рис. 1. Сопоставимые уровни защиты алгоритмов симметричного блочного шифрования и алгоритмов с асимметричным ключом

Можно заметить, что при одинаковом уровне безопасности алгоритмов (столбец 1), размер ключа при применении алгоритмов, основанных на эллиптических кривых, значительно меньше (столбец 5). В столбце 5 указан диапазон значений *f* (размер *n*, где *n* – порядок базовой точки *G*). При размере ключей на порядок меньше размеров для алгоритма RSA и алгоритмов, на базе схемы Диффи-Хэллмана, применение устройств с ограниченными вычислительными ресурсами и ограничениями на объем памяти становится более актуальным.

Эллиптические кривые

Кривые, описываемые уравнением третей степени, относятся к эллиптическим кривым. Эти кривые имеют много особенностей, которые необходимо учитывать при их применении в криптографии. Общее уравнение кривой третьей степени имеет вид [1]:

$$y^2 + axy + by = x^3 + cx^2 + dx + i$$

На практике в алгоритмах с использованием эллиптических кривых применяют кривые, описываемые уравнением $y^2 = x^3 + ax + b$, характеристикой $K \neq 2, 3$, с исключением «особенных» кривых (каноническая форма Вейерштрасса). Поэтому кривые, удовлетворяющие всем требованиям (например – к любой точке кривой можно провести касательную) называют неособыми. Для исключения особенных кривых должно выполняться условие [1]:

$$4a^3 + 27b^2 \neq 0,$$

где $4a^3 + 27b^2 = \Delta$, дискриминант эллиптической кривой,
при $\Delta = 0$ кривая не будет эллиптической.
На рисунке 2 приведены примеры эллиптических кривых.

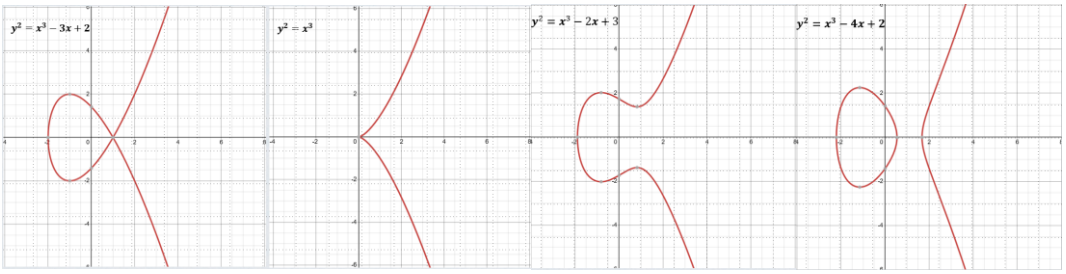


Рис. 2. Эллиптические кривые $y^2 = x^3 - 3x + 2$, $y^2 = x^3$ (являются «особенными»), $y^2 = x^3 - 2x + 3$ и $y^2 = x^3 - 4x + 2$

Можно заметить, что точки эллиптической кривой симметричны относительно оси *y*. Это свойство помогает при вычислении точек кривой. Ма-

тематически доказано, что три точки, находящиеся на одной прямой, удовлетворяют условию $P + Q + R = 0$. Геометрическое сложение точек эллиптической кривой представлено на рис. 3.

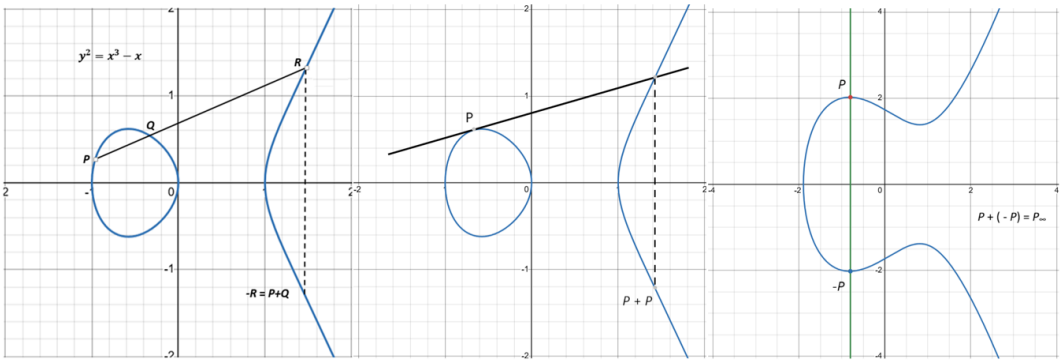


Рис. 3. Геометрическое представление операций

Для криптографических алгоритмов особый интерес представляют точки эллиптической кривой над конечным полем $\mathbb{R}$, причем вычисление точек производится по модулю над полем $\mathbb{F}_P$, т.е. применяется модулярная арифметика.

Если множество точек эллиптической кривой над полем $\mathbb{R}$ описывалось как $\left\{(x,y) \in \mathbb{R}^2 \;\middle|\; \begin{matrix} y^2 = x^3 + ax + b, \\ 4a^3 + 27b^2 \neq 0 \end{matrix}\right\} \cup \{0\}$

где $\{0\}$ – бесконечно удаленная точка, то над полем $\mathbb{F}_P$ эллиптическая кривая будет описываться как:

$$\left\{(x,y) \in \mathbb{F}_p \;\middle|\; \begin{matrix} y^2 = x^3 + ax + b \pmod p, \\ 4a^3 + 27b^2 \not\equiv 0 \bmod p) \end{matrix}\right\} \cup \{0\}.$$

Теперь наша эллиптическая кривая – это группа точек конечного поля $\mathbb{F}_p$ симметричные относительно оси x (у каждой точки есть обратная величина), которые удовлетворяют следующим свойствам: замыкание, ассоциативность, коммутативность. Обязательное наличие бесконечно удаленной точки $\mathcal{O}$. Группа точек является «абелевой» группой.

Сумма трех точек на одной прямой равна нулю ($P + Q + R = 0$). Но прямые над $\mathbb{F}_p$ отличаются от прямых над $\mathbb{R}$.

Прямая над $\mathbb{F}_p$ – это множество точек (x, y), удовлетворяющих уравнению $ax + by + c \equiv 0 \pmod p$. Добавление $(\mathrm{mod}\ p)$ изменяет вид прямой и делает ее «пилообразной» (рис. 4).

На рисунке слева кривая $y^2 = x^3 + 7x + 10 \pmod p$ с $p = 487$, а справа сложение точек для кривой $y^2 = x^3 - x + 3 \pmod{127}$, при $P =$

$(16,\ 20)$ и $Q = (41,\ 120)$. Соединяющая точки прямая $y \equiv 4x + 83 \pmod p$ как бы «повторяет» себя на плоскости [5].

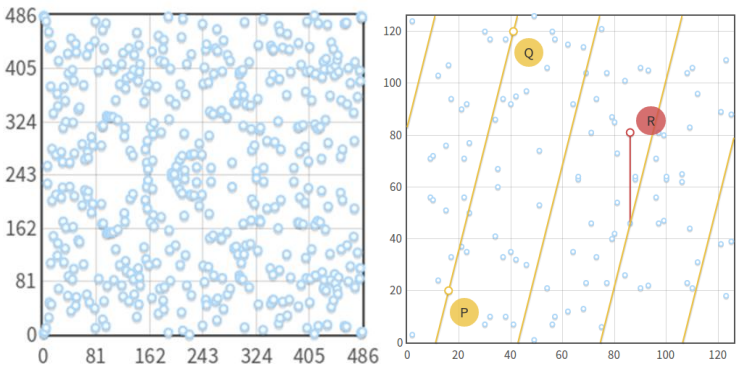


Рис. 4. Кривая $y^2 = x^3 + 7x + 10 \pmod p$ с $p = 487$ (слева)
сумма точек $P = (16,\ 20)$ и $Q = (41,\ 120)$(справа)

Еще одной особенностью эллиптических кривых является ***j***-инвариант – постоянная величина равная $j = 1728\frac{4a^3}{4a^3+27b^2}$ (для эллиптических кривых в форме Вейерштрасса). Этот параметр влияет на выбор эллиптической кривой в криптографии и тесно связан со стойкостью криптосистемы.

Стойкость криптосистемы

Несмотря на то, что размер ключа при применении эллиптических кривых в криптографических алгоритмах на порядок меньше ключей алгоритма RSA, которые необходимы для обеспечения одинакового уровня безопасности, существует достаточно большое количество ограничений на их применение.

Во-первых, это ограничение по дискриминанту для эллиптических кривых. Должно выполняться условие $4a^3 + 27b^2 \neq 0$, рассмотрено выше.

Во-вторых, эллиптические кривые можно разделить на суперсингулярные и несуперсингулярные (обычные). В криптографии рекомендовано использовать несуперсингулярные эллиптические кривые (один из параметров, характеризующих эти кривые, является ***j***-инвариант – постоянная величина равная $j = 1728\frac{4a^3}{4a^3+27b^2}$). При ***j***-инварианте равном 0, эллиптическая кривая является суперсингулярной.

В-третьих, суперсингулярные кривые очень чувствительны к атакам MOV (по первым буквам создателей – Менезес, Окамото, Ванстон), который основан на использовании «особой» функции, которая принимает на вход точку эллиптической кривой, а на выходе выдает элемент конечного

поля. Задача дискретного логарифмирования в конечном поле может быть решена за полиноминальное время.

При использовании несуперсингулярных эллиптических кривых может быть применен квантовый алгоритм Шора, где решение задачи дискретного логарифмирования, нахождение такого $\boldsymbol{k}$ по данным $y = g^k$, сводится к вычислению порядка другой функции, а именно: $f(x_1, x_2) = g^{x_1} y^{x_2}$, где g образующая группы с числом элементов, равным q. Период функции представляется парой чисел (w_1, w_2): $f(w_1 + x_1, w_2 + x_2) = f(x_1, x_2)$.

Тогда решение задачи дискретного логарифмирования будет иметь вид: $k = -\frac{w_1}{w_2} (\mathrm{mod}\ q)$ [3].

В-четвертых, в рекомендациях NIST[1] предлагается использовать только пять простых эллиптических кривых и десять бинарных, причем кривые были выбраны из соображений эффективной реализации на процессорах различной производительности, что при данных условиях относит эти эллиптические кривые к «подозрительным».

В-пятых, хотя в настоящее время полноценных квантовых компьютеров еще не появилось (прогнозируемый сток появления – 10 лет), угроза «нивелирования» стойкости криптографических алгоритмов с использованием эллиптических кривых становится актуальной. При применении квантовых компьютеров для факторизации больших чисел и решении задачи дискретного логарифмирования (в случае с эллиптическими кривыми, где размер ключа на порядок меньше при том же уровне безопасности) потребуется количество «проходов» меньше, чем для вскрытия алгоритма RSA, с которым и «конкурируют» алгоритмы с применением эллиптических кривых.

Решение возникающих проблем

С появлением квантового алгоритма Шора, способного за субэкспонициальное время «взламывать» криптографические алгоритмы, основанные на сложности решения задачи факторизации больших чисел и дискретного логарифмирования (даже при том, что эффективных квартовых компьютеров пока нет), возникла «задача» разработки новых алгоритмов шифрования, способных эффективно противостоять квантовой угрозе.

Разработка таких алгоритмов идет в двух направлениях, квантовой и постквантовой криптографии и в большей степени относится к ассиметрич-

[1] NIST (National Institute of Standards and Technology) – Национальный институт стандартов и технологий США

ной криптографии (криптографии с открытым ключом), которая может эффективно решить задачу распределения ключей.

Первое направление основано на использовании квантовой теории передачи информации, которая реализуется в системах квантового распределения ключей (КРК) и использует специальное оборудование (основной недостаток).

Второе направление – это использование математических методов. Если есть «односторонние» математические функций, которые не подвержены атакам с применением современных компьютеров, то можно предположить, что есть математические функций, которые не подвержены атакам (например, с применение алгоритма Шора) с применением квантовых компьютеров. Другими словами, гораздо легче «перенастроить» криптографические алгоритмы, использующие эти «функции», чем создать эффективный квантовый компьютер.

NIST уже инициировал процесс поиска и стандартизации квантово-устойчивых криптографических алгоритмов с открытым ключом. Такие стандарты с использованием алгоритмов на основе решетки модулей и на основе хэшей уже стандартизованы в 2024 году (FIPS)[2].

Алгоритмы, основанные на применении эллиптических кривых, также являются претендентами на применение в постквантовой криптографии. Эти алгоритмы отличаются от алгоритмов с использованием эллиптических кривых, применяемых в настоящее время.

Первое – они используют суперсингулярные эллиптические кривые, которые чувствительны к атакам MOV, но с применением *изогений*, теории кватернионов [6] и теории графов. Применение этих методов делаю криптографические алгоритмы на изогениях эллиптических кривых устойчивыми к атакам с применением квантовых компьютеров [4].

Изогении

Пусть $E1$ и $E2$ – эллиптические кривые, определенные над конечным полем $\mathbb{F}_q$. Изогения $\emptyset : E1 \rightarrow E2$, определенная над $\mathbb{F}_q$, является непостоянным рациональным отображением, определенным над $\mathbb{F}_q$, которое также является групповым гомоморфизмом от $E1$ ($\mathbb{F}_q$) до $E2$ ($\mathbb{F}_q$).

[2] FIPS 203, FIPS 204 и FIPS 205, в которых описаны алгоритмы, созданные на основе CRYSTALS-Dilithium (теории решеток), CRYSTALS-KYBER (применение хеш-функций) и SPHINCS+ (схема подписи на основе хэша без сохранения состояния), были опубликованы 13 августа 2024 года.

Степень изогении – это ее степень в виде рационального отображения. Для разделимых изогений иметь степень «означает иметь ядро определенного размера» (количество точек $E1$ переходящих в бесконечно удаленную точку $E2$). Каждая изогения степени больше 1 может быть включена в композицию изогений простой степени над $\mathbb{F}_q$ [5]. Эллиптические кривые $E1$ и $E2$ являются изогенными, если определены над одним полем $\mathbb{F}_q$ и количество точек у них одинаковое.

Каждая изогения имеет двойственную изогению (причем только одну, предполагающая обратное преобразование), т.е. если есть изогения $\emptyset: E_1 \to E_2$, то двойственная к ней $\widehat{\emptyset}: E_2 \to E_1$ (рис. 3, слева).

ℓ-группа кручения (степень изогении) E, обозначаемая $E[\ell]$, является множеством всех точек $P \in E(\mathbb{F}_q)$ такой, что ℓP является тождеством. Для ℓ такой, что $p \nmid \ell$ мы имеем $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$ [4].

При умножении изогении на ее двойственную получится точка кривой $E2$, умноженная на целое число ℓ (рис. 3, в центре). Результат наложения графов эллиптических кривых дает представление о сложности проведения атак на криптографический плгоритм с применением изогений (рис. 3, справа) [7].

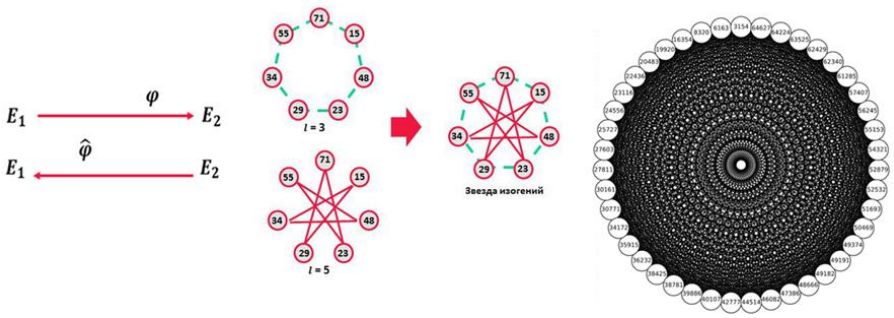


Рис. 3. Изогении, умножение и перестановка графов

Криптосистемы с открытым ключом, основанные на суперсингулярных кривых

Luca de Feo, David Jao, and Jerome Plut разработали и обосновали протоколы ЭЦП, обмена ключей и шифрования, основанные на суперсингулярных эллиптических кривых. Все протоколы основаны на коммутативной схеме, представленной на рис. 4 (слева), где ϕ и ψ – случайные вершины на графиках изогений степеней ℓ_A и ℓ_B соответственно. Их безопасность основана на сложности нахождения пути, соединяющего две заданные вершины в графе суперсингулярных изогений.

Обмен ключами

Протокол обмена ключами представляет собой вариацию на основе схемы Диффи-Хеллмана. Общедоступными параметрами являются суперсингулярная кривая E_0, определенная над $\mathbb{F}_{p^2}$, и основания $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$. Абонент **А** выбирает два случайных числа m_A, n_A , вычисляет изогению $\phi_A : E_0 \to E_A$ (это закрытые параметры), вычисляет отображение $\{\phi_A(P_B), \phi_A(Q_B)\} \subset E_A$ по своей секретной изогении ϕ_A и отправляет эти точки абоненту **Б** вместе с E_A (это открытые параметры). Абонент **Б** производит аналогичные действия, используя свои числа m_B, n_B. На рис. 4 (справа) стрелками показаны параметры, передаваемые «открыто».

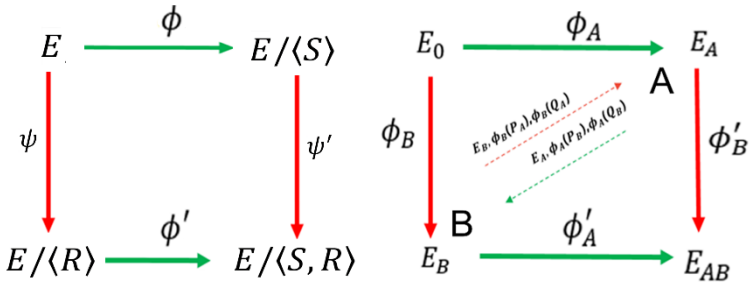


Рис. 4. Коммутативные схемы протоколов

Имея закрытые ключи и параметры передаваемые открыто абоненты **А** и **Б** могут построить изогении ϕ'_A и ϕ'_B, по которым они построят кривую E_{AB}, $\boldsymbol{j}$-инвариант, которой и будет общим секретом.

Заключение

На данный момент сложно оценить потребность в постквантовой криптографии, ведь квантового компьютера, способного ее взломать, пока не существует. Однако активность в NSA и NIST вызывает подозрения. Причины такой спешки остаются неясными.

Тем не менее, стоит проявить осторожность и начать изучение новой и перспективной области криптографии.

Список используемых источников

1. Болотов А., Гашков С., Фролов А., Часовских А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: КомКнига, 2024. 376 с

2. Баркер Э. Рекомендация по управлению ключами, часть 1: отчет NIST. Отдел компьютерной безопасности Лаборатория информационных технологий, Министерство торговли США, 2020. 54–55 с. URL: https://doi.org/10.6028/NIST.SP.800-57pt1r5 (дата обращения: 20.12.2024).

3. Шор В.: Алгоритмы квантовых вычислений: дискретные логарифмы и факторизация: 35-й ежегодный симпозиум по основам информатики (FOCS 1994), стр. 124–134.

4. Джао Д., Фео Л. На пути к квантово-устойчивым криптосистемам из изогений суперсингулярных эллиптических кривых. В: Янг, Б.-Й. (ред.) PQCrypto 2011. LNCS, том 7071, стр. 19–34. Springer, Heidelberg (2011). DOI:10.1007/978-3-642-25405-5_2.

5. Хабр: [сайт]/ Доступно о криптографии на эллиптических кривых. Андреа Корбеллини, – Текст: электронный. URL: https://habr.com/ru/articles/335906/. (дата обращения: 22.12.2024).

6. Хабр: [сайт]/ Доступно о кватернионах и их преимуществах. Иеремия ван Остен, – Текст: электронный. URL: https://habr.com/ru/articles/426863/ (дата обращения: 25.12.2024).

7. Хабр: [сайт]/ Постквантовая криптография и закат RSA – реальная угроза или мнимое будущее? Текст: электронный. URL: https://habr.com/ru/companies/neobit/articles/332942/ (дата обращения: 22.12.2024).

POST-QUANTUM CRYPTOGRAPHY, ISN'T IT TIME TO START WORRYING

Perevoznik Yu., Gvozdkov I., Likar A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Recent reports from quantum computer developers suggest certain thoughts about the future of asymmetric cryptography based on "one-way" functions. Organizations such as NIST and the NSA have already announced a competition to create attack-resistant asymmetric algorithms using quantum computers. The article will consider one of the "one-sided" functions capable of ensuring the security of information systems in the post-Quantum era.

Key words: *cryptography, elliptic curves, isogeny, quantum computer, post-quantum cryptography*

УДК:004.056.53
ГРНТИ: 81.93.29

ГИБРИДНЫЕ HONEYPOT- И HONEYNET-РЕШЕНИЯ ДЛЯ КИБЕРБЕЗОПАСНОСТИ НА ОСНОВЕ ПОРТАТИВНЫХ ВЫСОКОПРОИЗВОДИТЕЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ ПЛАТФОРМ

Р. Б. Петрив

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

Настоящая статья посвящена исследованию возможности использования портативных вычислительных платформ, в частности ноутбуков Maibenden 5-й серии на базе процессоров AMD и одноплатных вычислительных платформ Orange Pi 5 с гипервизором 1 типа Proxmox для развертывания Honeypot- и Honeynet-решений. Обсуждаются аспекты применения в выявлении техник атак на инфраструктуру и деанонимизации злоумышленника. Приведены основные этапы настройки и использования решения.

информационная безопасность, обманные технологии, Honeypot, Honeynet, Proxmox, деанонимизация злоумышленника

В условиях растущих угроз информационной безопасности, обеспечение защиты сетевых инфраструктур требует современных и доступных решений.

Несмотря на то, что абсолютного и всеобъемлющего решения по обеспечению информационной безопасности о защите сетевых активов не существует, высокий уровень защищенности может быть достигнут с помощью ряда мер и технических средств, одним из которых может быть Honeypot- и Honeynet-решение, позволяющее не только отвлечь злоумышленника, но и выявить техники его преступной деятельности. При этом известное ограничение Тьюринга, в связи с которым имитационная модель не может быть сложнее самого процесса или устройства, которые она моделирует, никак не сказывается на качестве обеспечения высокой перцептивной (с точки зрения наблюдателя в рамках используемых им средств наблюдения) или, иными словами, имитационной достоверности в связи с тем что возможности злоумышленника по разведке в сетевой инфраструктуре имеют ряд существенных ограничений, и может быть сравнительно легко реализована задача вывода ими нужных стороне защиты данных. Концептуальные требования к техническим решениям, рассмотренные в [1], позволили разработать и представить прототип недорогого программно-аппаратного

комплекса [2], с высокой степенью достоверности имитирующего сетевые сервисы, позволяющего при этом осуществлять гибкую настройку и адаптацию к конкретным условиям применения. Вместе с тем решение имело ограниченный характер, поскольку программный комплекс, который разворачивался на аппаратной платформе Raspberry Pi 4, представлял Honeypot-решение в виде рабочей станции с набором настраиваемых сервисов с использованием модифицированного кода [3], и построение на его основе Honeynet [4], то есть имитации сетевой инфраструктуры, имело ряд ограничений, поскольку масштабирование могло производиться только в направлении увеличения рабочих станций и соответственно программно-аппаратных комплектов, могло использоваться в составе Honeynet (имитации сетей и сегментов сетей), но само в полной мере развернуть Honeynet не позволяло.

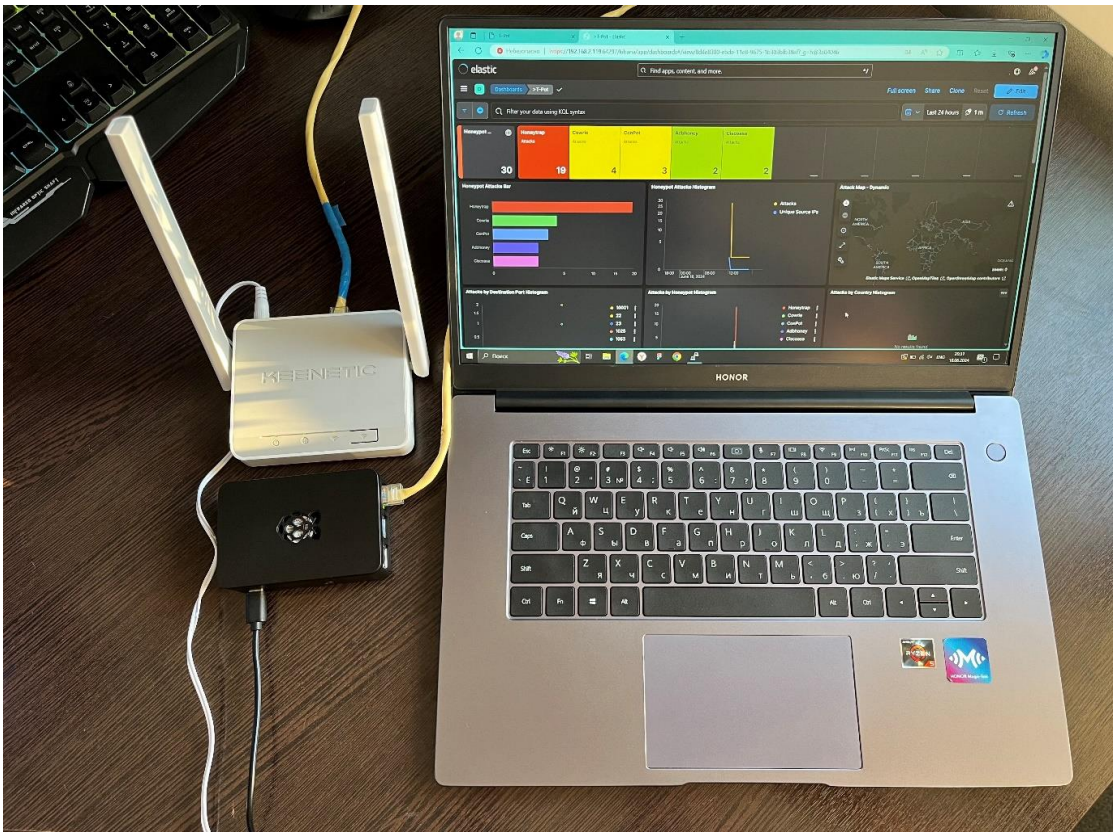


Рис. 1. Масштабируемое Honeypot решение на базе одноплатной вычислительной платформы Raspberry Pi

Преодолеть ограничение и обеспечить возможность развертывания Honeynet с высокой степенью имитационной достоверности возможно путем использования гипервизора 1 типа с открытым исходным кодом Proxmox [5], путем развертывания на портативных высокопроизводитель-

ных вычислительных платформах (рис. 2). В рамках гипервизора может развертываться Honeynet, в том числе с использованием беспроводного сегмента, при этом методы обнаружения, описанные в [6]. можно обойти путем гибридного способа построения Honeynet, в частности задействования устройств на базе микроконтроллеров ESP 32, ESP 8266 (которые часто используются в IOT устройствах) для имитации сети, например, из датчиков системы АСУ ТП.

Для развертывания гипервизора на одноплатной вычислительной платформе в связи с отсутствием официальной поддержки устройства со стороны проекта Proxmox была использована модификация неофициальной версии из [7].

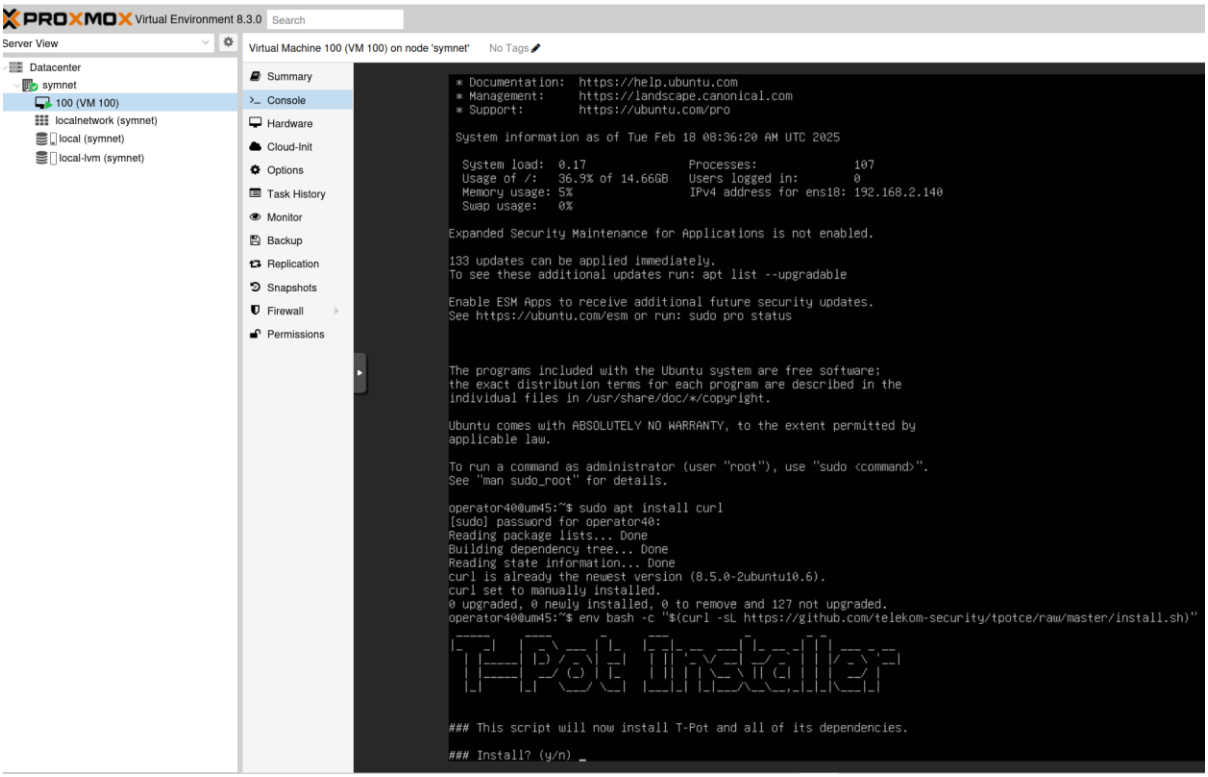


Рис. 2. Развертывание виртуальной рабочей станции с Honeypot решениями на базе модифицированного кода [3]

Проведенный эксперимент позволил подготовить к дальнейшим испытаниям 2 прототипа Honeynet платформы: на базе ноутбука Maibenden 5xx серии с процесором AMD Ryzen 7 (8 Core, 16 Threads 32 Gb RAM) и одноплатной вычислительной платформы Orange Pi 5 (8 Core, 16 Threads 16 Gb RAM).

Платформы возможно использовать как самостоятельно (поскольку виртуализация на основе гипервизоров 1 типа в настоящее время широко используется в производственной среде), так и в сочетании с программно-

аппаратными и аппаратными сетевыми устройствами. Важным критерием эффективности будет использование оптимального, соответствующего реальным практикам набора сервисов-ловушек, поэтому ни одно решение не должно запускаться «из коробки», поскольку немедленно выдает себя большим количеством различных сервисов на открытых портах (рис. 3), что в реальности встречается только на учебных объектах в лабораторной среде.

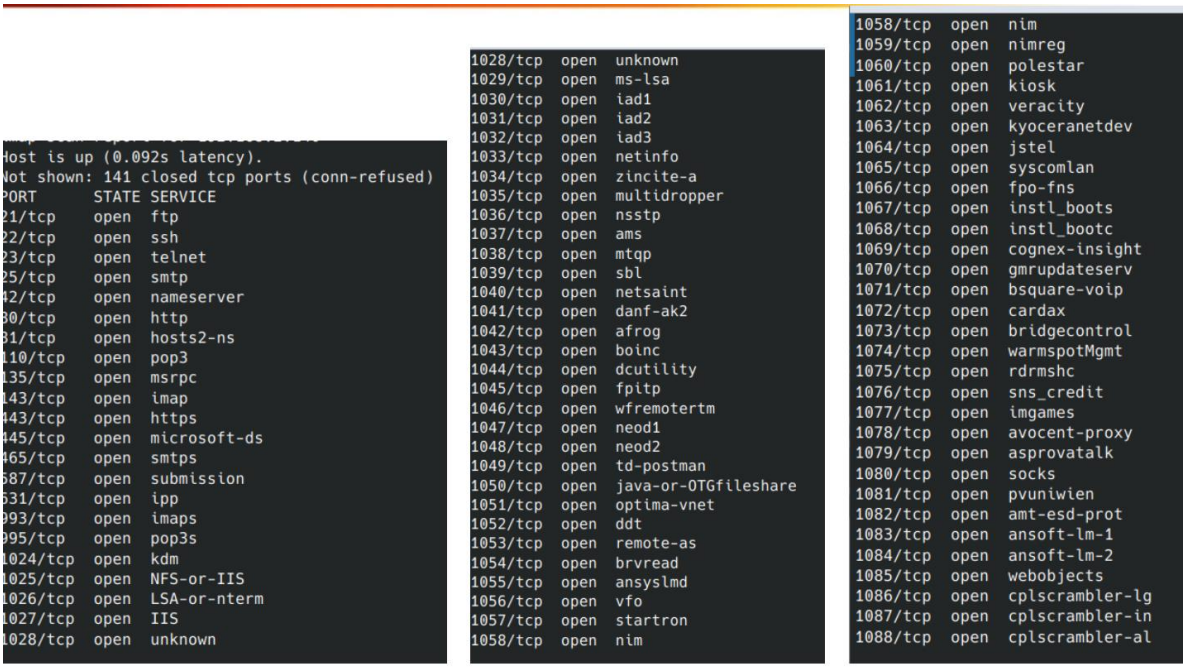


Рис. 3. Пример неверного развертывания сервисов-ловушек на рабочей станции в составе Honeynet

Honeynet для защиты промышленных сетей с беспроводным сегментом, содержащие сервисы имитирующие рабочие станции и объекты АСУ ТП могут дополняться фиктивными уязвимостями межсетевых экранов и формирования у злоумышленника ложной картины возможности передвижения по сети, использования доступа в Интернет (в составе Honeynet могут использоваться программно-аппаратные сетевые заглушки, описание которых выходит за рамки данной статьи и будет приведено в следующих). Важной особенностью Honeynet на основе портативных вычислительных платформ является возможность их автономной работы, то есть отсутствие реальной связи с какими бы то ни было реальными сетевыми системами.

Функциональность предложенных решений также может быть существенно повышена путем создания информационного наполнения файловыми объектами со стеганографическими метками (для возможности более точного выявления каналов утечки информации) и активными метками (для деанонимизации злоумышленника) по принципам, показанным в [8].

Список используемых источников

1. Красов А. В., Петрив Р. Б., Сахаров Д. В., Сторожук Н. Л., Ушаков И. А. Масштабируемое HONEYPOT-решение для обеспечения безопасности в корпоративных сетях. Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86-97.

2. Коломийцев Р. К. Разработка решений по повышению безопасности сетей с использованием обманных технологий. Дипломная работа. Руководитель Петрив Р. Б. СПб.: СПбГУТ, 2023.

3. T-Pot - The All in One Multi Honeypot Platform. [Электронный ресурс]. URL: https://github.com/telekom-security/tpotce/ (дата обращения 10.10.2024).

4. The Honeynet Project [Электронный ресурс]. URL: https://www.honeynet.org/ (дата обращения 10.10.2024).

5. Proxmox. Гипервизор 1 типа с открытым исходным кодом. [Электронный ресурс]. URL: https://proxmox.com (дата обращения 10.10.2024).

6. Коломийцев Р. К., Петрив Р. Б. Методы обнаружения HONEYPOT в корпоративной сети //Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т. СПб.: СПбГУТ, 2024. С. 450-453.

7. Proxmox-Port. Гипервизор 1 типа с открытым исходным кодом, неофициальная версия для Orange Pi [Электронный ресурс]. URL: https://github.com/jiangcuo/Proxmox-Port (дата обращения 10.10.2024).

8. Canarytokens [Электронный ресурс]. URL: https://github.com/thinkst/canarytokens (дата обращения 10.10.2024).

HYBRID HONEYPOT AND HONEYNET SOLUTIONS FOR CYBERSECURITY BASED ON PORTABLE HIGH-PERFORMANCE COMPUTING PLATFORMS

Petriv R.B.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents a research of a possibility of using compact computational hardware platforms, in particular Maibenden 5xx series AMD based notepads and single board Orange Pi 5 computers with type 1 hypervizor Proxmox for Honeypot and Honeynet solutions deployment. The aspects of usage, attack methodology discovery and attacker identity deanonimization are discussed. Basic stages of solution setting up and usage are presented.

Key words: *Information security, deception technologies, Honeypot, Honeynet, Proxmox, attacker identity deanonymization*

УДК 004.056
ГРНТИ 81.93.29

МЕТОДИКА ОПТИМИЗАЦИИ ПЛАНА РАСПРЕДЕЛЕНИЯ ФАЙЛОВ В РАСПРЕДЕЛЕННОМ ХРАНИЛИЩЕ ДАННЫХ SIEM-СИСТЕМ

И. Б. Саенко, Д. С. Иванцов

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Представлена методика оптимизации плана распределения файлов в распределенном хранилище данных SIEM-систем, учитывающая критерии устойчивости и оперативности функционирования. Раскрыта структура методики и ее основные этапы. Рассмотрен вопрос оптимизации распределения файлов после реконфигурации распределенного хранилища данных.

методика оптимизации; план распределения; распределенное хранилище данных; управление информацией и событиями безопасности

Предлагаемая методика предназначена для использования проектировщиками и разработчиками распределенных хранилищ данных (РХД) SIEM-систем с целью снижения среднего времени реакции системы на запросы пользователей, а также для административного персонала, обеспечивающего функционирование РХД в повседневное время. Она представляет собой инструмент, позволяющий сформировать оптимальный план распределения файлов, таким образом, что показатель оперативности выводится на максимум и удовлетворяются предъявляемые требования к РХД по устойчивости в условиях дестабилизирующих воздействий со стороны противника [1].

Данная методика состоит из четырех этапов:

1) подготовка исходных данных;

2) решение задачи формирования множества предпочтительных планов распределения файлов на этапах проектирования и реконфигурации РХД [2];

3) решение задачи поиска оптимального плана распределения файлов;

4) распределение (перераспределение) файлов по узлам хранения в соответствии с оптимальным планом распределения.

Общая структура методики представлена на рисунке 1.

Исследуем эффективность предложенной методики оптимизации [3].

Эксперимент проводился для следующей конфигурации:

– РХД состоит из n узлов;
– в РХД размещаются m файлов.

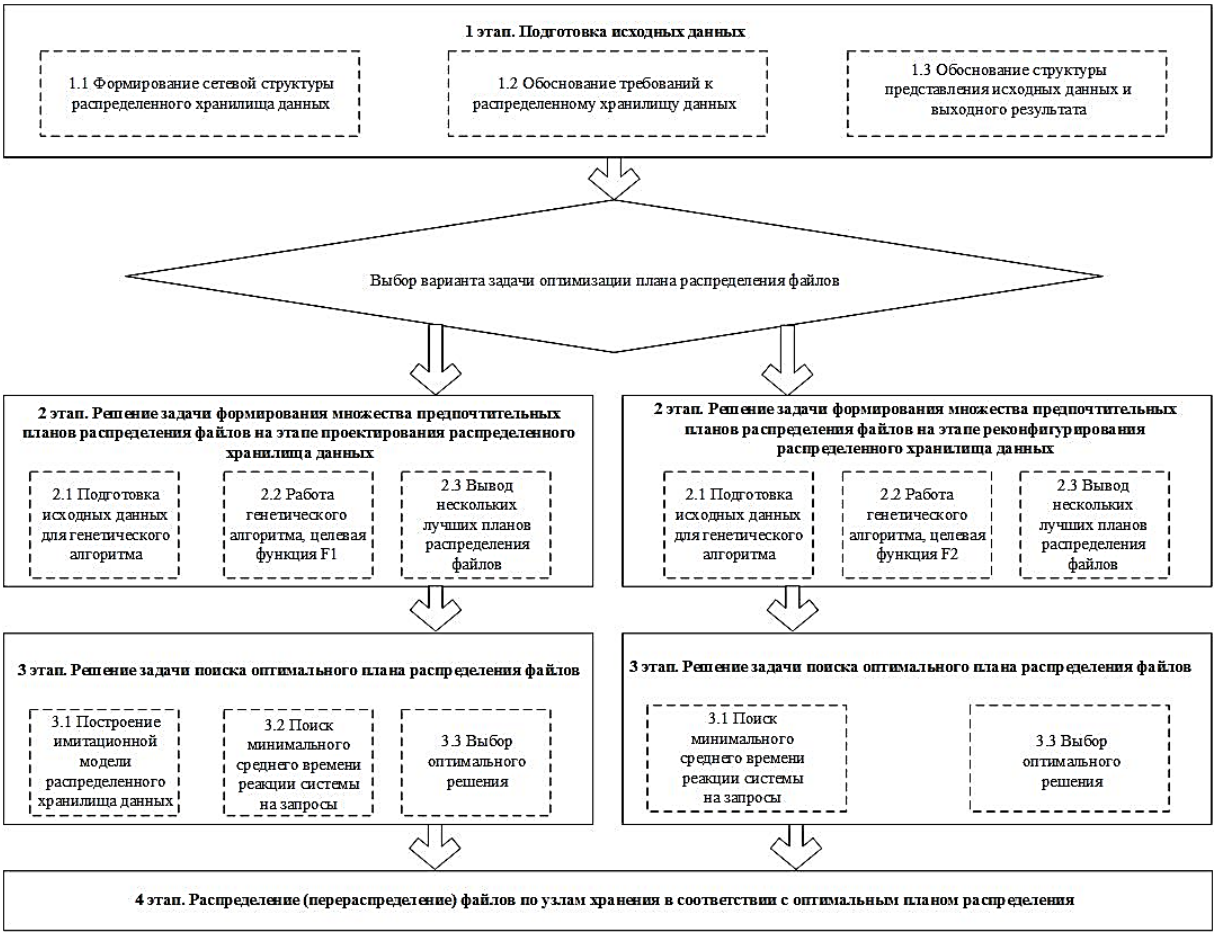


Рис. 1. Общая структура и взаимосвязь этапов методики оптимизации плана распределения файлов в РХД

– объем v_i i-го файла, интенсивность λ_j запросов к файлу с j-го узла задаются целочисленными массивами, а коэффициенты пропускных способностей c_{jl} между узлами j и l, вероятность PR_{li} формирования запросов с l-го узла к i-му файлу задаются вещественными матрицами;
– количество различных файлов $m = 20$;
– количество узлов хранения файлов в РХД $n = 5$;
– объем i-го файла $v_i \in [500; 150000]$ Кб, $i = \overline{1,m}$;
– интенсивность запросов к файлу с j-го узла $\lambda_j \in [1; 100]$ запросов/ч, $j = \overline{1,n}$;
– коэффициенты пропускных способностей между узлами j и l $c_{jl} \in [0{,}5; 100]$ Мбит/с, $j = \overline{1,n}$, $l = \overline{1,n}$;

– вероятность формирования запросов с l-го узла к i-му файлу $PR_{li} \in [0; 1]$, $l = \overline{1, n}$, $i = \overline{1, m}$.

Для решения оптимизационной задачи будем применять генетический алгоритм. В таблице 1 приведены гиперпараметры генетического алгоритма. По результатам серии экспериментов было вычислено среднее значение на каждой итерации (поколении), которое было принято в качестве оценки истинного значения исследуемой функции.

ТАБЛИЦА 1. Гиперпараметры генетического алгоритма

Гиперпараметр	Значение
Тип популяции	Битовый двумерный массив
Размер популяции	50
Вероятность скрещивания	0,8
Вероятность мутации	0,2
Тип оператора отбора родительских особей	Равновероятностный
Тип оператора скрещивания	Адаптивный N-точечный
Тип оператора мутации	Зависимый от ограничений

Для анализа влияния интенсивности запросов на значение вероятности того, что среднее время реакции системы на запросы пользователей будет не больше допустимого, был проведен ряд экспериментов. На рисунке 2 приведены графики зависимостей значений показателя оперативности для различных значений интенсивности запросов λ_j ($j = \overline{1, n}$) от количества поколений алгоритма при фиксированных значениях остальных гиперпараметров. Данные зависимости получены на основе результатов эксперимента с помощью программы формирования множества предпочтительных планов распределения файлов [4].

В таблице 2 приведен результат распределения файлов по узлам хранения при $\lambda_j \in [1; 10]$ запросов/час (итоговое значение показателя оперативности $P_{\text{оп}} = 0{,}967$). Результат для наглядности представлен в транспонированном виде [5].

Для проверки корректности работы предложенного генетического алгоритма задача была решена также с помощью метода множителей Лагранжа. Для тех же исходных данных и значений параметров, что и в приведенном выше эксперименте, полученное значение показателя оперативности равно $P_{\text{оп}} = 0{,}978$.

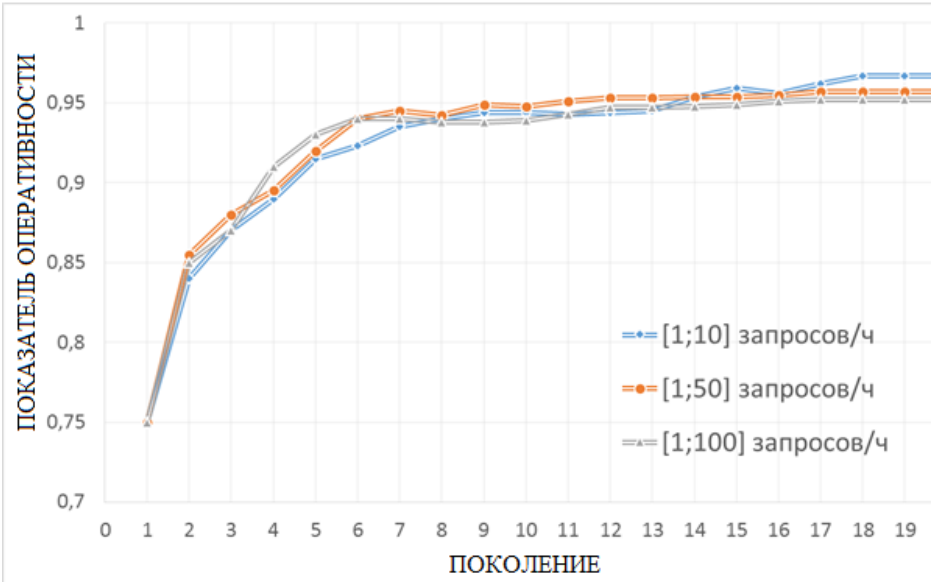


Рис. 2. Зависимости значений показателя оперативности от количества поколений при различных значениях интенсивности запросов

ТАБЛИЦА 2. Результат распределения файлов по узлам хранения

Файл / Узел	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	0	0	1	0	0	1	0	0	0	1	1	1	0	1	1	1	1	0
2	1	1	0	1	1	0	0	0	1	0	0	0	1	1	0	1	0	0	1	1
3	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0	0	1	1	0	0
4	1	0	1	0	0	0	0	1	1	1	0	1	0	0	0	1	1	0	0	0
5	0	0	0	1	0	0	1	0	0	0	0	0	0	1	1	1	1	1	1	0

Анализ приведенных результатов показывает, что значения показателя оперативности, полученные двумя алгоритмами, достаточно близки (отклонение не превышает 1,2 %). Разница значений вызвана несколько различными результатами распределения файла по узлам хранения РХД. Однако необходимо отметить, что предложенный генетический алгоритм, по сути, является приближенным методом. Однако он дает решения, в достаточной степени близкие к оптимальному. Кроме того, установлено, что при увеличении числа узлов и файлов время поиска решения увеличивается нелинейно, однако количество итераций генетического алгоритма практически не изменяется.

Таким образом, полученный в статье результат позволяет утверждать о возможности достижения с помощью предложенной методики более высокой оперативности функционирования РХД при условии его требуемой устойчивости.

Список используемых источников

1. Котенко И. В., Саенко И. Б., Паращук И. Б. Критерии оценки доступности информационных, телекоммуникационных и других критически важных ресурсов в интересах анализа их защищенности // Региональная информатика и информационная безопасность. Сборник трудов XII Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2021. Вып. 10. С. 97-101.

2. 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. № 2, pp. 98–110.

3. Саенко И. Б., Котенко И. В. Генетическая оптимизация и визуальный анализ при формировании схем доступа в ВЛВС // Информационные технологии и вычислительные системы. 2015. № 1. С. 33-46.

4. Иванцов Д. С., Саенко И. Б. Подход к обеспечению устойчивости и оперативности функционирования распределенных хранилищ данных о безопасности информации // XIX Санкт-Петербургская международная конференция «Региональная информатика (РИ-2024)». Санкт-Петербург, 2024, с. 108-110.

5. Богданов М. Д., Рудинский И. Д. Использование генетического алгоритма для решения задачи поиска оптимального пути // Вестник науки и образования Северо-Запада России, 2023, Т. 9, № 2, с. 76-88.

A TECHNIQUE FOR OPTIMIZING THE FILE DISTRIBUTION PLAN IN DISTRIBUTED DATA STORAGES OF SIEM SYSTEMS

Saenko I., Ivantsov D.
Saint Petersburg Federal Research Center Russian Academy of Sciences

The paper presents a technique for optimizing the plan of file distribution in distributed data storages of SIEM systems, taking into account the criteria of reliability and efficiency of operation. The structure of the technique and its main stages are disclosed. The issue of optimization of file distribution after reconfiguration of a distributed data storage is considered.

Key words: *optimization technique; distribution plan; distributed data storage; security information and event management*

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ МОДЕЛЕЙ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ ГРУППАХ

Д. В. Сахаров, С. В. Борисов

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

Социальные сети перестали являться только средством коммуникации. Их используют также для продвижения бизнеса, предоставления товаров и услуг, оглашения мнений и новостных событий. Данной способ распространения информации также применяется для намеренного введения людей в заблуждение путем проведения информационных кампаний. Для исследования распространения информации в социальных группах необходимо исследовать известные существующие модели, и сделать вывод о применимости подхода к использованию данного инструмента в социальных сетях.

информационная безопасность, социальные сети, модель распространения информации, социальная инженерия, ложная информация, фейковая информация.

Актуальность вопроса исследования распространения фейковой информации в социальных группах определяется:
– ростом количества информационных кампаний;
– массовостью распространения свободных инструментов для генерации мультимедиа [1];
– продолжающимся ростом атак социальной инженерии.

Целью работы является выявление актуальных моделей распространения информации в социальных группах для их применения к исследованию распространения фейковой информации на площадках социальных сетей.

Задачи работы:
– исследовать существующие модели;
– провести сравнительный анализ;
– предложить дальнейшие направления исследования.

Линейная модель коммуникации SMCRE

Линейная модель коммуникации SMCRE [2] представляет собой простейшую модель распространения информации в линейном виде (рис. 1). Преимуществом данной модели является ее простота, однако современные процессы распространения данная модель описать не может, как следствие, для описания данных в соцсетях данная модель нерелевантна.



Рис. 1. Линейная модель коммуникации SMCRE

Клеточный автомат

Клеточный автомат представляет собой динамическую систему, состоящую из однородных клеток, соединенных между собой. Состояние каждой клетки определяется клетками в окрестности выбранной. Состояние автомата *j* в момент времени *t+1* определяется как:

$$y_j = F\big(y_j(t), O(j), t\big),$$

где F – заданное правило, $O(j)$ – соседи, t – шаг.

Преимущество данной модели – масштабируемость, недостаток – отсутствие гибкости для описания процессов в соцсетях.

Модель независимых каскадов

Существует граф $G = (V, E)$, в котором каждому узлу v в момент времени t присваивается переменная: 0 – узел не инфицирован, 1 – инфицирован. Вероятность активации узла между активированным v и неактивированным узлом u равняется вероятности p_{vu}, являющейся весом ребра. Количества активных узлов на шаге *t* является суммой вероятностей того, что каждый узел будет активен в этом время. Вершина является участником сети, а ребро – зафиксированный факт действия в отношении друг друга [3].

Преимущество – масштабируемость, то есть возможно спрогнозировать распространение, недостаток: отсутствие гибкости для описания современных процессов.

Эпидемиологические модели на основе SIR

Эпидемиологические модели представляют собой мощную базу для описания процессов распространения информации в обществе. Классическая модель состоит из групп восприимчивых (susceptible), зараженных (infected) и выздоровевших (recovered) (рис. 2). Особи переходят из одной группы в другую, пока не настанет конец эпидемии.



Рис. 2. Эпидемиологическая модель на основе SIR

Модель описывается системой дифференциальных уравнений. Совершенствование данной модели представляет собой добавление новых групп и процессов [4]:

$$\frac{dS}{dt} = -\beta SI;$$
$$\frac{dI}{dt} = \beta SI - \gamma I;$$
$$\frac{dR}{dt} = \gamma I,$$

где β – эффективная частота контактов, показывающую какую часть общего числа контактов в единицу времени – γ, привела к заражению.

Преимущества: высокая адаптируемость – добавление групп, введение новых коэффициентов, масштабируемость. Стоит отметить большое количество современных исследований процесса распространения информации в социальных сетях с применением данной модели [5, 6, 7, 8], особенно в иностранной научной литературе, что является показателем актуальности применения данного инструмента.

Приведем сводную таблицу, показывающую релевантность рассмотренных моделей (табл. 1).

ТАБЛИЦА 1. Сводная таблица сравнения рассмотренных моделей

Модель	Адаптируемость (гибкость)	Масштабируемость	Релевантность
Линейная модель SMCRE	✗	✗	✗
Клеточный автомат	✗	✓	✗
Независимых каскадов	✗	✓	✓
Эпидемиологическая модель SIR	✓	✓	✓

Для исследования вопроса распространения целесообразно использовать модели независимых каскадов и эпидемиологических моделей.

Список используемых источников

1. Борисов С. В. Актуальность проблемы выявления сгенерированного видео с использованием технологий искусственного интеллекта в социальных сетях и цифровых медиа / С. В. Борисов // Безопасные информационные технологии : Сборник трудов Тринадцатой международной научно-технической конференции, Москва, 30 октября – 01 2024 года. Москва: МГТУ им. Н.Э.Баумана, 2024. С. 42-45. EDN IMJYMW.

2. Kaahwa, Mark & Zhu, Chang & Muhumuza, Moses & Mutyebere, Rodgers & Karemera, Charles. (2019). The Effectiveness of Audio Media in Enhancing Farm-ers' Knowledge: The Case of Smallholder Banana Farm-ers in Western Uganda. International Journal of Recent Contributions from Engineering, Science & IT (iJES). 7. 68. 10.3991/ijes.v7i2.10847.

3. Торопов Б. А. Модель независимых каскадов распространения репоста в онлайновой социальной сети // Кибернетика и программирование. 2016. № 5. С. 199-205. DOI: 10.7256/2306-4196.2016.5.20624 URL: https://nbpublish.com/library_read_article.php ?id=20624.

4. Konstantinov I. S. Mathematical analysis of SIR model with incubation period / I. S. Konstantinov, A. T. T. Taha // Research Result. Information Technologies. 2024. Vol. 9. № 3. P. 3-9. DOI 10.18413/2518-1092-2024-9-3-0-1. EDN CEUOWY.

5. Cao Z., Guo L. The Stability of MSIR Epidemic Model with Natural Age and Infection-Age. Journal of Xinjiang University (Natural Science Edition in Chinese and English), 2024, 41(4): 419-426. https://doi.org/10.13568/j.cnki.651094.651316.2023.11.16.0002.

6. Singh H. K., Pandey D.N. Analysis of the Chickenpox Disease Evolution in an MSEIR Model Using Fractal-Fractional Differential Operator. Differ Equ Dyn Syst (2024). https://doi.org/10.1007/s12591-024-00690-1.

7. Alkhazzan, Abdulwasea, et al. "A novel SVIR epidemic model with jumps for understanding the dynamics of the spread of dual diseases." Chaos: An Interdisciplinary Journal of Nonlinear Science 34.9 (2024).

8. Hasan Md & Islam, Saiful & Podder, Chandra. (2021). IVESR Rumor Spreading Model in Homogeneous Network with Hesitating and Forgetting Mechanisms. Journal of Applied Mathematics and Computation. 5. 105-118. 10.26855/jamc.2021.06.005.

ANALYSIS OF INFORMATION DISSEMINATION MODELS IN SOCIAL GROUPS

Sakharov D., Borisov S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Social media is no longer just a means of communication. They are also used to promote businesses, provide goods and services, and spread opinions and news events. This method of spreading information is also used to intentionally mislead people through information campaigns. To study the dissemination of information in social groups, it is necessary to investigate known existing models and conclude that the approach to using this tool in social networks is applicable.

Key words: *information security, social networks, information dissemination model, social engineering, false information, fake information*

УДК 004.056.5
ГРНТИ 81.93.29

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА: ОБЗОР АНТИФРОД-РЕШЕНИЙ

Д. В. Сахаров, Г. А. Демидов

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

Современные технологии защиты от телефонного мошенничества становятся критически важными в условиях растущей угрозы со стороны злоумышленников. В статье рассматриваются современные антифрод-решения, направленные на защиту от этих угроз. Анализируются основные механизмы защиты, а также уделяется внимание новым технологиям, включая искусственный интеллект и машинное обучение, которые позволяют повышать эффективность защиты.

телефонное мошенничество, злоумышленников, антифрод-решения, искусственный интеллект, машинное обучение

Телефонное мошенничество представляет собой одну из самых острых угроз в сфере кибербезопасности, что делает необходимость разработки эффективных антифрод-решений крайне актуальной [1-3]. В условиях глобальной цифровизации, когда мобильные телефоны стали неотъемлемой частью повседневной жизни, масштабы проблемы стали значительно увеличиваться. Согласно данным Центробанка (рис. 1), в 2023 году количество операций без согласия клиентов увеличилось на 15 % по сравнению с предыдущим годом, что подтверждает актуальность разработки эффективных антифрод-решений.

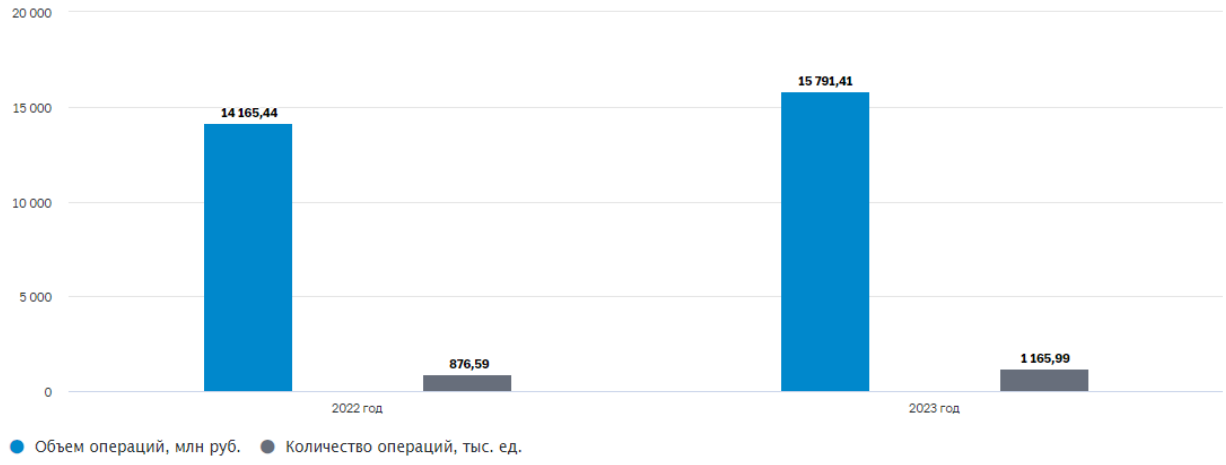


Рис. 1. Динамика общего объема и количества операций без согласия клиентов в 2022-2023 годах

Классификация угроз телефонного мошенничества

Злоумышленники используют различные методы воздействия, чтобы обманом получить доступ к личным данным, деньгам или конфиденциальной информации. Важно различать различные виды мошенничества, так как каждый из них требует специфических методов защиты и борьбы.

Основные типы телефонного мошенничества:

1. Фишинг через телефонные звонки (vishing): Злоумышленники выдают себя за сотрудников банков, государственных учреждений или техподдержки, чтобы получить доступ к конфиденциальной информации, такой как пароли, данные банковских карт или коды подтверждения. Они часто создают ощущение срочности и давления, чтобы заставить жертву выполнить нужные действия, например, передать код из СМС или совершить перевод средств. Этот способ остается одним из самых распространенных из-за его простоты и высокой эффективности.

2. Мошенничество через подмену номеров (spoofing): Используя специальные технологии, мошенники меняют номер звонящего, чтобы он выглядел как номер доверенной организации или знакомого человека. Это вызывает ложное чувство безопасности и нередко приводит к раскрытию личных данных или выполнению мошеннических действий. Этот способ часто комбинируется с vishing, что делает атаки еще более убедительными. Особой популярностью spoofing пользуется для целевых атак на корпоративные структуры и государственные учреждения.

3. Социальная инженерия и обман: Этот вид мошенничества основан на манипуляции и психологическом давлении. Злоумышленники используют сценарии, такие как угроза блокировки счета, обещание выигрыша или просьба помочь близким. Социальная инженерия полагается на доверие и эмоции, что делает ее особенно опасной. Мошенники искусно подбирают схемы воздействия, воздействуя на психоэмоциональное состояние жертвы, что значительно усложняет выявление таких атак.

Эти виды мошенничества являются серьезной угрозой, поэтому для их предотвращения необходимы эффективные меры защиты, адаптированные под специфику каждой угрозы.

Основные подходы к защите от телефонного мошенничества

Среди основных подходов, направленных на предотвращение подобных угроз, можно выделить использование черных списков для блокировки известных мошенников, технологии анализа голосового трафика, методы выявления аномалий в поведении вызовов и интеграцию антифрод-систем с операторами

связи и мобильными приложениями [4, 5]. Эти методы помогут сформировать многослойную систему защиты, способную эффективно реагировать как на традиционные, так и на новые формы телефонного мошенничества.

Использование черных списков и блокировки известных мошенников. Одним из базовых методов противодействия телефонному мошенничеству является использование черных списков номеров, устройств и других идентификаторов, связанных с ранее выявленной мошеннической активностью. Такие списки формируются на основе данных операторов связи, правоохранительных органов и специализированных служб по анализу угроз. При поступлении вызова номер проверяется по базе данных, и при совпадении вызов блокируется автоматически.

Примеры черных списков можно найти в сервисах Truecaller и Hiya, позволяющих фильтровать нежелательные звонки, или в решениях операторов, таких как МТС, которые блокируют подозрительные номера в рамках услуг защиты от спама.

Преимущества черных списков – высокая эффективность в блокировке повторяющихся угроз, простота внедрения и оперативность работы. Метод позволяет мгновенно заблокировать звонки от известных мошенников, снижая риски для пользователей. Однако он менее эффективен против новых угроз, номеров, не внесенных в базы данных, и подмененных номеров, использующих технологии spoofing. Массовые атаки могут перегружать списки, требуя их регулярного обновления.

Применение технологий анализа голосового трафика. Такие системы как распознавание речи и голосовая биометрия, помогают выявлять мошенничество по содержанию речи и характеристикам голоса. Анализ текста распознает сценарии социальной инженерии, а биометрия – идентифицирует подозрительных абонентов по уникальным голосовым параметрам, даже без черных списков.

Примером являются технологии Pindrop для финансовых учреждений и голосовая биометрия, используемая Сбербанком для аутентификации. Эти методы эффективно выявляют мошенников, даже при использовании подменных номеров, и повышают точность идентификации, не завися от номеров. Однако их эффективность может снижаться из-за плохого качества связи, низкой громкости или шума.

Методы выявления аномалий в поведении вызовов. Для борьбы с неизвестными угрозами широко используются методы анализа аномалий, которые позволяют выявлять подозрительные действия на основе отклонений от стандартного поведения [6, 7].

Такие методы включают:

– анализ временных и географических паттернов вызовов,
– обнаружение необычно высокой активности вызовов на определенные номера,
– идентификацию попыток скрытия идентификаторов вызывающих устройств.

Примеры таких систем включают решение компании RSA Security, которая использует алгоритмы для анализа аномальных вызовов, и системы, внедренные в некоторых российских операторах связи для защиты от мошенничества.

Преимущества этих методов заключаются в их способности обнаруживать ранее неизвестные угрозы, не представленные в черных списках, путем анализа поведенческих паттернов. Такие системы могут эффективно реагировать на новые схемы мошенничества, которые основаны на изменении привычных методов [8, 9] Недостатками же являются высокие требования к вычислительным мощностям и сложности в обучении моделей на качественных данных. Кроме того, существует риск ложных срабатываний, когда действия легитимных пользователей могут быть ошибочно классифицированы как мошенничество из-за нестандартного поведения, что требует дополнительной настройки алгоритмов и внимательного анализа данных.

Интеграция антифрод-систем с операторами связи и мобильными приложениями. Данный метод позволяет эффективнее бороться с телефонным мошенничеством, так как операторы связи предоставляют данные о вызовах, включая маршрутизацию, длительность и геопозицию, что помогает быстро выявлять подозрительные активности. Мобильные приложения, интегрированные с антифрод-системами, уведомляют пользователей о потенциальных угрозах, предоставляют обратную связь и ускоряют реагирование благодаря локальной обработке данных.

Такая интеграция является сотрудничеством оператора связи МТС с банками для защиты от мошенничества с помощью СМС-оповещений и блокировки подозрительных звонков.

Преимущества включают высокую скорость реагирования, возможность блокировки мошеннических вызовов до их достижения пользователя, улучшение точности фильтрации и повышение удобства для клиентов, которым предоставляется информация и инструменты для оперативных действий.

Будущее антифрод-решений

Телефонное мошенничество продолжает развиваться, становясь серьезной угрозой кибербезопасности. Методы, такие как vishing и spoofing, ста-

новятся сложнее, требуя от антифрод-систем быстрой адаптации. Рост числа операций без согласия клиентов подчеркивает необходимость более эффективных мер защиты.

Развитие нейронных сетей и голосовой биометрии для анализа речи. Современные нейронные сети анализируют речь, выявляют скрытые паттерны мошеннических звонков и используют голосовые биометрические параметры для идентификации злоумышленников [10, 11]. Это особенно эффективно при подмене голоса и номера. Голосовая биометрия также используется для аутентификации пользователей, повышая защиту в банковских и других сервисах.

Усовершенствованные модели глубокого обучения смогут анализировать эмоции, намерения и контекст разговоров, предугадывая сценарии мошенничества, даже с применением новейших технологий подмены голоса и номеров.

Тренды в интеграции антифрод-систем с повседневными устройствами. С ростом популярности умных устройств и мобильных приложений наблюдается тенденция к интеграции антифрод-систем с такими платформами. Это включает:

– использование виртуальных помощников (например, Google Assistant, Siri) для предупреждения о подозрительных вызовах;
– внедрение антифрод-функций в приложения с уведомлениями в реальном времени и подтверждением операций;
– интеграцию с операторами связи для блокировки угроз на уровне инфраструктуры.

В будущем антифрод-системы будут активнее взаимодействовать с носимыми гаджетами, такими как умные часы и наушники, которые смогут предупреждать пользователя о рисках голосовыми или вибросигналами.

Заключение

Современные угрозы телефонного мошенничества требуют комплексного подхода, объединяющего искусственный интеллект, голосовую биометрию и межотраслевое сотрудничество. Интеграция антифрод-систем с операторами связи, мобильными приложениями и повседневными устройствами повышает удобство и скорость реагирования на угрозы. Несмотря на вызовы, такие как защита конфиденциальности и обработка больших данных, развитие нейронных сетей и биометрической аутентификации формирует перспективу создания универсальных адаптивных систем, способных эффективно противостоять мошенничеству в условиях цифровой эпохи.

Список используемых источников:

1. Костарев С. В., Карганов В. В., Липатников В. А. Технологии защиты информации в условиях кибернетического противоборства // Санкт-Петербург, 2020.
2. Ярцев А. Г., Лавров В. В. Алгоритмы оценки рисков и принятия решений по определению мошенничества в современных антифрод-системах //Теплотехника и информатика в образовании, науке и производстве (ТИМ'2021). Екатеринбург, 2021.С. 331-335.
3. 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. VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С. В. Бачевского. 2018. С. 191-195.
4. Сенцова А. Ю., Тимергазин В. Э., Ильясова Р. И. Антифрод-система как инструмент предотвращения мошенничества //Информационные технологии. Проблемы и решения. 2021. Т. 4. №. 17. С. 101-107.
5. Борисов С. В., Севостьянов В. А., Цветков А. Ю. Определение признаков фишинговых сообщений в электронной почте // В сборнике: Студенческая весна-2023. Материалы 77-ой региональной научно-технической конференции студентов, аспирантов и молодых ученых. Санкт-Петербург, 2023. С. 88-92.
6. Карев А. С., Бирих Э. В., Сахаров Д. В., Виткова Л. А. Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 66-70.
7. Андрианов В. И., Виткова Л. А., Сахаров Д. В. Исследование алгоритма защиты общедоступных персональных данных в информационных системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 227-231.
8. Тимергазин В. Э., Ильясова Р. И., Сенцова А. Ю. Противодействие схемам мошеннических действий с помощью антифрод-систем //Мавлютовские чтения. 2021. С. 570-575.
9. Бирих Э. В., Ферапонтова С. С. К вопросу об аудите персональных данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С. В. Бачевского. 2018. С. 111-114.
10. Замятина Е. В. Использование генеративно-состязательных сетей в антифрод-системах коммерческого банка // Технические системы и технологические процессы. 2018. С. 84-86.
11. Шашкин В. С., Сахаров Д. В., Яковлев В. А., Андрианов В. И Основные угрозы социальной инженерии в государственных учреждениях // В сборнике: Материалы Всероссийской научно-практической конференции "Национальная безопасность России: актуальные аспекты" ГНИИ "Нацразвитие". Июль 2018. Сборник избранных статей. 2018. С. 36-46.

MODERN PHONE FRAUD PROTECTION TECHNOLOGIES: AN OVERVIEW OF ANTI-FRAUD SOLUTIONS

Sakharov D., Demidov G.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Modern technologies for protecting against telephone fraud are becoming critically important in the face of a growing threat from intruders. The article discusses modern anti-fraud solutions aimed at protecting against these threats. The main protection mechanisms are analyzed, and attention is also paid to new technologies, including artificial intelligence and machine learning, which make it possible to increase the effectiveness of protection.

***Key words**: phone fraud, intruders, anti-fraud solutions, artificial intelligence, machine learning*

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ ФЕЙКОВЫХ АККАУНТОВ ОБЪЕДИНЕННЫХ В БОТНЕТЫ В СОЦИАЛЬНЫХ СЕТЯХ

Д. В. Сахаров, В. С. Шашкин

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

В условиях современного мира, характеризующегося высокими скоростями распространения информации, проблема распространения деструктивной информации и фейковых новостей, в частности, приобретает все большую актуальность. Анализ фейковых аккаунтов в социальных сетях позволяет минимизировать последствия их деструктивных активностей благодаря обнаружению «замороженных» ботнетов. Своевременное обнаружение таких аккаунтов способствует принятию превентивных мер по их деактивации.

информационная безопасность, социальные сети, ботнет, фейки

Введение

Исследование активности деструктивных ботнетов в социальных сетях продемонстрировало высокую результативность по сравнению с ручным анализом профилей и представляет собой подход, кардинально отличающийся от концепции реагирования на уже совершенную публикацию деструктивного контента после его размещения. А также подтвердило обоснованность выбранного вектора защиты от ботнетов в социальных сетях [1].

Авторы продемонстрировали способ определения одиночных фейковых аккаунтов исходя из факторов заполнения профиля злоумышленником. Помимо прочего полученные результаты позволяют сделать предположение, что фейковые учетные записи являются частью организованных ботнетов, не только в целях создания взаимной активности, симулирующей действия реальных пользователей для повышения доверия к профилю, но и для массированной информационной атаки.

Исследование

Самый популярный метод блокировки фейковых аккаунтов, основанный на лингвистическом анализе деструктивного контента ограничен из-за:

– необходимости постоянно пополнять и актуализировать трендовые направления и темы информационных противостояний, что, по своей сути, ставит правоохранительные органы или администрацию социаль-

ных сетей изначально в проигрышное положение. Один из методов ведения информационных войн основан на предварительном «прогревании» целевой аудитории. Злоумышленники активно распространяют определенную позицию в широких масштабах перед основным вбросом фейковых новостей. После публикации ложной информации они подкрепляют свою точку зрения, ссылаясь на уже сформированную ими же позицию. Этот подход применялся еще во времена Второй мировой войны. Йозеф Геббельс, главный пропагандист Третьего Рейха, использовал государственный аппарат для предварительной подготовки общественного мнения к важным реформам, проводимым правительством Германии. Данная методика позволяет злоумышленникам заблаговременно и более углубленно распространять контент, который после перехода фейка в активную фазу, становится запрещенным и попадает в базы для мониторинга;

– использования злоумышленниками методов искажения сообщений. К таким методам относятся: замена букв русского алфавита на буквы и символы других языков, схожие по написанию; использование изображений с нужным текстом вместо текстовых сообщений; намеренное искажение написания слов и т. д. Эти подходы значительно снижают эффективность автоматического лингвистического анализа или требуют дополнительных ресурсов для применения методов искусственного интеллекта;
– огромного объема анализируемых данных [2].

Базовая методика определения одиночных недостоверных учетных записей в социальных сетях [3] позволила обнаруживать «замороженные» аккаунты злоумышленников еще до момента их использования (публикации деструктивного контента), что помимо прочего позволяет анализировать векторы будущих информационных атак, посредством исследования повторяющихся и легитимных сообщений с этих страниц. Данный анализ векторов позволяет оперативно пополнять базы для лингвистического анализа сообщений в социальных сетях.

Параллельный анализ больших данных, полученных во время разработки и применения методики борьбы с деструктивным контентом, позволил обнаружить закономерности в поведении лиц управляющих данными ботнетами. Помимо применения имеющихся «готовых» профилей в сети ботнетов, для создания активности на «пустых» учетных записях, в целях укрепления легенды «настоящего профиля живого человека», данные ботнеты используются для совместного распространения фейковых новостей. Операторы ботнетов после публикации фейковой новости с одной из ячеек

ботнета, начинают проявлять лояльность к автору и создавать нужную атмосферу для «правильного» восприятия опубликованного деструктивного контента. Исходя из анализа подобных событий, было выявлено, что процесс, как публикации, так и фейковой поддержки целевой новости, полностью автоматизирован средствами API социальной сети, что указывает на серьезную предварительную подготовку, использование ресурсоемкого оборудования и SIM-ферм, для регистрации новых учетных записей.

Экспериментальная часть

Аудит собранного банка данных посредством применения теории графов позволил построить связи между потенциальными ячейками ботнета и выявить их иерархию. Узлами показаны обнаруженные недостоверные учетные записи, кратность ребра определялась согласно критериям оценки связей между фейковыми аккаунтами, представленными в таблице 1.

ТАБЛИЦА 1. Критерии оценки связи между недостоверными страницами

Признак	Описание признака	Вес признака	Перманентные мультиребра
Односторонняя отметка «мне нравится»	P1 поставил отметку «мне нравится» P2 || P2 поставил отметку «мне нравится» P1	0.1	Нет
Односторонний комментарий	P1 оставил комментарий P2 || P2 оставил комментарий P1	0.15	Да
Обоюдная отметка «мне нравится»	P1 поставил отметку «мне нравится» P2 && P2 поставил отметку «мне нравится» P1	0.1	Нет
Обоюдные комментарии	P1 оставил комментарий P2 && P2 оставил комментарий P1	0.15	Да
Добавление в подписчики	P1 добавил P2 в друзья, P2 оставил P1 в подписчиках || P2 добавил P1 в друзья, P1 оставил P2 в подписчиках	0.1	Нет
Добавление в друзья	P1 и P2 двусторонне добавили в друзья оба аккаунта	0.2	Да
Репост записи со страницы	P1 сделал репост записи P2 || P2 сделал репост записи P1	0.2	Да

Граф определен авторами с разрешением кратных ребер. Наличие мультиребер между узлами (недостоверными пользователями) обозначает

отношение фейковых аккаунтов к одному ботнету. Для узлов, имеющих признак не отмеченный перманентными мультиребрами, минимальная сумма весов признаков, для установления кратных ребер – 0,2.

Способ объединения учетных записей злоумышленников в потенциальные сети представлен в виде блок-схемы на рисунке 1.

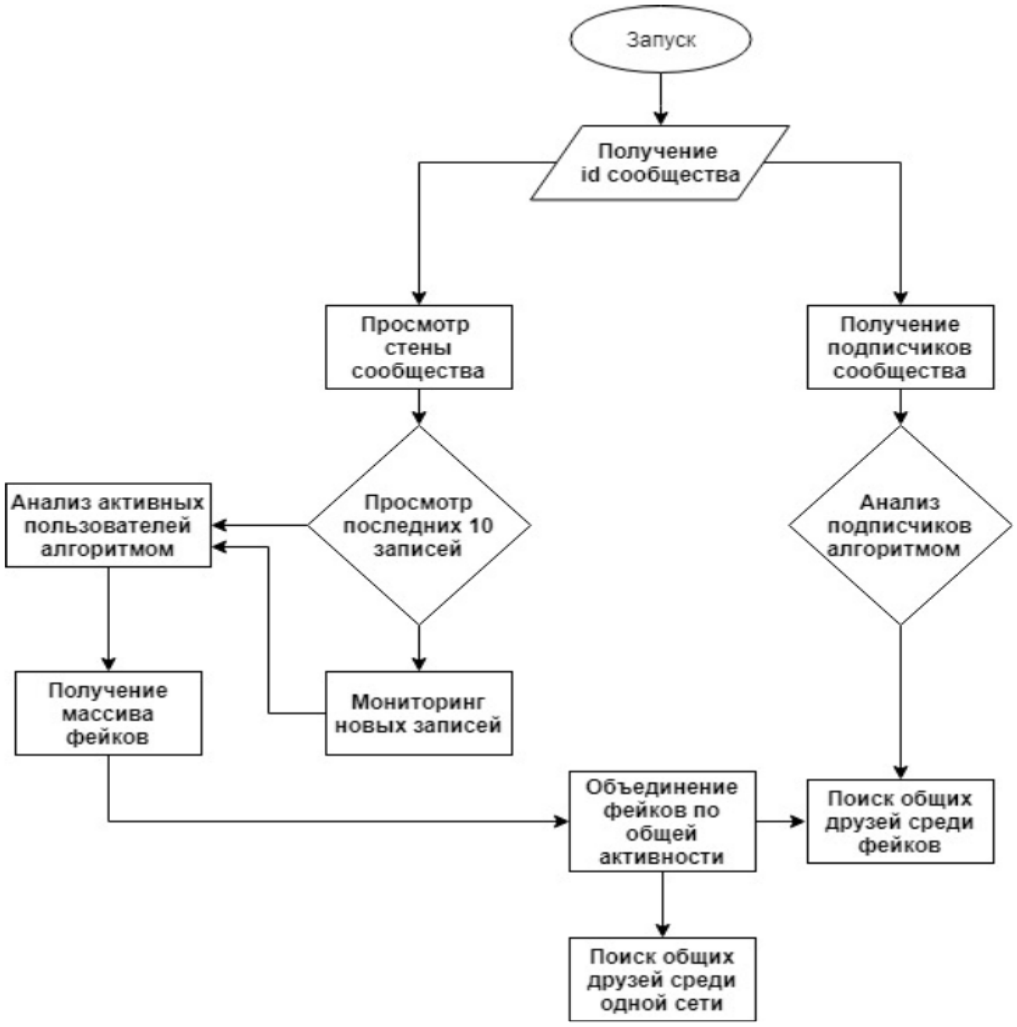


Рис. 1. Блок-схема алгоритма объединения учетных записей злоумышленников в потенциальные сети

Результаты

Основополагающей целью объединения фейковых аккаунтов в группы является мониторинг и анализ их дальнейшей активности. Следовательно, сравнивать эффективность работы алгоритма объединения недостоверных пользователей следует по количеству заблокированных и ожидающих блокировки с результатами блокировки одиночных фейковых аккаунтов.

Вначале сравним результаты заблокированных ботнетов и одиночных аккаунтов на рисунке 2.

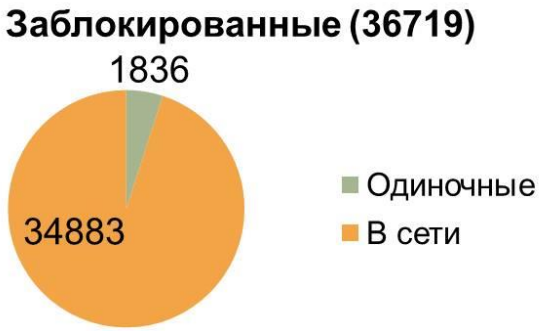


Рис. 2. Сравнение заблокированных аккаунтов

Как видно на рисунке 2, около 5 % от заблокированных недостоверных учетных записей являются одиночными, и что составляет около 60 % от всех выявленных одиночных аккаунтов.

Далее сравним статистику по аккаунтам, ожидающим блокировку на рисунке 3.



Рис. 3. Сравнение ожидающих блокировку аккаунтов

Представленный на рисунке 3 анализ недостоверных учетных записей, ожидающих блокировку, отражает подавляющее большинство объединенных в ботнет фейковых аккаунтов (99,6 %) от общего количества рассматриваемых профилей.

Заключение

Вышеописанное исследование подтвердило ключевую гипотезу проводимого исследования, фейковые аккаунты, распространяющие деструктивный контент в социальных сетях, объединяются в ботнеты, и в подавляющем большинстве находятся в стадии ожидания. Следовательно, существует необходимость в выявлении и дальнейшем мониторинге таких ботнетов в социальных сетях.

Список используемых источников

1. Борисов С. В., Мосикян А. А., Сахаров Д. В. Боты в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 560-563.
2. Виткова Л. А., Сахаров Д. В., Голузина Д. Р. Модель вредоносной информации и ее распространителя в социальных сетях // Защита информации. Инсайд. 2020. № 3 (93). С. 66-72.
3. Сахаров Д. В., Шашкин В. С. Система противодействия распространению вредоносной информации в социальных сетях // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. ССПб: СПбГУТ, 2020. С. 783-787.

ANALYSIS OF FAKE ACCOUNTS UNITED INTO BOTNETS IN SOCIAL NETWORKS

Sakharov D., Shashkin V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the conditions of the modern world, characterized by high speeds of information dissemination, the problem of dissemination of destructive information and fake news in particular is becoming increasingly relevant. Analysis of fake accounts in social networks allows to minimize the consequences of their destructive activities by detecting "frozen" botnets. Timely detection of such accounts helps to take preventive measures to deactivate them.

Key words: *information security, social networks, botnet, fakes*

УДК 004.05
ГРНТИ 81.93.29

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТ ДИНАМИЧЕСКОГО АНАЛИЗА

Д. А. Свечников, М. С. Авдеев, П. Н. Горбачев

Академия Федеральной службы охраны Российской Федерации

Динамический анализ является основным инструментом для выявления уязвимостей и исследования поведения программного обеспечения. В статье рассматривается подход к защите программ от динамического анализа путем модификации компилятора clang и добавления в него специальных проходов. Решение позволит усложнить процесс динамического анализа, затруднить извлечение информации о логике работы программы и скрыть критические участки кода.

защита программного обеспечения, динамический анализ, обфускация, clang, LLVM, модификация компилятора, проходы, временные метки, ptrace

Защита программного обеспечения от злонамеренного воздействия в настоящее время является важной задачей. Динамический анализ, включающий в себя такие методы как отладка, трассировка и мониторинг памяти, представляет собой эффективный инструмент для анализа поведения программ, поиска уязвимостей и извлечения конфиденциальной информации. Злоумышленники, обладая доступом к исполняемому коду, могут использовать динамический анализ для детального изучения логики работы программы, выявления слабых мест и разработки эксплойтов [1, 2, 3].

Традиционные методы, такие как шифрование и разграничение доступа, не обеспечивают эффективную защиту от динамического анализа. В связи с этим, актуальным является направление разработки инструментов, усложняющих процесс динамического анализа, делая его более трудоемким и менее результативным [4].

В статье предлагается подход к защите программного обеспечения от динамического анализа путем модификации компилятора clang путем добавления в него собственного модуля с разработанными проходами, модифицирующими промежуточное представление LLVM IR (Low Level Virtual Machine Intermediate Representation).

LLVM – это инфраструктура компилятора, предоставляющая богатый набор инструментов для работы с кодом на различных этапах компиляции, включая оптимизацию и преобразование.

Для достижения цели предполагается разработка модуля LLVM, включающего в себя проходы обнаружения отладчика на основе временных меток и функции ptrace, которые встраиваются в процесс компиляции, изменяют структуру и логику работы программы, что в целом затрудняет ее анализ.

Метод временных меток позволяет контролировать время, которое злоумышленник затрачивает на анализ кода программы. Для реализации данного метода в код каждой функции программы, подвергающейся обфускации, встраиваются две временные метки, записывающие текущее время входа в начало базового блока и выхода из него. Если время, прошедшее между двумя метками, превышает ожидаемое, то предполагается, что программа находится на изучении и ее выполнение приостанавливается.

Второй метод основан на выявлении отладчика посредством функции ptrace. Появление ошибки, сформированной ptrace сигнализирует о том, что программа в данный момент анализируется и ее выполнение будет немедленно приостановлено.

Алгоритм функционирования модифицированного компилятора clang представлен на рис. 1.

1. Программа на языке C/C++ передается компилятору clang.

2. Первый этап компиляции: clang выполняет лексический, синтаксический и семантический анализ исходного кода, преобразуя его в промежуточное представление LLVM IR.

3. Второй этап компиляции: выполняется оптимизация промежуточного представления LLVM IR и вставка пользовательских проходов, делая его более защищенным от динамического анализа.

4. Третий этап компиляции: LLVM компилятор преобразует модифицированное промежуточное представление LLVM IR в машинный код для целевой архитектуры (x86, ARM и т. д.).

Полученный машинный код является конечным результатом компиляции и содержит защиту от динамического анализа.

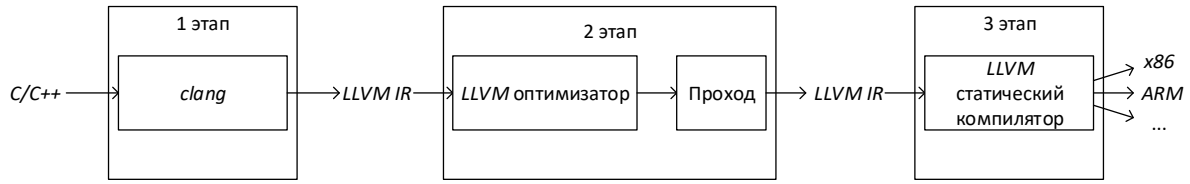


Рис. 1. Блок-схема алгоритма работы обфусцирующего компилятора

К преимуществу данного подхода относится то, что разработчик обеспечивает защиту программного обеспечения уже на этапе компиляции.

При реализации предлагаемого обфусцирующего компилятора были решены следующие задачи:

1. Получен исходный код проекта LLVM версии 17.0.6 и компилятор clang.

2. Разработан модуль, реализующий метод run с собственными проходами, которые наследуются от класса llvm::PassInfoMixin<…>.

3. Внесены изменения в файл PassBuilder.cpp, для регистрации модуля в системе проходов LLVM.

4. Собран проект LLVM, включающий компилятор clang.

5. Проведено тестирование обфусцирующего компилятора clang на различных программах.

В результате работы обфускатора формируется исполняемый файл, в котором увеличено количество базовых блоков и условных переходов по сравнению с обычным компилятором. Предлагаемое решение позволяет значительно увеличить время, затрачиваемое злоумышленником на анализ программы.

Предложенный подход имеет большое практическое значение и может эффективно использоваться для защиты критически важного программного обеспечения. Дальнейшие исследования и разработки в области обфускации и защиты от динамического анализа позволят создать надежные и эффективные средства защиты программного обеспечения.

Список использованных источников

1. Обфускация как метод защиты программного обеспечения. URL: https://habr.com/ru/articles/533954/ (дата обращения 17.03.2025).

2. Динамический анализ кода: цели, принцип работы, плюсы и минусы, варианты внедрения. URL: https://rt-solar.ru/products/solar_appscreener/blog/ 3974 (дата обращения: 17.03.2025).

3. Обфускация кода – что, как и зачем. URL: https://habr. com/ru/articles/735812/ (дата обращения 17.03.2025).

4. Протектор и LLVM-обфускатор. Сравнение двух подходов к решению задачи запутывания кода. URL: https://habr.com/ru/companies/aktiv-company/articles/779990/ (дата обращения 17.03.2025).

PROTECTION OF SOFTWARE FROM DYNAMIC ANALYSIS

Svechnikov D., Avdeev M., Gorbachev P.
Russian Federation Security Guard Service Federal Academy

Dynamic analysis is a powerful tool for identifying vulnerabilities and investigating software behavior. This article discusses an approach to protecting programs from dynamic analysis by modifying the clang compiler and adding custom passes to it. These passes are aimed at complicating the dynamic analysis process, making it difficult to extract information about the logic of the program, and hiding critical parts of the code.

Key words: *software protection, dynamic analysis, obfuscation, clang, LLVM, compiler modification, passes, timestamps, ptrace*

УДК 004.05
ГРНТИ 81.93.29

ПОВЫШЕНИЕ ОПЕРАТИВНОСТИ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ КЛАССА СЛЕПАЯ SQL-ИНЪЕКЦИЯ

Д. А. Свечников М. Р. Астахов, П. Н. Горбачев

Академия Федеральной службы охраны Российской Федерации

В статье рассматриваются подходы к эксплуатации слепой SQL-инъекции: алгоритм бисекции и групповой подход с использованием словаря, созданного с помощью инструмента CeWL. Анализируются их преимущества и недостатки. Показано, что алгоритм бисекции является более надежным и универсальным решением, в то время как групповой подход с использованием словаря обеспечивает более быстрое извлечение данных при наличии контекстуально релевантных слов.

слепая SQL-инъекция, алгоритм бисекции, групповой подход, CeWL, эксплуатация уязвимостей, информационная безопасность, тестирование на проникновение

Одним из наиболее распространенных классов уязвимостей веб-приложений являются SQL-инъекции (SQLi) позволяющие злоумышленникам получить несанкционированный доступ к базам данных. Слепая SQL-инъекция (Blind SQLi) – это особый случай, при котором приложение не возвращает явных данных об ошибке или содержимом базы данных. В таких ситуациях злоумышленнику для получения информации приходится полагаться на второстепенные факторы, такие как временные задержки ответа от сервера или логические условия.

Сравнение инструментов, обнаруживающих уязвимости класса слепая SQL-инъекция приведены в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ инструментов

Инструмент	Основной алгоритм	Скорость сканирования
SQLMap	Алгоритм бисекции	Высокая
Havij	Алгоритм перебора	Средняя
BBQSQL	Алгоритм бисекции	Высокая
Sqlninja	Алгоритм перебора	Средняя
jSQL	Алгоритм бисекции	Высокая

Проведено сравнение группового алгоритма с использованием словаря, созданного с помощью Custom Word List Generator (CeWL) и алгоритма бисекции. Выявлено, что алгоритм бисекции более предпочтителен, чем метод перебора.

Алгоритм бисекции, или алгоритм деления пополам, широко используется для эксплуатации слепой SQL-инъекции. Этот метод основан на последовательном сужении диапазона возможных значений символов, пока не будет найдено точное значение. Задается начальный диапазон значений ASCII (например, от 32 до 126). Середина диапазона проверяется с помощью логического условия, например:

```
SELECT CASE WHEN (ASCII(SUBSTRING((SELECT username FROM users WHERE id=1), 1, 1))
> 64) THEN SLEEP(5) ELSE 0 END;
```

Если условие истинно (есть задержка), диапазон сужается до правой части. Если ложно – до левой. Процесс повторяется до тех пор, пока диапазон не сузится до одного значения.

Групповой подход предполагает проверку блоков символов вместо проверки одного символа за раз. Для создания словаря можно использовать инструмент CeWL, который анализирует текстовый контент целевого сайта и создает список уникальных слов. Используя CeWL, собираются ключевые слова с сайта, например:

```
cewl http://example.com -w dictionary.txt
```

Из собранных слов формируются возможные комбинации имен таблиц или полей, например, добавлением суффиксов и префиксов (tbl_, _info, user_). Эти комбинации проверяются блоками с помощью SQL-запросов:

```
SELECT CASE WHEN (SUBSTRING((SELECT username FROM users WHERE id=1), 1, 5) =
'user_') THEN SLEEP(5) ELSE 0 END;
```

Сравнение алгоритмов представлено в таблице 2.

ТАБЛИЦА 2. Сравнительный анализ алгоритмов

Критерий	Алгоритм бисекции	Групповой алгоритм
Количество запросов	Большое (по одному символу)	Небольшое (блоки символов)
Универсальность	Высокая	Зависит от подготовленных данных
Простота реализации	Простая	Сложная, требует дополнительной обработки
Скорость извлечения данных	Медленная для длинных строк	Быстрая при блочной проверке
Зависимость контента от сайта	Нет	Да

Групповой подход с использованием словаря, созданного инструментом CeWL, является наиболее эффективным и предпочтительным в большинстве случаев при эксплуатации слепой SQL-инъекции.

Для сравнения предложенного метода была разработана утилита, использующая групповой алгоритм для выявления уязвимостей класса слепая SQL-инъекция. Для проведения исследований разработаны стенды, отражающие тематику блога, интернет-магазина, форума и содержащих уязвимости. Стенды 4, 5 и 6 являются прототипами стендов 1, 2 и 3 с другим набором исходных данных.

Исследование времени обнаружения уязвимостей класса слепая SQL-инъекция посредством разработанной утилиты (групповой алгоритм) и инструментом sqlmap (алгоритм бисекции) представлено на рис. 1.

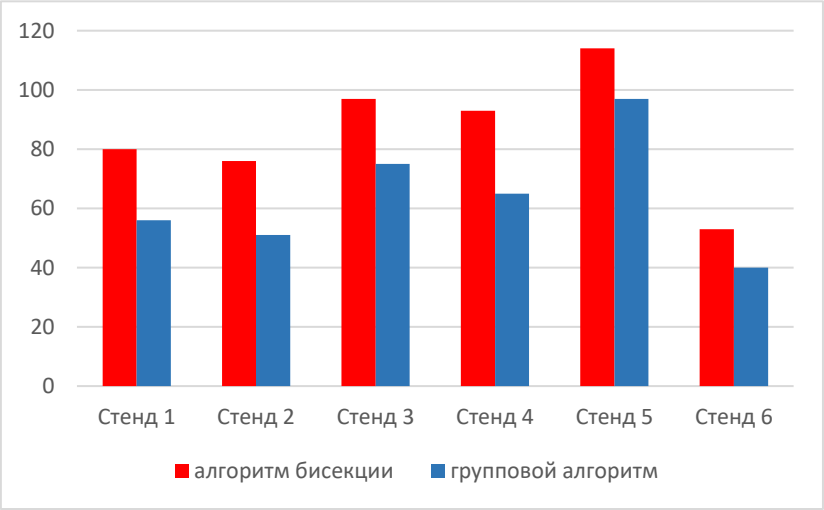


Рис. 1. Зависимость времени обнаружения уязвимостей класса слепая SQL-инъекция от используемой утилиты

Результаты, полученные в ходе эксперимента, свидетельствуют, что групповой алгоритм для обнаружения уязвимостей класса слепая SQL-инъекция является наиболее предпочтительным. Формирование словаря в перспективе заменит нейросеть, которая будет генерировать более контекстуально релевантные словари.

Список использованных источников

1. Самый быстрый укол. Оптимизируем Blind SQL-инъекцию // URL: https://xakep.ru/2021/09/21/blind-sqli-optimize/ (дата обращения: 17.03.2025).
2. Быстрые техники эксплуатации Blind SQL Injection // URL: https://pt-corp.storage.yandexcloud.net/upload/corporate/ru-ru/analytics/PT-devteev-FAST-blind-SQL-Injection-rus.pdf (дата обращения: 17.03.2025).

IMPROVING THE EFFICIENCY OF DETECTING VULNERABILITIES OF THE BLIND SQL INJECTION CLASS

Svechnikov D., Astakhov M., Gorbachev P.
Russian Federation Security Guard Service Federal Academy

The article discusses approaches to the operation of blind SQL injection: a bisection algorithm and a group approach using a dictionary created using the CeWL tool. Their advantages and disadvantages are analyzed. It is shown that the bisection algorithm is a more reliable and universal solution, while the group approach using a dictionary provides faster data extraction in the presence of contextually relevant words.

Key words: *blind SQL injection, bisection algorithm, group approach, CeWL, vulnerability exploitation, information security, penetration testing*

УДК 004.7
ГРНТИ 50.11.35

АНАЛИЗ СПОСОБОВ УПРАВЛЕНИЯ ПРОГРАММНО-КОНФИГУРИРУЕМОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ

Д. А. Свечников, П. Н. Горбачев, П. А. Рощупкина, А. С. Смольянинов

Академия Федеральной службы охраны Российской Федерации

В статье представлен сравнительный анализ современных способов управления информационными инфраструктурами: императивный, оркестрация и автоматизация, искусственный интеллект, машинного обучения, микросервисная архитектура и контейнеризация. На основе анализа предложен рациональный способ для реализации системы управления программно-конфигурируемой информационной инфраструктуры. Предложены рекомендации по выбору и комбинированию подходов в зависимости от задач и требований к программно-конфигурируемой информационной инфраструктуре.

программно-конфигурируемая информационная инфраструктура, императивный подход, оркестрация, автоматизация, искусственный интеллект, контейнеризация.

Управление программно-конфигурируемой информационной инфраструктурой (ПКИИ) – это сложная и многогранная задача, которая требует применения современных технологий и подходов. ПКИИ включает в себя управление сетевыми ресурсами, вычислительными мощностями, системами хранения данных и приложениями, которые могут динамически адаптироваться к изменяющимся требованиям [1]. Для выбора рационального подхода к управлению проектируемой ПКИИ необходимо провести анализ существующих решений, выделить их преимущества, недостатки и области применения.

Императивный подход к управлению программно-конфигурируемой инфраструктурой предполагает явное указание системе конкретных шагов для достижения нужного состояния, что хорошо подходит для простых или разовых задач. Он дает точный контроль и гибкость для нестандартных действий, реализуется через скрипты и командную строку, но плохо масштабируется, подвержен человеческим ошибкам и неэффективен для динамичных сред.

В современных информационных инфраструктурах все чаще используются оркестрация и автоматизация, которые позволяют управлять виртуаль-

ными машинами, контейнерами и сетевыми ресурсами без постоянного вмешательства администратора. Эти подходы повышают эффективность, обеспечивают масштабируемость и автовосстановление, но требуют значительных вычислительных ресурсов. Применяются в облачных средах и центрах обработки данных.

Искусственный интеллект и машинное обучение (AI/ML) применяются для прогнозирования сбоев, оптимизации ресурсов и повышения автоматизации. Эти технологии позволяют автоматизировать сложные процессы и анализировать угрозы, эффективность их применения зависит от качества данных, а сами системы ресурсоемки и уязвимы к атакам.

Микросервисная архитектура и контейнеризация разбивают приложения на независимые компоненты, что обеспечивает гибкость, масштабируемость и отказоустойчивость. Однако управление множеством микросервисов и контейнеров требует сложных инструментов оркестрации. Основное применение находят в облачных приложениях и распределенных системах [2].

Результаты анализа представлены в Таблице 1. Для решения задачи разработки ПКИИ рационально применить способ контейнеризации. Данный способ может использоваться совместно с другими, например, с оркестрацией и автоматизацией.

ТАБЛИЦА 1. Анализ способов управления ПКИИ

Критерии сравнения	Императивный подход	Оркестрация и автоматизация	AI/ML	Контейнеризация
Уровень автоматизации	Низкий	Высокий	Очень высокий	Высокий
Масштабируемость	Низкая	Высокая	Очень высокая	Высокая
Безопасность	Средняя	Высокая	Средняя	Высокая
Гибкость	Средняя	Высокая	Высокая	Высокая
Стоимость реализации	Низкая	Средняя	Очень высокая	Средняя
Сложность реализации	Низкая	Средняя	Высокая	Высокая

В качестве инструментов реализации данного подхода предлагается использовать Docker и Ansible. Их выбор обусловлен широким распростране-

нием, функциональными возможностями и совместимостью. Docker, являясь ведущей платформой для контейнеризации, позволяет упаковывать приложения и их зависимости в изолированные контейнеры, что гарантирует их стабильную работу в любом окружении – от локальных серверов до облачных платформ. Ansible, в свою очередь, предоставляет простые, но эффективные средства для автоматизации конфигурации и оркестрации, что делает его идеальным инструментом для управления инфраструктурой, включающей множество контейнеров и серверов.

Комбинирование Docker и Ansible обеспечивает ряд ключевых преимуществ. Во-первых, Docker значительно ускоряет процесс развертывания приложений: контейнеры запускаются за секунды, а их легковесность позволяет эффективно использовать ресурсы инфраструктуры. Во-вторых, Ansible, работает по принципу идемпотентности и гарантирует, что каждая операция конфигурации приведет к одному и тому же результату, независимо от начального состояния системы. Это особенно важно для обеспечения стабильности и предсказуемости в крупных распределенных средах. Кроме того, Ansible упрощает масштабирование инфраструктуры за счет централизованного управления через конфигурационные файлы, а его декларативный подход к описанию задач делает процесс настройки прозрачным и легко воспроизводимым.

Еще одним важным аспектом является унификация сред разработки, тестирования и эксплуатации. Docker обеспечивает идентичное поведение приложений на всех этапах их жизненного цикла, что минимизирует риски, связанные с расхождениями в окружениях. Ansible дополняет эту возможность, позволяя автоматизировать не только развертывание контейнеров, но и настройку всей сопутствующей инфраструктуры: сетевых параметров, систем мониторинга, балансировки нагрузки и других критически важных компонентов.

Эффективность способов управления ПКИИ, а также средств его реализации можно оценить посредством времени, затрачиваемого на развертывание и настройку фрагмента программно-конфигурируемой информационной инфраструктуры.

В ходе проведенного исследования было выяснено, что развертывание фрагмента ПКИИ с использованием ручной настройки занимает порядка 120 мин., использование контейнеризации с помощью Docker позволяет ускорить этот процесс в 4 раза, а при совместном использовании Docker и Ansible время развертывания сокращается в десятки раз и составляет 5 мин.

Таким образом, сочетание Docker и Ansible представляет собой сбалансированное решение для управления ПКИИ, объединяющее преимущества контейнеризации, автоматизации и оркестрации. Этот подход особенно эффективен в гибридных и облачных средах, где требуется одновременно гибкость, масштабируемость и централизованное управление. Благодаря своей простоте, надежности и широким возможностям интеграции, Docker и Ansible являются основными инструментами для построения современной, отказоустойчивой и легко управляемой ИТ-инфраструктуры. Данный метод использован для автоматизации развертывания CTF-инфраструктуры соревнований по информационной безопасности.

Список используемых источников

1. Моррис К. Программирование инфраструктуры. М.: БХВ-Петербург, 2024. 416 с.
2. Сейерс Э. Х., Милл И. Docker на практике. М.: ДМК Пресс, 2020. 516 с.

ANALYSIS OF APPROACHES TO MANAGING SOFTWARE-DEFINED INFORMATION INFRASTRUCTURES

Svechnikov D., Gorbachev P., Roshchupkina P., Smolyaninov A.
Russian Federation Security Guard Service Federal Academy

The article presents a comparative analysis of modern approaches to managing information infrastructures: imperative, orchestration and automation, artificial intelligence, machine learning, microservice architecture, and containerization. Based on the analysis, a rational method for implementing a software-defined information infrastructure management system is proposed. Recommendations are provided for selecting and combining approaches depending on the tasks and requirements of the software-defined information infrastructure.

Key words: *software-defined information infrastructure (SDII), imperative approach, orchestration, automation, artificial intelligence (AI), containerization*

УДК 004.056.53
ГРНТИ 50.41.27

ДЕТАЛИЗАЦИЯ МОДЕЛИ АТАКИ «ПЕРЕХВАТ СЕССИИ TCP» НА ОСНОВЕ CYBER KILL CHAIN

О. Л. Спицин[1], А. А. Шевченко[2], Н. А. Калиникин[1], М. А. Ткачев[1]

[1]Военная Академия Связи им. Маршала Советского союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается детализированная модель атаки TCP Session Hijacking, основанная на структуре Cyber Kill Chain. Анализируется каждый этап атаки. Особое внимание уделено методам обнаружения, предотвращения и минимизации последствий атаки на каждом этапе. В статье также исследуется связь атаки с фазами Cyber Kill Chain. Предлагаются стратегии противодействия в рамках основных категорий: обнаружение, запрет, срыв, ослабление, обман и уничтожение. Работа направлена на повышение осведомленности специалистов по кибербезопасности о методах проведения и защиты от этой атаки, а также предоставляет четкие шаги для предотвращения компрометации сетевых соединений.

TCP Session Hijacking, Cyber Kill Chain, кибербезопасность, защита сети, противодействие атакам

Введение

С каждым годом методы кибератак становятся все более изощренными, а их последствия – все более разрушительными. В условиях стремительного роста цифровизации и удаленного взаимодействия между пользователями, одной из наиболее опасных атак остается TCP Session Hijacking (перехват сессии TCP). Эта угроза представляет собой перехват управления установленной TCP-сессией, что позволяет злоумышленнику получить доступ к конфиденциальным данным, выполнять несанкционированные действия или нарушать работу системы [1].

Для понимания механизмов и защиты от подобных атак важно рассматривать их в рамках концептуальных моделей, таких как Cyber Kill Chain. Эта модель была разработана для описания жизненного цикла кибератаки и включает в себя этапы от подготовки до достижения конечных целей. Она позволяет структурировать анализ угроз и выстраивать многоуровневую защиту.

Cyber Kill Chain

Cyber Kill Chain – это модель, разработанная корпорацией Lockheed Martin для описания жизненного цикла кибератаки [2]. Изначально она применялась в военных операциях, но со временем была адаптирована для кибербезопасности. Эта модель помогает понять действия злоумышленников и выстроить эффективную защиту на всех этапах атаки, начиная от ее подготовки и заканчивая реализацией конечных целей.

Этапы Cyber Kill Chain

1. Разведка (Reconnaissance): злоумышленник собирает информацию о целевой системе, инфраструктуре и пользователях.

2. Вооружение (Weaponization): создание вредоносного инструмента на основе собранных данных.

3. Доставка (Delivery): внедрение вредоносного ПО или команд в целевую систему.

4. Заражение (Exploitation): использование уязвимости для выполнения вредоносных действий.

5. Инсталляция (Installation): закрепление доступа в системе.

6. Получение управления (Command and Control, C2): установление канала для передачи команд и контроля над зараженной системой.

7. Выполнение целей (Actions on Objectives): реализация целей атаки: кража данных, эскалация привилегий, уничтожение ресурсов.

Cyber Kill Chain широко используется для анализа кибератак, так как она позволяет специалистам по безопасности выявлять и устранять слабые места на каждом этапе. Она также служит инструментом для разработки многоуровневой защиты, улучшения систем мониторинга и оценки эффективности внедренных мер безопасности. Знание этой модели помогает реагировать на инциденты быстрее, минимизируя возможный ущерб, а также повышает готовность организаций к предотвращению угроз. Cyber Kill Chain стала одним из ключевых стандартов в кибербезопасности, предлагая структурированный и системный подход к борьбе с атаками [3].

Перехват сессии TCP

Атака перехват сессии *TCP* эксплуатирует особенности протокола *TCP*, который управляет передачей данных в сети через установление и поддержание соединения между двумя узлами [4]. Атакующий вмешивается в уже

установленное соединение, притворяясь одним из его участников. Это позволяет злоумышленнику перехватывать данные, отправлять команды от имени легитимного участника или нарушать работу системы [5]. Этапы атаки представлены на рисунке 1.

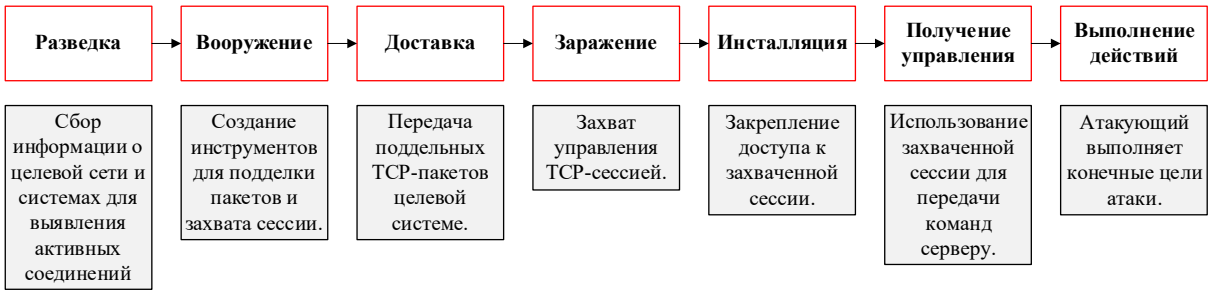


Рис. 1. Этапы атаки TCP Session Hijacking на основе Cyber Kill Chain

ТАБЛИЦА 1. Противодействия для атаки TCP Session Hijacking на разных этапах

Этап	Обнаружение	Запрет	Срыв	Ослабление	Обман	Уничтожение
Разведка	Мониторинг трафика (IDS/IPS), выявление сниффинга.	Блокировка несанкционированных сканирований	Шифрование трафика (TLS), использование безопасных протоколов.	Ограничение доступа к данным через сегментацию сети (VLAN).	Создание ложных данных для анализа трафика.	Прерывание соединения с подозрительными устройствами.
Вооружение	Анализ активности по генерации поддельных пакетов.	Ограничение возможностей создания фальшивых пакетов через межсетевые экраны.	Усложнение алгоритмов генерации Sequence Numbers.	Регулярное обновление ПО и устранение уязвимостей в TCP.	Распространение ложной конфигурации TCP для усложнения атаки.	Удаление уязвимых конфигураций TCP.
Доставка	Обнаружение поддельных пакетов через DPI или сигнатуры IDS.	Фильтрация пакетов с поддельными IP-адресами.	Установка правил маршрутизации для исключения подмен.	Уменьшение поверхности атаки через ограничение открытых портов.	Внедрение ложных ответов в трафик для путаницы злоумышленника.	Прерывание подозрительных соединений.

Этап	Обнаружение	Запрет	Срыв	Ослабление	Обман	Уничтожение
Заражение	Мониторинг активности TCP-сессий на предмет аномалий.	Применение MFA для защиты доступа.	Блокировка подозрительных соединений через firewall.	Ограничение прав пользователей, минимизация привилегий.	Генерация ложных подтверждений (ACK) для сбивания с толку.	Прерывание захваченных сессий.
Инсталляция	Логирование системных изменений и активностей.	Блокировка внедрения вредоносных конфигураций.	Ограничение записи в системные файлы.	Минимизация доступа к критическим ресурсам.	Создание фальшивых уязвимостей для отвлечения атакующего.	Удаление вредоносного ПО или конфигураций.
Получение управления	Анализ командного трафика через DPI.	Блокировка C2-каналов.	Отключение подозрительных соединений.	Ограничение внешних соединений до известных IP-адресов.	Имитирование успешной атаки для выявления источника угрозы.	Прерывание взаимодействия с C2-узлом атакующего.
Выполнение действий	Анализ эксфильтрации данных, логирование всех операций.	Блокировка отправки данных за пределы сети.	Уменьшение объема передаваемых данных.	Сегментация данных для снижения влияния эксфильтрации.	Внедрение ложной информации для эксфильтрации.	Уничтожение украденных данных через удаленные команды.

Таблица 1 охватывает все этапы атаки и меры защиты, которые можно внедрить на каждом этапе для предотвращения или смягчения последствий атаки TCP Session Hijacking [6].

Категории противодействия:

1. Обнаружение: Использование инструментов и методов для выявления атаки (IDS/IPS, мониторинг трафика, логирование).

2. Запрет: Применение средств защиты для предотвращения выполнения конкретных действий (firewalls, фильтрация пакетов).

3. Срыв: Меры, затрудняющие выполнение атаки (шифрование, блокировка соединений).

4. Ослабление: Уменьшение потенциального ущерба от атаки (минимизация привилегий, сегментация сети).

5. Обман: Создание ложных данных или конфигураций, чтобы запутать атакующего.

6. Уничтожение: Полное удаление угрозы, включая завершение сессий, удаление данных и устранение атакующего из сети.

Заключение

TCP Session Hijacking – это сложная и опасная атака, эксплуатирующая фундаментальные свойства протокола TCP для захвата активных соединений. Использование модели Cyber Kill Chain позволяет структурировать понимание этой атаки, разбивая ее на последовательные этапы: от сбора информации и подготовки инструментария до достижения конечных целей злоумышленника [7]. Такой подход предоставляет системным администраторам и специалистам по кибербезопасности возможность выявлять слабые места на каждом этапе атаки и выстраивать многоуровневую защиту.

Моделирование TCP Session Hijacking на основе Cyber Kill Chain служит не только инструментом для анализа угроз, но и важным шагом в создании более защищенной сетевой инфраструктуры [8]. Применение этой модели на практике позволяет выстроить проактивный подход к кибербезопасности, минимизировать риски и обеспечить устойчивость сетей перед все более сложными атаками.

Список используемых источников

1. Schou, L. Practical TCP/IP and Ethernet Networking. Wrox, 2014. С. 350.

2. Pieters A. The Hacker Playbook 3: Practical Guide To Penetration Testing. Wiley, 2020. С. 720.

3. Шевченко А. А. Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве / А. А. Шевченко // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 года. Санкт-Петербург: ФГКВОУВО «Военная академия связи Имени Маршала Советского Союза С.М.Буденного» МО РФ, 2020. С. 237-241.

4. Липатников В. А. Модель оценки процесса подготовки и реализации вторжений в сетях IP-телефонии / В. А. Липатников, В. С. Косолапов, А. А. Шевченко, Д. С. Сокол // Информация и космос. 2021. № 4. С. 55-69.

5. Kaufman, C. Network Security Essentials: Applications and Standards. Pearson, 2018. С. 512.

6. Korshunov G. A. Decision support systems for information protection in the management of the information network / G. A. Korshunov, V. A. Lipatnikov, A. A. Shevchenko // Fuzzy Technologies in the Industry - FTI 2018: Proceedings of the II International Scientific and Practical Conference, Ulyanovsk, 23–25 октября 2018 года. Ulyanovsk: Ульяновский государственный технический университет, 2018. P. 418-426.

7. Yang L., & Zhang H. Principles of Network and System Administration. Wiley, 2013. C. 700.

8. Cornwell S. Practical Network Security Monitoring // No Starch Press, 2019. C. 400.

DETAILING THE TCP SESSION INTERCEPTION ATTACK MODEL BASED ON CYBER KILL CHAIN

Spicin O., Shevchenko A., Kalinikin A., Tkachew M.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses a detailed TCP Session Hijacking attack model based on the Cyber Kill Chain structure. Each stage of the attack is analyzed. Special attention is paid to the methods of detecting, preventing and minimizing the consequences of an attack at each stage. The article also explores the connection between the attack and the phases of the Cyber Kill Chain. Counteraction strategies are proposed within the main categories: detection, prohibition, disruption, weakening, deception and destruction. The work is aimed at raising awareness among cybersecurity professionals about the methods of conducting and protecting against this attack, as well as providing clear steps to prevent compromise of network connections.

Key words: *TCP Session Hijacking, Cyber Kill Chain, cybersecurity, network protection, countering attacks*

УДК 004.056.53
ГРНТИ 50.41.27

КЛЮЧЕВЫЕ ОСОБЕННОСТИ РЕАЛИЗАЦИИ КОМПЬЮТЕРНОЙ АТАКИ НА СЕТЬ ПЕРЕДАЧИ ДАННЫХ ТИПА «АНАЛИЗ СЕТЕВОГО ТРАФИКА»

О. Л. Спицин[1], А. А. Шевченко[2], Н. А. Калиникин[1], М. А. Ткачёв[1]

[1]Военная Академия Связи им. Маршала Советского союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются ключевые особенности реализации компьютерной атаки на сеть передачи данных, известной как «анализ сетевого трафика». Описываются методы и технологии, которые могут быть использованы злоумышленниками для перехвата и анализа данных, передаваемых по сети. Также обсуждаются возможные последствия таких атак и способы их предотвращения. Статья будет полезна специалистам в области информационной безопасности, а также всем, кто интересуется вопросами защиты компьютерных сетей от несанкционированного доступа.

анализ сетевого траффика, воздействия на сеть передачи данных, методы обнаружения и предотвращения атак

В современном мире информационные технологии играют ключевую роль в жизни общества. Сети передачи данных (СПД) стали неотъемлемой частью нашей повседневной жизни, обеспечивая нам доступ к информации, коммуникациям и развлечениям. Однако вместе с ростом значимости информационных технологий возрастает и риск несанкционированного доступа к данным, их утечки или искажения. В связи с этим возникает необходимость в применении различных методов защиты СПД.

Одним из таких методов является анализ сетевого трафика. Этот метод позволяет отслеживать и анализировать данные, передаваемые по сети, с целью выявления возможных угроз и аномалий.

Анализ сетевого трафика – это процесс мониторинга и анализа данных, передаваемых через сеть. Он позволяет выявить подозрительную активность, такую как попытки несанкционированного доступа, распространение вредоносного программного обеспечения (ПО) и другие угрозы безопасности.

Существует два основных подхода к анализу сетевого трафика: пассивный и активный. Пассивный анализ предполагает сбор и анализ данных без вмешательства в работу сети. Активный анализ, напротив, предполагает вмешательство в работу сети с целью проверки ее безопасности.

Атака «анализ сетевого трафика» (traffic analysis attack) направлена на сбор и анализ сетевого трафика для выявления чувствительной информации, таких как пароли, данные пользователей, структура сети и поведение пользователей. Этот тип атаки позволяет злоумышленнику пассивно наблюдать за сетью, не вмешиваясь напрямую в передаваемые данные. На рис. 1 представлено поэтапное описание атаки и влияние каждого этапа на атакуемую сеть.

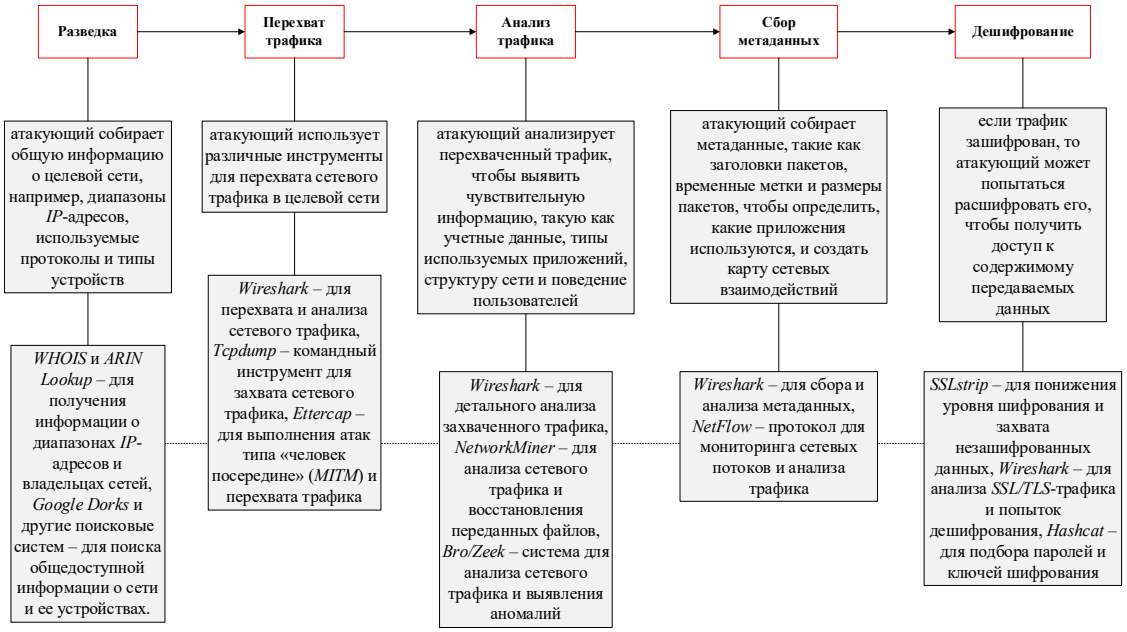


Рис. 1. Этапы атаки на сеть передачи данных типа «анализ сетевого трафика»

На этапе «разведка» атакующий собирает общую информацию о целевой сети, например, диапазоны IP-адресов, используемые протоколы и типы устройств. Это начальный этап, который помогает определить границы сети и общие характеристики. Для этого он может использовать следующие инструменты: WHOIS и ARIN Lookup – для получения информации о диапазонах IP-адресов и владельцах сетей, Google Dorks и другие поисковые систем – для поиска общедоступной информации о сети и ее устройствах. На данном этапе реализации атаки влияние на сеть не оказывается, а злоумышленник добывает ценную информацию для дальнейших действий.

На этапе «перехват трафика» атакующий использует различные инструменты для перехвата сетевого трафика в целевой сети. Это позволяет ему видеть все данные, которые передаются по сети. Для этого он использует следующие инструменты: Wireshark – для перехвата и анализа сетевого трафика, Tcpdump – командный инструмент для захвата сетевого трафика, Ettercap – для выполнения атак типа «человек посередине» (MITM) и перехвата трафика. На данном этапе реализации атаки пассивное захватывание

трафика обычно не оказывает заметного влияния на сеть, но при использовании Ettercap могут возникнуть временные нарушения связи [1].

На этапе «анализ трафика» атакующий анализирует перехваченный трафик, чтобы выявить чувствительную информацию, такую как учетные данные, типы используемых приложений, структуру сети и поведение пользователей. Для этого он может использовать следующие инструменты: Wireshark – для детального анализа захваченного трафика, NetworkMiner – для анализа сетевого трафика и восстановления переданных файлов, Bro/Zeek – система для анализа сетевого трафика и выявления аномалий. На данном этапе непосредственного воздействия на сеть нет, но анализ трафика может привести к утечке конфиденциальной информации и нарушению безопасности.

На этапе «сбор метаданных» атакующий собирает метаданные, такие как заголовки пакетов, временные метки и размеры пакетов, чтобы определить, какие приложения используются, и создать карту сетевых взаимодействий. Для этого он использует следующие инструменты: Wireshark – для сбора и анализа метаданных, NetFlow – протокол для мониторинга сетевых потоков и анализа трафика. Пассивное наблюдение за метаданными не оказывает непосредственного влияния на сеть, но предоставляет атакующему информацию для более точного планирования атак [2].

На этапе «дешифрование» если трафик зашифрован, то атакующий может попытаться расшифровать его, чтобы получить доступ к содержимому передаваемых данных. Для этого он может использовать следующие инструменты: SSLstrip – для понижения уровня шифрования и захвата незашифрованных данных, Wireshark – для анализа SSL/TLS-трафика и попыток дешифрования, Hashcat – для подбора паролей и ключей шифрования. Попытки дешифрования могут быть замечены системами IDS/IPS. Успешное дешифрование приводит к утечке конфиденциальной информации.

Чтобы обнаружить и предотвратить атаки, возможно использовать журналы безопасности и событий, а также системы обнаружения и предотвращения вторжений. Журналы сетевых устройств позволяют проанализировать подозрительные действия, например, большое количество запросов к DNS-серверам или аномальные объемы трафика. А IDS/IPS помогают выявить попытки перехвата трафика и другое аномальное поведение. Для этого в системах используются правила и сигнатуры для анализа трафика.

Для мониторинга сетевых журналов и выявления аномалий возможно использовать Wazuh. С его помощью получится настроить правила и декодеры, которые помогут обнаружить подозрительные действия, связанные с анализом трафика. Также для мониторинга сетевого трафика и выявления подозрительной активности подойдет Wireshark.

Шифрование данных помогает защитить их от перехвата. Для этого возможно использовать SSL/TLS – внедрить шифрование для всех критически важных сервисов и приложений. А еще для защиты сетевого трафика между удаленными пользователями и корпоративной сетью подойдут виртуальные частные сети (VPN) [3].

Далее приведены примеры настройки Wazuh для обнаружения атак данного типа:

1. Для настройки мониторинга сетевых журналов необходимо добавить конфигурацию для мониторинга сетевых журналов в файл /var/ossec/etc/ossec.conf. Данная конфигурация представлена на рис. 2.

```
<localfile>
    <log_format>syslog</log_format>
    <location>/var/log/network.log</location>
</localfile>
```

Рис. 2. Конфигурация для мониторинга сетевых журналов в Wazuh

2. Создание правил для обнаружения подозрительной активности. Пример правила для обнаружения аномального трафика для *Wazuh* представлен на рис. 3.

```
<group name="network_anomalies">
    <rule id="100003" level="10">
        <decoded_as>syslog</decoded_as>
        <description>Suspicious network activity
detected</description>
        <match>anomaly</match>
        <frequency>5</frequency>
        <timeframe>60</timeframe>
        <options>no_full_log</options>
    </rule>
</group>
```

Рис. 3. Конфигурация для обнаружения подозрительной активности в Wazuh

Атака типа «анализ сетевого трафика» проходит через несколько ключевых этапов, начиная с разведки и заканчивая дешифрованием. Каждый этап может привести к различным последствиям, таким как утечка конфиденциальной информации, нарушение безопасности и компрометация сети. Защита от таких атак включает в себя использование шифрования, систем IDS/IPS, мониторинг сетевого трафика и регулярное обновление систем.

Список используемых источников

1. Korshunov, G. A. Decision support systems for information protection in the management of the information network / G. A. Korshunov, V. A. Lipatnikov, A. A. Shevchenko // Fuzzy Technologies in the Industry - FTI 2018: Proceedings of the II International Scientific and Practical Conference, Ulyanovsk, 23–25 октября 2018 года. – Ulyanovsk: Ульяновский государственный технический университет, 2018. P. 418-426.
2. Липатников В. А. Модель оценки процесса подготовки и реализации вторжений в сетях IP-телефонии / В. А. Липатников, В. С. Косолапов, А. А. Шевченко, Д. С. Сокол // Информация и космос. 2021. № 4. С. 55-69.
3. Шевченко А. А. Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве / А. А. Шевченко // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 года. – Санкт-Петербург: ФГКВОУВО «Военная академия связи им. Маршала Советского Союза С. М. Буденного» МО РФ, 2020. С. 237-241.

KEY FEATURES OF THE IMPLEMENTATION OF A COMPUTER ATTACK ON A DATA TRANSMISSION NETWORK SUCH AS "NETWORK TRAFFIC ANALYSIS"

Spicin O., Shevchenko A., Kalinikin A., Tkachew M.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the key features of the implementation of a computer attack on a data transmission network, known as "network traffic analysis". It describes methods and technologies that can be used by attackers to intercept and analyze data transmitted over the network. The possible consequences of such attacks and ways to prevent them are also discussed. The article will be useful for information security specialists, as well as for anyone interested in protecting computer networks from unauthorized access.

Key words: *analysis of network traffic, the impact on the data transmission network, methods for detecting and preventing attacks*

УДК 004.852
ГРНТИ 28.23.25

ОСНОВНЫЕ КОНЦЕПЦИИ НЕЙРОННЫХ СЕТЕЙ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

Д. Ф. Ткачев, В. А. Задбоев

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

Статья посвящена повышению уровня информационной безопасности сетей передачи данных с использованием комплексной защиты их нескольких нейронных. Обоснована актуальность применения искусственного интеллекта для защиты сетей передачи данных от кибератак в условиях усложняющихся угроз. Описаны актуальные нейронные сети в информационной безопасности, их преимущества и недостатки. Предложена система обнаружения аномалий в сети с последующим обнаружением противника на основе нейронных сетей.

искусственный интеллект, нейронные сети, кибератаки, сети передачи данных, информационная безопасность, обнаружение аномалий

Актуальность: современные сети передачи данных постоянно подвержены постоянно развивающимся угрозам со стороны противника. В новых кибератаках появилось направление с применением искусственного интеллекта [1-3]. Поэтому требуется применение искусственного интеллекта и в области защиты СПД от кибератак. В статьях [4-5] представлены способы обнаружения противника в сети и его местоположения, однако данные способы работают без применения искусственного интеллекта, отчего у заявленных способов низкая точность и скорость работы. В статье [6] проведена попытка исправить ситуацию путем внедрения ложной сети для отвлечения противника, таким образом повысилась защищенность СПД, но время реакции на аномалии. Искусственный интеллект, как комплекс технологических решений включает в себя процессы и сервисы по обработке, анализу и синтезу решений готовых решений, поэтому способен к адаптивным кибератакам в СПД.

В рамках научного исследования рассматривается применение НС для информационной безопасности СПД за счет комплексного использования нескольких НС при обнаружении аномалий в сети. Благодаря своей способности обрабатывать данные в потоке и адаптироваться к изменениям в ре-

альном времени, этот метод будет мощным инструментом для активной защиты СПД.

Целью статьи является применение НС для повышения информационной безопасности СПД.

Задачей является разработка комплексной системы защиты СПД сна основе применения нескольких НС.

НС является математическая модель, пытающаяся имитировать работу биологических нейронов мозга. Она состоит из множества узлов (нейронов), соединенных между собой. Каждый нейрон получает входные сигналы, обрабатывает их и выдает результат на выход [7].

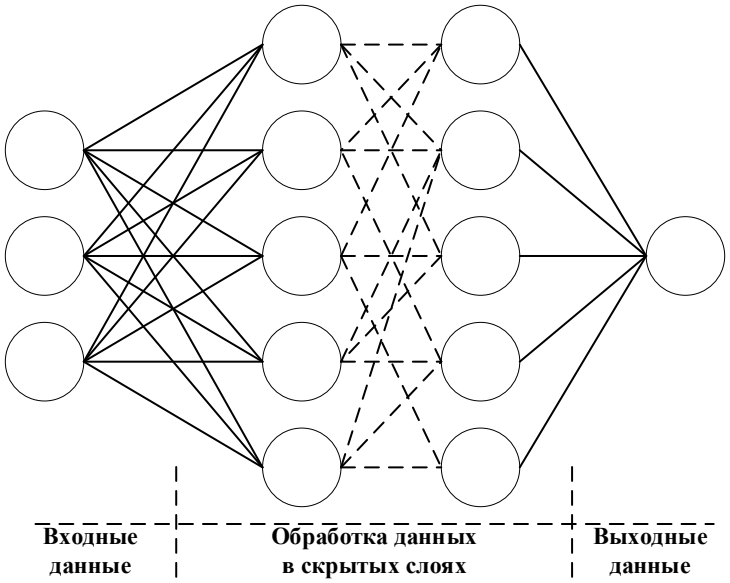


Рис. 1. Основа работы НС

Как видно из рис. 1, на входном слое принимаются данные для анализа, которые обрабатываются в скрытых слоях для обнаружения сложных зависимостей, по итогу чего представляется результат работы, например, «Аномалия обнаружена» или «Аномалия не обнаружена».

Существует два основных способа обучения НС: супервайзированное в котором модель обучается на помеченных данных (заранее известны аномальный трафик или нет) и несупервайзированное обучение, в котором данные не помечены.

Целью заявленных способов является попытка научить НС предсказывать правильные метки для новых данных.

Перед обучением НС также следует выбрать предпочтительную архитектуру НС, так как в зависимости от задач и особенностей данных предпочтительны разные модели, наиболее популярными в отрасли СПД являются:

1. Многослойный перцептрон (MLP) – простая архитектура с несколькими скрытыми слоями, которая хороша для задач классификации, если данные уже преобразованы в числовые признаки.

Пример использования: классификация трафика как «нормальный» или «атака».

Преимуществами являются простота реализации и эффективность при работе со структурированными данными.

К недостаткам относят неэффективность для анализа временных рядов или последовательностей.

2. Сверточные нейронные сети (CNN) – архитектура, основанная на свертках (фильтрах), которые выявляют пространственные зависимости для анализа заголовков пакетов или других структурированных данных.

Пример использования: поиск сигнатур атак в потоках данных.

Преимуществами являются автоматическое извлечение признаков и эффективность при анализе данных с пространственной структурой.

К недостаткам относят требовательность к большим вычислительным ресурсам.

3. Рекуррентные нейронные сети (RNN) и LSTM – это модели, которые работают с последовательностями данных (например, временными рядами) для анализа временных зависимостей в сетевом трафике.

Пример использования: обнаружение атак, которые проявляются в течение времени.

Преимуществами являются учет контекста и последовательности событий, а также эффективность при анализе динамического трафика.

К недостаткам относят требовательность к большим вычислительным ресурсам и большому объему данных.

4. Автокодировщики (Autoencoders) – данная модель, способна восстанавливать входные данные после их сжатия, применяется для выявления аномалий (например, необычного трафика).

Преимуществами являются отсутствие требований к помеченным данным и эффективность в задачах несупервайзированного обучения.

К недостаткам относят трудности в интерпретации результатов.

Рекомендации по выбору архитектуры.

На основе представленных архитектур можно сделать вывод, что ни одна не способна идеально обрабатывать данные в потоке с высоким процентом правильных выходных значений, однако часть представленных НС способны работать в месте для разграничения обязанностей при выполнении задач.

Так, например, можно использовать систему представленная на рис. 2.

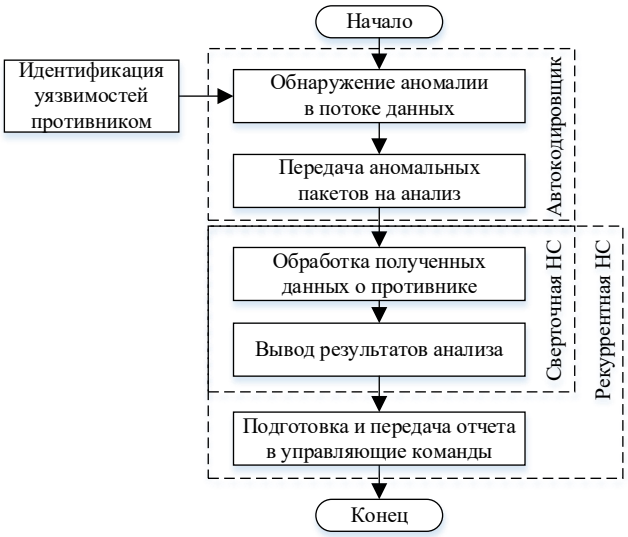


Рис. 2. Система обнаружения вторжений в СПД

В представленной системе «Автокодировщики» отвечают за обнаружение аномалий в трафике, а сверточные и рекуррентные НС отвечают за определение типов и целей атаки.

Предположим, требуется обнаружить *DDoS*-атаки. Набор данных содержит следующие параметры:

– *IP*-адрес источника;
– порт назначения;
– размер пакета;
– частота передачи.

При обнаружении аномалии с помощью «Автокодировщика», подается сигнал для сверточной НС, которая получает преобразовывает данные в числовые признаки (например, IP-адрес можно закодировать как целое число) и на их основе выводит результаты об обнаруженной атаке, рекуррентная НС в данной ситуации выступает как вспомогательная, для определения продолжительных атак.

Заключение. В ходе исследования описаны актуальные нейронные сети в информационной безопасности, их преимущества и недостатки. Предложена система обнаружения аномалий в сети с последующим обнаружением противника на основе нейронных сетей. Использование НС для активной защиты СПД подтверждает свою эффективность в условиях возрастающей сложности кибератак, так как предложенный метод позволяет в автоматическом режиме с повышенной точностью обнаруживать угрозы на основе потоковых данных.

Список используемых источников

1. Беседин М. Д., Задбоев В. А., Полищук В. Р. анализ принципов работы DNS-серверов и DDoS-атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. Т. 2. С. 108-112.

2. Котенко И. В., Саенко И. Б., Бортникер П. В. Методика обнаружения сетевых вторжений на основе интеграции методов вейвлет-анализа и математической статистики // Правовая информатика. 2024. № 4. С. 23-31. doi:10.24412/1994-1404-2024-4-23-31.

3. Липатников В. А., Мелехов К. В., Задбоев В. А. Способ активной защиты информационно-вычислительных сетей от многоэтапных атак // Региональная информатика и информационная безопасность: сб. тр / Под ред. Б. Я. Советова, Р. М. Юсупова, В. В. Касаткина. Санкт-Петербург: Изд-во Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. С. 112-114.

4. Задбоев В. А., Липатников В. А., Мелехов К. В. Активная защита информационно-вычислительной сети от атак типа advanced persistent threat // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническя и научно-методическая конференция в 4 т., СПб.: СПбГУТ, 2024. Т. 2. С. 347-351.

5. Липатников В. А., Шевченко А. А., Мелехов К. В., Задбоев В. А. Способ обнаружения географического местоположения нарушителя безопасности информации в сети передачи данных // Состояние и перспективы развития современной науки по направлению «ИТ-технологии»: сб. тр / Под. ред. Г. Н. Семенова, В. И. Попова. Анапа: Изд-во ФГАУ «ВИТ «ЭРА», 2023. Том 2. С. 178-183.

6. Задбоев В. А., Липатников В. А., Шевченко А. А. Обеспечение информационной безопасности на основе методов выделенной сети и определения местоположения // Военная связь будущего. Квантовый скачок как неизбежность: материалы междунар. науч.-практ. конф., Санкт-Петербург, 10–11 ноября 2023 года. СПб: ФГК ВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» МО РФ, 2023. С. 85-89.

7. Котенко И. В., Саенко И. Б., Лаута О. С. Протестное программное обеспечение: анализ и подход к обнаружению, основанный на машинном обучении // Вопросы кибербезопасности. 2024. № 6. С. 42-52. doi:10.21681/2311-3456-2024-6-42-52.

BASIC CONCEPTS OF NEURAL NETWORKS IN DATA NETWORKS

Zadboev V., Tkachev D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is devoted to increasing the level of information security of data transmission networks using complex protection of several neural networks. The relevance of using artificial intelligence to protect data transmission networks from cyber-attacks in the context of increasingly complex threats is substantiated. The current neural networks in information security, their advantages and disadvantages are described. A system for detecting anomalies in the network with subsequent detection of an adversary based on neural networks is proposed.

Key words: *artificial intelligence, neural networks, cyber-attacks, data networks, information security, anomaly detection*

УДК 004.056.57
ГРНТИ 81.93.29

ОБЗОР СЕТЕВЫХ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ ДЛЯ ОБНАРУЖЕНИЯ КАНАЛОВ УПРАВЛЕНИЯ ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

И. А. Ушаков, М. А. Скорых

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

В условиях развития информатизации общества обеспечение компьютерной безопасности продолжает являться актуальной задачей. Одним из видов деструктивных действий злоумышленников является установка вредоносного программного обеспечения на скомпрометированные устройства. В статье рассматриваются варианты реализации каналов управления вредоносным программным обеспечением в компьютерных сетях, приведен обзор сетевых атрибутов, которые могут выступать в качестве индикаторов компрометации. Перечислены возможные способы детектирования каналов управления ВПО.

обнаружение угроз, компьютерные атаки, вредоносное программное обеспечение, системы обнаружения вторжений, индикаторы компрометации, Threat Intelligence, Threat Hunting

В текущей ситуации цифровизации всех сфер жизнедеятельности общества обеспечение информационной безопасности систем, обеспечивающих обработку информации, продолжает быть актуальным. Злоумышленники, взламывая компьютерные системы тем или иным способом, могут закрепляться на скомпрометированных устройствах путем установки вредоносного программного обеспечения (далее – ВПО). Для передачи команд со списком задач от центра удаленного управления (ЦУУ) ВПО к жертве используется канал управления ВПО (Command and Control, C2). Типовая схема работы ВПО, функционирующего в IP-сетях, представлена на рис. 1.

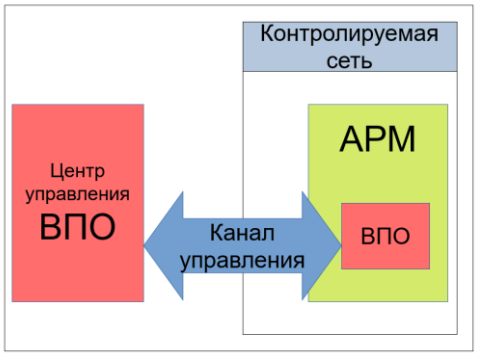


Рис. 1. Типовая схема работы ВПО в IP-сетях

Канал управления ВПО в IP-сетях как правило реализуется следующими способами:

1. С помощью общеизвестных протоколов 3-го и 7-го уровня модели OSI – HTTP, HTTPS, SMTP, DNS, SSH, ICMP и т.д. Примерами вредоносного ПО, которое использует данный способ организации канала управления являются: Cobalt Strike, Merlin, Sliver, Havoc, Iodine в соответствующих режимах функционирования. На рис. 2 представлен канал управления ВПО Iodine на базе протокола DNS (рис. 2).

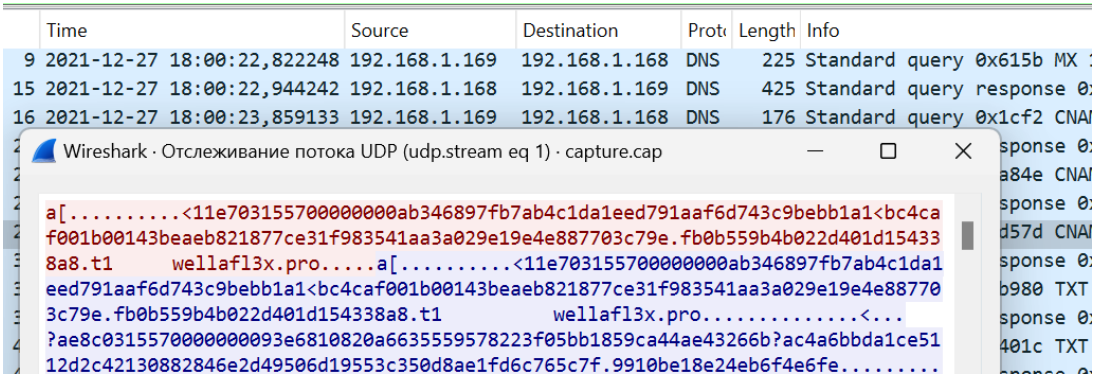


Рис. 2. Пример организации канала управления ВПО посредством утилиты IOdine

2. С помощью протоколов 7-го уровня модели OSI, разработанных создателем ВПО. Данный вариант канала управления чаще используется злоумышленниками на этапе первичного доступа к системе (пример – простейший bash реверс-шелл), либо в случае разработки злоумышленником собственного фреймворка постэксплуатации. На рис. 3 представлен канал управления ВПО, организованный при помощи Powershell реверс-шелла.

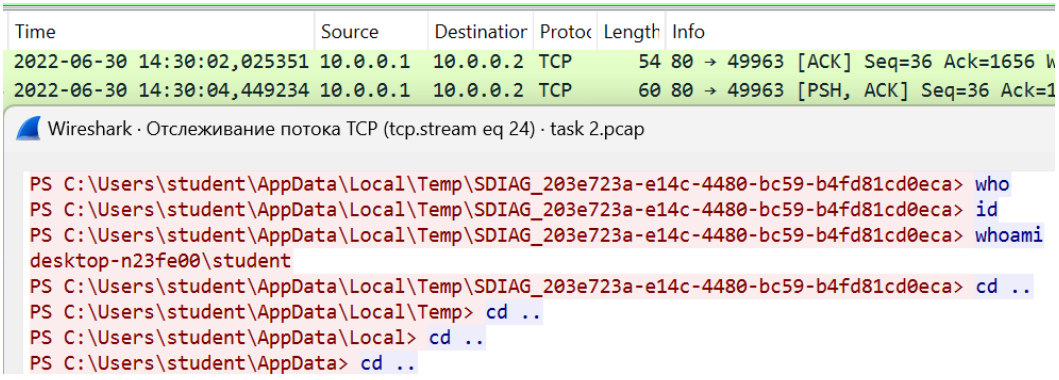


Рис. 3. Пример организации канала управления ВПО посредством PowerShell реверс-шелла

Для выявления каналов управления ВПО в сетевом трафике могут использоваться сигнатурные системы обнаружения вторжений. Однако слабой стороной такого подхода является невозможность обнаружения каналов управления ВПО, трафик которых не детектируется существующими сигна-

турами. Учитывая тот факт, что многие сетевые протоколы, используемые злоумышленниками, включают в себя методы криптографической защиты, а также постоянно растущее количество новых экземпляров ВПО, вопрос увеличения эффективности существующих средств обнаружения деструктивных действий хакеров встает особо остро.

Одним из вариантов повышения эффективности обнаружения каналов управления ВПО является применение технологии Threat Hunting. Согласно глоссарию Лаборатории Касперского [1] Threat Hunting – это процесс проактивного обнаружения вредоносной деятельности в компьютерных сетях. Для применения методов Threat Hunting в целях обнаружения каналов управления ВПО необходимо определить перечень сетевых атрибутов, которые могут выступать в качестве индикаторов компрометации (Indicators of compromise, IOC).

Сетевыми индикаторами компрометации, которые могут быть изучены в процессе анализа ВПО и реагирования на компьютерные инциденты, а затем агрегированы в соответствующие базы репутации являются:

1. IP-адреса. Данный сетевой атрибут является одним из наиболее распространенных индикаторов компрометации. IP-адреса почти всегда встречаются в отчетах компаний по результатам реагирования на компьютерный инцидент, агрегируются в различных базах репутации, таких как AbuseIPDB [2], и Threat Intelligence-платформах. Стоит отметить, что данный IOC имеет относительно короткий срок жизни, что требует усилий по поддержанию баз репутации в актуальном состоянии.

2. Доменные имена. Одним из распространенных способов, используемых злоумышленниками для маскировки канала управления ВПО, является регистрация DNS-записей. С помощью доменных имен злоумышленники могут динамически менять IP-адреса своих ЦУУ, использовать такие протоколы как Secure Sockets Layer (SSL) и Transport layer security (TLS), маскируясь под легитимный пользовательский сетевой трафик и т.д. Данный индикатор компрометации имеет б*о*льший срок жизни по сравнению с IP-адресами, однако, злоумышленникам не составляет сложности менять доменные адреса.

3. Информация о сертификатах X.509 [3]. Злоумышленники при регистрации сертификатов могут указывать специфичные значения для таких полей как Common Name (CN), Organization (O), Organization Unit (OU), Locality (L) и т.д. Так, например, ВПО DcRAT в конфигурации по умолчанию в поле сертификата Common Name содержит строку «DcRat Server».

Эти параметры инфраструктуры открытых ключей легко извлекаются из сетевого трафика и также могут быть использованы в целях проактивного поиска угроз.

4. JA3. Метод JA3 хэширования был рассмотрен в блоге Salesforce Engineering Джоном Альтхаусом в 2017 году [4]. JA3 хэш представляет собой отпечаток клиентского приложения в SSL/TLS-соединении. Данный подход обеспечивает идентификацию клиентского приложения в TLS-соединении [5]. Используя данный метод появляется возможность детектировать в сетевом трафике SSL-соединения создаваемые ВПО. Примером базы репутации таких индикаторов компрометации служит ресурс SSL Blacklist [6].

5. JA4+. JA4+ – это набор методов снятия сетевых отпечатков [7], являются продолжением метода JA3. Использование семейства этих отпечатков позволяет обнаруживать различные варианты компьютерных атак, включая каналы управления ВПО. Список JA4+ отпечатков представлен в таблице №1.

ТАБЛИЦА 1. Список отпечатков JA4+

Полное название отпечатка	Сокращенное название отпечатка	Описание
JA4	JA4	TLS-отпечаток клиента
JA4Server	JA4S	TLS-отпечаток сервера
JA4HTTP	JA4H	HTTP-отпечаток клиента
JA4Latency	JA4L	Отпечаток временной задержки от клиента до сервера
JA4LatencyServer	JA4LS	Отпечаток временной задержки от сервера до клиента
JA4X509	JA4X	Отпечаток сертификата X509 TLS
JA4SSH	JA4SSH	SSH-отпечаток
JA4TCP	JA4T	TCP-отпечаток клиента
JA4TCPServer	JA4TS	TCP-отпечаток сервера

Указанные индикаторы компрометации могут быть использованы в целях повышения эффективности обнаружения каналов управления ВПО систем обнаружения вторжений в двух вариантах:

– используя базы репутации известного ранее ВПО определять сетевое взаимодействие, созданное злоумышленниками;
– зная сетевые атрибуты общеизвестных ресурсов, принятых за легитимные (такие как Yandex, Google, Госуслуги и т.д.) можно исключить сетевые взаимодействия с ними из рассмотрения на предмет наличия канала управления ВПО, тем самым сузив круг поиска и уменьшив вероятность ложноположительной ошибки.

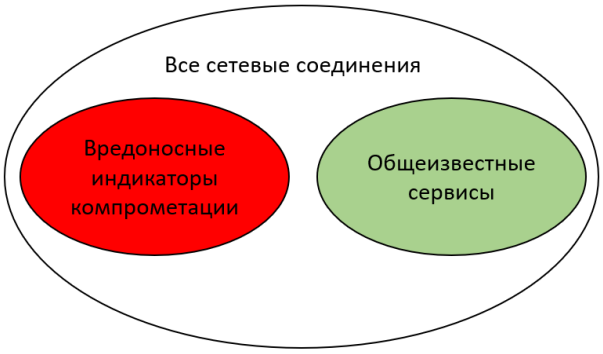


Рис. 4. Диаграмма Эйлера-Венна, отображающая сетевые соединения с учетом баз репутации индикаторов компрометации

Из рис. 4 видно, что использование перечисленных в статье индикаторов компрометации поможет «окрасить» специалистам по информационной безопасности все сетевые соединения, наблюдаемые в контролируемых информационных системах, что в свою очередь повысит эффективность обнаружения каналов управления ВПО.

Список используемых источников

1. Активный поиск угроз // Энциклопедия «Касперского». URL: https://encyclopedia.kaspersky.ru/glossary/threat-hunting/ (дата обращения 02.01.2025).

2. AbuseIPDB. URL: https://www.abuseipdb.com/ (дата обращения 02.01.2025).

3. The State of SSL/TLS Certificate Usage in Malware C&C Communications. Mohamad Mokbel // TrendMicro Research. URL: https://www.trendmicro.com/content/dam/trendmicro/global/en/research/21/i/ssl-tls-technical-brief/ssl-tls-technical-brief.pdf (дата обращения 02.01.2025).

4. Open Sourcing JA3 // Salesforce Engineering Blog. URL: https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41/ (дата обращения 02.01.2025).

5. Скорых М. А. Использование JA3 хэшей в качестве индикаторов компрометации / М. А. Скорых // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 901-905. EDN QCPTNI.

6. SSL Blacklist. URL: https://sslbl.abuse.ch/ (дата обращения 02.01.2025).
7. FoxIO-LLC/ja4 // GitHub, Inc. URL: https://github.com/FoxIO-LLC/ja4/tree/main (дата обращения 02.01.2025).

AN OVERVIEW OF NETWORK INDICATORS OF COMPROMISE FOR DETECTING MALWARE COMMAND AND CONTROL CHANNELS

Ushakov I. A., Skorykh M.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the conditions of high informatization of public life, ensuring computer security continues to be a relevant task. One of the types of destructive actions of intruders is the installation of malicious software on compromised devices. The article considers options for implementing channels for controlling malicious software in IP networks. An overview of network attributes that can act as indicators of compromise is given. Possible methods for detecting malware control channels are listed.

Key words: *Malware, indicators of compromise, computer attacks, IDS, Threat intelligence, threat hunting*

УДК 004.056(082)
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СЕТЯХ LTE

И. А. Ушаков, А. И. Черкашин

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

В статье рассматриваются принципы аутентификации и регистрации абонентов в сетях LTE, процессы шифрования и дешифрования трафика абонентов, передаваемого в сетях LTE. Также в статье рассматривается инфраструктура сети связи четвертого поколения, компоненты архитектуры безопасности и их взаимосвязь, проведен анализ организационных и технических мер обеспечения защиты информации.

сети LTE, безопасность, GSM, IPSec, виртуальные частные сети

Безопасность в сетях LTE (Long-Term Evolution) и LTE-A (Long-Term Evolution- Advanced) является одним из ключевых аспектов работы сети, влияющая на качество, скорость передаваемого абонентского трафика сети, а также объем передаваемого трафика, проходящего через сеть LTE. Основным аспектом обеспечения безопасности в сетях LTE является алгоритм, при котором генерируются и вычисляются секретные ключи непосредственно перед каждой операцией, проводимой в сетях LTE. Данные ключи изменяются от сеанса к сеансу в зависимости от действий абонента (UE). В сетях LTE в отличие от сетей предыдущих поколений (GSM) используется протокол взаимной аутентификации, т.е. дополнительно к проверке обслуживающей сетью идентичности абонента выполняется процедура проверки мобильным устройством легитимности обслуживающей сети. Также отличительной особенностью безопасности сетей LTE в отличие от сетей предыдущих поколений является механизм контроля целостности (integrity protection). Данный механизм осуществляет проверку идентичности отправителя сигнальных сообщений.

Существуют ряд критериев безопасности в сетях LTE:

– аутентификация абонента в сети LTE при начальном подключении UE;
– защита принимаемых и передаваемых сообщений, как сигнальных, так и пользовательских (user plane, control plane);
– защита абонентов в сети LTE;
– защита абонентских устройств от подключений к нелегитимным сетям;
– шифрование данных и сообщений, используемых в сетях LTE;
– минимизация ошибок (BER) и улучшение качества трафика.

При защите абонентов в процессе обслуживания в сети поток данных скрывают временными идентификаторами. Для обеспечения безопасности внутри сети применяют принцип туннелирования соединений. Для обеспечения наилучшей безопасности сети применяют шифрование разных сегментов сети, а также интерфейсов, используемых в сетях LTE. Соответственно шифрованию подвергаются пакеты S1 и X2 при помощи IPsec ESP рис. 1, а также сигнальный трафик, используемый в этих интерфейсах [1, 4, 5].



Рис. 1. Архитектура сети LTE и шифрация трафика при помощи IPsec [2]

Когда мобильный абонент UE проходит регистрацию и аутентификацию в сети LTE, необходимо обеспечение безопасности и реализацию подлинности данного абонента. Для этого необходима генерация ключей, которые инициируют и поддерживают алгоритмы функциональной безопасности в сети, в том числе и ключ K_{ASME} . При прохождении взаимной аутентификации абонента с сетью LTE идет процедура согласования ключей, известная как AKA (Authentication and Key Agreement). Результатом данной процедуры является генерация алгоритмов безопасности, в том числе и инициализация промежуточного ключа K_{ASME}. Как правило, при регистрации и установлении соединения между USIM (UE) и центром аутентификации (Auc/HSS), происходит контроль механизма AKA, который необходим для генерации ключей. Этот процесс занимает доли секунды. Соответственно, для увеличения скорости передачи данных в сетях LTE нужно включить функцию обновления ключевой информации без инициализации механизма AKA. Чтобы решить эту проблему в сетях LTE вводится использование иерархической инфраструктуры ключей. Принцип организации иерархической инфраструктуры ключей представлен на рис. 2. На рис. 2 по-

мимо инициализации промежуточного ключа K_{ASME} вводится генерация ключей: K_{eNB}, K_{NASint}, K_{NASenc}. Иерархия ключей в сетях LTE представлена на рис. 3. При инициализации механизма AKA для выполнения двусторонней аутентификации пользователя и сети, генерируются ключ шифрования CK и общие ключи безопасности, которые затем передаются из программного обеспечения USIM на мобильное оборудование (UE) и в центр аутентификации (Auc/HSS). UE и HSS, используя пару ключей (CK; IK) и идентификатор используемой сети, генерируют ключ K_{ASME}. Устанавливая зависимость ключа от сетевого идентификатора, центр аутентификации (Auc/HSS) гарантирует возможность использования ключа только в пределах этой сети [7].

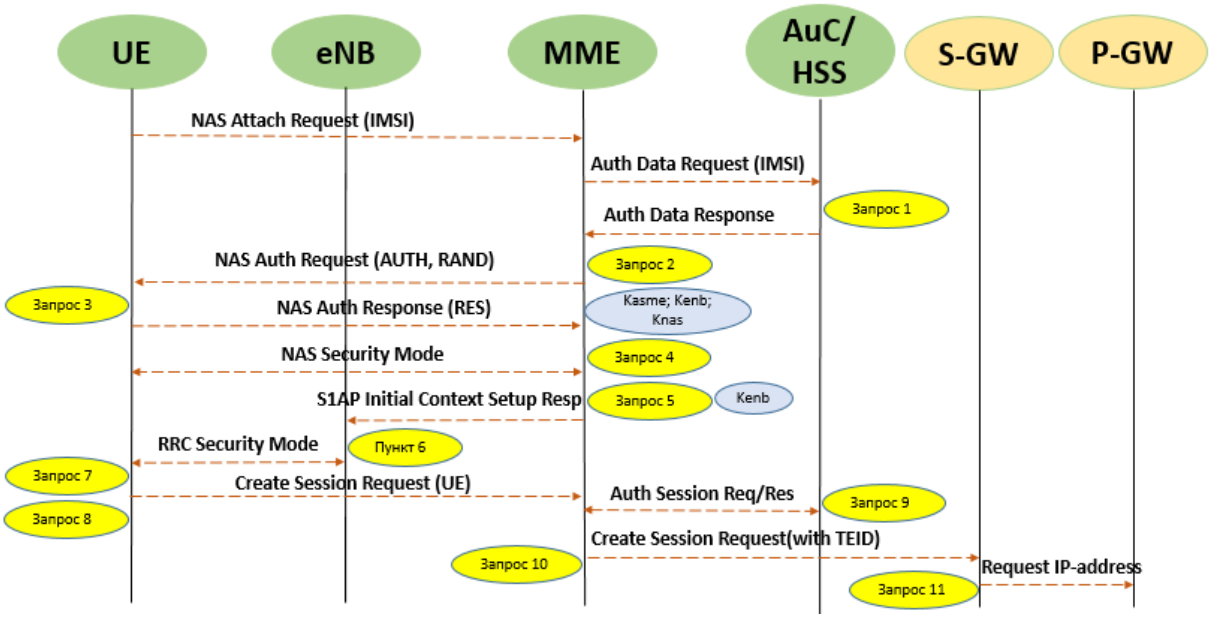


Рис. 2. Принцип аутентификации и генерации ключа абонентского терминала

На рис. 2 рассмотрен алгоритм аутентификации и создания ключа безопасности, а также дальнейшее его использование в сети LTE [6]. Рассмотрим подробнее этот процесс.

Запрос 1 начинается с сообщения NAS Attach Request с регистром IMSI и передается между абонентом мобильного устройства UE и маршрутизатором MME через подсистему базовых станций eNB сети LTE. Вследствие чего, MME перенаправляет этот запрос на регистр AuC/HSS (регистр аутентификации и регистрации мобильных абонентов). Таким образом, для регистрации абонента UE в сети, а также получения аутентификационных данных абонента UE, формируется запрос/ответ Auth Data Request и Auth Data Response через регистр AuC/HSS. После аутентификации данных регистрируемого абонента, сообщение Auth Data Request приходит обратно на маршрутизатор MME.

Далее, на регистр MME принимаются параметры IK, CK, полученные от центра аутентификации AuC/HSS, а также параметры XRES, RAND и AUTH. После чего формируется запрос 2: NAS Auth Request (RAND, AUTH) с параметрами AUTH и RAND через подсистему базовых станций в сторону абонента UE с его запросом аутентификации данного мобильного устройства.

После этого, абонентское устройство UE, получив параметры RAND, AUTH, производит внутренние вычисления IK, CK, а также RES, XMAC, используя свой внутренний ключ безопасности (AMF, RAND, AUTH). Далее формируется новый запрос 3: NAS Auth Response (RES) в сторону MME с результатом аутентификации от абонента UE.

На вход регистра MME поступает запрос 3 RES, после чего происходит его сравнение с параметром XRES и в случае их совпадения происходит успешная аутентификация абонента. В противном случае от MME генерируется ответ абоненту UE об ошибке аутентификации. После того, как прошла успешная аутентификация абонента, сбрасывается счетчик DL NAS и производятся вычисления ключей: K_{ASME}, K_{eNB}, K_{NASint} K_{NASenc}. Вследствие чего выполняются алгоритмы безопасности NAS (Non-Access Stratum). Соответственно, в этом запросе используется алгоритм шифрования, алгоритм контроля целостности, а также идентификатор ключей NAS и алгоритмы функциональной безопасности UE. Параллельно тому, как NAS получает команду режима безопасности, абонент по своим внутренним алгоритмам вычисляет ключи K_{ASME}, K_{eNB}, K_{NASint} K_{NASenc} и после производит отправку своих параметров режима безопасности в сторону MME в зашифрованном и защищенном виде. Эта процедура генерируется запросом 4: NAS Security Mode (NAS Security Mode Command и NAS Security Mode Complete).

Далее после того, как произведена генерация запроса NAS Security Mode с параметрами режима безопасности от абонента UE, в MME вычисляется и производится отправка ключа K_{eNB} в запросе 5: S1AP Initial Context Setup Resp на подсистему базовых станций eNB с начальной настройкой префикса S1AP (контекста ключа безопасности). Соответственно, получив запрос с ключом K_{eNB} базовая станция eNB по своим внутренним алгоритмам вычисляет ключи K_{RRCinc}, K_{RRCenc}, K_{UPenc}. Далее генерируется отправка команды ключа безопасности RRC с набором алгоритмов, ключевыми из которых являются алгоритм целостности и шифрования AS. Данные процедуры выполняются в Пункте 6 на схеме рис. 2.

После принятия команды ключа безопасности RRC Security key на стороне абонента UE вычисляются ключи K_{RRCinc}, K_{RRCenc}, K_{UPenc}. В заверше-

нии процесса абонентским устройством выполняется отправка сгенерированного ключа шифрования в подсистему базовых станций eNB с помощью алгоритма RRC. Данные выше процедуры происходят в запросе 7.

В случае передачи потоковых данных от абонента UE в сеть Интернет, абонент UE начинает взаимодействовать с пакетной корой сети LTE через шлюз S-GW/P-GW (рис 1). Для этого от абонента UE в сторону MME отправляется запрос 8: Create Session Request, который содержит в себе алгоритмы безопасности NAS. После этого MME переадресует запрос 9: Auth Session Req на регистр AuC/HSS для аутентификации абонента UE. AuC/HSS отправляет обратно Auth Session Res, после чего MME получает запрос с параметрами аутентификации абонента UE. Затем MME перенаправляет запрос 10 шлюзу S-GW. В данный запрос также входит идентификатор конечной точки туннеля (TEID), который назначается для PDN данного абонента UE в сети LTE.

Затем шлюз S-GW переадресует запрос 11 на шлюз P-GW для назначения IP-адреса данному абоненту UE и предоставления доступа в сеть Интернет [3].

Кроме того, при рассмотрении ключа K_{ASME} при реализации Запроса: NAS Auth Request/Response на стороне абонентского терминала (UE), базовой станции (eNodeB) и MME, посредством криптографической функции KDF (Key Derivation Function), происходит расчет ключей K_{eNB}, K_{NASint}, K_{NASenc}, K_{UPinc}, K_{UPenc}, K_{RRCinc} K_{RRCenc}, которые используются для защиты (шифрования и контроля целостности) пользовательского и сигнального трафика. Длины ключей составляют 128 бит.

Иерархия ключей [4] приведена на рисунке рис. 3

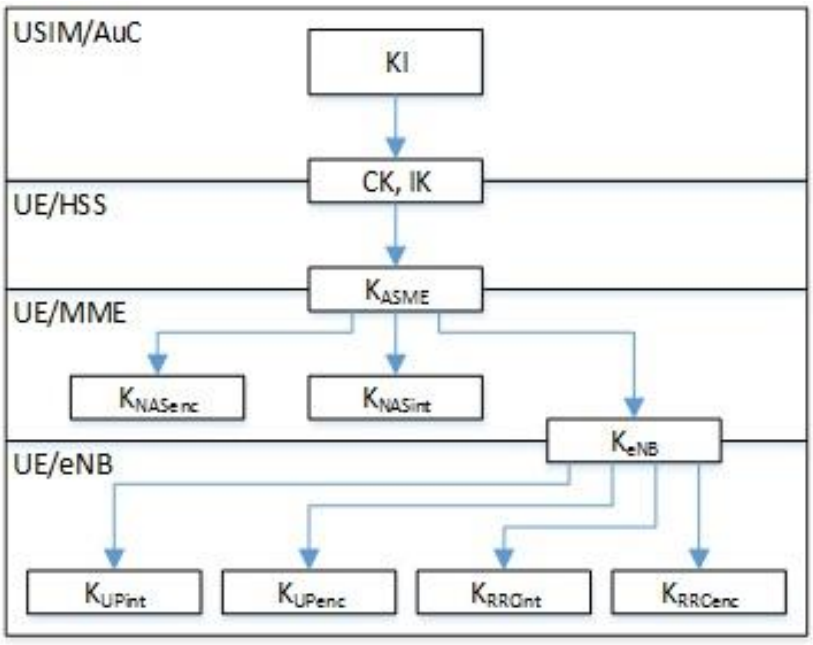


Рис. 3. Иерархия ключей в сетях LTE

Таким образом, перед началом шифрования трафика и контроля целостности между сетью и абонентским терминалом (UE), происходит согласование поддерживаемых алгоритмов. Безопасность в сетях LTE и, в частности, процесс генерации ключей безопасности, рассмотренный выше, играет существенную роль при аутентификации абонента. Потеря, либо повреждение целостности и, соответственно, утрата контроля подлинности данных ключей, ведут к ошибке регистрации абонентов в сетях LTE, а также к существенному ухудшению качества предоставленных сервисов.

Список используемых источников

1. Тихвинский В. О., Тереньев С. В., Юрчук А. Б. Сети Мобильной Связи LTE // Экотрендз. 2010. С. 81.

2. Algorithms for evaluating the effectiveness of information security systems in LTE networks // Tashkent University of Information Technologies URL: // https://core.ac.uk/download/pdf/74252615 (дата обращения: 25.02.2024 г.)

3. LTE Security Architecture// 3GLTEinfo URL: // LTE Security Architecture | 3GLTEInfo (дата обращения: 20.02.2024 г.)

4. Данилов В. И. Сети и стандарты мобильной связи // СПбГУТ. СПб., 2015. С. 20.

5. Сети стандарта LTE. Развитие технологий радиодоступа // СПбГУТ, 2016. 145 с.

6. Никитина А. В., Рыжков А. Е. Сети радиодоступа четвертого поколения стандарт LTE // изд-во СПб ГУТ. 2012. 86 с.

7. Голиков А. М., Исследование метода защиты трафика систем мобильной связи AES-128 // Томск, 2020. С. 7.

ANALYSIS OF SECURITY METHODS IN LTE NETWORKS

Ushakov I., Cherkashin A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the principles of authentication and registration of subscribers in LTE networks, the processes of encryption and decryption of subscriber traffic transmitted in LTE networks. The article also examines the infrastructure of the fourth generation communication network, the components of the security architecture and their interrelation, and analyzes organizational and technical measures to ensure information security.

Key words: *LTE networks, security, GSM, IPSec, virtual private networks*

УДК 004.056
ГРНТИ 81.93.29

ПОИСК СЛЕДОВ КИБЕРПРЕСТУПЛЕНИЙ С ПРИМЕНЕНИЕМ МАТРИЦЫ MITRE ATTACK

А. А. Чечулин, Е. А. Антонюк

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Для поиска следов киберпреступлений применяются различные методы, направленные на обнаружение и анализ данных, оставленных злоумышленниками после атаки. Применение регулярно обновляемых баз знаний действий злоумышленников в ходе проведения кибератак, может помочь значительно повысить эффективность методов расследования киберпреступлений. Исследование посвящено методам поиска и анализа следов киберпреступлений с использованием матрицы MITRE ATT&CK.

информационная безопасность, расследование информационных инцидентов, матрица MITRE ATT&CK

MITRE ATT&CK – широко применяемая база знаний и система классификаций действий злоумышленников, предпринимаемых ими в ходе кибератак. Модель ATT&CK включает в себя классификацию известных группировок или отдельных акторов, отслеживаемых государственными и частными организациями в сфере киберпреступлений [1]. В настоящее время многие организации применяют ее для оценки уровня своей кибербезопасности, активно интегрируют и продвигают ATT&CK в своих продуктах – решениях Endpoint Detection and Response (EDR), а также системах управления информационной безопасностью и событиями безопасности (SIEM) [2].

Используя матрицу MITRE ATT&CK в целях поиска следов киберпреступлений, можно провести анализ действий злоумышленников через призму тактик, техник и процедур, описанных в этой базе знаний. Поиск и анализ следов киберпреступлений с применением модели MITRE ATT&CK можно разделить на следующие этапы:

– обнаружение и сбор данных;
– расширение поиска;
– сопоставление данных с тактиками и техниками;
– анализ и верификация;
– визуализация и отчетность.

На этапе обнаружения и сбора данных, где проводится анализ сетевых и системных логов, а также изучение артефактов, таких как файлы и активные процессы, можно интегрировать популярные инструменты мониторинга, позволяющие в дальнейшем сопоставлять события с тактиками и техниками фреймворка MITRE ATT&CK. Этот процесс может включать анализ сетевых и системных логов, исследование артефактов, таких как файлы и процессы, а также работу с данными SIEM. Данные, которые собираются будут обрабатываться и анализироваться для понимания мотивов, целей и поведения нарушителя [3].

На следующем этапе – расширении поиска можно применять различные источники данных (data sources), предложенные MITRE ATT&CK для каждой техники. Например, источник данных File (DS0022) – может использоваться для идентификации вредоносных файлов по их метаданным, таким как имя, местоположение, размер и хэш. Или использовать источник данных Active Directory (DS0026) для мониторинга подозрительной активности в учетных записях, например, создание новых администраторов или изменение прав доступа. Эти источники данных помогают определять, какие события требуют внимания, а аномальная активность запросов к LSASS техники Credential Dumping (T1003) может быть выявлена через анализ журналов процессов. Кроме того, на данном этапе возможно обогащение данных, которое будет достигаться благодаря интеграции с платформами Threat Intelligence (TIP), что позволит связывать индикаторы атак (IoC) с конкретными техниками ATT&CK., например, связь эксплойта CVE-2023-38831 с техникой Exploitation for Client Execution (T1203) сделает этот процесс более информативным и целенаправленным.

Этап сопоставление данных с тактиками и техниками позволит эффективно идентифицировать подозрительные активности через призму тактик и техник матрицы. Например, при обнаружении фишингового письма с вредоносными вложениями проводится сопоставление с техникой Phishing for Initial Access (T1566) тактики Initial Access. Атака начинается с отправки целевым пользователям писем с вредоносными вложениями или ссылками, целью которых является заражение системы жертвы, в дальнейшем при анализе и верификации можно определить какими инструментами пользовались злоумышленники. Такой процесс сопоставления позволит более точно определить последовательность действий злоумышленника.

Следующий этап – анализ и верификация. На данном этапе можно анализировать поведение пользователей и систем на предмет отклонений от

нормы. Основные области анализа включают мониторинг активности привилегированных учетных записей, отслеживание запуска подозрительных процессов и изменения их характеристик, выявление неожиданных изменений в настройках системы. Если поведение отличается от ожидаемого, это может свидетельствовать об использовании техник из MITRE ATT&CK, таких как техника Account Discovery (T1087), где злоумышленник пытается получить список учетных записей, что проявляется в виде необычных запросов к Active Directory или техника Masquerading (T1036) – маскировка под легитимный процесс, которая может проявляться изменением имен исполняемых файлов или их расположения. В дальнейшем можно применить данные из платформ Threat Intelligence для связи тактик, техник и процедур с известными группировками злоумышленников. Например, APT29 может использовать специфические техники, что облегчает выявление атак этой группы. Такая стратегия анализа помогает глубже понять природу угроз и принять обоснованные решения расследованию киберпреступлений.

Этап визуализации и отчетности подразумевают построение матриц атак (Attack Trees) для наглядного представления этапов компрометации. Матрицы атак помогают визуально продемонстрировать путь злоумышленника от начальной стадии проникновения до достижения конечной цели. Они позволяют увидеть взаимосвязи между разными техниками и тактиками, применяемыми злоумышленниками, а также выявить ключевые моменты, где атака могла быть предотвращена или остановлена. Это способствует оптимизации стратегий расследования, позволяя сосредоточиться на наиболее важных аспектах. Также матрица атаки может применяться для документирования и составления отчета для передачи информации в правоохранительные органы для дальнейшего расследования. Этот этап поможет обеспечить комплексный взгляд на атаку и способствовать эффективному обмену информацией как внутри организации, так и вне ее.

Таким образом, применение матрицы MITRE ATT&CK позволит организовать систематический процесс расследования и обеспечить целостный подход к выявлению цифровых следов преступлений, что существенно улучшит качество анализа угроз. Сопоставление активности с техниками матрицы MITRE ATT&CK может помочь в использовании имеющихся знаний об атакующих при расследовании киберпреступлений.

Стоит отметить, что глубокое понимание почему, когда и кто может совершить вредоносное действие, гораздо полезнее при расследовании ки-

берпреступлений, чем борьба против известных классифицированных методов и процедур атак [4, 5].

Список используемых источников

1. Котенко И.В., Хмыров С.С., Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. 2022. № 4(50). С. 53–79.

2. Apurva Virkud, Muhammad Adil Inam, Andy Riddle, Jason Liu, Gang Wang, Adam Bates, University of Illinois Urbana-Champaign, How does Endpoint Detection use the MITRE ATT&CK Framework? URL: https://gangw.cs.illinois.edu/mitre24.pdf (дата обращения: 15.01.2025).

3. Friedman J., Bouchard M. Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks. – CyberEdge Group, 2015.

4. Anna Georgiadou, Spiros Mouzakitis, Dimitris Askounis Assessing, MITRE ATT&CK Risk Using a Cyber-Security Culture Framework, URL: https://www.mdpi.com/1424-8220/21/9/3267 (дата обращения: 16.02.2025).

5. Чечулин А.А., Горда М.Д., Котов А.А. Ключевые аспекты разработки междисциплинарной методики для внутренних расследований киберпреступлений // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 70–85. DOI: 10.61260/2218-130X-2024-3-70-85.

SEARCHING FOR CYBERCRIME TRACES USING THE MITRE ATTACK MATRIX

Chechulin A., Antonyuk E.
Federal Research Center of the Russian Academy of Sciences

Various methods are used to search for traces of cybercrime in order to detect and analyse the data left behind by attackers after an attack. The use of regularly updated databases of knowledge about the actions of attackers during cyberattacks can help significantly improve the effectiveness of cybercrime investigation techniques. The study focuses on methods for finding and analysing cybercrime traces using the MITRE ATTACK matrix.

Key words: *Information security, information incident investigation, MITRE ATT&CK matrix*

УДК 654.739
ГРНТИ 49.33.29

ОСНОВНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БЮДЖЕТНЫХ ОРГАНИЗАЦИЯХ И ПУТИ ИХ РЕШЕНИЯ

А. А. Чечулин, М. Д. Горда

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

В статье рассматриваются основные проблемы обеспечения информационной безопасности в бюджетных организациях. Особое внимание уделяется влиянию финансовых ограничений, кадровых проблем, регуляторных требований и вопросов импортозамещения на уровень защиты информации. Автор анализирует возможные пути решения выявленных проблем с учетом рисков и предлагаемых компенсирующих мер.

информационная безопасность, риски информационной безопасности

В современном мире каждая организация сталкивается с вопросом эффективного обеспечения информационной безопасности. Каждый день происходят десятки тысяч атак, часть из которых позволяет злоумышленникам проникнуть в инфраструктуру организаций и похитить конфиденциальные данные или нарушить процессы организаций. Однако у каждой организации есть свои особенности, в зависимости от отрасли, возможности финансирования ИБ и т.д.

Информационная безопасность включает в себя как техническую часть, так и организационную. В каждом из этих элементов ИБ, касательно бюджетных организаций, имеются определенные проблемы, решение которых позволило бы достичь более эффективной работы специалистов, а значит лучшей защиты организации от актуальных киберугроз. Одной из важнейших задач специалистов в области ИБ, а также руководителей подразделений – определить основные проблемы, найти пути решения с минимальными рисками для организации.

Первым делом, определим особенности бюджетных организаций, которые могут как прямо, так и косвенно повлиять на информационную безопасность. Первым аспектом будут являться финансовые ограничения. Бюджетные организации сталкиваются с жесткими рамками финансирования, где информационная безопасность часто оказывается не в приоритете. Процедуры госзакупок усложняют оперативное приобретение современных

средств защиты, а длительный цикл обновления приводит к использованию устаревшего оборудования и ПО. Далее идут аспекты, связанные с регуляторными требованиями и контролем. Государственные учреждения обязаны соблюдать строгие нормы и требования по защите информации (ФЗ-152, приказы ФСТЭК, ФСБ, Роскомнадзора и др.). Регулярные проверки требуют значительных ресурсов как финансовых, так и трудовых, а несоответствие может привести к штрафам, санкциям или даже приостановке деятельности организации.

К особенностям, также, можно отнести вопросы кадровой политики и отсутствия единой политики обеспечения информационной безопасности. Низкие зарплаты по сравнению с коммерческим сектором затрудняют привлечение квалифицированных специалистов по ИБ. Часто обязанности по ИБ выполняют системные администраторы, не имея специализированной подготовки. ИТ-инфраструктура бюджетных организаций часто разрознена: используются разные системы, устаревшие решения, что усложняет их защиту.

Также, к особенностям можно отнести возможную зависимость от импортного ПО и необходимость импортозамещения. Однако ограниченный выбор сертифицированных продуктов, нехватка специалистов для их внедрения и долгий процесс адаптации создают дополнительные риски для информационной безопасности.

Таким образом, основываясь на особенностях организации, можно разделить проблемы на 4 направления: квалификация сотрудников, уязвимое программное и аппаратное обеспечение, вопросы импортозамещения, соответствие требованиям регуляторов. На основе анализа проблем и потенциальных рисков применения конкретных компенсирующих мер были получены результаты, описанные в таблице 1.

ТАБЛИЦА 1. Оценка риска вариантов решения проблем.

Проблема	Решение	Уровень риска
Квалификация	Повышение квалификации сотрудников	Высокий
	Уменьшение количества сотрудников за счет увеличения качества их работы	Средний
	Увеличение заработной платы сотрудников	Средний
	Снижение требований к квалификации	Низкий

Проблема	Решение	Уровень риска
Уязвимое ПО/АО	Внутренние аудиты информационной безопасности	Средний
	Внешние аудиты информационной безопасности	Высокий
	Разработка стимулирующих мер для сотрудников	Средний
	Снижение требований к квалификации	Низкий
Импортозамещение	Частичное	Высокий
	Полное	Средний
	Переход на новое ПО/АО	Средний
Требования регуляторов	Повышение нормативных знаний сотрудников	Низкий
	Снижение требований к квалификации	Средний
	Разработка документации внешней организацией	Высокий
	Разработка документации внутри	Средний

На основе полученных возможных вариантов решения проблем можно сделать определенные выводы.

1. Информационная безопасность в бюджетных организациях однозначно требует комплексного подхода. Универсального метода не существует – каждая организация должна разрабатывать индивидуальные стратегии с учетом своих финансовых, кадровых и технических возможностей.

2. Финансовые ограничения являются одним из основных сдерживающим фактором развития информационной безопасности в бюджетных организациях. В отличие от коммерческих структур, бюджетные организации вынуждены работать в условиях строгого регулирования и недостаточного финансирования. Это приводит к нехватке ресурсов на приобретение современного оборудования, лицензированного ПО и обеспечение конкурентоспособных условий для специалистов.

3. Кадровый вопрос – один из ключевых в обеспечении информационной безопасности. Низкий уровень заработных плат стимулирует переход квалифицированных специалистов в другие организации и недостаточные знания сотрудников. Повышение квалификации является эффективным способом повышения уровня безопасности, но требует дополнительных ресур-

сов и несет риск ухода обученных сотрудников в частный сектор. Разработка методических и технических решений, снижающих требования к квалификации, способна частично компенсировать нехватку специалистов, но требует постоянного обновления и поддержки.

4. Слабая техническая база делает бюджетные организации уязвимыми к актуальным техникам атак. Недостаточная квалификация сотрудников ведет к низкому уровню администрирования ИТ-инфраструктуры, что может стать причиной критических уязвимостей, в том числе на периметре. Проведение регулярных аудитов – как внутренних, так и внешних – является одним из возможных решений, но его эффективность зависит от качества подготовки персонала и уровня финансирования.

5. Импортозамещение предлагает как возможности, так и риски. Переход на отечественные программные и аппаратные решения неизбежен, но требует значительных затрат на адаптацию и обучение сотрудников. Полное импортозамещение может привести к ограниченному выбору решений и снижению эффективности работы, в то время как частичное – к возможным санкциям со стороны регуляторов.

6. Соответствие требованиям регуляторов требует временных и финансовых затрат. С одной стороны, новые нормативные требования способствуют повышению уровня защиты информации. С другой стороны, их внедрение требует привлечения дополнительных ресурсов, что может создавать нагрузку на бюджетные организации. Альтернативные подходы, такие как привлечение внешних специалистов или разработка документации собственными силами, несут свои риски, включая вопросы качества и конфиденциальности.

На основе систематизированных знаний о проблемах и возможных путей их решения можно сформировать актуальные рекомендации в части устранения большего количества основных проблем информационной безопасности, а именно:

– формирование долгосрочной стратегии развития ИБ с учетом текущего уровня защиты, планируемых улучшений и возможных ограничений бюджета;
– разработка внутренних регламентов и методических материалов для снижения зависимости от уровня квалификации сотрудников;
– использование гибридного подхода к импортозамещению – анализ возможных рисков и возможностей перед переходом на отечественные решения;

– создание системы стимулирования сотрудников в области ИБ – нематериальные мотивационные механизмы, повышение внутреннего статуса специалистов;
– проведение регулярных аудитов и тестирований для выявления уязвимостей и повышения уровня защиты ИТ-инфраструктуры;
– оптимизация кадровой политики – баланс между повышением квалификации сотрудников и снижением требованиям к квалификации за счет разработки различных методик.

Список используемых источников

1. Информационная безопасность госучреждений // URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-gosuchrezhdenij/ (дата обращения 01.03.2025).

2. Десницкий В. А., Сахаров Д. В., Чечулин А. А., Ушаков И. А., Захарова Т. Е. Защита информации в центрах обработки данных. Учебное пособие. СПб.: СПбГУТ, 2019. 92 с.

3. Чечулин А. А., Горда М. Д., Котов А. А. Ключевые аспекты разработки междисциплинарной методики для внутренних расследований киберпреступлений // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 3. С. 70–85. DOI: 10.61260/2218-130X-2024-3-70-85.

KEY CHALLENGES IN ENSURING INFORMATION SECURITY IN BUDGETARY ORGANIZATIONS AND WAYS TO ADDRESS THEM

Chechulin A., Gorda M.
St. Petersburg Federal Research Center of the Russian Academy of Sciences

This paper examines the key challenges in ensuring information security in budgetary organizations. Particular attention is given to the impact of financial constraints, staffing issues, regulatory requirements, and import substitution policies on the overall level of information protection. The author analyzes potential solutions to the identified problems, considering associated risks and proposed compensatory measures.

Key words: *information security, information security risks*

УДК 004.056.5
ГРНТИ 81.93.29

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. АЛГОРИТМЫ ПРОТИВОДЕЙСТВИЯ АТАКАМ

А. А. Чечулин, А. П. Кюнер

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Стремительное развитие технологий обуславливает рост сервисов обработки и передачи информации, числа пользователей информационных систем, способов нарушения информационной безопасности. Одним из наиболее распространенных способов осуществления кибератаки является применение методов социальной инженерии. Основным недостатком существующих мер защиты от подобного рода угроз является отсутствие подробного описания атакующего и способов атаки. В статье приводится описание алгоритма, предназначенного для заполнения моделей элементов социо-инженерной атаки на основе исходных данных о сотруднике и компании, взятых из открытых источников, анкеты, информационной инфраструктуры, политики информационной безопасности. Предложенный алгоритм позволяет также автоматизировать процесс описания модели нарушителя информационной безопасности и разработать контрмеры.

социальная инженерия, алгоритм поиска жертв, фишинг, модель нарушителя

Разработка алгоритмов противодействия кибератакам с использованием методов социальной инженерии является важной задачей наряду с разработкой систем мониторинга, средств обнаружения вторжений, систем предотвращения утечек информации. К особенностям социальной инженерии можно отнести: сбор информации из открытых источников и путем неправомерного использования утечек данных, отсутствие необходимости в высокой квалификации атакующего, возможность применения в целевых и массовых атаках, наличие широкого спектра каналов осуществления атаки. Доступ к информационным технологиям большой не уделяющей внимание мерам предосторожности аудитории способствует атакам, эволюция и разнообразие методов атаки, является популярным способом обходи системы защиты информации, любые знания об объекте атаки могут оказаться полезными для выстраивания доверительных отношений также являются характеристиками данного рода атак.

Согласно статистике [1] в 2024 году спрос на предоставление услуг в части касающейся проверки (тестирования) информационной безопасности компаний имеет следующие особенности:

– социальная инженерия (проведение учений) – 33 %;
– пентест внешней инфраструктуры – 31 %;

– пентест внутренней инфраструктуры – 20 %;
– проверка безопасности Wi-Fi сетей – 7 %;
– анализ защищенности мобильных приложений – 6 %;
– редтиминг – 3 %.

По результатам моделирования фишинговых атак 13 % сотрудников попались на уловки мошенников. Авторы многих публикаций приводят в своих работах статистику кибератак, представляемую компанией Positive Technologies. Согласно приведенной на рисунке 1 статистики [2] за 3 квартал 2024 года половина успешных атак на организации была осуществлена с использованием злоумышленниками методов социальной инженерии.

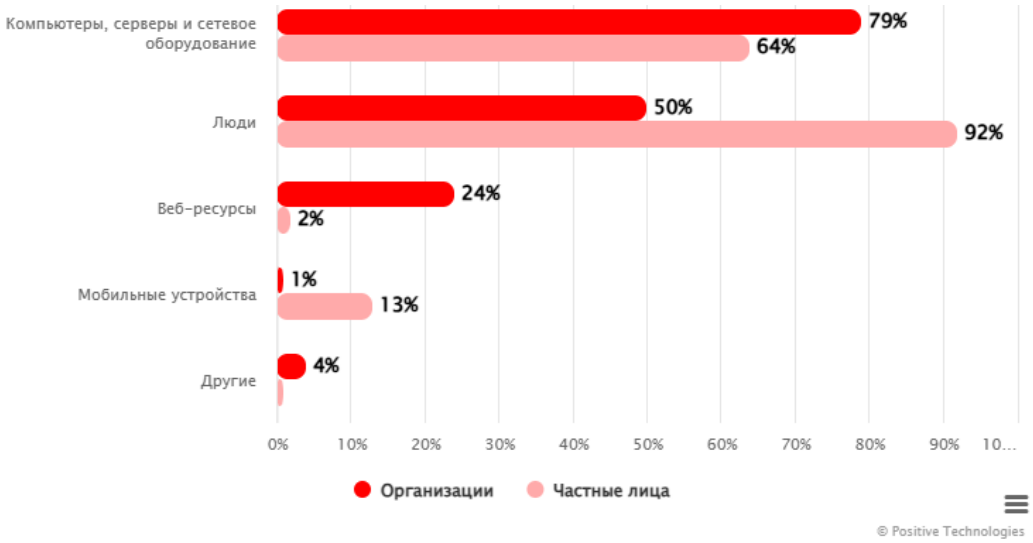


Рис. 1. Объекты атаки и доля успешных атак

Подводя итоги следует отметить актуальность использования мер защиты от атак в связи с качественным и количественным ростом числа осуществленных воздействий злоумышленников в отношении организаций и частных лиц. Для противодействия такого рода угрозам необходимо рассмотреть существующие алгоритмы защиты пользователей и разработать снижающие возможность применения социальной инженерии меры.

В работе Азарова А. А. [3] представлена оценка вероятности получения злоумышленников конфиденциальных сведений при наличии связей между пользователями. Дальнейшим развитием данной работы стал алгоритм оценки уязвимостей пользователей на основе характеристик из профиля в социальной сети «ВКонтакте» [4]. В исследованиях Hussain Aldawood [5] основное внимание сосредоточено на разработке многоуровневых обучающих программ и анализа их применения к различным категориям пользователей. В работе [6] противодействие приемам социальной инженерии заключается в применении политик безопасности для каждого элемента информационной системы. К ним относятся политика сетевой безопасности,

контроля доступа, физической безопасности, классификации информации, шифрования и др.

Вышеуказанные статьи являются частью диссертационных работ соответствующих авторов, тема которых имеет непосредственной отношение к защите от социальной инженерии. В ходе отбора диссертационных работ основным критерием является описание подходов к разработке методов повышения и оценки устойчивости пользователей при моделировании социоинженерных атак.

При разработке алгоритмов противодействия атакам, в дополнение к разработанным моделям элементов атаки [7], выделяются следующие направления: алгоритм уточнения целей атаки, алгоритм заполнения моделей элементов атаки, алгоритм выбора мер защиты, алгоритм оценки риска, алгоритм мониторинга угроз, алгоритм модификации моделей.

В данной статье приводится описание алгоритма уточнения объектов (целей атаки) в рамках целевой атаки в отношении сотрудников компании. В отличие от научной работы [8] представленный алгоритм учитывает степень осведомленности сотрудников в конфиденциальных сведениях и каналы осуществления атаки, учитываемые в разработке вышеупомянутых алгоритмов. На рисунке 2 приводится блок-схема алгоритма уточнения объектов атаки.

1. На первом этапе проводится сбор и обобщение данных о компании, информационных системах, администраторах систем, перечня обрабатываемых сведений, специфики подразделений.

2. Второй этап описывает процесс агрегации списка лиц, допущенных к конфиденциальным сведениям или информационным ресурсам.

3. Этап расчета уровня устойчивости позволяет определить склонность сотрудников к построению доверительных отношений с атакующим. К критериям оценки устойчивости относятся: осведомленность в методах атак, участие в киберучениях, психологическая устойчивость, опыт противодействия мошенникам, критическое мышление, знания в области компьютерных технологий или смежных.

4. Разработка шаблона атакуемого производится на основе совершенных атак. Анализ атак позволяет определить категории целей злоумышленника, а также сделать предположение об имеющихся знаниях.

5. Поиск потенциальных жертв злоумышленника можно проводить путем соответствия сотрудника шаблону ранее совершенных атак.

6. При несоответствии шаблону необходимо провести поиск информации о принадлежности сотрудника организации.

7. При отсутствии информации о сотруднике в открытом доступе проводится моделирование знаний злоумышленника путем ряда опросов.

8. При получении сведений о допущенных лицах, а также их подверженности атакам проводится ранжирование сотрудников по степени угрозы совершения в отношении них социо-инженерной атаки.

9. Для дальнейшего применения алгоритма выбора мер защиты необходимо в алгоритме уточнения целей выделить каналы осуществления атаки.

10. Результатом применения алгоритма уточнения целей является ранжированный список подверженных атаке сотрудников и каналов ее осуществления.

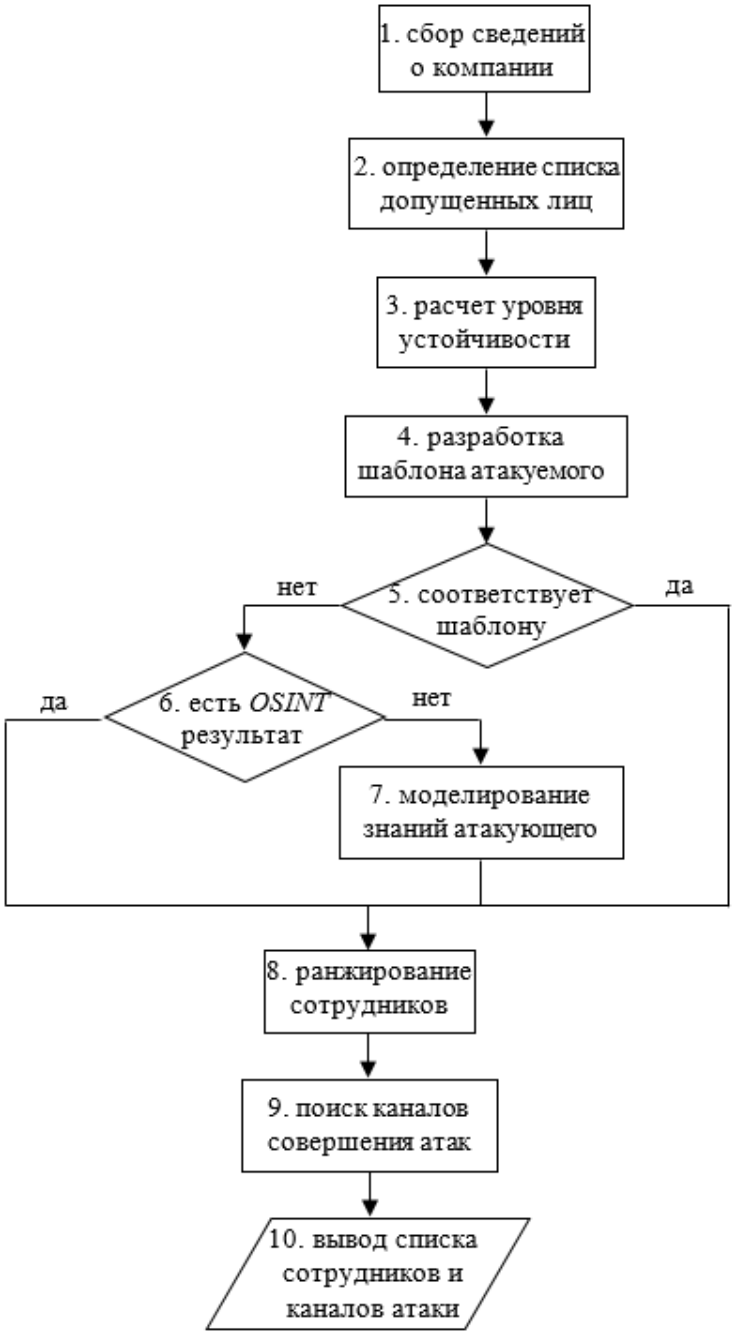


Рис. 2. Алгоритм уточнения целей атаки

Заключение

В данной работе было акцентировано внимание на актуальности проблемы защиты сотрудников от атак с применением методов социальной инженерии, представлен обзор подходов по обеспечению безопасности пользователей и существующие алгоритмы противодействия методам социальной инженерии. Предложенный в статье алгоритм позволяет разрабатывать на его основе комплекс организационных мер по обучению персонала, повышению защищенности используемых каналов связи, запланировать внедрение технических и организационных мер, принимать меры по защите наиболее подверженных атакам сотрудников. Алгоритм уточнения целей может быть адаптирован с минимальными изменениями для решения задач обеспечения безопасности сотрудников различных предприятий, для разработки превентивных мер и прогнозирования атак.

Список используемых источников

1. 13 уязвимостей на компанию: свежая ИБ-статистика от пентестеров. URL: https://habr.com/ru/companies/bastion/articles/876946/ (дата обращения 04.02.2025).

2. Актуальные киберугрозы: III квартал 2024 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/ (дата обращения 04.02.2025).

3. Азаров А. А. Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищенности персонала информационных систем от социо-инженерных атак / А. А. Азаров // Социальный компьютинг: основы, технологии развития, социально-гуманитарные эффекты (ISC-14): материалы Третьей Международной научно-практической конференции, Москва, 18–19 сентября 2014 года. М.: Московский государственный гуманитарный университет им. М. А. Шолохова, 2014. С. 116-120.

4. Подходы к разработке моделей для анализа текстовой информации в профилях социальной сети в целях построения профиля уязвимостей пользователя / Г. И. Багрецов, Н. А. Шиндарев, М. В. Абрамов, Т. В. Тулупьева // Международная конференция по мягким вычислениям и измерениям. 2017. Т. 1. С. 134-137.

5. Aldawood, Hussain & Skinner, Geoff. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 2019-2020.

6. Alharthi, Dalal & Regan, Amelia. (2021). Social Engineering InfoSec Policies. DOI 10.5121/csit.2021.110104.

7. Дайнеко А. С., Кюнер А. П., Чечулин А. А. Социальная инженерия. Модели атакующего и атакуемого // Актуальные проблемы инфотелекоммуникаций в науке и образовании XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 263-266.

8. Huseynov, Farid & Ozdenizci Kose, Busra. (2022). Using Machine Learning Algorithms to Predict Individuals' Tendency to be Victim of Social Engineering Attacks. Information Development. Vol.40. PP. 1-21. DOI 10.1177/02666669221116336.

SOCIAL ENGINEERING. ALGORITHMS OF COUNTERMEASURES AGAINST ATTACKS

Chechulin A., Kyuner A.
Saint Petersburg Federal Research Center of the Russian Academy of Sciences

Rapid development of technologies causes growth of information processing and transmission services, number of users of information systems and methods of information security violation. One of the most common ways of carrying out a cyberattack is the use of social engineering methods. The main disadvantage of existing defense mechanisms against such threats is the lack of a detailed description of the attacker and his methods. This article describes an algorithm designed to fill in models of elements of a social engineering attack based on initial data about an employee and a company taken from open sources, questionnaires, computer systems and information security policy. The proposed algorithm also allows automating the process of describing the model of an information security intruder for developing countermeasures.

***Key words**: social engineering, victim search algorithm, phishing, intruder model*

УДК 004.056.5
ГРНТИ 81.93.29

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ЗАМЕН ОПКОДОВ УСЛОВНЫХ ПЕРЕХОДОВ JVM НА РАБОТОСПОСОБНОСТЬ CLASS-ФАЙЛОВ

П. И. Шариков

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

Язык программирования Java является одним из популярных в мире. Появление новых языков программирования не отменяет того, что все существующие системы продолжают работать, разрабатываться и обновляться на Java. В связи с широкой распространенностью языка, необходимо предпринимать меры по защите прав на разработанное программное обеспечение. Существуют различные методики вложения в class-файлы Java цифровых водяных знаков. Однако в дополнительном исследовании нуждаются операции эквивалентных замен, в частности, как подобные замены могут влиять на работоспособность class-файлов и другие их параметры.

Java, цифровой водяной знак, байт-код, class-файл

Java-компилятор преобразует исходный код в байт-код, который исполняется виртуальной машиной Java (JVM) [1]. Байт-код состоит из инструкций (опкодов), которые соответствуют различным конструкциям языка и типам данных. Например, для работы с типом int используются специфические инструкции, такие как if_icmplt, а для double – dcmpg и iflt. Логические операции в Java можно заменять на эквивалентные с противоположным выражением, при этом важно корректно менять опкоды, чтобы сохранить логику программы и произвести вложение цифрового водяного знака [2].

Выделяются два типа водяных знаков: статические (вложение происходит в исходный код или данные программы) и динамические (генерируются во время исполнения программы). Статические водяные знаки более устойчивы к атакам и изменениям, в отличие от динамических, которые зависят от стабильности работы виртуальной машины Java.

Для создания цифрового водяного знака необходимо анализировать class-файлы java-приложения, чтобы определить, какие из них подходят для вложения, и минимальный объем информации, который возможно вложить [3].

Цифровой водяной знак создается на основе анализа class-файлов и минимального объема информации, который можно вложить, с использованием ключевого слова или криптографической хэш-функции [4]. Для удоб-

ства редактирования опкоды переводятся из HEX в бинарный формат. Таким образом, вложение цифрового водяного знака основывается на анализе опкодов class-файла, возможности вложения, оценке объема вложения и эквивалентных заменах опкодов байт-кода. Также, необходимо, чтобы соблюдались критерии, предъявляемые к цифровому водяному знаку, такие как неизменность функционала class-файла, сохранение работоспособности и скрытое вложение [5]. Ниже, в таблице 1 приведен фрагмент возможных эквивалентных замен опкодов в class-файле.

ТАБЛИЦА 1. Возможные опкоды для вложения ЦВЗ

Мнемоническое представление опкода	Байт-код (HEX)	Байт-код (BINARY)
ifnonnull	0xc7	11000111
if_icmpeq	0x9f	10011111
if_icmpne	0xa0	10100000
if_icmplt	0xa1	10100001
if_icmple	0xa4	10100100
if_icmpgt	0xa3	10100011
if_icmpge	0xa2	10100010
if_acmpeq	0xa5	10100101
if_acmpne	0xa6	10100110

Проведем эксперимент с простейшим class-файлом. Исходный код представлен в листинге 1.

Листинг 1. Исходный код class-файла с условными переходами

```
public class Main {
 public static void main(String[] args) {
 int first = 1;
 int second = 2;
 if (first > second) {
 System.out.println("first > second");
 }
 if (second == 0) {
 System.out.println("second == 0");
 } else {
 System.out.println("second != 0");
 }
 }
}
```

Очевидно, class-файл при исполнении всегда будет выводить в консоль один и тот же результат, а именно, «second != 0» (35 строка) в связи с тем, что значение переменной «first» не больше значения переменной «second», а переменная «second» не равна нулю. После компиляции, байт-код class-файла выглядит так, как продемонстрировано на рис. 1.

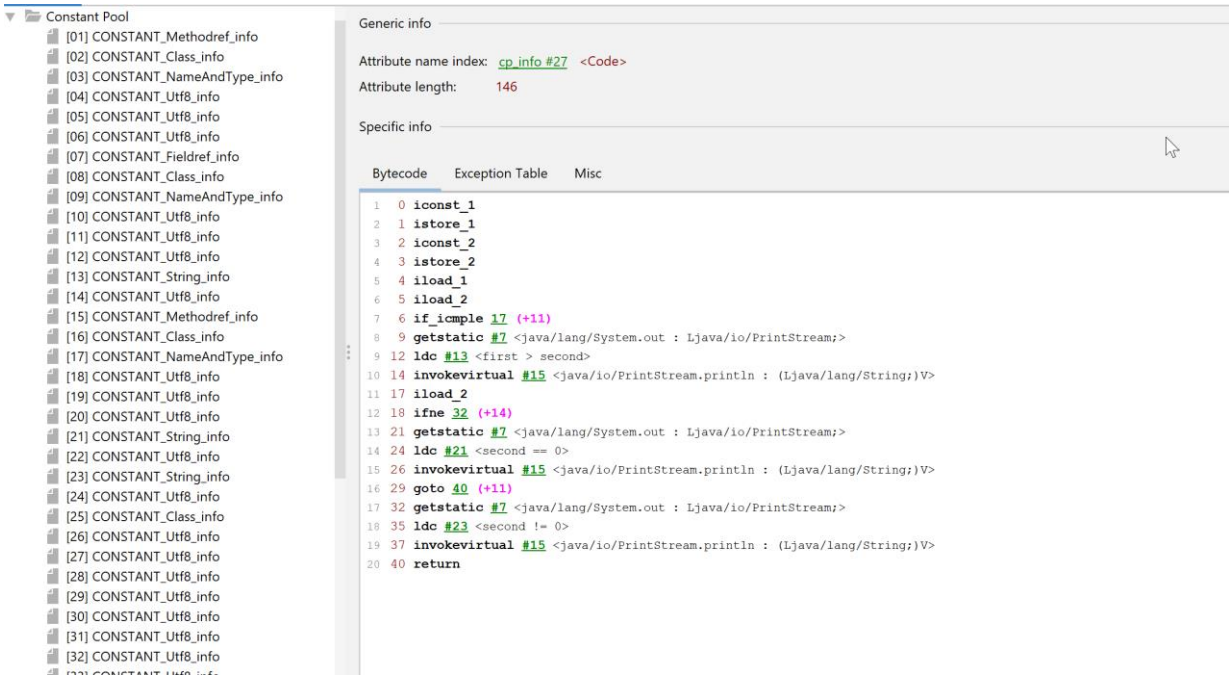


Рис. 1. Байт-код скомпилированного class-файла

Произведем 2 замены опкодов байт-кода отвечающих за операторы условных переходов. Первая замена не будет являться эквивалентной, так как заменяющий опкод из той же группы опкодов, но имеющий другую логику. Вторая замена будет являться эквивалентной, так как опкод имеет другое менмоническое представление, но ту же логику работы. Произведем замену «if_icmple -> if_icmpeq» опкода находящийся на 7 строке и замену «ifne -> ifge» опкода находящегося на 12 строке. После чего сохраним class-файл без перекомпиляции.

Результатом произведенных изменений является изменение логики работы class-файла с сохранением его работоспособности, а также неизменности размера. Рис. 2 демонстрирует неизменность размера class-файла, а рис. 3 демонстрирует сохранение работоспособности class-файла, но изменение логики работы.

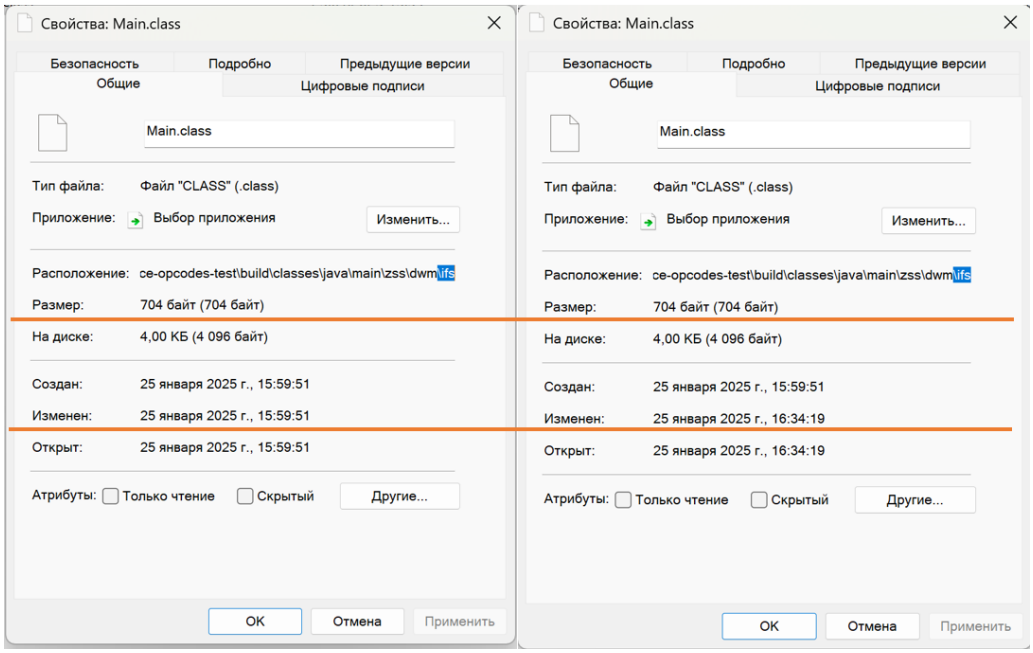


Рис. 2. Неизменность размера class-файла

```
C:\Users\shari>java -classpath C:\PROJECTS\replace-opcodes-test\build\classes\java\main zss.dwm.ifs.Main
first > second
second != 0
```

Рис. 3. Изменение логики работы class-файлов

Как видно из рис. 3, class-файл, переданный на исполнение в JVM, отработал без ошибок, но логика его работы изменилась. Так как был изменен опкод «if_icmple» на другой, но из той же группы опкодов произошло изменение в работе. Исходя из спецификации нового опкода «if_icmpeq» теперь в class-файле производится проверка на то, что значение переменной «first» меньше значения переменной «second». Результат данного сравнения «true», следовательно, выполняется печать сообщения «first > second», потому что данная строка не претерпела никаких изменений.

Таким образом, замена эквивалентных опкодов и простая замена опкодов из той же группы ответственной за операторы условных переходов не влияет на работоспособность class-файла в негативном ключе, при условии изменения веток условия. Также данную операцию можно совершать массово, отслеживая результат с помощью журналов [6].

Также, необходимо отметить, что замена опкодов условных переходов на опкоды из той же группы не повлияло на размер class-файла, что соответствует критерию скрытности цифрового водяного знака [7].

Список используемых источников

1. Arnold M. et al. Adaptive optimization in the Jalapeno JVM //Proceedings of the 15th ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications. 2000. С. 47-65.

2. Шариков П. И. Методика создания и вложения цифрового водяного знака в исполняемые JAVA файлы на основе замен опкодов / П. И. Шариков, А. В. Красов, С. И. Штеренберг // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11, № 3. С. 66-70. EDN YKVPJF.

3. Красов А. В. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполняемые и библиотечные файлы / А. В. Красов, С. И. Штеренберг // Актуальные проблемы инфотелекоммуникаций в науке и образовании. II Международная научно-техническая и научно-методическая конференция, СПб.: СПбГУТ, 2013. С. 847-852. EDN SMCRAZ.

4. An approach for stego-insider detection based on a hybrid nosql database / I. Kotenko, K. Izrailov, A. Krasov, I. Ushakov // Journal of Sensor and Actuator Networks. 2021. Vol. 10. № 2. DOI 10. 3390/jsan10020025. EDN IKOMVS.

5. Хомяков И. Н. Возможность скрытого вложения информации в байт-код Java / И. Н. Хомяков, А. В. Красов // Информационные технологии моделирования и управления. 2014. № 2(86). С. 185-191. EDN RZHODN.

6. Ушаков И. А. Методика обнаружения аномалий в сетевом трафике с использованием IPS на основе Security Onion / И. А. Ушаков, А. В. Красов, Д. Д. у. Мулладжанов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2022. № 1. С. 5-11. DOI 10. 46418/2079-8199_2022_1_1. EDN DSQOHB.

7. An approach for stego-insider detection based on a hybrid nosql database / I. Kotenko, K. Izrailov, A. Krasov, I. Ushakov // Journal of Sensor and Actuator Networks. 2021. Vol. 10. № 2. DOI 10. 3390/jsan10020025. EDN IKOMVS.

8. Шариков П. И., Цветков А. Ю., Сигачева В. В., Сиротина Л. К. Исследование и алгоритм предотвращения эксплуатации уязвимостей библиотеки журналирования Log4j в информационных системах java-приложений // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 4. С. 100-106. DOI 10. 46418/2079-8199_2023_4_19. EDN BULSOH.

INVESTIGATION OF THE IMPACT OF JVM CONDITIONAL JUMP OPCODE REPLACEMENTS ON CLASS FILE PERFORMANCE

Sharikov P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The Java programming language is one of the most popular in the world. The emergence of new programming languages does not change the fact that all existing systems continue to operate, be developed and updated in Java. Due to the widespread use of the language, it is necessary to take measures to protect the rights to the developed software. There are various methods for embedding digital watermarks in Java class files. However, equivalent replacement operations require additional research, in particular, how such replacements can affect the performance of class files and their other parameters.

Key words: *Java, digital watermark, bytecode, class file*

УДК 004.056.53
ГРНТИ 81.93.29

АНАЛИЗ МЕТОДОВ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ

А. А. Шевченко, Н. Д. Кириков, Ю. А. Кудрявцева

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

В условиях постоянной цифровизации и увеличения объемов передаваемой информации защита сетей передачи данных становится критически важной. Необходимость в быстром реагировании на угрозы постоянно возрастает, а количество ложноположительных реагирований в современных SIEM решениях все еще составляет большую долю, что обуславливает необходимость в исследовании существующих и разработке новых методов анализа событий безопасности.

локальные сети, SIEM, информационная безопасность, мониторинг

В системах управления информацией и событиями безопасности (далее SIEM) методы корреляции необходимы для обнаружения и идентификации потенциальных угроз безопасности путем анализа журналов и данных о событиях. Среди наиболее распространенных методов корреляции, использующихся в системах SIEM выделяются следующие:

– одним из самых распространенных подходов является корреляция событий по правилам, при котором заранее задаются условия, по которым система будет искать совпадения в событиях. Например, можно настроить правило, которое отслеживает несколько неудачных попыток входа в систему за короткий промежуток времени. Такие правила часто оформляют в виде текстовых файлов, как в Simple Event Correlator, где каждое условие описано отдельно [1];
– при поиске взаимосвязей между событиями часто используют предельные значения. Число входов, превышающее норму для конкретной среды, спровоцирует оповещение в SIEM системе [2];
– также при корреляции событий важно учитывать временной диапазон. Если сразу после входа в систему пользователь получает доступ к конфиденциальным данным, то система должна оповещать о потенциальной угрозе [3];
– одним из современных подходов является поиск аномалий, который основан на выявлении отклонений от нормального поведения системы или пользователя. Если, скажем, IP-адрес, обычно связанный с рутинными действиями, внезапно начинает проявлять подозрительную активность,

система может это зафиксировать. Такую модель поведения реализует, например, SureLog [4];
– по сущностям (группам) – события и журналы безопасности группируются по пользователям, устройствам или приложениям, что позволяет получить целостное представление о происходящем;
– если при корреляции учитывать взаимосвязи между источниками данных (сетевой трафик, журналы и другие источники данных) то возможно выявить атаки, которые предполагают скрытие присутствия только в одном источнике данных;
– изучая поведение пользователей и приложений, можно обнаружить действия, выходящие за рамки нормы. Такие отклонения могут свидетельствовать о попытке реализации сценария атаки;
– некоторые атаки разворачиваются в несколько этапов – например, от начального доступа до повышения привилегий и получения конфиденциальной информации. Выявление таких последовательностей помогает быстрее распознать угрозу;
– алгоритмы машинного обучения могут прогнозировать угрозы на основе предыдущего опыта. В отличие от правил, они позволяют выявлять нестандартные угрозы, которые не укладываются в заранее заданные шаблоны;
– метод, объединяющий информацию из различных источников, что позволяет точнее оценить контекст угрозы и выявить связь между, казалось бы, разрозненными событиями, называется кросс-корреляцией;
– учет актуальности атаки позволяет уделать внимание не только самому инциденту, но и его значимости: насколько критична система, на которую направлена атака, и какую ценность имеет атакуемая информация;
– учет геолокации при поиске взаимосвязей. Попытка входа в систему из страны, с которой организация не взаимодействует, может быть воспринята как подозрительная активность;
– SIEM может сверяться с базами данных вредоносных IP-адресов, доменов и хэшей файлов. Если входящее событие соответствует одному из таких источников, оно немедленно помечается как потенциально опасное;
– сопоставление с сигнатурами. Метод основан на сравнении текущих событий с уже известными шаблонами вредоносного поведения. Это позволяет оперативно распознать угрозу на основе ранее зафиксированных атак.

В таблице 1 представлено сравнение вышеперечисленных методов корреляции, из которого понятно, что наиболее эффективными из них являются: корреляция на основе групп, корреляция на основе геолокации, корреляция на основе потоков, корреляция на основе потоков информации об угрозах.

ТАБЛИЦА 1. Сравнение методов корреляции

Название	Стоимость	Нагрузка на сеть	Количество ложноположительных срабатываний
Корреляция на основе правил	низкая	низкая	среднее
Корреляция на основе предельных значений	низкая	низкая	высокое
Корреляция по времени	низкая	низкая	высокое
Корреляция на основе аномалий	высокая	средняя	низкое
Корреляция по группам	средняя	низкая	низкое
Корреляция на основе потоков.	низкая	низкая	низкое
Поведенческая корреляция	высокая	высокая	низкое
Корреляция событий на основе обнаруженных последовательностей	высокая	средняя	низкое
Корреляция на основе машинного обучения (ML) и искусственного интеллекта	высокая	высокая	низкое
Кросс-корреляция	средняя	средняя	низкое
Корреляция, основанная на актуальности атак	средняя	низкая	среднее
Корреляция на основе геолокации	низкая	низкая	низкое
Корреляция на основе потоков информации об угрозах	среднее	низкая	низкое
Сопоставление шаблонов	высокая	высокая	низкое

Следует учесть, что каждый из представленных методов корреляции должен использоваться совместно с другими в определенных ситуациях,

определенных участках сети, что позволит SIEM выявлять угрозы безопасности информации, которые могли остаться незамеченными, если бы использовался только один из них.

Список используемых источников

1. Risto Vaarandi, Bernhards Blumbergs and Emin Çalışkan, Simple Event Correlator - Best Practices for Creating Scalable Configurations // URL: https://ieeexplore. ieee.org/document/7108181 (дата обращения: 05.02.2025).

2. Splunk Documentation // URL: https://docs.splunk.com/Documentation/PCI/5.3.2/ Install/CreateNewCorrelationSearches3 2025 (дата обращения: 03.02.2025).

3. Laiba Siddiqui IT Events & Event Correlation: A Complete Guide // URL: https://www.splun k.com/en_us/blog/learn/it-eventcorrelation.html (дата обращения: 01.02.2025).

4. Surelogsiem Federated Anomaly Detection Engine Using Classification // URL: https://surelogsiem.com/surelog-siem-federated-anomaly-detection-engine-using-classification/ (дата обращения: 31.01.2025).

ANALYSIS OF METHODS FOR CORRELATION OF SECURITY EVENTS IN SIEM SYSTEMS

Shevchenko A., Kirikov N., Kudryavtseva J.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

In the context of constant digitalization and increasing volumes of transmitted information, the protection of data transmission networks is becoming critical. The need for a quick response to threats is constantly increasing, and the number of false positive responses in modern SIEM solutions still makes up a large share, which necessitates the study of existing and the development of new methods for analyzing security events.

Key words: *LAN, SIEM, information security, monitoring*

УДК 511+519.719.2
ГРНТИ 27.15+27.45.17

ПРОВЕРКИ ПРОСТОТЫ ЧИСЛА С ПОМОЩЬЮ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

С. Н. Шемякин

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

Большие простые числа являются долговременными параметрами несимметричных шифров, которые используются при вычислении цифровых подписей сообщений, формировании общих ключей для симметричных шифров в сетях передачи данных. Время действия открытых параметров ограничено, поэтому приходится искать новые, не использовавшиеся ранее простые числа.

несимметричные шифры, эллиптические кривые, поиск больших простых чисел

Для проверки простоты числа n достаточно найти его каноническое разложение. Однако при больших $n \approx 2^{256}$ при этом потребуется значительный объем вычислений, так как задача факторизации целых чисел является вычислительно сложной. Известен полиномиальный алгоритм распознавания простоты числа, изложенный в [1, 2, 3, 4]. Его асимптотическая сложность оценивается выражением $O\left((\log_2 n)^{12} pol\ (\log_2 \log_2 n)\right)$. На практике, однако получается, что реальная сложность данного алгоритма настолько высока, что он представляет собой пока только теоретический интерес.

Поэтому для проверки простоты чисел разработаны другие эффективные алгоритмы, называемые тестами простоты. Согласно [5] под тестом простоты «детерминированный или вероятностный алгоритм, позволяющий для любого целого $n > 1$, не находя его канонического разложения, определять, является ли число n простым или составным».

Применяемые в настоящее время алгоритмы распознавания простоты числа n состоят из трех частей или этапов проверки.

Этап 1. Отсеивание испытываемого числа при наличии у него малых простых делителей. Заготавливается таблица первых простых чисел и производится деление числа n на числа из этой таблицы. При получении целого результата деления число n отсеивается, как не выдержавшее испытаний первого этапа, выбирается для проверки следующее число. На данном этапе

возможно использование признаков делимости, их применение имеет незначительную вычислительную сложность [6].

Будем полагать число n нечетным и не делящимся на 5. Тогда имеет место

Теорема 1. Пусть n записано в десятичной системе исчисления, для пробного делителя m выполняется условие $p_m(10) = k$ или $10^k = 1 \pmod m$. Число n делится на число m без остатка тогда и только когда на m делится сумма чисел, которые получаются при разбиении справа налево десятичной записи числа n на отрезки по k цифр в каждом отрезке.

Доказательство элементарно.

Примеры

1. Признак деления на 7. Длина отрезка находится из уравнения $10^k = 1 \pmod 7$, $k = 6$. Число n делится или не делится на 7, смотря по тому, делится или нет на 7 сумма чисел, получающихся при разбиении записи n на отрезки по 6 десятичных цифр в каждом. В то же время при записи числа n в двоичном виде получаем $k = 3$, причем отрезки со значениями (000) и (111) можно исключить.

2. Признак деления на 11. Длина отрезка $k = 2$ для десятичной записи. Число n делится на 11тогда и только тогда, когда на 11 делится сумма чисел в отрезках по две цифры.

Этап 2. Отсеивание испытываемого числа после выявлении у него свойства «число n - составное». При этом рекомендуется использование вероятностного теста Миллера-Рабина [2, 3, 4], который при одном испытании распознает свойство «составное» (если число n составное) с вероятностью 0,75. Трудоемкость данного теста при проведении одного испытания оценивается величиной $O(\log^3 n)$, количество испытаний обычно 1000 и более.

Этап 3. После завершения второго этапа проверки наличия свойства простоты можно сказать, что число n является простым с высокой вероятностью. Содержанием этапа 3 проверки является распознавание наличия некоторого достаточного признака простоты. При этом возможно использование вероятностного теста [7], который использует свойства эллиптических кривых.

Ограничимся только теми сведениями (без доказательства) об эллиптических кривых над конечными полями, которые необходимы для понимания алгоритма проверки простоты целых чисел. Изложение в основном следует [2].

Определение 1. Алгебраической кривой порядка n над полем K называется множество $E_K = \{(x, y) \in K^{(2)} \mid F(x, y) = 0\}$, где $F(x, y) \in K[x, y]$ – многочлен степени n над полем K.

Элементы множества E_K называются точками кривой.

Определение 2. Кривая E_K называется гладкой, если все ее точки являются простыми.

Пусть $GF(p)$ поле из p элементов. Рассмотрим многочлен от двух переменных $F(x, y)$ вида

$$F(x, y) = y^2 - x^3 - ax - b = 0. \quad (1)$$

Лемма 1. Пусть $GF(p)$ - конечное поле из p элементов, $a, b \in GF(p)$. Тогда многочлен $f(x) = x^3 + ax + b$ над этим полем не имеет кратных корней в том и только в том случае, когда выполнено условие $4a^3 + 27b^2 \neq 0$.

Определение 3. Эллиптической кривой называется множество $E_p(a, b)$, состоящее из всех точек гладкой алгебраической кривой, заданной многочленом $F(x, y)$ вида (1), и еще одного элемента O, называемого «точка в бесконечности».

Оказывается, что точки P эллиптической кривой образуют конечную аддитивную абелеву группу, нулем в этой группе является точка O. Более того, они образуют групповое кольцо над кольцом целых чисел. Временная сложность сложения двух точек $P_1 + P_2$ эллиптической кривой оценивается как $O(\log^2 p)$ двоичных операций. Для вычисления произведения mP точки P на число m можно воспользоваться бинарным алгоритмом или алгоритмом Кнута. При этом потребуется $O(\log_2 m)$ сложений точек.

Одним из основных вопросов при описании свойств групп точек эллиптических кривых является вычисление порядка этих групп.

Теорема 2. (Хассе) Для порядка $M = |E_p|$ группы точек произвольной эллиптической кривой E_p выполняется соотношение $|M - (p + 1)| \leq 2\sqrt{p}$.

Приведем два частных случая, в которых порядок группы точек эллиптической кривой находятся легко.

Теорема 3. Пусть $p > 3$ простое число, $p \equiv 3 \pmod 4$, $a \in GF(p)^*$.
Тогда $M = |E_p(a, 0)| = p + 1$.

Теорема 4. Пусть $p > 3$ простое число, $p \equiv 2 \pmod 3$, $b \in GF(p)^*$.
Тогда $M = |E_p(0, b)| = p + 1$.

Для произвольной эллиптической кривой порядок M группы ее точек можно найти с помощью полиномиальных алгоритмов Шуфа с временной сложностью $O(\log p)^8$ или SEA с временной сложностью $O(\log p)^6$ [3, 8].

Далее будем полагать, что проверяемое на простоту число n прошло первый и второй этапы проверки и для него выполняются условия теоремы 3 или 4. В этом случае порядок группы точек эллиптической кривой будет равен $n + 1$ (если n – простое число) и можно будет исключить использование алгоритма SEA.

Итак, будем считать, что нам дано целое псевдопростое число n, и настолько большое, что получение его канонического разложения с помощью алгоритмов факторизации невозможно. Тесты проверки простоты целых чисел, связанные с эллиптическими кривыми, основаны на следующей теореме, представляющей собой аналог теоремы Поклингтона.

Теорема 5. Пусть n – нечетное число, $(n, 6) = 1$ (условие заведомо выполняется после этапа 1), $a, b \in \mathbb{Z}_n$, $(4a^3 + 27b^2, n) = 1$, $E_n(a, b)$ – эллиптическая конфигурация по модулю n (то есть число n возможно составное), нашлась точка P на данной конфигурации, порядок группы будет (если n - простое) $M = m = n + 1$, существует такой простой делитель q числа m, что

$$q > \left(\sqrt[4]{n} + 1\right)^2,$$

и определены точки $mP = O$, $(m/q)P \neq O$. Тогда n – простое число.

Из последней теоремы можно сделать следующий вывод. Если при заданном n нашлись m, его делитель $q > \left(\sqrt[4]{n} + 1\right)^2$, и точка $P \in E_n(a, b)$, для которых $mP = O$ и $(m/q)P \neq O$, то для доказательства простоты числа n надо лишь проверить простоту числа q.

Таким образом задача проверки простоты большого числа n сводится к задаче проверки простоты меньшего числа q.

Результатом работы вероятностного теста простоты [2, 7] является последовательность целых чисел

$$n = n_0 > n_1 > \ldots > n_t,$$

причем $n_{i+1} < 0{,}5n_i$, тогда длина последовательности не превышает $\log n$. Последний член последовательности имеет уже относительно небольшую величину, и его простота устанавливается напрямую, например, методом решета Эратосфена.

Оценка трудоемкости алгоритма. При условии выполнимости ряда правдоподобных предположений о распределении простых чисел средняя временная сложность теста оценивается величиной $O(\log^{12} n)$. При этом основные временные затраты происходят при выполнении алгоритма Шуфа.

Список используемых источников

1. Agrawal M., Kayal N., Saxena N. PRIMES is in P. Preprint, August 2002.

2. Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии: Учебное пособие. СПб.: Издательство «Лань», 2011. 400 с. (Учебники для вузов. Специальная литература).

3. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. 2е изд. М.: МЦНМО, 2007.

4. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. М.: МЦНМО, 2002. 104 с.

5. Дискретная математика: энцикл. / гл. ред. В. Я. Козлов. М.: Большая российская энциклопедия, 2004. 382 с.

6. Бухштаб А. А. Теория чисел: учебное пособие для вузов / А. А. Бухштаб. 8-е изд., стер. Санкт-Петербург: Лань, 2024. 384 с.

7. Goldwasser, S. Almost all prime can be quickly certified / S. Goldwasser, J. Killian // Proc. 18th Annual ACM Symp. on Theory of Computing. 1986. PP. 316–329.

8. Ростовцев А. Г. Эллиптические кривые в криптографии. Теория и вычислительные алгоритмы. СПб.: НПО «Профессионал», 2010. 364 с.

CHECKING THE PRIMALITY OF A NUMBER USING ELLIPTIC CURVES

Shemyakin S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Large prime numbers are long-term parameters of asymmetric ciphers, which are used in calculating digital signatures of messages and forming common keys for symmetric ciphers in data transmission networks. The validity period of the open parameters is limited, so we have to look for new, previously unused primes.

Key words: *Asymmetric ciphers, elliptic curves, and the search for large primes*

УДК 004.056
ГРНТИ 81.93.29

ГИПОТЕЗА О ДОСТИЖЕНИИ ТЕХНОЛОГИЧЕСКОЙ СИНГУЛЯРНОСТИ ЧЕРЕЗ КВАЗИБИОЛОГИЧЕСКУЮ ПАРАДИГМУ ОПИСАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ IDS

С. И. Штеренберг

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

В общем стремлении достигнуть параметра наступления квазибиологического консенсуса для ИТ-решения в рамках Индустрии 5.0 принято решение о выдвижении гипотезы о достижении технологической сингулярности через квазибиологическую парадигму описания интеллектуальных IDS (пер. с англ. абрв. – система обнаружения вторжений), в рамках которой устанавливается особый «цифровой ДНК» для систем защиты информации (далее – СЗИ) в 2-фазных режимах работы пакетно-нейросетевых программ (далее – ПНП).

технологическая сингулярность, интеллектуальные IDS, цифровой ДНК, Индустрии 5.0, квазибиологическая парадигма

При достижении технологической сингулярности через квазибиологическую парадигму описания интеллектуальных IDS предполагает, что развитие искусственного интеллекта и интеграция его с биологическими системами могут привести к созданию нового типа интеллектуальных систем, способных к самообучению, адаптации и эволюции на уровне, превышающем возможности современных технологий [1].

В основе этой гипотезы лежит идея о том, что объединение принципов работы биологических систем с технологиями искусственного интеллекта может создать новый класс интеллектуальных систем, способных к самоорганизации, самовосстановлению и саморазвитию. Технологическая сингулярность в данном контексте может рассматриваться как момент, когда интеллектуальные IDS достигнут уровня развития, при котором они смогут самостоятельно создавать новые технологии и алгоритмы, превосходящие существующие [2]. Это может привести к экспоненциальному росту производительности и возможностей интеллектуальных систем, что, в свою очередь, может ускорить процесс достижения технологической сингулярности.

Такие системы будут обладать способностью к обучению на основе опыта, адаптации к изменяющимся условиям и эволюции своих алгоритмов и структур для достижения более высоких уровней эффективности и производительности. Одним из ключевых аспектов этой гипотезы является использование квазибиологических подходов для описания и моделирования

интеллектуальных IDS. Квазибиологические подходы предполагают использование аналогий и метафор из биологии для понимания и описания сложных систем, включая искусственный интеллект. Это включает в себя применение понятий, таких как эволюция, адаптация, мутация и естественный отбор, для создания интеллектуальных систем, способных к самосовершенствованию и развитию [3].

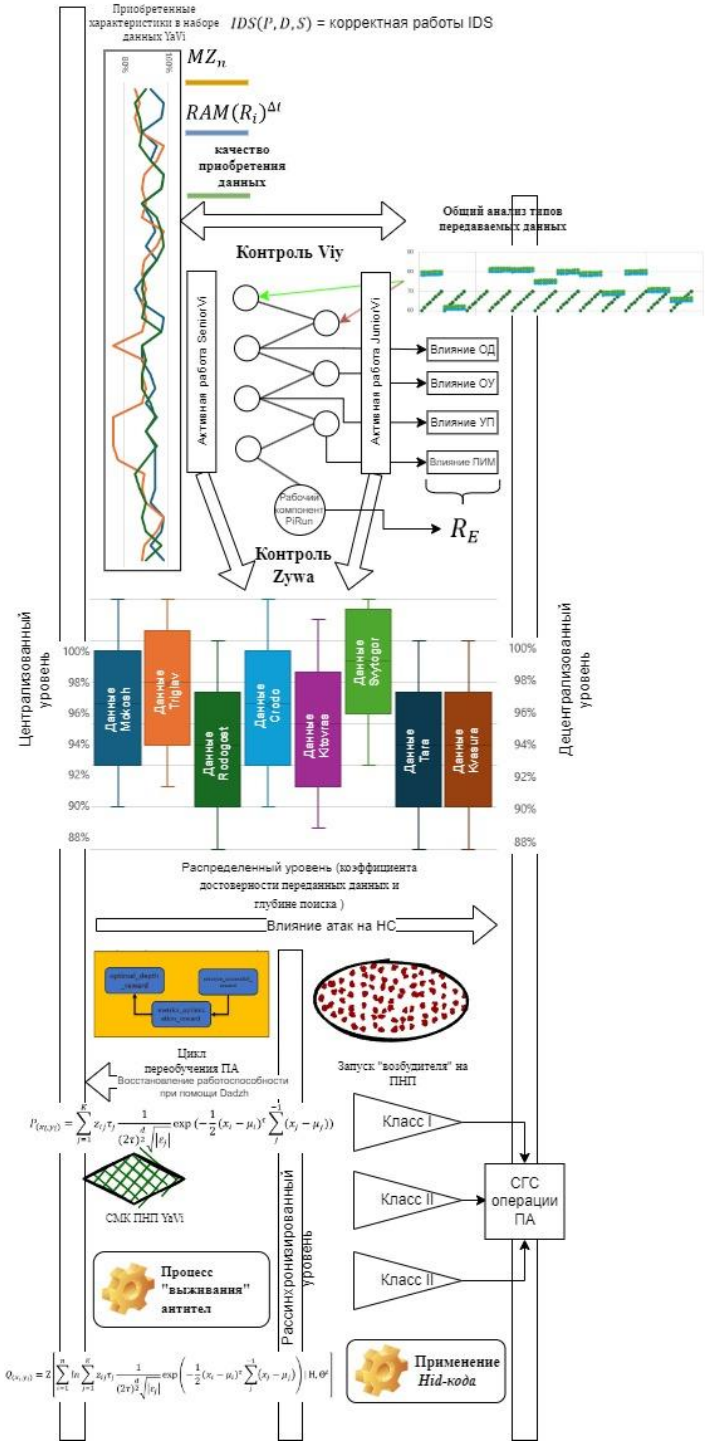


Рис. 1. Общие параметры активного состояния поэтапного перехода в разных 2-фазных режимах работы ПНП в РИС («Цифровой ДНК»)

В стремлении достигнуть параметра квазибиологического консенсуса [3,5] для ИТ-решения в рамках Индустрии 5.0 принято решение о выдвижении гипотезы о достижении технологической сингулярности через квазибиологическую парадигму описания интеллектуальных IDS, в рамках которой устанавливается особый «цифровой ДНК» для СЗИ в 2-фазных режимах работы ПНП (см. рис 1). При сохранении активного состояния децентрализованной ПНП в IDS утверждает [5,6], что если система удовлетворяет условиям согласованности данных (consistency), доступности (availability) и устойчивости к фрагментации (partition tolerance), то существует возможность поддерживать активное состояние программы в условиях асинхронной передачи данных и отсутствия глобальных часов.

Доказательство этой теоремы основывается на принципах работы распределенных систем и особенностях ПНП. Согласованность (взаимозаменяемость) данных гарантирует, что все узлы системы имеют актуальные и непротиворечивые данные, что критически важно для корректной работы нейросетевых моделей [4]. Доступность обеспечивает возможность получения ответов от системы даже в условиях частичной недоступности некоторых узлов, что позволяет поддерживать активность программы. Устойчивость к фрагментации обеспечивает способность системы функционировать даже при разделении на изолированные секции, что особенно важно для децентрализованных систем (рис. 2).

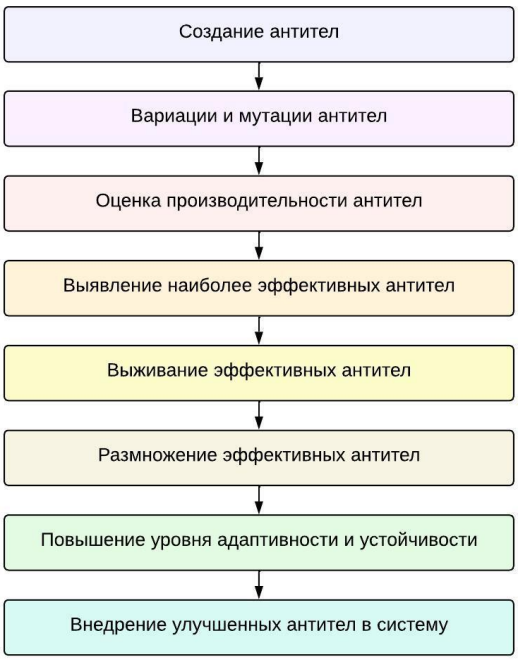


Рис. 2. Процесс "выживания" антител

$$loss_{rec} = -\log R\left(r + \sum_{i=1}^{N} x_i\right) - r\log P_1(y) + \log P_2(z) - \sum_{i=1}^{N} x_i \log P(q) \quad (1)$$

$$\begin{cases} var(\{X_i, \dots, X_n\}) = \sum_{i=1}^{n} \frac{X_j}{X}\left(\frac{1}{X_j}\sum\nolimits_{x \epsilon X_j} x^2 - \bar{x}_j^2\right) \\ var(\{Y_i, \dots, Y_n\}) = \sum_{i=1}^{n} \frac{Y_j}{Y}\left(\frac{1}{Y_j}\sum\nolimits_{y \epsilon Y_j} y^2 - y_j^2\right) \\ \dots \\ var(\{Z_i, \dots, Z_n\}) = \sum_{i=1}^{n} \frac{Z_j}{Z}\left(\frac{1}{Z_j}\sum\nolimits_{z \epsilon Z_j} z^2 - \bar{z}_j^2\right) \end{cases} \quad (2)$$

$$CL(w, t) = \prod_{i} P(x_i|y_i)^t \quad (3)$$

$$\delta_{\text{изм}} = \mu^{\oplus} - \mu^{\ominus} = k_s\left(\frac{1}{P}\sum\nolimits_{x_i, y_i, z_i{}^{\oplus} \in P} x_i, y_i, z_i{}^{\oplus} - \frac{1}{N}\sum\nolimits_{x_i, y_i, z_i{}^{\ominus} \in N} x_i, y_i, z_i{}^{\ominus}\right) \quad (4)$$

$$\delta = \sum_{i=1}^{n} x_i, y_i, z_i \quad (5)$$

где формула (1) – оценка коэффициента потерь для программных агентов (далее – ПА), формула (2) – общая вариативность изменений при адаптации ПА в разных режимах, формула (3) – условное правдоподобие в структурном восстановлении IDS, формула (4) – измененного перцетрона при известном весе перцетрона по формуле (5).

СЗИ непрерывно адаптируется на основе накопленной информации, улучшая свою производительность и устойчивость к новым угрозам. Этот процесс включает постоянное обновление алгоритмов и стратегий защиты на основе обратной связи от успешно обработанных угроз и анализа изменяющейся «угрозовой ситуации» [6].

Обучение и адаптация являются фундаментальными компонентами (рис. 3) обеспечения постоянной эволюции и усовершенствования защитных возможностей, что делает систему способной эффективно реагировать на новые и развивающиеся угрозы [7].



Рис. 3. Процесс обучения и адаптации СЗИ

Вывод

Разработка квазибиологически инспирированных алгоритмов и технологий, которые будут имитировать работу квазибиологических систем, таких как иммунная система или нейронные сети, дополнительно снабжает эти системы обучаемыми и самообучаемыми модулями, способными к адаптации к новым угрозам и изменениям в окружающей среде. Эволюционные селективные алгоритмы усиливают процесс обнаружения и адаптации к новым видам угроз. Одной из концепций развития эволюционных селективных алгоритмов в интеллектуальной IDS является использование генетического программирования для поиска оптимальных параметров и структур обнаружения угроз. Это позволяет IDS обучаться на основе имеющихся данных и автоматически адаптироваться к новым угрозам, что повышает ее эффективность и точность. Использование многопопуляционных способов эволюционной оптимизации (клональная селекция, генетические алгоритмы и т.д.) для создания различных групп алгоритмов обнаружения атак на ПА, каждая из которых, возможно, специализируется на определенном типе угроз, повышает общую надежность системы и снижает вероятность ложных срабатываний. Свойства квазибиологической парадигмы, такие как адаптивность, самоорганизация и эмерджентное поведение, могут быть успешно сохранены и применены при разработке интеллектуальных IDS в рамках концепции Индустрия 5.0.

Список используемых источников

1. Шелухин О. И., Шариков А. Ю. Имитация поведения компьютерной системы с помощью искусственных нейронных сетей // T-Comm: Телекоммуникации и транспорт. 2021. Том 15. № 5. С. 29-37.

2. Шаго Ф. Н. Методика оптимизации планирования аудита системы менеджмента информационной безопасности / Ф. Н. Шаго, И. А. Зикратов // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2(90). С. 111-117.

3. Майоров А. В. Модель представления Больших данных о компьютерных атаках в формате nosql / А. В. Майоров, А. В. Красов, И. А. Ушаков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47-54.

4. Александров А. Ю., Платонов А. В., Старков В. Н., Степенко Н. А. Математическое моделирование и исследование устойчивости биологических сообществ: Учебное пособие. 2е изд., испр. и доп. СПб.: Издательство «Лань», 2016. 272 с.

5. Доктырбай Ш. А. Определение критериев методики управления качеством интеллектуальных интегрированных биометрических систем / Ш. А. Доктырбай, Л. К. Птицына // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 622-626.

6. Шичкина Ю. А. Модель распознавания информационных угроз с использованием рекуррентной нейронной сети / Ю. А. Шичкина, Р. Р. Фаткиева, И. А. Пузако // III Международная конференция по нейронным сетям и нейротехнологиям (NEURONT'2022): сборник докладов, Санкт-Петербург, 16 июня 2022 года. Санкт-Петербург: Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина), 2022. С. 53-57.

7. Козлов С. В. Процессные аспекты обеспечения интероперабельности в автоматизированных системах, создаваемых на основе информационных и когнитивных технологий / С. В. Козлов // Безопасные информационные технологии : Сборник трудов Двенадцатой международной научно-технической конференции, Москва, 01–02 ноября 2023 года. Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), 2023. С. 80-88.

THE HYPOTHESIS OF ACHIEVING A TECHNOLOGICAL SINGULARITY THROUGH A QUASI-BIOLOGICAL PARADIGM OF DESCRIBING INTELLIGENT IDS

Shterenberg S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In a general effort to achieve a quasi-biological consensus for an IT solution within Industry 5.0, it was decided to hypothesize the achievement of a technological singularity through a quasi-biological paradigm for describing intelligent IDS, which establishes a special "digital DNA" for information security systems in two-phase modes of operation of batch neural network programs.

Key words: *Technological singularity, intelligent IDS, digital DNA, Industry 5.0, quasi-biological paradigm.*

СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

УДК 621.373.9
ГРНТИ 49.33

РЕГУЛИРУЕМЫЙ ЦИФРОВОЙ ГЕНЕРАТОР ШУМА СРЕДНЕ-ВЫСОКОЧАСТОТНОГО ДИАПАЗОНА

А. И. Бояринцев, А. А. Повзнер, К. О. Хохлов, И. Д. Манько

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина

Генераторы шума применяются в радиотехнике, устройствах тестирования и проверки оборудования на электромагнитную совместимость, устойчивость), а также в области защиты от каналов утечки информации. В данной работе проводится сравнительный анализ существующих на рынке генераторов шума и представляется собственная разработка. На обсуждение выносится вопрос целесообразности дальнейшего прототипирования и испытания устройства.

генератор шума, частотный спектр, спектральная плотность сигнала

Генераторы шума *(ГШ)* представляют собой устройства генерации случайных электрических сигналов с различными частотами, амплитудами и фазами для имитации реальных шумовых процессов. В настоящее время зарубежными и российскими фирмами [1] производятся генераторы, отвечающие различным требованиям заказчика. Следует отметить, что наибольшим спросом на современном рынке обладают генераторы, предназначенные для защиты речевых каналов информации от утечек, образующие маскирующие помехи. Генераторы шума можно классифицировать по следующим пунктам:

– схемотехническое исполнение и принцип формирования шумового сигнала. На данный момент существует два основных способа формирования шумового сигнала, которые подразделяются на различные варианты их

схемотехнического исполнения – формирователи аналоговых (непрерывных) и цифровых (дискретных) случайных сигналов;
– свойства шумового сигнала, формируемого генератором. Генераторы можно классифицировать по поведению спектральной плотности шума (белый шум, розовый шум и прочие) [2]. Наиболее важным качеством генератора шума является распределение его спектральной плотности, способность к генерации устойчивого сигнала на максимально широком диапазоне частот.

Согласно сравнительному анализу, проведенному в [3] на основании критерия уровня качества генераторов шума для защиты от утечки информации, было показано, что, по оценке 13 наиболее важных параметров генераторов шума, включая технические, массогабаритные, эксплуатационные и ценовые, он находится в интервале от нуля до единицы. При этом лишь три генератора из 23 рассмотренных в работе [3] превышают значение 0,6, и лишь один – 0,7. Немалую роль в образовании нормированного единичного показателя играла цена – согласно прейскуранта популярного магазина гражданской аппаратуры для информационной защиты цена на такие приборы варьируется от 19 тысяч до нескольких миллионов рублей [4]. Очевидно, что задача генерации белого шума трудоемка:
– наличие энергопотерь. Даже высокая приложенная мощность будет многократно уменьшена при рассмотрении амплитуды сигнала на узком наборе частот;
– аналоговое (непрерывное) формирование постоянного уровня сигнала предполагает наличие зависимости коэффициента полезного действия генератора шума от коэффициента антенны, предполагающего как усиление, так и ослабление полезного сигнала на определенных частотных интервалах.

Авторами предлагается к рассмотрению структурная схема устройства-генератора шума, предназначенного для формирования как регулируемых цифровых интервалов сигналов, так и нерегулируемого аналогового сигнала – белого шума. Основополагающей идеей работы устройства, как источника помех, является выдача в эфир пачек импульсов с регулируемыми интервалами и длительностями, но со случайными периодами повторения.

Принцип работы устройства. Принципиальная схема

Устройство, структурная схема которого показана на рисунке 1, предназначено для генерации маломощного сигнала для последующего усиле-

ния с регулируемой длительностью и частотой повторения. Основными функциональными блоками являются опорный генератор (прецизионный кварцевый тактовый генератор), а также генератор белого шума, построенный на базе шумовых характеристик стабилитрона с последующей схемой многократного усиления на высокочастотных транзисторах. Операционные сигналы, используемые в устройстве для формирования выходного сигнала ограничены амплитудой 4,5 В. Максимальная частота работы опорного генератора f была ограничена набором компонент, используемых для создания опытного образца, и составляет 125 МГц. Полоса генерации генератора белого шума ограничена верхней граничной частотой транзисторной сборки усилителя и составляет порядка 200 МГц.

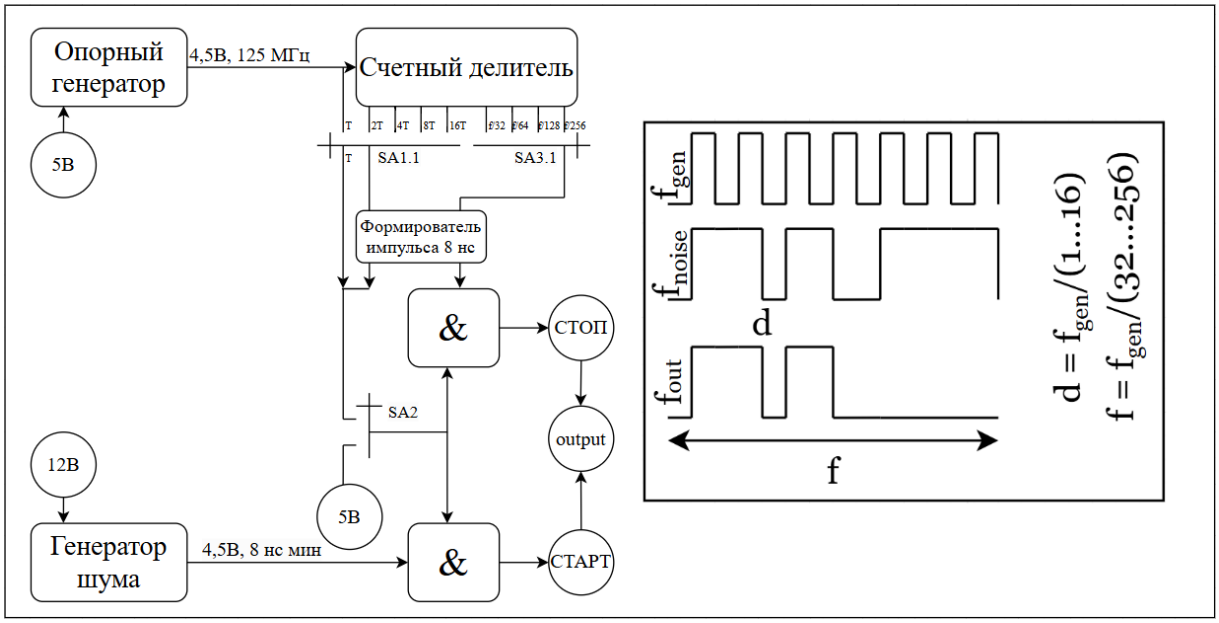


Рис. 1. Структурная схема разрабатываемого устройства. Вставка на рисунке (справа) демонстрирует выходные сигналы опорного генератора (fgen), цифрового генератора шума (fnoise), а также выходного сигнала устройства (fout)

Введем уточнения, что отдельные блоки устройства могут быть использованы для генерации сигналов как регулируемой частоты (тактовый генератор + делитель частоты), так и аналогового белого шума, а также цифрового шума (амплитуда импульсов ГШ без формирователя – 1,5-2В, ГШ с формирователем – 4,5В).

Однако, основная идея работы устройства заключается в генерации сигналов с неравномерным распределением амплитуд спектральных составляющих сигнала. Спектральный анализ прямоугольного сигнала дает распределение вида (sin x)/x с максимумом амплитуды первой гармоники на частоте повторения сигнала.

$$F(\omega) = 2A\,sin\left(\frac{\omega\tau}{2}\right)/\omega, \quad (1)$$

где $\omega = 2\pi f$, τ – длительность импульса, f – опорная частота

При этом сам импульс представляет собой последовательность импульсов, со спектральной составляющей, выраженной через интегрирование равновероятностных событий в интервале $\tau > x > (\tau - \tau_n)$, описываемых распределением Пуассона:

$$F(\omega) = \sum_{\tau_n} 2A/\omega \int sin\left(\frac{\omega x}{2}\right) dx, \quad (2)$$

где наличие или отсутствие x в интервале описывается вероятностным распределением Пуассона:

$$x = exp\,(-p(x))p(x), \quad (3)$$

При этом, если период повторения сигнала T является постоянным, сам выходной сигнал – последовательность импульсов неравных длительностей. Можно задать случайное распределение амплитуд гармоник, кратных частоте повторения сигнала. Это позволит равномерно расширить спектральную полосу сигнала и увеличить энергоэффективность в сравнении с аналоговым генератором шума [5] (рис. 2).

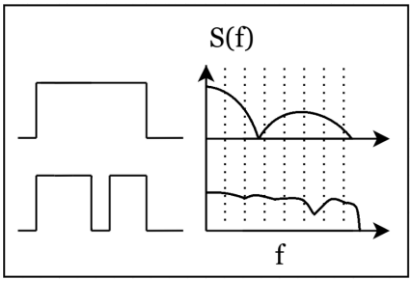


Рис. 2. Зависимость спектральной плотности сигнала от формы сигнала

Таким образом, сигнал, получаемый в результате слияния сигналов опорного генератора и цифрового генератора шума, имеет ряд преимуществ:

– генерация сигналов случайного дискретного частотного спектра в широкой регулируемой частотной полосе;
– высокая термостабильность и помехоустойчивость за счет использования цифровых компонент;
– низкое энергопотребление и возможность простого согласования с последующими схемами усилителей по мощности.

Наряду с преимуществами имеют место и некоторые недостатки, которые представляется возможным устранить при следующих итерациях разработки прибора:

– относительно низкая частота генерации, ограниченная параметрами цифровых компонент схемы и опорного генератора;
– дискретность регулировки выходного сигнала по частоте.

При устремлении параметра $p(x)$ в формуле (3) к значению 0,5 возможно рассмотреть использование устройства для моделирования стохастических флуктуаций в конденсированных средах.

Заключение

Разрабатываемый генератор шума может быть использован, благодаря описанному выше свойству выходного, сигнала в антенной технике и устройствах подавления нежелательных сигналов широкого частотного спектра, а также в устройствах наведения помех, используемых в радиолокации и генераторах сигнала на аппаратуре проведения испытаний по проверке на электромагнитную совместимость, устойчивость (ЭМС). Ввиду простоты изготовления и дешевизны компонентов такие устройства могут быть полезными для защиты каналов связи от утечки информации как в проводные линии, так и на в области радиосигнала. Однако вопрос целесообразности дальнейшего модернизирования и разработки прибора наталкивается на необходимость обсуждения принципиальной схемы, а также проведению испытаний по измерению частотных характеристик опытного образца.

Список используемых источников

1. Винокуров С. А., Кочемасов В. Н., Сафин А. Р. Генераторы шума (обзор) // Известия вузов России. Радиоэлектроника. 2023. Т. 26. № 4. С. 6–32.

2. Гребенюк К. А Основные виды шумов в электронных полупроводниковых приборах // Известия Саратовского университета 2012. Т. 12. № 1. С. 63–65.

3. Martyniuk G. et al. Analysis of the quality of noise generators // Bulletin of Akbai KAZNPU. Series of physical and mathematical sciences. 2023. Vol. 84. № 4.

4. Генераторы шума. Каталог // Detector Systems URL: https://detsys.ru/catalog/prostranstvennoe_zashumlenie/?srsltid=AfmBOorv85FQWfGEXSVaITiai-3U195P31Q5iydb_f52SbOVnjlWJ0Rb (дата обращения: 15.01.2025).

5. Соловьева Е. Б., Иншаков Ю. М. Исследование разрывных периодических сигналов с использованием измерительного комплекса LabWIEV // Качество, инновации, образование. 2020. № 5(169). С. 72-79.

ADJUSTABLE DIGITAL NOISE GENERATOR OF THE MEDIUM-HIGH FREQUENCY RANGE

Boyarintsev A., Povzner A., Khokhlov K., Manko I.
Ural Federal University named after the first President of Russia B. N. Yeltsin

Noise generators are used in radio engineering, devices for testing and verifying equipment for electromagnetic compatibility, stability, as well as in the field of protection against information leakage channels. This paper provides a comparative analysis of existing noise generators on the market and presents its own development. The issue of the expediency of further prototyping and testing of the device is being discussed.

Key words: *noise generator, frequency spectrum, spectral density of the signal*

УДК 621.391
ГРНТИ 49.01.85

УПРАВЛЕНИЕ НАДЕЖНОСТЬЮ ФУНКЦИОНИРОВАНИЯ ТЕХНИКИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ В ИНТЕРЕСАХ ВНЕДРЕНИЯ СТРАТЕГИЙ ПРОГНОЗНОГО ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

П. А. Будко[1], А. А. Южакова[2]

[1]ПАО «Интелтех»
[2]Военная академия связи им. Маршала Советского Союза С. М. Буденного

Сбои и другие нарушения нормального функционирования техники связи специального назначения ведут к перебоям или полной блокировке работы всей системы связи, поэтому управление надежностью ее функционирования на всех этапах жизненного цикла и переход к стратегии прогнозного технического обслуживания являются крайне важными задачами.

надежность, техническое обслуживание, техника связи специального назначения

Переход от существующей на сегодня в войсках планово-предупредительной стратегии технического обслуживания и ремонта техники связи специального назначения к другой стратегии – по ее фактическому техническому состоянию позволяет в наибольшей степени использовать ресурс каждого отдельного средства связи, что достигается уменьшением числа преждевременных вмешательств в его работу [1].

При реализации данной стратегии процедуры технического обслуживания и ремонта осуществляются в зависимости от проводимых мероприятий по техническому диагностированию объекта контроля и прогнозу его технического состояния. Фактически данная стратегия устраняет недостатки планово-предупредительной стратегии, снижая число необоснованного ремонтного вмешательства для не выработавшего эксплуатационный ресурс изделия. Ее основным преимуществом является полное расходование ресурса и предсказуемость наступления отказа благодаря проведению циклов мониторинга технического состояния объектов контроля. В то же время к недостаткам можно отнести затраты на проведение циклов мониторинга технического состояния и невозможность долгосрочного планирования в проведении мероприятий технического обслуживания и ремонта.

Помимо этого, в процессе своего жизненного цикла техника связи специального назначения подвержена различным внешним дестабилизирующим воздействиям, что ведет не только к внезапным отказам, которые характеризуются скачкообразным изменением метрики какого-либо параметра, но и к постепенным отказам, связанным с деградационными процессами и постепенными изменениями метрик одного или нескольких параметров.

Важно отметить, что на появление внезапного отказа зачастую влияют внешние факторы, и, в данном случае, органы технического обеспечения связи и автоматизированных систем управления могут бороться постфактум только с их последствиями, но их первостепенной задачей является поддержание техники связи в работоспособном состоянии и постоянной готовности к применению по назначению. Соответственно, данная задача трансформируется в предотвращение наступления отказов методами теории надежности и методами прогнозирования, что определяет актуальность перехода уже к прогнозной стратегии технического обслуживания и ремонта (рис. 1).

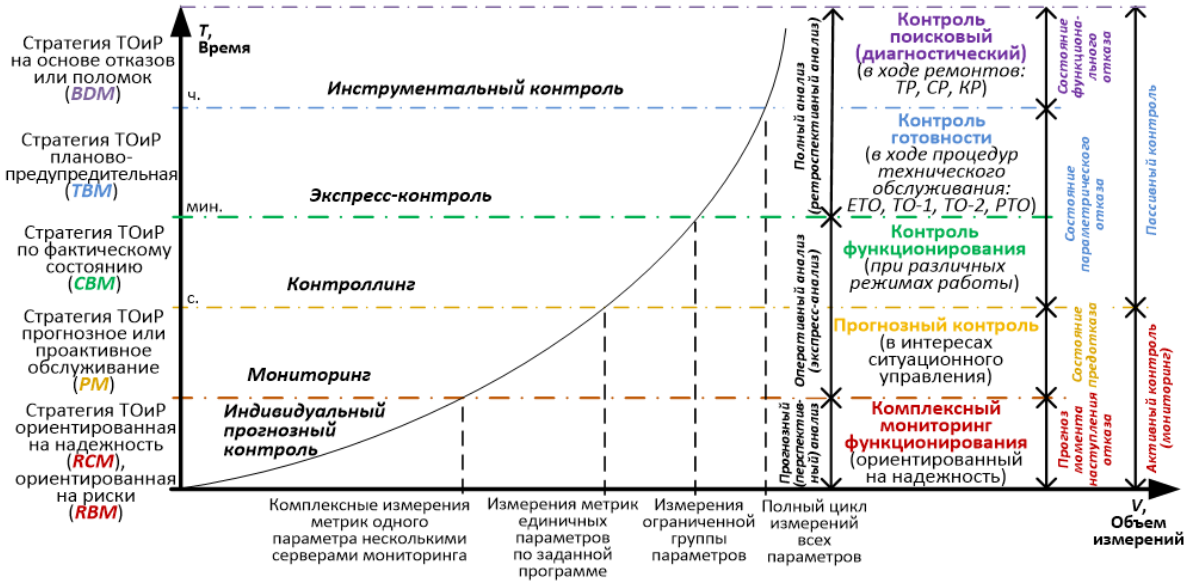


Рис. 1. Кумуляция развития стратегий управления надежностью техники связи специального назначения

Помимо этого, появление современных технологий искусственного интеллекта [2, 3] требует дальнейшего развития новой стратегии управления надежностью, активно продвигаемой мировым научным сообществом.

Сущность прогнозной стратегии [4, 5] заключается в снижении динамики развития неисправностей или их полного устранения за счет предварительного выявления в ходе мониторинга технического состояния техники

связи специального назначения. Достоинствами такой стратегии являются выявление и устранение неисправностей на ранней стадии их развития, что увеличивает срок службы оборудования и проведение только необходимых ремонтных мероприятий. К недостаткам можно отнести повышенные требования к компетенциям обслуживающего персонала, а также дополнительные затраты на развертывание систем мониторинга и разработку методик прогнозирования.

Управление надежностью функционирования путем прогнозирования того или иного вида технического состояния [6, 7] играет важную роль при индивидуальном планировании эксплуатации. Умение предсказать возможный момент отказа особенно важно при недопущении потери работоспособности и снижении боевой готовности.

Прогнозное или проактивное обслуживание относят к стратегиям «гарантированного управления» надежностью, а прогнозирование – к основному способу определения достижения надежности системы. Действительно, данная стратегия обеспечивает с заданной достоверностью гарантированное предупреждение постепенных скрытых параметрических отказов на заданном интервале функционирования, за счет определения предотказного вида технического состояния.

Таким образом, управление надежностью функционирования техники связи специального назначения на всех этапах жизненного цикла и переход от предполагающей регламентированные по времени и полноте проводимых мероприятий виды технического обслуживания и виды ремонтов к стратегии прогнозного технического обслуживания являются обоснованно крайне важными задачами.

Список используемых источников

1. Ажмухамедов И. М., Гостюнин Ю. А. Выбор стратегии технического обслуживания и ремонта оборудования сетей связи на предприятиях нефтегазового комплекса // Инженерный вестник Дона. 2017. № 2. С. 74-83.

2. Абрамов О. В., Назаров Д. А. Методы и средства интеллектуальной поддержки прогноза технического состояния систем ответственного назначения // Информатика и системы управления. 2022. № 4 (74). С. 54-63.

3. Чихачев А. В., Будко П. А., Шмидт А. А. Применение алгоритмов машинного обучения для решения задач прогнозирования технического состояния средств радиосвязи // Телекоммуникации и связь. 2024. № 3 (03). С. 33-39.

4. Абрамов О. В. Прогнозирование состояния и планирование эксплуатации систем ответственного назначения // Надежность и качество сложных систем. 2020. № 3 (31). С. 5-14.

5. Будко П. А., Шмидт А. А., Голюнов М. В., Сафиулов Д. М. Прогнозирование технического состояния в системе технического обеспечения связи и автоматизированных систем управления // IX Межвузовская научно-практическая конференция «Проблемы технического обеспечения войск в современных условиях». Труды конференции: Сборник материалов. СПб.: ВАС, 2024. С. 40-44.

6. Гришин В. В., Шаулов В. А., Галяутдинов Д. Н. Стратегия «гарантированного управления» надежностью радиоэлектронных систем информационного обмена с космическими аппаратами // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посв. Дню радио. 2024. № 1 (79). С. 23-25.

7. Абрамов О. В. Розенбаум А. Н. Управление эксплуатацией систем ответственного назначения. Владивосток: Дальнаука, 2000. 200 с.

MANAGING THE RELIABILITY OF SPECIAL-PURPOSE COMMUNICATION EQUIPMENT IN THE INTERESTS OF IMPLEMENTING PREDICTIVE MAINTENANCE STRATEGIES

Budko P.[1], Yuzhakova A.[2]
[1]PJSC "Inteltech"
[2]Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Failures and other disruptions to the normal functioning of special-purpose communications equipment led to disruptions or complete blockage of the entire communication system, therefore, managing the reliability of its functioning at all stages of its life cycle and switching to a predictive maintenance strategy are extremely important tasks.

Key words: *reliability, maintenance, special-purpose communication technology*

УДК 37.012
ГРНТИ 14.07.09

К ВОПРОСУ О ВНЕДРЕНИИ АДАПТИВНОЙ СИСТЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБРАЗОВАТЕЛЬНЫЕ ПРОЦЕССЫ ВУЗОВ

Н. А. Васильев, А. Д. Такшеев, С. Е. Тарасенко

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

Статья посвящена разработке методов адаптивных систем подготовки специалистов в условиях быстро меняющейся экономической и технологической среды. В работе рассматриваются теоретические основы и практические подходы к созданию адаптивных образовательных систем, которые могут гибко реагировать на изменения в экономике и технологиях. Особое внимание уделяется использованию современных информационных технологий и методов диагностики для оценки готовности специалистов к профессиональной деятельности.

адаптивные системы, система образования, структурно-функциональный анализ

Переход России к ограниченным рыночным отношениям, обусловленный разрывом связей с Западом, выявил многочисленные проблемы в структуре отечественной экономики. Новая реальность подчеркнула стороны российской промышленности, требующие особого внимания и развития, дефицит квалифицированных специалистов в области информационных технологий и искусственного интеллекта, необходимых для поддержания прежнего уровня жизни, а также необходимость подготовки высокопрофессиональных военных кадров. Мировая практика показывает, что выход из кризиса обычно начинается с масштабных вложений в образование. Развитые страны получают значительный объем своего национального дохода именно благодаря повышению образовательного уровня населения.

В настоящее время все острее чувствуется разрыв между процессом подготовки специалиста к профессиональной деятельности и требованиями, которые практика предъявляет к уровню его подготовленности. Отмеченный разрыв является следствием довольно быстрых изменений в экономической и политической сферах деятельности государства и слишком медленного реагирования на эти изменения системы высшего образования [1]. Для эффективного решения указанных проблем подготовка в вузах должна реализовываться в основе комплексного, централизованного, единого по за-

мыслу, целям и установкам управления образовательным процессом вуза. Первым шагом к решению этой проблемы является отказ от болонской системы образования и переход к российской системе, что обеспечит поддержание соответствия уровня образования выпускников с темпами развития государства и воспрепятствует оттоку интеллектуального ресурса страны. При решении указанной задачи, одним из важнейших направлений развития образовательной системы вуза являются: проведение исследований, направленных на рассмотрение особенностей текущей и перспективной деятельности выпускников, согласование целей обучения с задачами, решаемыми выпускниками на практике; совершенствование методик обучения; создание условий творческой самостоятельности обучаемых; широкого внедрения в образовательный процесс новых информационных и педагогических технологий.

Вопросам совершенствования образовательных систем в целом, а также частным вопросам совершенствования образовательного процесса в вузах посвящен целый ряд научных исследований [2, 3, 4], однако представленные в них решения не отвечают постоянно меняющимся требованиям практики, особенностям текущего периода социально-экономического прогресса, современным технологическим возможностям, позволяющим сформировать качественно новую, компьютеризированную систему управления процессом обучения в вузе.

Поставленной цели невозможно достичь простым сокращением учебных программ путем их усечения, и прямолинейной интенсификацией образовательного процесса за счет уплотнения объема информации, подлежащей усвоению. Решить указанную выше проблему, с учетом существующего противоречия между системой подготовки специалистов в вузе и динамически меняющимися требованиями практики к качеству подготовки специалистов, можно не только при помощи принятия отечественной образовательной системы, но и на основе разработки принципиально новой образовательной методологии. При этом достаточно очевидно, что новая методология должна опираться на адаптацию процесса подготовки специалиста к динамически меняющимся требованиям к выпускникам и условиям их социальной среды обитания. В указанных условиях, единственно возможным путем обеспечения требуемого качества подготовки выпускника является построение адаптивной образовательной системы вуза, основанной на использовании новых информационных технологий.

Устранить существующие недостатки поможет новый образовательный подход в виде методологии построения адаптивной системы специалистов, схема которого представлена на рис. 1. Причем основное внимание стоит уделить разработке математической модели процесса управления формированием профессионально-важных качеств обучаемых, диагностики уровня его готовности к профессиональной деятельности.

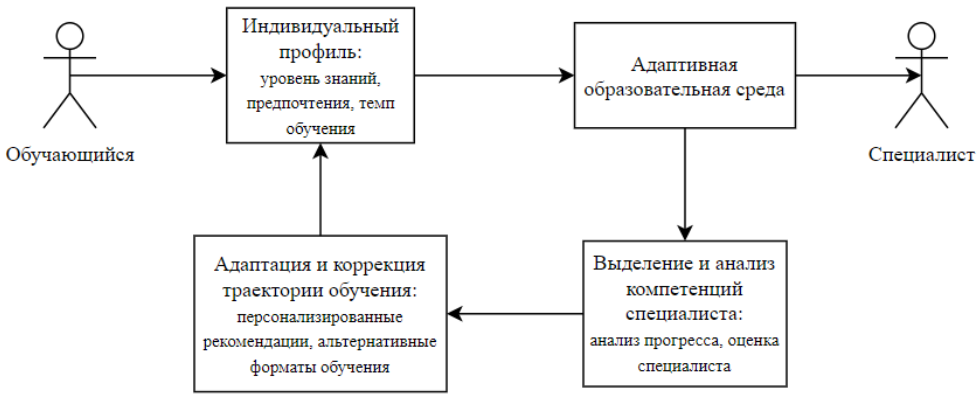


Рис. 1. Схема адаптивной системы подготовки специалистов

Для начала необходимо дать общую характеристику современного состояния системы образования и проанализировать пути повышения качества подготовки специалистов в вузе. Стоит показать, что решение проблемы повышения качества подготовки специалистов, возможна за счет построения образовательной системы вуза, обладающей свойством адаптивности к условиям и требованиям их профессиональной деятельности. Также стоит приводить принципы построения адаптивной системы управления качеством подготовки военных специалистов и произвести выбор и обоснование критериев и показателей качества образовательной системы вуза.

Затем необходимо обобщить и развить методологические основы построения модели специалиста, а также определить состав его профессионально-важных качеств. На основании использования аппарата анализа можно выделить системообразующие показатели и параметры, адекватно отражающие результаты практической деятельности выпускников, а также произвести математическое моделирование процесса управления формированием профессионально важны качеств специалиста при обучении в вузе в условиях нечеткости исходной информации.

Также предлагается разработать диагностический комплекс оценки готовности специалиста к профессиональной деятельности на основе исполь-

зования современных технологических подходов, в рамках которого будет разработана общая схема объединения частных показателей качества подготовки специалиста в интегральный показатель.

В завершении предлагается провести структурно-функциональный анализ степени соответствия профессиональной подготовки специалистов требованиям практики и рассмотреть методики оценки качества подготовки специалиста на основе использования современных технологических подходов, в рамках которой осуществляется оценка: соответствия качества подготовки специалистов, уровня соответствия морально психологических, профессиональных качеств специалиста требованиям практической деятельности. В результате анализа должна быть разработана методика оценки уровня значимости параметров и показателей качества подготовки специалиста, базовых учебных дисциплин и видов занятий для обеспечения требуемого уровня качества подготовки специалиста по результатам анализа отзывов о результатах их деятельности. На рис. 2 представлены примеры компетенций, по которым возможно проводить оценку специалиста.

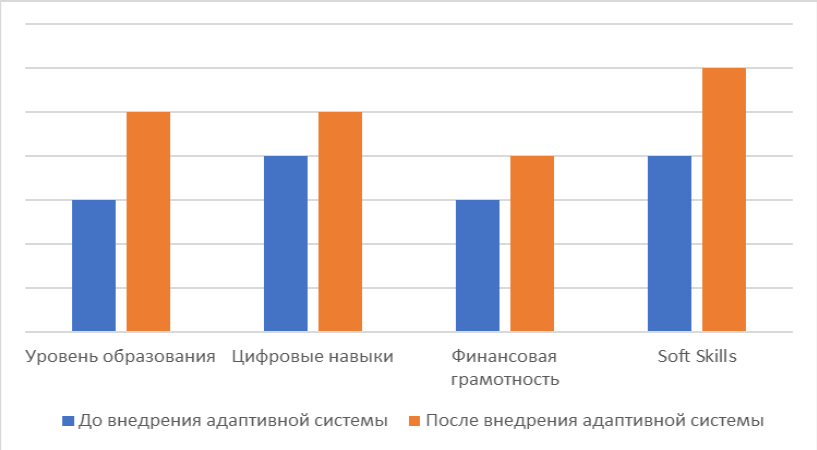


Рис. 2. Предполагаемое изменение компетенций специалиста после внедрения адаптивной системы в образовательные процессы ВУЗов

Также необходимо привести методику определения уровня значимости учебных дисциплин и видов занятий в процессе подготовки специалиста.

В заключение следует отметить, что в условиях перехода России к ограниченным рыночным отношениям и необходимости подготовки высококвалифицированных кадров в различных областях, особое значение приобретает развитие адаптивной образовательной системы.

Разработка новой методологии построения такой системы должна опираться на принципы адаптации к динамически меняющимся требованиям к выпускникам и условиям их профессиональной деятельности. Это позволит

обеспечить требуемое качество подготовки специалистов и повысить уровень их конкурентоспособности на рынке труда.

Таким образом, построение адаптивной образовательной системы вуза, основанной на использовании новых информационных технологий, является перспективным путем обеспечения требуемого качества подготовки выпускника.

Список используемых источников

1. Тебекин А. В. и др. Приоритеты инновационного развития высшего образования как адекватная реакция на тенденции развития общества в новой реальности //Профессиональное образование в современном мире. 2021. Т. 11. №. 1. С. 66-75.

2. Агентова Г. В. Пути совершенствования образовательной системы в России //Вестник Российского государственного торгово-экономического университета (РГТЭУ). 2013. № 11-12. С. 166-176.

3. Пулявина Н. С. Возможности применения инструментов дизайн-мышления для совершенствования электронных информационно-образовательных систем // ЭПП. 2021. № 2.

4. Барашков П. Н., Житницкий М. И., Захаров А. М. Интенсификация учебно-воспитательного процесса в ВУЗе. Проблемы управления, эффективности и пути их решения. СПб.: Издательство Академии связи им С. М. Буденного, 1990.

ON THE ISSUE OF THE INTRODUCTION OF AN ADAPTIVE SYSTEM OF TRAINING SPECIALISTS IN THE EDUCATIONAL PROCESSES OF UNIVERSITIES

Vasiliev N., Taksheev A., Tarasenko S.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is devoted to the development of methods of adaptive systems for training specialists in a rapidly changing economic and technological environment. The paper examines the theoretical foundations and practical approaches to creating adaptive educational systems that can flexibly respond to changes in the economy and technology. Special attention is paid to the use of modern information technologies and diagnostic methods to assess the readiness of specialists for professional activity.

Key words: *adaptive systems, education system, structural and functional analysis*

УДК 004.588
ГРНТИ 78.25.33

ПРЕДЛАГАЕМЫЙ СПОСОБ ИСПОЛЬЗОВАНИЯ УЧЕБНО-ТРЕНИРОВОЧНОЙ КАРТЫ В СОВЕРШЕНСТВОВАНИИ НАВЫКОВ РАБОТЫ НА ПЕРВИЧНОМ МУЛЬТИПЛЕКСОРЕ

А. В. Глушко, В. А. Гриднев, Р. С. Знобищев, И. Г. Стахеев

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

В статье рассматривается способ подготовки специалистов в области инфокоммуникационных технологий и систем специальной связи с помощью учебно-тренировочных карт. Предложенные способ подготовки выпускников военного учебного центра с помощью учебно-тренировочных карт позволяет повысить уровень практических навыков по эксплуатации мультиплексоров и телекоммуникационного оборудования. Статья может быть полезна студентам и педагогическим работникам образовательных организаций, а также руководящему составу.

способ использования учебно-тренировочных карт позволяет повысить качество обучения на мультиплексорах специалистов с помощью активизации у них психических познавательных процессов

Процесс подготовки специалиста в вузе надо рассматривать, как единый процесс обучения и воспитания [1].

В условиях проведения военной специальной операции (СВО) возросла потребность специалистах, подготовленных в области инфокоммуникационных технологий и систем специальной связи, которые обладают необходимыми военно-профессиональными качествами, глубокими знаниями, твердыми практическими навыками и морально-психологической устойчивостью.

Важным условием обучения является использование в подготовке студентов военного учебного центра в области инфокоммуникационных технологий современных средств и способов обучения, которые повышают качество усвоение учебного материала и формируют устойчивые практические навыки в эксплуатации штатной и новой поступающей в войска техники, а также средств связи.

Процесс трансформации знаний в навыки и умения выглядит следующим образом: знания – начальные умения – простые навыки – сложные навыки – сложные умения [1].

Чтобы обеспечить последовательную трансформацию знаний и умений в навыки на электропроводных средств связи применяют учебно-тренировочных карт (УТК), которые обладают некоторыми преимуществами при запоминании и позволяют быстрее и качественнее усвоить учебный В УТК сгруппирована вся основная информация по эксплуатации средств связи и за счет использования зрительной памяти, которая несет более 80 % всей информации при изучении учебного материала, происходит более быстрое и качественное ее запоминание. Учебный материал в УТК распределен пошагово по мере выполнения практических действий, что позволяет строго следовать описанному в УТК порядку эксплуатации мультиплексора и в случае возникновения проблем или ошибок определяет последующие действия, которые возвращают на предыдущий уровень и позволяют выбрать правильный шаг в меню. Такое обучение обеспечивает формирование правильных навыков по эксплуатации оборудования.

В УТК упрощен процесс восприятия сложных элементов оборудования за счет дробления его на простые (пошаговые) действия, которые позволяют поэтапно освоить изучаемую большую задачу и сформировать правильные практические навыки в работе на мультиплексоре.

В системах военного назначения очень велики информационные потоки. Поэтому к человеку-оператору предъявляются высокие требования в отношении скорости действий, их точности и надежности [1].

Для обеспечения быстрой и качественной подготовки выпускников военного учебного центра (ВУЦ) на кафедре электропроводных средств связи с целью изучения порядка эксплуатации телекоммуникационных средств применяются учебные задачи, в которые включен полный цикл обмена информации в разных режимах работы с разными оконечными средствами. Задачи по эксплуатации средств связи имеют большой объем действий и информации, поэтому это требует времени на их усвоение. В связи с этим большие задачи дробятся на более мелкие этапы, которые называются нормативами. В содержание норматива включены конкретные действия при эксплуатации оборудования, которые выполняются на время и выставляются оценки (отлично, хорошо или удовлетворительно) в зависимости от времени, затраченного на его выполнение. Если все действия по эксплуатации выполнены правильно в полном объеме и в установленное время, то выставляется оценка в соответствии с установленными критериями. Оценка определяет уровень практической подготовленности у выпускника практических навыков в работе на телекоммуникационном оборудовании.

Рассмотрим подробнее выполнение норматива по подготовке к работе первичного мультиплексора. В объеме норматива, выполняется проверка не всего первичного мультиплексора, а только одного блока. В качестве примера возьмем норматив по проверке работоспособности блока МК-8 мультиплексора (МП). В нормативе определен объем действий, которые необходимо выполнить обучаемому за определенное время. Для улучшения запоминания учебный материал представлен в виде отдельных слайдов с необходимыми действиями, в последовательном порядке вместе с текстовым кратким содержанием, в котором содержится только нужный материал. Для выполнения норматива необходимо в последовательном порядке выполнить следующий объем работ:

Терминал управления включен, программное обеспечение управлением мультиплексором активировано, сетевой элемент в рабочем поле программы создан, настройки блока и коммутации установлены в значение по умолчанию, питание мультиплексора включено (ТУНП) (рис. 1). Проверить работу аварийной сигнализации блока мультиплексора (АС МП) (рис. 2). По двум первичным групповым трактам, указанным в задании, установить ближний шлейф, режим работы 16 канального интервала «31 АИ», включить контроль CRC (УБШ) (рис. 3). Для задействованных групповых трактов: включить схему резервирования линии «1+1» (СХРЛ) (рис. 4), с автоматическим выбором направления приема, установить приоритеты источникам синхросигнала согласно заданию (ПИС) (рис. 5). По не задействованным трактам включить маскирование аварии потери входного сигнала (МАПС) (Рис.6) и проконтролировать изменение состояния органов аварийной сигнализации блока (КОАС) (рис. 7).

Перечисленные выше задачи специалист, выполняет пошагово сверяя свои действия с информацией указанной на слайдах в УТК:

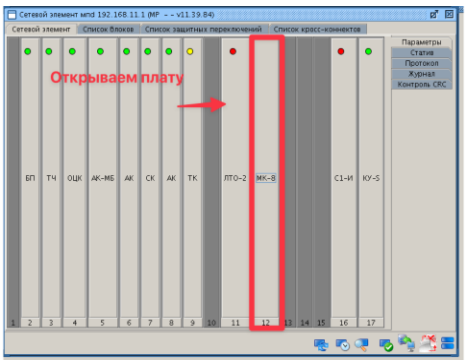


Рис. 1. ТУНП

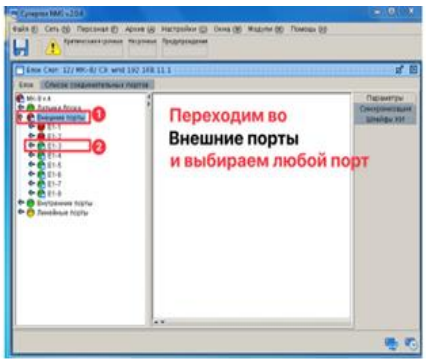


Рис. 2. АС МП

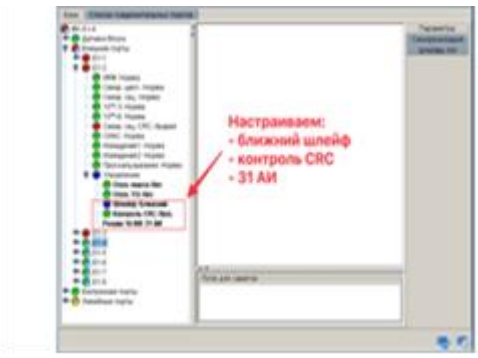


Рис. 3. УБШ

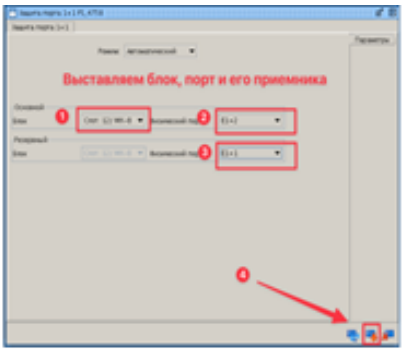


Рис. 4. СХРЛ

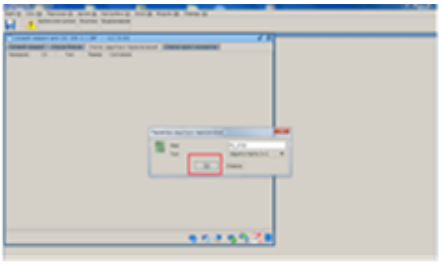


Рис. 5. ПИС

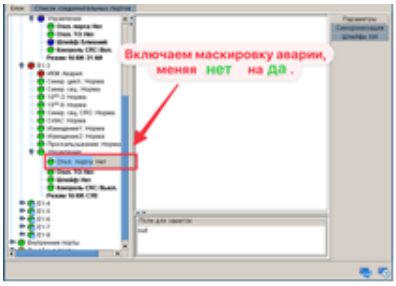


Рис. 6. МАПС

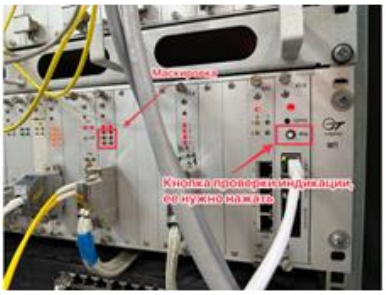


Рис. 7. КОАС

В результате таких действий специалист нарабатывает все необходимы операции, которые закрепляются в моторной памяти и на их основе формируются устойчивые практические навыки, что положительно влияет на успеваемость и качество учебного процесса.

Таким образом, применение УТК при обучении выпускников на кафедре электропроводных средств связи позволяет повысить качество подготовки специалистов в области инфокоммуникационных технологий и сократить сроки усвоения учебного материала за счет внедрении в учебный процесс современных способов обучения. таких как УТК и Применение способа визуальной и двигательной памятей, которые является составной частью психических познавательных процессов студентов позволяет рас-

ширить возможности выпускников. Все это вместе позволяют оптимизировать обучение студентов за счет поэтапного изучения сложных средств связи и совершенствования у них уровня практических компетенций.

Список используемых источников

1. Ахутин В. М., Зараковский Г. М., Королев Б. А. и др. Инженерная психология в военном деле / под общ. ред. Б. Ф. Ломова. М.: Воениздат, 1983. 224 с.

PROPOSED METHOD OF USING A TRAINING CARD TO IMPROVE WORK SKILLS ON A PRIMARY MULTIPLEXER

Glushko A., Gridnev V., Znobishchev R., Stakheev I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses a method of training specialists in the field of infocommunication technologies and special communication systems using training cards (TC). The proposed method of training graduates of the military training center (MTC) using the TTC allows to improve the level of practical skills in the operation of multiplexers and telecommunications equipment. The article can be useful for students and teaching staff of educational organizations, as well as for management.

Key words: *the method of using the TTC allows to improve the quality of training on multiplexers of specialists by activating their mental cognitive processes*

УДК 355.233.23
ГРНТИ 78.25.33

СПОСОБ КОНТРОЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНО-ВАЖНЫХ КАЧЕСТВ У СТУДЕНТОВ ВОЕННОГО УЧЕБНОГО ЦЕНТРА В УСЛОВИЯХ ПРОВЕДЕНИЯ СВО

В. А. Гриднев, Д. А. Груздев, И. Г. Стахеев

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

В статье рассматриваются вопросы повышения качества подготовки выпускников военного учебного центра с помощью контроля за формированием профессионально- важных качеств у студентов в условиях проведения специальной военной операции. Уровень развития этих качеств оказывает большое влияние на успешность подготовки специалистов по связи в области телекоммуникаций. Предлагается способ контроля за совершенствованием профессионально-важных качеств у студентов в ходе обучения в военном учебном центре позволяют определить слабые места в развитии и формировании качеств выработать эффективный метод воздействия.

Предложенный способ контроля, формирования и развития профессионально-важных качеств у специалистов по связи может быть полезен педагогическому и руководящему составу ВУЦ.

способ повышения качества подготовки выпускников военного учебного центра с помощью контроля за формированием профессионально-важных качеств у студентов в ходе обучения

В настоящее время особенно актуальной является проблема подготовки специалистов для войск связи, которая стала еще более острой в условиях проведения РФ специальной военной операции (СВО).

Начало подготовки специалистов в военном учебном центре (ВУЦ) осуществляется с момента набора абитуриентов в университет, когда происходит оценка готовности кандидатов к обучению. Отбор кандидатов проходит по нескольким направлениям: по состоянию здоровья и профессиональной психологической пригодности, по результатам единого государственного экзамена (ЕГЭ) и по результатам уровня физической подготовленности.

Главным условием отбора кандидатов является соответствие качеств кандидатов вышеперечисленным требованиям. Но в современных условиях к этим требованиям необходимо еще добавить и контроль по наличию у абитуриентов уровня развития морально-психологических качеств (МПК), который является базовым для студентов ВУЦ. Такие требования как мотивация, направленность, желание являются базовыми и формируют жизненные установки у студента. От них зависит выбор будущей профессии и успешное обучение и ее освоение. Если жизненные установки сформированы, и абитуриент сделал правильный выбор, то это положительно скажется на его обучении в ВУЦ и не будет колебаний после поступления и в ходе учебы, и он после выпуска пойдет служить в войска.

Еще одним важным условием в подготовке специалистов являются знания, которые абитуриент получил в школе, которые являются базой для успешного обучения в ВУЦ, а также необходимо оценивать способность абитуриента к изучению нового учебного материал. Скорость переработки информации на прямую влияет на результаты успеваемости. Результаты интеллектуальной деятельности абитуриента, как правило отражаются в баллах, полученных на ЕГЭ и аттестате о среднем образовании.

Для управления подготовкой студентов необходим постоянный контроль не только за уровнем развития у него знаний и уровнем развития ПВК на начальном этапе, но и контроль успешности развития ПВК по этапам обучения.

Зная уровень развития ПВК студента на первом курсе, можно планировать с ним индивидуальную и воспитательную работу, в ходе которой наметить задачи по корректировке требуемых качеств. Такие действия позволяют управлять развитием ПВК студента по мере обучения его на каждом курсе и в итоге подготовить выпускника с требуемым уровнем компетенций.

В современных условиях существует острая потребность, прежде всего, в хорошо подготовленных специалистах для войск связи, обладающих всеми необходимыми военно-профессиональными качествами (морально-психологической устойчивостью, целеустремленностью и направленностью на выполнение задачи, глубокими знаниями, твердыми практическими навыками) [1]. Рассмотрим факторы (рис. 1), которые необходимо

учитывать с начала поступления и в ходе обучения студента в ВУЦ для его успешной подготовки.

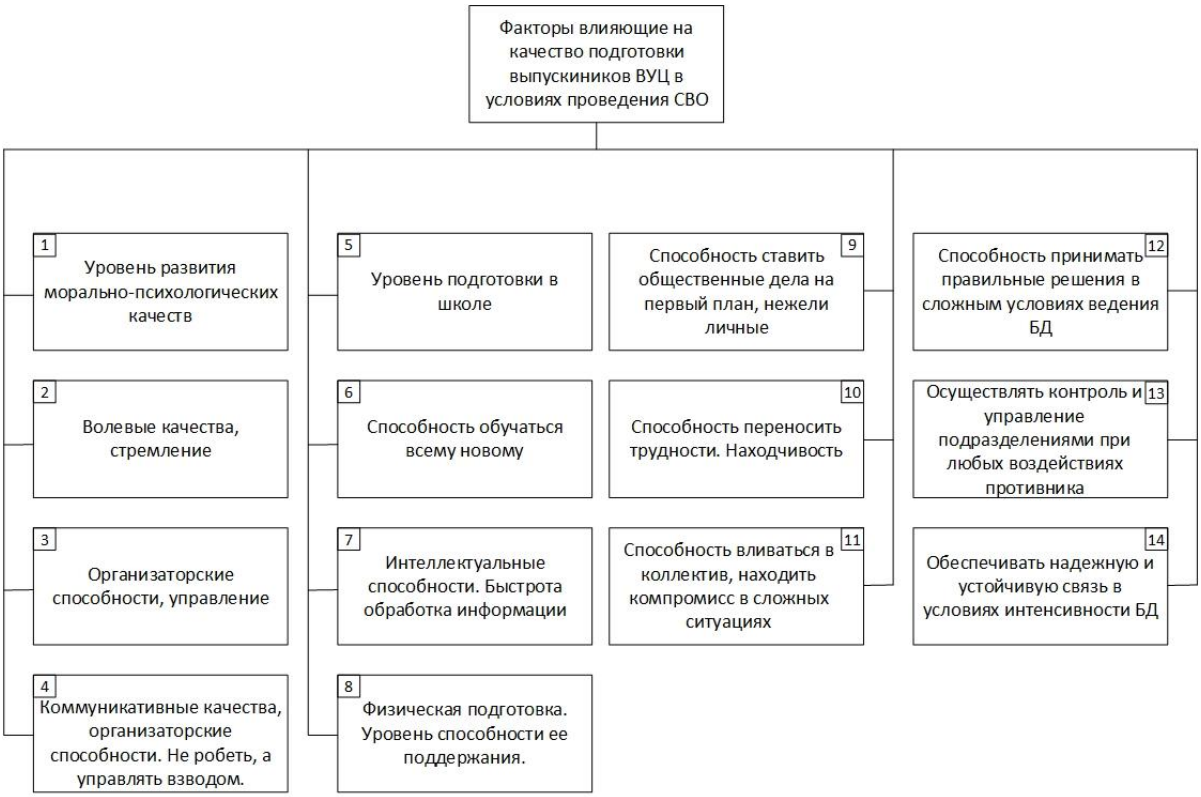


Рис. 1. Схема факторов

В таблице 1 представлены уровни развития ПВК у студента по курсам обучения. Для индивидуальной и воспитательной работы собираются и анализируются все необходимые данные по развитию уровней ПВК у студента на всех курсах обучения.

ТАБЛИЦА 1. Уровни развития ПВК у студента по курсам обучения

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Студент 1 курса	5	6	4	3	4	5	3	3	5	6	6	5	4	5
Студент 2 курса	6	6,5	4	5	4,5	5,2	5,5	4	5,3	7,1	6,4	5,8	4,7	7
Студент 3 курса	7	7	5,3	6,4	5,8	5,4	6,8	5,9	5,8	8,2	7,2	6,6	5,8	7,9
Студент 4 курса	8	7,5	6,6	7,6	6,3	6,1	7,1	6,4	6,1	8,5	7,7	7,1	6,1	8,4
Студент 5 курса	9	8	7	8,1	6,8	7,3	8,2	7,7	6,9	9,1	8,3	8,2	7,5	9,5

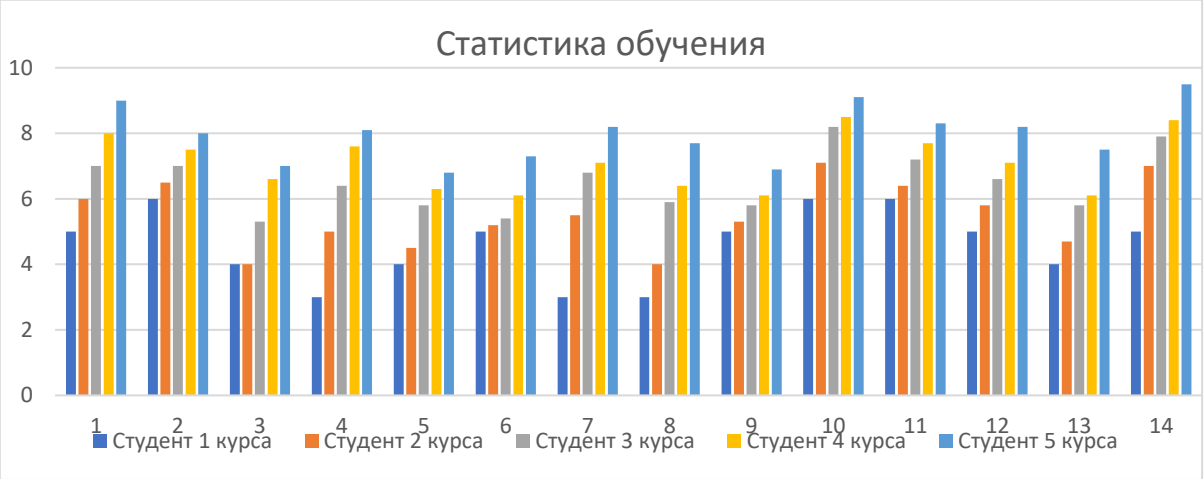


Рис. 2. Гистограмма успешности формирования ПВК по курсам обучения

На рисунке 2 представлена гистограмма успешности формирования ПВК у студента по курсам обучения. Данные контроля используются для формирования и последующего развития определенных качеств у студента, которые требуют внимания. На основании данных контроля куратор группы составляет план индивидуальной работы со студентом с учетом не только компенсации у него недостаточного уровня развития отдельных ПВК, но планирует развитие остальных качеств необходимых выпускнику ВУЦ. В плане индивидуальной работы намечаются комплексные мероприятия, которые позволят, используя различные методы воздействия достичь намеченных результатов. В ходе индивидуальной и воспитательной работы, за студентами имеющими задолженности закрепляются студенты, которые успешно знают нужную дисциплину, что позволяет быстрее сформировать необходимые знания у задолжника и сдать отчетность. Если у студента слабо развиты организаторские способности ему поручают иногда заменять командира отделения и командовать отделением. Если такая же проблема с коммуникативными способностями, то ему поручают чаще вести информирование студентов учебной группы. От простого к сложному, поэтапно формируются необходимые ПВК, что положительно влияет на качество учебного процесса.

Высокий уровень развития ПВК определяет способности выпускников к самостоятельной службе и позволяет во всех условиях обеспечивать надежную и устойчивую связь.

Таким образом, контроль за уровнем формирования и развитие ПВК у студентов на каждом этапе процесса обучения в ВУЦ и своевременная корректировка ПВК через индивидуальную воспитательную работу с ними оказывает эффективное влияние на качество подготовки выпускников.

Список используемых источников

1. Александров В. А., Гриднев В. А., Груздев Д. А.. Формирование профессионально-важных качеств специалистов в военном учебном центре // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция. Сб. Науч. ст. в 4-х томах. Том 4. Под редакцией Макаренко С. И., сост. В. С. Елагин, Е. А. Аникевич. СПб.: СПбГУТ. 2023. С. 527–532.

METHOD OF CONTROL OF FORMATION OF PROFESSIONALLY IMPORTANT QUALITIES IN STUDENTS OF MILITARY TRAINING CENTER IN CONDITIONS OF CONDUCTING SVO

Gridnev V., Gruzdev D., Stakheev I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article considers the issues of improving the quality of training graduates of the military training center by monitoring the formation of professionally important qualities in students in the conditions of a special military operation. The level of development of these qualities has a great influence on the success of training communications specialists in the field of telecommunications. A method of monitoring the improvement of professionally important qualities in students during training at the military training center is proposed, which allows identifying weak points in the development and formation of qualities and developing an effective method of influence. The proposed method of monitoring, forming and developing professionally important qualities in communications specialists can be useful for the teaching and management staff of the military training center.

Key words: *the proposed method of control, formation and development of professional-important qualities in communication specialists can be useful for pedagogical and managerial staff of the military training center.*

УДК 355.233.23
ГРНТИ 78.25.33

ПРЕДЛАГАЕМЫЙ СПОСОБ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ В УСЛОВИЯХ ПРОВЕДЕНИЯ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

В. А. Гриднев, И. Г. Стахеев

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

В статье рассматриваются проблемы совершенствования подготовки специалистов в области телекоммуникаций в условиях проведения специальной военной операции (СВО). Предлагается способ совершенствования подготовки специалистов в области телекоммуникационных технологий путем углубления их подготовки за счет добавления практических занятий, направленных на изучение опыта СВО. Практические занятия проводятся в часы самостоятельной работы и направленны на изучение новой информации, технологий и техники связи, которые используются в ходе проведения СВО.

Предложенный способ подготовки специалистов в области телекоммуникаций может быть полезен, как выпускникам военного учебного центра (ВУЦ), так и профессорско-педагогическому составу ВУЦ.

способ совершенствования подготовки специалистов в области телекоммуникационных технологий с учетом опыта проведения СВО

Проблемы совершенствования подготовки специалистов в ВС РФ приобрели еще большую актуальность в условиях проведения специальной военной операции (СВО).

С началом СВО старые шаблоны и взгляды на подготовку специалистов для вооруженных сил РФ претерпели изменение. Каждой новая война совершенствуется способы вооруженной борьбы и в след за этим происходит совершенствование методов подготовки войск и появляются новые образцы военной техники.

Применение новых подходов ведения боевых действий и новых образцов техники и средств связи проходит локально. После получения положительных результатов испытаний формируются новые взгляды и требования по подготовке специалистов и внедрению новой техники в ВС РФ.

Вышеуказанное развитие оказало влияние и на изменение системы военного образования, которая осуществляет подготовку специалистов для МО РФ. В результате создаются и обосновываются новые методы ведения

вооруженной борьбы, а на их основе формируются новые методики и способы подготовки специалистов.

В современных условиях существует острая потребность, прежде всего, в хорошо подготовленных специалистах для войск связи, обладающих всеми необходимыми военно-профессиональными качествами (морально-психологической устойчивостью, целеустремленностью и направленностью на выполнение задачи, глубокими знаниями, твердыми практическими навыками) [1].

Для решения проблемы качества подготовки специалистов первоначально следует изучить причины, которые породили эти проблемы и выработать решения по их устранению.

В условиях проведения боевых действий появляется много новой информации, которая важная и ее необходимо использовать для подготовки военных связистов путем добавления в учебные программы обучения специалистов. Из поступающей информации необходимо выбрать значимую для обучения. Причем новую информацию необходимо добавлять очень быстро, так как от нее на поле боя зависит не только живучесть конкретного солдата, но и всех подразделений.

Конечная цель, обозначенная в программе обучения, это подготовка специалиста, который способен обеспечить связь (управление войсками и оружием) должностным лицам подразделений и соединений в условиях ведения современной войны. А для этого необходимо выполнить целый комплекс мероприятий, которые обязательны для ее обеспечения. Это соблюдение мер безопасности связи, защита системы связи от технических средств разведки противника, радиоэлектронная защита системы связи, защита системы связи от средств поражения противника, инженерное оборудование и маскировка системы связи, выполнение мероприятий по радиационной, химической и биологической защите техники и личного состава подразделений связи, мероприятия по охране, обороне объектов связи и т.д.

Студент военного учебного центра должен быть подготовлен к практическим действиям и быстрому принятию решений за счет обучения всем необходимым приемам на практических занятиях.

Задача программы обучения предполагает научить специалистов по связи практически правильно выполнять все требования, которые определены программой подготовки. Совершенствование навыков осуществляется на практических занятиях и тренажерах. Проверить уровень практической

подготовленности студента возможно путем сдачи нормативов и выполнения учебных задач.

Важным условием в подготовке специалиста в области телекоммуникаций является разработка и внедрение нового методического материала на основе сформированной программы обучения.

Действующие методики обучения необходимо дорабатывать с учетом развития новых способов вооруженной борьбы.

Решением проблем подготовки специалистов и поиск новых методов их обучения, которые остро стоят перед МО РФ занимается все учебные заведения ВС РФ и в том числе военный учебный центр (ВУЦ) при Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича (СПБ ГУТ).

ВУЦ СПбГУТ готовит специалистов в области телекоммуникаций для ВС РФ. В настоящее время потребность в подготовленных специалистах в области телекоммуникаций увеличивается, так как растет численность войск и имеются потери личного состава в ходе боевых действий.

Актуальной является проблема не просто подготовки специалистов, а в первую очередь проблема быстрой и качественной подготовки специалистов для войск связи. Причем важным условием является подготовка специалистов всесторонне и качественно подготовленных. Которые были бы способны в условиях интенсивной вооруженной борьбы обеспечивать своевременную, надежную и устойчивую связь в интересах должностных лиц, управляющих войсками и оружием.

Современные требования к подготовке специалистов, которые были изложены выше предписывают необходимость готовить и обучать не только тому, что есть в утвержденной программе обучения, но и новым идеям и технике, информация о которых поступает в ВУЦ из зоны проведения СВО. Новая информация поступает на кафедру от выпускников ВУЦ, участвующих в боевых действиях и офицеров-преподавателей, которые принимали участие либо в боевых действиях, либо занимались подготовкой добровольцев в учебных центрах МО РФ в зоне боевых действий. Таким образом существует обратная связь с выпускниками ВУЦ через разные платформы, в которых обсуждаются злободневные вопросы. Такая обратная связь позволяет быть в курсе современных событий и сократить время решениях актуальных вопросов так, как исключается бюрократическая машина главном управлении связи ВС РФ, которая эти вопросы будет решать значительно дольше и отправит их для решения все равно в учебные заведения.

В результате вышеперечисленного возникает ситуация, когда изучать необходимо все, что имеет отношение к применению связи в ходе боевых действий. В следствии такого положения дел объем информации, который необходимо изучить значительно возрастает, а время, выделенное в программах обучения специалистов в области телекоммуникаций, остается прежним. Изменить время обучения в программах подготовки специалистов не просто, так как это решение принимается в ГУС ВС РФ. Ждать изменений, которые должны поступить от руководящего состава главного ГУС ВС РФ не рационально, так как такие проблемы решаются долго или вообще остаются не решенными в силу объективных обстоятельств. Поэтому необходимо искать наиболее быстрые и оптимальные пути решения проблемы подготовки специалистов в новых условиях.

Выход из этого положения уже есть, и он заключается в том, что необходимо готовить выпускников по имеющимся программам обучения в том же объеме часов, а в часы самостоятельной подготовки проводить практические занятия по новой технике связи и новым подходам в обеспечении связи с учетом всей имеющейся информации на этот счет.

Всестороннему и качественному обучению специалистов для войск связи могут помочь новые подходы обучения студентов, которые были адаптированным к современным условиям и новым требованиям на кафедре ПЭС и ФПС ВУЦ. На кафедре организованы и проводятся практические занятия в часы отведенные для самостоятельной работы с выпускниками ВУЦ по применению новой техники связи с учетом опыта организации связи в зоне проведения СВО. Организаторами практических занятий являются офицеры-преподаватели, которые участвовали в обучении добровольцев на учебных полигонах и несли боевое дежурство на центрах боевого управления соединений, участвующих в проведении СВО. Они занимались подготовкой специалистов по связи для боевых действий и помогали в организации связи подразделениям, участвующим в проведении боевых действиях.

На кафедре руками преподавателей создана аудитория, которая оборудована с учетом современных требований. В оборудованной аудитории имеются средства связи, которые используются в настоящее время на поле боя. Практические занятия по подготовке студентов выпускников проводятся в часы самостоятельной работы и другое свободное время. Каждый студент участвует в организации реальной связи на новых средствах связи с другими военными учебными центрами города и РФ. В ходе практических занятий происходит совершенствование навыков практической работы на новых

средствах связи. Такие занятия помогают формировать военно-профессиональные качества и развивать компетенции по организации и применению новых средств связи у выпускников, что в целом повышает уровень качества подготовки специалистов для войск связи.

Таким образом, проблему подготовки высоко квалифицированных специалистов в области телекоммуникаций для войск связи ВС РФ возможно решить способом выделения времени на практическую работу выпускников в часы самостоятельной подготовки и дополнительных занятий. Имеющийся опыт таких практических занятий показал их востребованность у студентов выпускного курса потому, что на занятиях дается практика по организации связи во всех ее тонкостях и предоставляется возможность каждому самостоятельно организовать связь не только в своем учебном заведении, но и с ВУЦ других регионов, что очень ценно с точки зрения первого практического опыта. Такие занятия вызывают интерес и уверенность в организации связи у выпускников.

Список используемых источников

1. Александров В. А., Гриднев В. А., Груздев Д. А. Формирование профессионально-важных качеств специалистов в военном учебном центре // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 4-х томах. Том 4. Под редакцией Макаренко С. И., сост. В. С. Елагин, Е. А. Аникевич. СПб.: СПбГУТ, 2023. С. 527–532.

THE PROPOSED METHOD OF TRAINING SPECIALISTS IN THE FIELD OF TELECOMMUNICATIONS IN THE CONDITIONS OF A SPECIAL MILITARY OPERATION.

Gridnev V., Stakheev I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article considers the problems of improving the training of specialists in the field of telecommunications in the conditions of a special military operation (SMO). A method is proposed for improving the training of specialists in the field of telecommunications technologies by deepening their training by adding practical classes aimed at studying the experience of SMO. Practical classes are, held during independent work hours and are, aimed at studying new information, technologies and communication equipment that are, used during the SMO. The proposed method of training specialists in the field of telecommunications can be useful for both graduates of the military training center (MTC) and the teaching staff of the MTC.

Key words: *a method for improving the training of specialists in the field of telecommunications technologies taking into account the experience of conducting SMO*

УДК 355/359.07
ГРИТИ 49.47.31

РАЗРАБОТКА АЛГОРИТМА ДЕЙСТВИЙ ОТВЕТСТВЕННЫХ ЗА ОРГАНИЗАЦИЮ ФПС В ВОИНСКОЙ ЧАСТИ

Д. А. Груздев, В. В. Загорельский, А. А. Марченков

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

Подготовка должностных лиц, ответственных за организацию ФПС, с высоким уровнем специальной подготовки является необходимым условием выполнения требований, предъявляемых к качеству фельдъегерско-почтовой связи: своевременность и безопасность, выполнение которых обеспечит высокую эффективность данного вида связи. В докладе предложена методика, существенно облегчающая работу по организации ФПС в воинской части.

фельдъегерско-почтовая связь, активные методы обучения, военно-специальная подготовка

Об интерактивных методах в обучении и необходимости широко использовать их при подготовке специалистов фельдъегерско-почтовой связи (ФПС) мы говорили ранее. Использование данных методов позволяет направлять и координировать работу обучаемого, для достижения целей учебного процесса в максимально короткие сроки [1].

В данной статье рассматриваются проблемы организации ФПС в воинской части. В чем актуальность данного вопроса?

Фельдъегерско-почтовая связь Вооруженных Сил Российской Федерации обеспечивается узлами и станциями фельдъегерско-почтовой связи, а также воинскими фельдъегерями (нарочными) воинских частей, воинскими почтальонами (уполномоченными) воинских частей и подразделений. Деятельность вышеперечисленных должностных лиц определяется введенным в действие новым руководящим документом по организации ФПС в воинской части – Инструкции по организации фельдъегерско-почтовой связи в объединениях, соединениях, воинских частях и организациях Вооруженных Сил Российской Федерации.

ФПС в воинской части организует командир воинской части на основании ежегодно издаваемого им приказа, содержащего перечень вопросов, изложенных в Инструкции. Воинские отправления, посылаемые и получаемые воинскими частями, а также почтовые отправления и телеграммы, получаемые и отправляемые личным составом воинских частей, являются военным грузом, подлежащим беспрепятственной и своевременной доставке по назначению узлами (станциями) ФПС, нарочными воинских частей, воинскими почтальонами (уполномоченными) воинских частей и подразделе-

ний [2]. Поэтому обучение подготовки к отправке всех видов воинских почтовых отправлений (адресование, прошивка, опечатывание, оформление сопроводительных форм документов, взимание оплаты) должно проводиться на занятиях по военно-специальной подготовке в соответствии с руководящим документом, а чтобы организовать этот процесс, командиры должны знать порядок правильных действий и обучить соответствующие категории должностных лиц.

Проводимая работа по разработке методических рекомендаций для ускоренной подготовке специалистов, назначенных приказом командира части за организацию ФПС, позволит в кротчайший срок и с высоким качеством их подготовить для выполнения своих функций.

Методика включает Алгоритм действий командира части по организации ФПС и Обучающую программу для занятий по военно-специальной подготовке делопроизводителей, уполномоченных воинских частей, воинских почтальонов воинской части, воинских фельдъегерей, ответственных за отправку регистрируемой воинской корреспонденции и корреспонденции ограниченного доступа.

Пример алгоритма действий командира части по организации ФПС:

Что нужно подготовить:

1. Выделить помещение для обмена почты воинских почтальонов подразделений.

2. Выделить транспорт для получения воинских почтовых отправлений.

3. Оборудовать стенд (рис. 1).

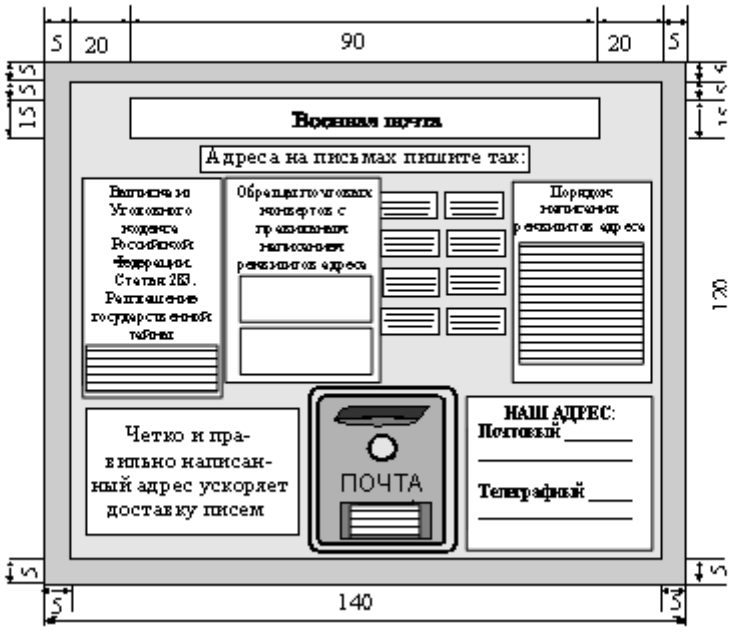


Рис. 1. Образец стенда Воинская почта

Издать приказ Об организации ФПС в воинской части на год, в котором определить:

1. Организацию ФПС и основные задачи.

2. Порядок ведения служебной и личной переписки с указанием почтового и телеграфного адресов.

3. Порядок назначения воинского фельдъегеря (нарочного) и воинского почтальона (уполномоченного) воинской части.

4. Порядок назначения воинских почтальонов подразделений.

5. Порядок приема и отправки секретных отправлений в воинской части.

6. Порядок приема и отправки почтовых отправлений, телеграмм и периодической печати в воинской части.

7. Порядок обеспечения военнослужащих, проходящих военную службу по призыву, маркированными почтовыми конвертами «Воинская корреспонденция».

8. Задачи должностных лиц воинской части по организации и всестороннему обеспечению ФПС.

9. Порядок и сроки проведения учебных сборов с воинскими почтальонами воинской части и подразделений.

10. Порядок осуществления контроля за исполнением настоящего приказа.

Фрагмент Обучающей программы для занятий по военно-специальной подготовке (рис. 2).

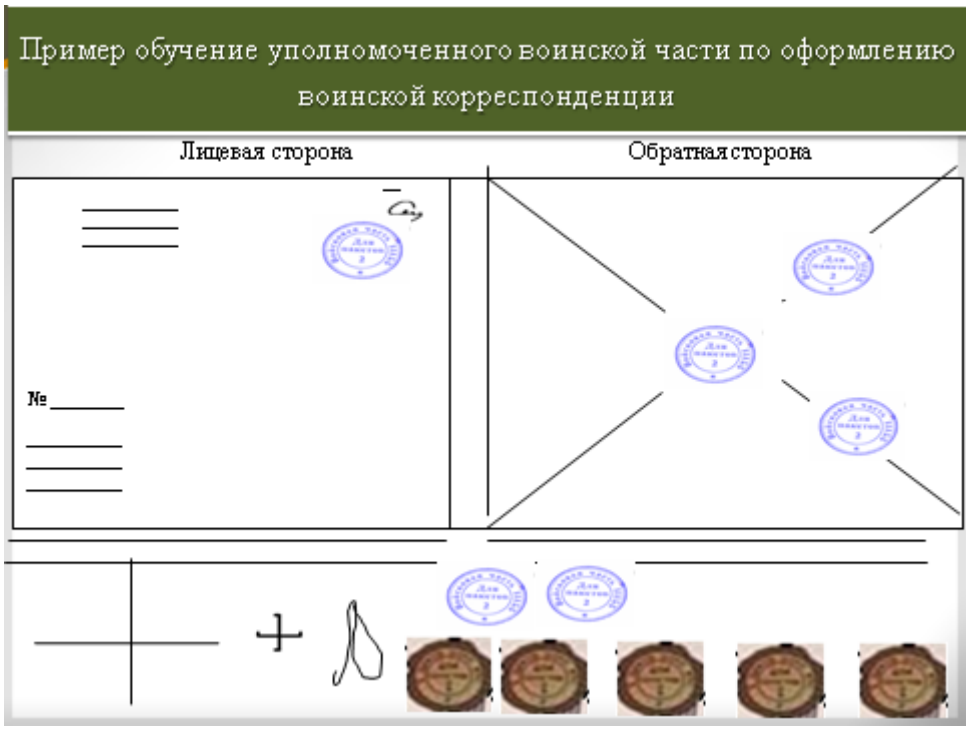


Рис. 2. Опечатывание конверта мастичной печатью «Для пакетов»

Проверка актуальности данной работы и эффективность обучения должностных лиц по военно-специальной подготовке будет проведена во время учебного сбора студентов, обучающихся по военно-учетным специальностям «Организация фельдъегерско-почтовой связи» и «Специалист фельдъегерско-почтовой связи. Начальник экспедиции» на узле ФПС объединения.

Список используемых источников

1. Загорельский В. В., Марченков А. А. Повышение эффективности обучения специалистов фельдъегерско-почтовой связи с использованием БКУТС. Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. Р. В. Кирička; сост. А. А. Нестеров. СПб.: СПбГУТ, 2024. Т. 3. 846 с.

2. Организация фельдъегерско-почтовой связи. Часть 2: учебное пособие / В. В. Загорельский, А. А. Марченков, Е. Н. Сидоренко. СПб.: СПбГУТ. 2023 г. 110 с.

Статья представлена научным руководителем, доцентом кафедры Проводной электросвязи и фельдъегерско-почтовой связи, кандидатом технических наук, полковником А. В. Брыдченко.

DEVELOPMENT OF AN ALGORITHM OF ACTIONS FOR THOSE RESPONSIBLE FOR ORGANIZING FPS IN A MILITARY UNIT

Gruzdev D., Zagorelsky V., Marchenkov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Training officials responsible for organizing FPS with a high level of special training is a necessary condition for meeting the requirements for the quality of courier-postal communications: timeliness and safety, the implementation of which will ensure high efficiency of this type of communication. The report proposes a methodology that significantly facilitates the work on organizing FPS in a military unit.

Key words: *courier-postal communications, active teaching methods, military-special training*

УДК 519.876.2
ГРНТИ 28.29.07

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ С ДИСКРЕТНЫМ СОСТОЯНИЕМ И НЕПРЕРЫВНЫМ ВРЕМЕНЕМ НА ПРИМЕРЕ МОДЕЛИ ВОЗНИКНОВЕНИЯ ОТКАЗОВ И БОЕВЫХ ПОВРЕЖДЕНИЙ ВОЕННОЙ ТЕХНИКИ СВЯЗИ

А. В. Косырев

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

Моделирование процессов с дискретным состоянием и непрерывным временем представляет собой методологический подход, применяемый для анализа динамических систем, способных пребывать в конечном числе дискретных состояний, при этом переходы между этими состояниями осуществляются в случайные моменты времени. Данные процессы формализуются посредством марковских процессов или цепей Маркова с непрерывным временем, где будущее состояние системы зависит исключительно от текущего состояния и не зависит от предыстории (свойство марковости). Такой подход широко используется для изучения стохастических систем в различных областях, таких как теория массового обслуживания, теория надежности, биоинформатика и других.

В данной статье рассмотрена модель отказов и боевых повреждений военной техники связи, которая позволяет производит расчет вероятности возникновения определенных видов событий, будь то отказ или боевое повреждение. Цель достигается путем моделирования процессов возникновения отказов и боевых повреждений на основе составления и решения дифференциальных уравнений состояний Колмогорова.

модель отказов и повреждений, отказ, повреждение, дифференциальные уравнения

Дифференциальные уравнения представляют собой одну из наиболее распространенных и универсальных форм математического описания динамических систем. Они активно применяются для моделирования переходных процессов, возникающих в системах различной физической, биологической, химической и технической природы. Такие уравнения позволяют формализовать зависимости между изменяющимися во времени параметрами системы, отражая их динамику через производные искомых функций. Благодаря своей общности, дифференциальные уравнения служат ключевым инструментом для анализа и прогнозирования поведения сложных систем, где важную роль играют временные изменения и взаимодействия между компонентами.

Для моделирования процесса возникновения отказов и боевых повреждений используется непрерывная цепь Маркова [1].

Пусть система характеризуется *n* состояниями $S_0, S_1, S_2, \ldots, S_n$, а переход из состояния в состояние может осуществляться в любой момент времени.

Для любого *t* вероятности состояний $P_0(t), P_1(t), \ldots, P_n(t)$, где $P_i(t)$ – вероятность того, что в момент времени *t* система *S* будет находиться в состоянии $S_i(i = 0,1,\ldots,n)$.

Вероятности состояний $P_i(t)$ находят путем решения системы дифференциальных уравнений (уравнений Колмогорова) [2]:

$$\frac{dP_i(t)}{dt} = \sum_{j=1}^{n} \lambda_{ji} P_j(t) - P_i(t) \sum_{j=1}^{n} \lambda_{ij}, \qquad (1)$$

где $\lambda_{ij} P_i(t)$ – поток вероятности перехода из одного состояния в другое; $\sum_{i=1}^{n} P_i(t) = 1$.

Уравнения (1) составляют по размеченному графу (рис. 1).

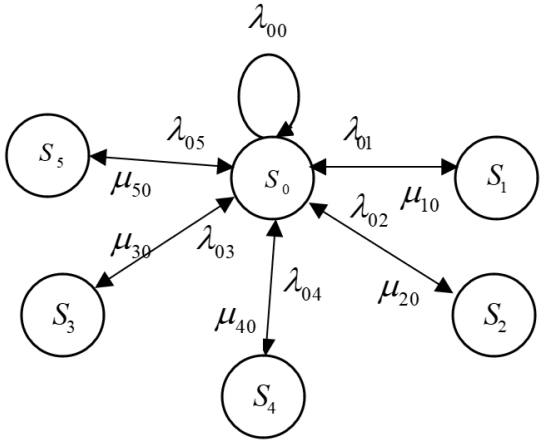


Рис. 1. Граф переходных процессов модели возникновения отказов и боевых повреждений военной техники связи

Для данного примера система может находиться в следующих состояниях: S_0 – работоспособна (начальное состояние), S_1 – работоспособна и позволяет выполнять задачи по предназначению (ошибки персонала), S_2 – работоспособна, но не позволяет выполнить задачи по предназначению, S_3 – не работоспособна и имеет эксплуатационный отказ, S_4 – не работоспособна имеет деградационный отказ, S_5 – не работоспособна, имеет боевое повреждение.

В основе моделирования марковских процессов с непрерывным временем лежит правило, согласно которому производная вероятности нахожде-

ния системы в определенном состоянии определяется как разность между суммарным потоком вероятностей, поступающих в данное состояние из всех других состояний, и суммарным потоком вероятностей, выходящих из данного состояния во все остальные. Математически это правило выражается через систему дифференциальных уравнений Колмогорова, где скорость изменения вероятности каждого состояния зависит от интенсивностей переходов между состояниями. Данный подход обеспечивает корректное описание динамики вероятностного распределения системы во времени.

В предельном стационарном режиме, когда система достигает равновесия, вероятности нахождения в каждом из состояний становятся постоянными, а их производные по времени равны нулю. В этом случае система дифференциальных уравнений Колмогорова преобразуется в систему линейных алгебраических уравнений, где неизвестными являются стационарные вероятности состояний. Такая система допускает аналитическое решение, что позволяет определить установившиеся значения вероятностей для каждого состояния системы. Этот подход широко используется для анализа долгосрочного поведения марковских процессов и оценки их устойчивых характеристик.

Для нахождения точного значения $P_0, P_1, \ldots, P_n$ к уравнениям добавляют нормировочное условие $P_0 + P_1 + \ldots + P_n = 1$.

Для решения системы дифференциальных уравнений предлагается следующее программное обеспечение Matlab [3], Mathcad [4], наиболее просто и наглядно данные расчеты производит в визуальной среде Simulink, являющейся дополнением к Matlab. Пример графического отображения результата расчетов имеет следующий вид (рис. 2).

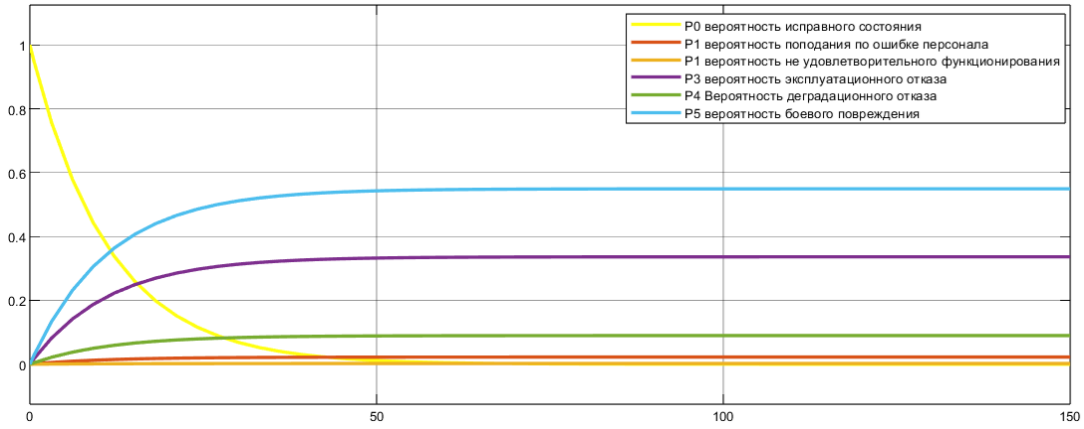


Рис. 2. График зависимости вероятности состояния от времени

Итогом моделирование систем с дискретным состоянием и непрерывным временем является возможность нахождения как предельной вероятно-

стей нахождения системы в определенном состоянии, так и конкретных значений в разных временных точках протекающего процесса.

Список используемых источников

1. Сазанов В. В., Паращук И. Б., Логинов В. А., Елизаров В. В. Математическое обеспечение АСУ войсками: Учеб. пособие / Под ред. И. Б. Паращука. СПб.: ВАС, 2018. 256 с.

2. Колмогоров А. Н. Математика XIX века. Чебышевские направления в теории функций. Обыкновенные дифференциальные уравнения. Вариационное исчисление. Теория конечных разностей. М.: Наука, 1987. 318 с.

3. Макаров Е. Инженерные расчеты в Mathcad 15: Учебный курс. СПб.: Питер, 2011. 400 с.

4. Дьяков Д. П. Matlab полный самоучитель. Эл. изд. Саратов: Профобразование, 2017. 768 с.

MODELING OF PROCESSES WITH DISCRETE STATE AND CONTINUOUS TIME USING THE EXAMPLE OF A MODEL OF OCCURRENCE OF FAILURES AND COMBAT DAMAGE TO MILITARY COMMUNICATIONS EQUIPMENT

Kosyrev A.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Modeling processes with a discrete state and continuous time is a methodological approach used to analyze dynamic systems capable of residing in a finite number of discrete states, with transitions between these states occurring at random points in time. These processes are formalized through Markov processes or continuous-time Markov chains, where the future state of the system depends solely on the current state and does not depend on the background (Markov property). This approach is widely used to study stochastic systems in various fields such as queuing theory, reliability theory, bioinformatics, and others.

This article examines a model of failures and combat damage of military communications equipment, which allows calculating the probability of certain types of events, whether it is failure or combat damage. The goal is achieved by modeling the processes of failures and combat damage based on the compilation and solution of Kolmogorov differential equations of states.

Key words: *failure and damage model, failure, damage, differential equations*

УДК 621.391
ГРНТИ 49.33.29

ВАРИАНТ ФОРМИРОВАНИЯ ОРТОГОНАЛЬНЫХ СИГНАЛОВ ДЛЯ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

С. С. Манаенко, В. В. Сазонов, Альбадр Х. Б., К. А. Луконин

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

В современных системах связи специального назначения непрерывно решается задача по повышению помехоустойчивости. Повышение помехоустойчивости всегда связано со снижением энергии используемых сигналов. Вариантом решения данной задачи является использование ортогональных сигналов с изменяющейся структурой. В статье разработан алгоритм формирования ортогональных сигналов с известными и новыми структурами, обладающими заданными энергетическими, структурными, информационными, временными и пространственными характеристиками. Использование разработанного варианта формирования ортогональных сигналов в системах связи специального назначения позволит повысить ее помехоустойчивость.

ансамбль дискретных ортогональных в усиленном смысле сигналов, собственные вектора бидиагональной эрмитовой матрицы

Одним из свойств систем связи (СС) специального назначения (СН) является помехоустойчивость, характеризующая ее способность обеспечивать связь с требуемым качеством в условиях воздействия на нее всех видов помех, включая, в первую очередь, преднамеренные помехи. В работе [1] доказано, что применение ансамблей дискретных ортогональных в усиленном смысле сигналов (АДОУСС) способствует созданию, оптимальной СС СН. Следовательно, для обеспечения требуемой помехоустойчивости СС СН, одним из эффективных способов является использование в ней АДОУСС.

Однако, для обеспечения высокой помехоустойчивости, необходимо решать задачу повышения скрытности АДОУСС, включающую в себя энергетическую, структурную, информационную, временную и пространственную составляющие.

Использование ортогональных сигналов с заданными энергетическими, структурными, информационными, временными и пространственными характеристиками позволит повысить помехоустойчивость СС СН.

Однако количество известных АДОУСС и подходы к упорядоченному изменению сформированных структур ограничивает помехоустойчивость проектируемых СС СН [1].

Целью статьи является разработать алгоритм формирования АДОУСС для помехоустойчивых СС СН с требуемыми энергетическими, структурными, информационными, временными и пространственными характеристиками.

Рассмотрим первую составляющую скрытности – энергетическую скрытность СС СН. Известно [2–4], что энергетическая скрытность направлена на существенное затруднение обнаружения сигналов СС СН разведывательным приемником. Использование в СС СН сигналов с «большой» базой ($B >> 1$) позволит увеличить энергетическую скрытность. При этом для многочастотных и фазоманипулированных сигналов [5] базу сигнала (B) можно полагать равной размерности сигнала (N). Таким образом, чем больше размерность АДОУСС (N), тем больше энергетическая скрытность СС СН.

Рассмотрим вторую составляющую скрытности – структурную скрытность СС СН, при условии, что сигнал обнаружен разведывательным приемником. Известно [2, 3], что раскрытие структуры сигнала, разведывательным приемником, осуществляется сопоставление обнаруженного сигнала с одним из множества наиболее похожих структур известных сигналов. Таким образом, чем больше число степеней свободы, которыми обладает АДОУСС тем больше структурная скрытность СС СН.

Рассмотрим третью составляющую скрытности – информационную скрытность СС СН, при условии, что уже разведывательным приемником вскрыта структура принимаемого сигнала. Известно [2, 3], что информационная скрытность СС СН определяет способность противостоять мерам, направленным на раскрытие смысла передаваемого сообщения разведывательным приемником. Раскрытие передаваемого сообщения означает отождествление его с той информацией, которая передавалось. Следовательно, чем больше число вариантов сопоставления АДОУСС с информацией, которая передавалась, тем больше информационная скрытность СС СН.

Рассмотрим четвертую составляющую скрытности – временную скрытность СС СН. Известно [3], что временная скрытность СС СН определяет способность противостоять мерам, направленным на раскрытие временных режимов работы (тактико-технических характеристик, порядок смены используемых режимов работы) разведывательным приемником. В результате, чем больше разветвлений в алгоритме формирования АДОУСС, тем больше временная скрытность СС СН.

Рассмотрим пятую составляющую скрытности – пространственную скрытность СС СН, как и другие виды скрытности, является условным событием и зависит от параметров используемых сигналов (направление прихода, мощности) и может быть оценена радиусом зоны, в пределах которой может находиться разведывательный приемник. В итоге, чем ближе к разведывательному приемнику, тем необходимо активней использовать приемы, повышающие скрытность.

При этом, помимо повышения характеристик скрытности, необходимо выполнение требований к используемым сигналам по спектральным и корреляционным характеристикам.

Как следствие этого, для достижения поставленной цели необходимо изменить алгоритм формирования АДОУСС [1], построенный на основе свойств собственных векторов бидиагональной эрмитовой матрицы (БЭМ):

$$Q = \begin{vmatrix} 0 & q_{1,2}e^{j\varphi_{1,2}} & 0 & . & 0 & 0 \\ q_{2,1}e^{j\varphi^{*}_{2,1}} & 0 & q_{2,3}e^{j\varphi_{2,3}} & . & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & 0 & q_{M-1,N}e^{j\varphi_{M-1,N}} \\ 0 & 0 & 0 & . & q_{M,N-1}e^{j\varphi^{*}_{M,N-1}} & 0 \end{vmatrix} \quad (1)$$

где $q_{M-1,N} = q_{M,N-1}$ – модули, а $\phi_{M-1,N} = \phi^{*}_{M,N-1}$ – комплексно-сопряженные аргументы коэффициентов.

Собственные вектора БЭМ построчно описывают структуру АДОУСС вида:

$$X = \begin{vmatrix} a_{11}e^{j\psi_{1,1}} & a_{12}e^{j\psi_{1,2}} & \dots & a_{1N}e^{j\psi_{1,N}} \\ a_{21}e^{j\psi_{2,1}} & a_{22}e^{j\psi_{2,2}} & \dots & a_{2N}e^{j\psi_{2,N}} \\ . & . & . & . \\ a_{M1}e^{j\psi_{M,1}} & a_{M2}e^{j\psi_{M,2}} & \dots & a_{MN}e^{j\psi_{M,N}} \end{vmatrix}, \quad (2)$$

где $a_{1,N}$- амплитуды и $\psi_{1,N}$- фаза единичных элементов сигналов.

В работе [6] доказано, что на значения амплитуд $a_{1,N}$ влияют модули коэффициентов $q_{M-1,N}$, принимающих α возможных состояний, а на фазы $\psi_{1,N}$ - аргументы $\phi_{M-1,N}$, принимающих β возможных состояний БЭМ (1).

Количество C_N формируемых структур АДОУСС (2) будет напрямую зависеть от значений α и β, состояний диагональных коэффициентов исходной БЭМ (1) и ее размерности N:

$$\mathrm{C}_N = (\alpha \cdot \beta)^{N-1}. \quad (3)$$

Количество возможных вариантов формируемых АДОУСС при использовании вышеизложенного математического аппарата (1÷3) показан в таблице 1.

ТАБЛИЦА 1. Количество формируемых АДОУСС

Размерность АДОУСС	Количество состояний коэффициентов БЭМ							
	$\alpha = 1$				$\alpha = 2$			
	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$	$\beta = 1$	$\beta = 2$	$\beta = 3$	$\beta = 4$
N=4	1	8	27	64	8	64	216	512
N=8	1	128	$2{,}187\cdot10^{3}$	$1{,}638\cdot10^{4}$	128	$1{,}638\cdot10^{4}$	$2{,}799\cdot10^{5}$	$2{,}097\cdot10^{6}$
N=16	1	$3{,}277\cdot10^{4}$	$1{,}435\cdot10^{7}$	$1{,}074\cdot10^{9}$	$3{,}277\cdot10^{4}$	$1{,}074\cdot10^{9}$	$4{,}702\cdot10^{11}$	$3{,}518\cdot10^{13}$
N=32	1	$2{,}147\cdot10^{9}$	$6{,}177\cdot10^{14}$	$4{,}612\cdot10^{18}$	$2{,}147\cdot10^{9}$	$4{,}612\cdot10^{18}$	$1{,}326\cdot10^{24}$	$9{,}904\cdot10^{27}$
N=64	1	$9{,}223\cdot10^{18}$	$1{,}145\cdot10^{30}$	$8{,}507\cdot10^{37}$	$9{,}223\cdot10^{18}$	$8{,}507\cdot10^{37}$	$1{,}056\cdot10^{49}$	$7{,}846\cdot10^{56}$

Из анализа таблицы 1 следует, что при росте размерности N исходной БЭМ Q (1), количество C_N возможных формируемых структур АДОУСС (2) возрастает по экспоненциальному закону, при этом скорость возрастания напрямую зависит от числа возможных состояний $\alpha \cup \beta$ диагональных коэффициентов $q_{k-1,k}$ и $\psi_{k-1,k}$, что в свою очередь способствует увеличению скрытности СС СН.

Целенаправленно изменяя размерность (N), значения модулей (α), значения аргументов (β) БЭМ (1) на выходе алгоритма, будут получены требуемые характеристики при формировании АДОУСС:

$$З_N = \{з_{N,1}, з_{N,2}, з_{N,3}, з_{N,4}, з_{N,5}\}^T,$$

где $з_{N,1}$ – требования к энергетическим характеристикам сигналов, $з_{N,2}$ – требования к структуре сигналов, $з_{N,3}$ – требования к информативности принимаемых сигналов, $з_{N,4}$- требования к порядку смены параметров сигналов, $з_{N,5}$ – требования к сигналам относительно близости к разведывательному приемнику.

Вводя размерность N, модули $q_{M-1,N}$ и аргументы $\phi_{M-1,N}$ БЭМ (1), используя операторы формирования (расчета собственных векторов), перемешивания, характеристик и контроля можно сформировать АДОУСС (2) с заданными характеристиками. Алгоритм формирования АДОУСС для СС СН с требуемыми характеристиками скрытности показан на рис. 1.

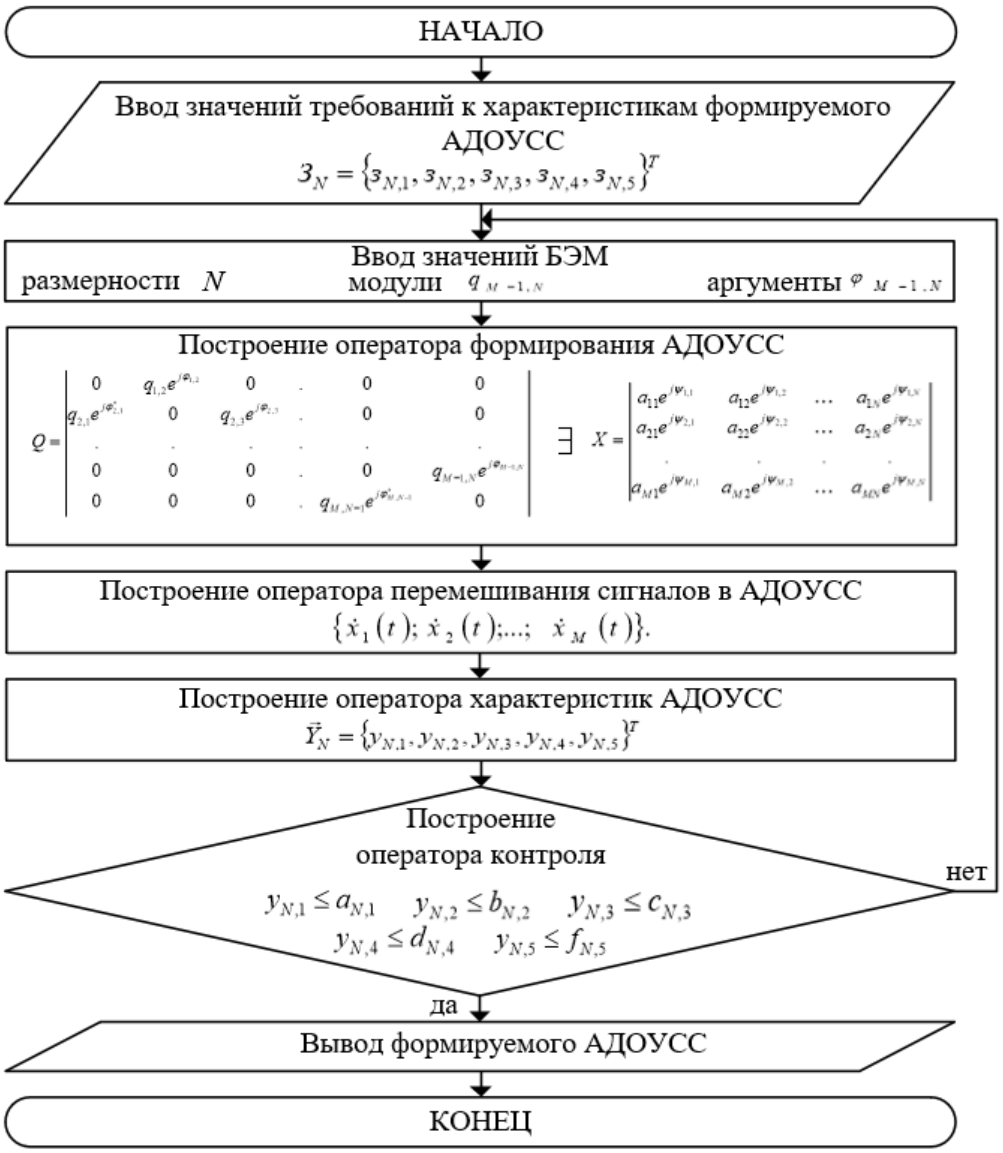


Рис. 1. Алгоритм формирования АДОУСС для СС СН
с требуемыми характеристиками скрытности

Следует также отметить, что с использованием математического аппарата [1] и алгоритма (рис. 1) можно получать не только новые, но и известные ансамбли дискретных ортогональных сигналов (Уолша, Варакина, Стифлера, D-коды), используя только одно состояние модулей ($\alpha = 1$) и два состояния аргументов ($\beta = 2$) исходной БЭМ (количественная оценка вариантов структур представлена в таблица 1). Например, для размерности БЭМ $N = 4$, модулей $q_{1,2} = 1000$, $q_{2,3} = 1$, $q_{3,4} = 1000$ и аргументов $\phi_{M-1,N}$ принимающих два значения $0 \cap \pi$ можно получить 8 структур АДОУСС как показано на рис. 2.

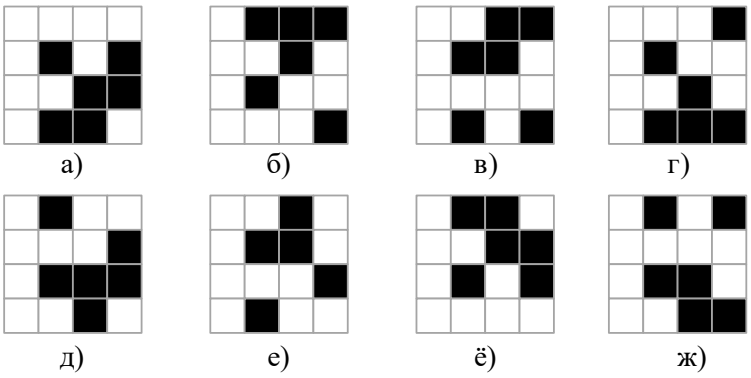


Рис. 2 Построчные структуры (□ – 0, ■ – π) АДОУСС для СС СН
а) $\phi_{1,2} = 0,\ \phi_{2,3} = 0,\ \phi_{3,4} = 0$, б) $\phi_{1,2} = \pi,\ \phi_{2,3} = 0,\ \phi_{3,4} = 0$,
в) $\phi_{1,2} = 0,\ \phi_{2,3} = \pi,\ \phi_{3,4} = 0$, г) $\phi_{1,2} = 0,\ \phi_{2,3} = 0,\ \phi_{3,4} = \pi$,
д) $\phi_{1,2} = \pi,\ \phi_{2,3} = \pi,\ \phi_{3,4} = 0$, е) $\phi_{1,2} = 0,\ \phi_{2,3} = \pi,\ \phi_{3,4} = \pi$,
е) $\phi_{1,2} = \pi,\ \phi_{2,3} = 0,\ \phi_{3,4} = \pi$, ж) $\phi_{1,2} = \pi,\ \phi_{2,3} = \pi,\ \phi_{3,4} = \pi$

Следовательно, разработанный алгоритм формирования АДОУСС, может найти свое применение в СС СН предъявляющие повышенные требования к помехоустойчивости.

Список используемых источников

1. Пашинцев В. П. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн: / В. П. Пашинцев, О. П. Малофей, А. П. Жук, М. В. Самус, Д. В. Гайчук, В. В. Сазонов. М.: Физматлит. 2010. 264 с.

2. Жук А. П., Студеникин А. В., Жук Е. П. Алгоритм и устройство формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов // Системы управления, связи и безопасности. 2020. №3. С. 1-21.

3. Помехозащищенность радиосистем со сложными сигналами / Г. И. Тузов, В. А. Сивов, В. И. Прытков и др. Под ред. Г. И. Тузова. М.: Радио и связь, 1985. 264 с.

4. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: Свое издательство, 2013. 166 с.: ил.

5. Варакин Л. Е. Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с.

6. Жук А. П., Сазонов В. В. Влияние коэффициентов второй диагонали эрмитовой матрицы на корреляционные и спектральные свойства определяемых ею ортогональных в усиленном смысле сигналов / Физика волновых процессов и радиотехнические системы. / Периодический теоретический и научно-практический журнал Самара, 2007. Том 10, № 6. С. 52-55.

ORTHOGONAL SIGNAL CONDITIONING OPTION FOR A SPECIAL-PURPOSE COMMUNICATIONS SYSTEM

Manaenko C., Sazonov V., Albadr H., Lukonin K.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

In modern special-purpose communication systems, the task of improving noise immunity is continuously being addressed. Improving immunity is always associated with reduction of energy of used signals. A variant of solving this problem is the use of orthogonal signals with changing structure. In the article developed an algorithm for the formation of orthogonal signals with known and new structures possessing the specified energy, structural, information, temporal and spatial characteristics. The use of the developed variant of orthogonal signals formation in special-purpose communication systems will increase its noise immunity.

Key words: *ensemble of discrete orthogonal signals in the amplified sense, eigenvectors of the bidiagonal Hermite matrix*

УДК 621.396.4
ГРНТИ 50.37.03

АВТОНОМНАЯ НАВИГАЦИЯ БПЛА С ФУНКЦИЕЙ ИЗБЕГАНИЯ ПРЕПЯТСТВИЙ И ПЛАНИРОВАНИЯ ТРАЕКТОРИИ НА ОСНОВЕ МАШИННОГО ЗРЕНИЯ

А. И. Попов, М. Р. Семкина, Э. Ф. Тухбатуллина

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

Разработка беспилотных летательных аппаратов становится все актуальнее из-за повышения требований к военным системам. В статье представлен метод автономной навигации с визуальным сопровождением для БПЛА. Используется карта для планирования маршрута, и бортовая камера для восприятия окружающей среды. Для предотвращения столкновений предложен метод обнаружения препятствий на основе оптического потока. Управление осуществляется одноплатным компьютером, а алгоритмы работают в режиме онлайн и реального времени.

беспилотный летательный аппарат, планирование траектории, облет препятствий, компьютерное зрение

В последние годы разработка и применение беспилотных летательных аппаратов (БПЛА) становится более полномасштабной. Последние несколько десятилетий беспилотные летательные аппараты использовались для военных и гражданских операций, таких как воздушная инспекция и моделирование местности. Благодаря достижениям в области связи, управления и вычислительных технологий, а также снижению стоимости аппаратного обеспечения, отрасль приложила значительные усилия для создания незаменимого инструмента в нашей повседневной жизни. Благодаря интеграции с инерциальным измерительным блоком, GPS и другими датчиками, реализация автономного полета становится возможной, но все еще требует дальнейших исследований [1].

В областях исследований робототехники автономная навигация обычно включает в себя возможности планирования траектории и обхода препятствий. Одна из важных задач заключается в обеспечении оптимального маршрута для безопасного движения. Путевые точки при планировании маршрута используются для управления курсом беспилотного летательного аппарата. Как правило, траектории полета планируются в автономном режиме с помощью географической информационной системы (ГИС).

В данной статье исследуется автономная навигация беспилотного летательного аппарата квадрокоптерного типа в реальных условиях.

При планировании маршрута на основе карты до начала автономной навигации основной целью является предотвращение столкновений во время полета. Это особенно важно при полете на малой высоте с препятствиями, не указанными на картах, такими как деревья, светофоры и движущиеся объекты [2].

В этом исследовании интегрируется онлайн-схема обхода препятствий и автономная схема планирования траектории для автономного управления полетом. Используется метод автономного наведения на основе карты, чтобы сгенерировать начальный маршрут, применяя алгоритм быстрого поиска случайного дерева. Затем используются путевые точки сгенерированного маршрута для управления полетом. Во время навигации бортовая камера эксплуатируется для получения последовательности изображений для построения поля оптического потока и обнаружения препятствий, как показано на рисунке 1. Она обеспечивает логическую связь между движением квадрокоптера и возникающими препятствиями для навигации. Для повышения надежности подхода используется несколько методов машинного обучения. Предложенные алгоритмы реализованы на одноплатном компьютере для обработки данных в режиме реального времени.



Рис. 1. Метод обхода препятствий на основе зрения с использованием оптического потока

Система обхода препятствий

Алгоритм работы, предлагаемого метода обхода препятствий, показан на рис. 2. Он состоит из нескольких этапов, начиная с получения изображения, предварительной обработки, расчета оптического потока, обнаружения препятствий и принятия окончательного решения.

На этапе предварительной обработки полученная последовательность изображений сначала обрабатывается с пониженной дискретизацией, чтобы уменьшить вычислительную нагрузку на последующих этапах обработки.

Затем изображения преобразуются в оттенки серого и выполняется фильтрация по Гауссу для удаления шума.



Рис. 2. Системная блок-схема предлагаемого алгоритма обхода препятствий

Для обнаружения изменений в изображении обычно используются методы оптического потока, который заключается в использовании последовательности изображений для идентификации векторов движения, вызванных относительным изменением между камерой и окружающей средой. В этой работе применяется метод плотного оптического потока для расчета динамических изменений в местности [3].

Для получения наилучшего результата необходимо объединить методы анализа движения потенциальных препятствий с методом оптического потока [3], изображения которого получены с камеры непрерывно и могут рассматриваться как функция времени: *I(t)*. Яркость пикселя *(x, y)* в момент времени *t* может быть выражена через *I(x, y, t)*. То есть изображение обрабатывается в зависимости от времени и местоположения. Диапазон яркости – это интенсивность пикселей на изображении.

Проекция точки 3D-сцены на изображении рассчитывается в разные моменты времени, в то время как значение яркости пикселя изображения в последовательности изображений фиксируется одна и та же пространственная точка. Учитывая, что пиксель находится в позиции *(x, y)* в момент вре-

мени *t*, предполагается, что он перемещается в позицию *(x + dx, y + dy)dt* в момент времени *t + dt*. Поскольку яркость остается прежней, используется выражение 1 оптического потока:

$$I(x + dx, y + dy, t + dt) = I(x, y, t) \quad (1)$$

Информация, получаемая из поля оптического потока, представляет собой соотношение между скоростью и глубиной, а не абсолютное расстояние. Когда камера продвигается, наиболее близкие области имеют большие векторы движения. Когда БПЛА движется вперед, поле оптического потока может быть нестабильным, например, при изменении направления движения в навигационных точках. В таких случаях может срабатывать ложная тревога о препятствии. Чтобы решить эту проблему, одним из способов является игнорирование или компенсация векторов оптического потока, вызванных неожиданным движением камеры или тряской.

Поскольку поле оптического потока представляет различные направления движения, вызванные перемещениями камеры и объектов на местности, можно выделить независимые области движения, связанные с объектами, путем сегментации изображения. Чтобы проверить, относится ли область из поля зрения оптического потока к препятствию, выполняется ряд операций.

Во-первых, если векторы движения превышают заданный порог более чем на 70 % поля оптического потока, это рассматривается как результат дрожания камеры, и текущий кадр изображения отбрасывается. Затем данные бортового inertial measurement unit (IMU) – инерциального измерительного блока используются для проверки состояния дрона. Если боковое движение задается управляющей командой, вычисление оптического потока компенсируется с использованием этих данных.

Во-вторых, в большинстве случаев препятствия на переднем плане будут неподвижны, смешаны с фоном. Для решения этой проблемы используется процесс кластеризации [4]. В реализации применяется плавающее окно для объединения векторов движения со сравнимыми величинами.

В-третьих, чтобы сделать алгоритм обхода препятствий более надежным с точки зрения определенных угроз в различных ситуациях, БПЛА будет поворачивать в противоположную сторону от препятствия до тех пор, пока траектория движения не будет свободной от препятствия. В этом случае используются левые и правые повороты, а также управление подъемом.

Автономная навигационная система

Алгоритм обхода препятствий интегрирован с технологией планирования траектории для создания автономной навигационной системы. Как показано на рисунке 3, он состоит из трех подсистем для автономного полета: (1) система наведения, (2) навигационная система и (3) система управления [5].

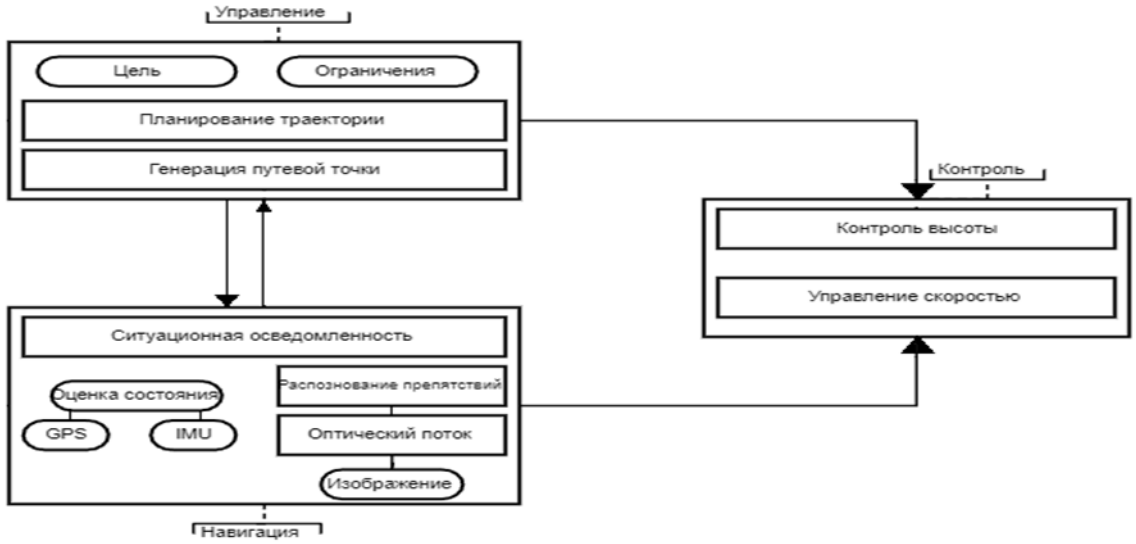


Рис. 3. Схема автономной навигационной системы

Планирование траектории предназначено для управления полетом, автономной навигации и управления движением. Его можно разделить на два типа: статическое и динамическое планирование.

Динамическое планирование заключается в интеграции алгоритма обхода препятствий и создании нового маршрута к месту назначения.

Статическое планирование маршрута выполняется в автономном режиме с учетом особенностей рельефа местности и возможностей БПЛА. Целью является определение оптимальной навигационной траектории на основе картографической информации, обеспечивая безопасность полета БПЛА. Планирование предварительного маршрута включает в себя указание пункта назначения, путевых точек и навигационных ограничений, таких как высота и время полета. Большие объекты, такие как здания, моделируются в виртуальной среде для планирования маршрута, с использованием координат GPS.

Таким образом, результатом планирования маршрута является набор путевых точек для навигации БПЛА. Когда дрон достигнет путевой точки, следующая путевая точка будет использоваться для того, чтобы направить его на следующий шаг к месту назначения.

Результат планирования траектории затем преобразуется в среду 3D-модель, созданную в соответствии с реальной местностью.

В данной работе представлена автономная система управления полетом квадрокоптера с визуальным сопровождением. Она включает в себя планирование траектории и методы обхода препятствий в режиме реального времени. Такой алгоритм позволяет обнаруживать встречные препятствия и направлять квадрокоптер в нужном направлении. Предлагаемые алгоритмы разработаны для встроенной платформы с целью обеспечения возможности оперативной обработки данных. В текущей системе не учитывалось наличие движущихся препятствий. Другие подходы, которые используют анализ изображений и видеопотока с БПЛА, также вызывают интерес и будут рассмотрены в следующих работах и исследованиях.

Список используемых источников

1. Беспилотные летательные аппараты. Основы устройства и функционирования. / П. П. Афанасьев, И. С. Голубев, В. Н. Новиков, С. Г. Парафесь, М. Д. Пестов, И. К. Туркин / Под редакцией И. С. Голубева и И. К. Туркина. Изд. второе, переработанное и дополненное. М., 2008. 656 с.: ил.

2. Алешин Б. С. и др. Ориентация и навигация подвижных объектов: современные информационные технологии / Б. С. Алешин, А. А. Афонин, К. К. Веремеенко, Б. В. Кошелев, В. Е. Плеханов, В. А. Тихонов, А. В. Тювин, Е. П. Федосеев; под ред. Б. С. Алешина, К. К. Веремеенко, А. И. Черноморского // М.: Изд-во Физматлит, 2006. 422 с.

3. Домненко В. М., Бурсов М. В., Иванова Т. В. Моделирование формирования оптического изображения. Учебное пособие. СПб: НИУ ИТМО, 2011. 141 с.

4. Марков Л. С. Теоретико-методологические основы кластерного подхода. Новосибирск: ИЭОПП СО РАН, 2015. 300 с.

Ведерников, Ю. В. Основы теории структурной оптимизации систем контроля и управления беспилотными летательными аппаратами: учеб. пособие. 2-е изд. / Ю. В. Ведерников. Санкт-Петербург: Политехника, 2022. 367 с.: ил.

AUTONOMOUS UAV NAVIGATION WITH OBSTACLE AVOIDANCE AND TRAJECTORY PLANNING BASED ON MACHINE VISION

Popov A., Semkina M., Tukhbatullina E.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The development of unmanned aerial vehicles (UAVs) is becoming increasingly relevant due to the increasing demands on military systems. The article presents a method of autonomous navigation with visual guidance for UAVs. A map is used to plan the route, and an onboard camera is used to perceive the environment. A method for detecting obstacles based on optical flow is proposed to prevent collisions. The control is carried out by a single-board computer, and the algorithms work online and in real time.

Key words: *unmanned aerial vehicle, trajectory planning, obstacle avoidance, computer vision*

УДК 621.396.4
ГРНТИ 50.37.03

НАВИГАЦИЯ ДРОНОВ НА ОСНОВЕ ТЕХНОЛОГИИ БПЛА-РПС С ИСПОЛЬЗОВАНИЕМ РЕГИОНОВ И ПРИГРАНИЧНЫХ ЗОН

А. И. Попов, М. Р. Семкина, Э. Ф. Тухбатуллина

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

БПЛА выполняют различные функции, включая доставку и наблюдение. Они способны ориентироваться в сложных условиях и справляться с динамичными объектами. Для автоматизации управления предлагается новая стратегия обработки данных на основе глубокой сверточной нейронной сети для навигации БПЛА. Новая сверточная нейронная сеть на основе дрона с разделением преобразованием-слиянием областей и ребер использует сверточные блоки для анализа областей и границ, что помогает различать цели и фон в перегруженной среде. Модель генерирует угол поворота и вероятность столкновения для упрощения управления движением дронов.

дрон, сверточная нейронная сеть, разделение преобразование-слияние

БПЛА (беспилотные летательные аппараты) – одна из наиболее значимых дисциплин в области новейших технологий, при этом автономные дроны являются ключевым объектом изучения. Автономный полет, также называемый сампилотированием, означает способность беспилотника совершать воздушные перемещения без помощи человека. Беспилотники, управляемые человеком, сталкиваются со многими функциональными и эксплуатационными проблемами. Важной открытой проблемой в робототехнике является безопасная и надежная внешняя навигация автономных систем. Автономный дрон должен не только работать, избегая столкновений, но и безопасно взаимодействовать с другими дронами в окружающей среде. Для решения таких задач используется двухэтапный процесс с использованием традиционных подходов, который включает в себя автоматизированную локализацию на заданной карте (с использованием визуального, GPS или/и любого другого датчика дальности) и ручное управление дронами, чтобы избежать помех при достижении к своей цели [1], [2]. БПЛА, эффективно летающий по местности, должен следить за маршрутом и реагировать на опасные препятствия так же, как это сделал бы любой другой наземный пилотируемый аппарат. Архитектура БПЛА-РПС (дрона с разделением преобразованием-слиянием областей и ребер) совместима с

размерами карты объектов и позволяет создавать многоклассовые задачи, изменяя начальный и конечный слои.

CHC с глубоким усилением канала для автономии беспилотника

Точный анализ изображений в реальном времени в изменяющейся среде сложен из-за следующих факторов: низкая контрастность между границами переднего плана и фона, высокая вариабельность текстуры, значительные различия в размере, форме и положении переднего плана на изображениях и слабая освещенность. Кроме того, эти снимки сильно искажены из-за изменения уровня шума в окружающей среде. В этой работе описывается подход к автоматизации беспилотных летательных аппаратов на основе глубокой сверточной нейронной сети (CHC). Предложенный подход используется для прогнозирования угла поворота и вероятности столкновения.

В этом контексте разрабатывается новый классификатор CHC, основанный на инновационной технологии БПЛА-РПС [3], которая включает в себя повторные процедуры определения угла поворота и вероятности столкновения. Процесс навигации дрона показан на рис. 1.

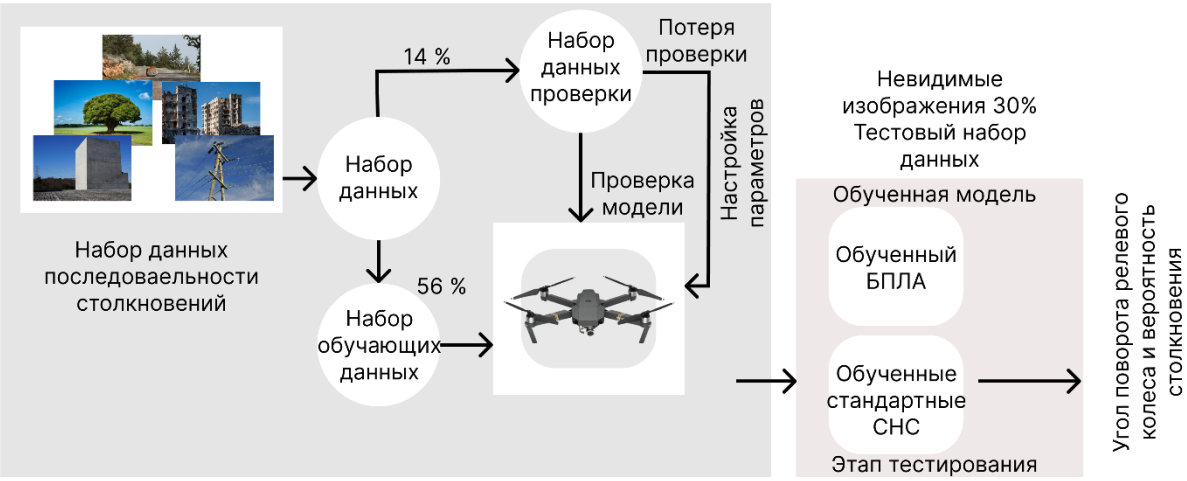


Рис. 1. Распределение набора данных для БПЛА-РПС

Предлагаемые CHC-системы БПЛА-РПС обладают широкими возможностями поиска закономерностей, поэтому они так широко используются при обработке изображений [4]. Благодаря возможности автоматического выделения признаков, CHC превзошел традиционные алгоритмы машинного обучения в задачах визуального наблюдения. Он использует метод свертки для использования структурной информации изображения и динамически извлекает иерархии объектов в зависимости от предполагаемого

применения. Чтобы исследовать проблему переднего плана в БПЛА-РПС, были разработаны и внедрены уникальные блоки свертки, основанные на методах разделения преобразования-слияния (РПС). Впервые был разработан отдельный блок, который последовательно выполняет операции на основе областей и регионов в каждой ветви, чтобы получить полный набор свойств на многих уровнях, особенно тех, которые связаны с однородностью областей, изменениями текстуры и границами фона.

БПЛА-РПС создает уникальные блоки свертки на основе РПС для решения проблемы "задний план-передний план". Предлагаемый блок состоит из четырех функциональных блоков. Принцип выделения признаков на основе областей и регионов тщательно применяется в каждом ответвлении, с объединением максимальных и средних значений, а также сверткой и повторной активацией для получения детализированных отличительных признаков. Чтобы извлечь шаблоны из набора данных изображений, БПЛА-РПС разделяет входные данные на четыре ветви, использует оператор для изучения вариаций, характерных для конкретного региона, и их четких границ, а затем использует операцию конкатенации для объединения выходных данных из множества путей. БПЛА-РПС извлекает набор функций абстрактного уровня, последовательно соединяя два блока РПС с идентичной топологией. В конце процесса используется отключение, за которым следует активация и два полностью соединенных параллельных уровня для прогнозирования угла поворота рулевого колеса и расчета вероятности столкновения с другим дроном.

Данные о транспортном средстве на изображениях сильно различаются, поэтому для отличного распознавания необходим мощный канал СНС. С помощью усиления канала [5] улучшена способность распознавания предлагаемого БПЛА-РПС. В нем предложена концепция усиления канала для решения сложных задач. Извлечение значимых характеристик из искаженных изображений стало возможным благодаря среднему сглаживанию содержимого изображения внутри записанных искаженных изображений. Операции с областями и регионами помогают управлять однородностью и сглаживанием областей, а также систематическим использованием ресурсов внутри данного блока. Это помогает определить отличительные характеристики границ или регионов.

Модели СНС обучаются и оцениваются с использованием метода несогласованной перекрестной проверки. Набор данных был разделен на три части: обучающий набор, набор для проверки и набор для тестирования. Для

оценки модели был использован тестовый набор, который отличался от наборов данных для обучения и валидации.

С помощью выходных сигналов БПЛА получает команду лететь со скоростью движения вперед, равной v_k, и углом поворота θ_k. Сеть использует вероятность столкновения для регулирования скорости движения вперед: когда вероятность столкновения равна нулю, транспортным средствам дается команда двигаться с максимальной скоростью, т.е. V_{max}, и они останавливаются, когда вероятность столкновения близка к 1. Скорость движения вперед фильтруется с помощью фильтра нижних частот ($1 > \alpha > 0$), как показано в выражении 1.

$$v_k = (1 - a)v_{k-1} + a(1 - p_t)V_{max} \quad (1)$$

Аналогичным образом, прогнозируемый угол поворота рулевого колеса также преобразуется в угол рыскания (поворот вокруг оси z). Мы преобразуем s_k из диапазона [-1, 1] в требуемый угол рыскания θ_k в диапазоне $[\frac{-\pi}{2}; \frac{\pi}{2}]$ и фильтруем его с помощью нижних частот, как показано в выражении 2.

$$\theta_k = (1 - \beta)\theta_{k-1} + \beta(\frac{\pi}{2})s_k \quad (2)$$

Данная стратегия динамической навигации разработана для начинающих, которая позволит точно управлять дроном с помощью всего лишь одной камеры переднего обзора. Преимущество этого метода заключается в том, что он позволяет рассчитать вероятность столкновения, используя одно изображение, без предварительного знания скорости платформы.

Дроны могут сталкиваться с различными трудностями при навигации в нестабильных и высокодинамичных средах. В этой статье представлена новая архитектура под названием БПЛА-РПС, которая позволяет безопасно управлять дроном на местности. Эта архитектура основана на концепции разделения, преобразования-слияния. Причина высокой производительности БПЛА-РПС заключается в том, что он позволяет лучше улавливать изменения текстуры и выделять характерные черты. Кроме того, выполняются операции с областями и обеспечивается однородность региона, что помогает беспилотнику различать фоновую и переднюю поверхность в сложных сценариях. Такую модель было бы полезно использовать в операциях, связанных с навигацией, таких как доставка по воздуху.

Список используемых источников

1. Слияние нескольких датчиков для надежного автономного полета в помещениях и на открытом воздухе с помощью винтокрылого аппарата/ С. Шен, Ю. Мулгаонкар, Н. Майкл и В. Кумар - в сборнике Робот. Авто, май 2014 г. С. 4974-4981.
2. Хаметов Р. С. Автономная система навигации и ориентирования беспилотных летательных аппаратов для полетов в городе: задачи и требования функционирования / Р. С. Хаметов, Я. А. Темник, П. Е. Шведов, В. К. Исламов. Текст: непосредственный // Молодой ученый. 2018. № 45 (231). С. 37-42.
3. Варламов А. С. Перспективы развития систем и средств комплексов с беспилотными летательными аппаратами / А. С. Варламов, А. В. Седых, Д. С. Бачурин. Текст: непосредственный // Молодой ученый. 2023. № 47 (494). С. 25-27.
4. Фостер Д. Генеративное глубокое обучение. Творческий потенциал нейронных сетей. СПб.: Питер, 2020. 336 с.: ил. (Серия «Бестселлеры O'Reilly»).
5. Вакуленко С. А., Жихарева А. А. Практический курс по нейронным сетям. СПб: Университет ИТМО, 2018. 71 с.
6. Ростовцев В. С. Искусственные нейронные сети: учебник / В. С. Ростовцев. Киров: Изд-во ВятГУ, 2014. 208 с. Э4743
7. Шолле Ф. Глубокое обучение на Python. 2-е межд. издание. СПб.: Питер, 2023. 576 с.: ил. (Серия «Библиотека программиста»).
8. Гафаров Ф. М. Искусственные нейронные сети и приложения: учеб. пособие / Ф. М. Гафаров, А. Ф. Галимянов. Казань: Изд-во Казан. ун-та, 2018. 121 с.
9. Ковалев М. А. Беспилотные летательные аппараты вертикального взлета: сборка, настройка и программирование: учебное пособие / М. А. Ковалев, Д. Н. Овакимян. Самара: Издательство Самарского университета, 2023. 96 с.

DRONE NAVIGATION BASED ON UAV-RPS TECHNOLOGY, USING REGIONS AND BORDER ZONES

Popov A., Semkina M., Tukhbatullina E.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

UAVs (unmanned aerial vehicles) perform various functions, including delivery and surveillance. They are able to navigate in difficult conditions and cope with dynamic objects. To automate control, a new data processing strategy based on a deep convolutional neural network (SNN) for UAV navigation is proposed. A new convolutional neural network based on a drone with separation transformation-fusion of regions and edges (UAV-RPS) uses convolutional blocks to analyze regions and boundaries, which helps to distinguish between targets and background in an overloaded environment. The model generates the angle of rotation and the probability of collision to simplify drone movement control.

Key words: *drone, convolutional neural network, split transform-merge*

УДК 623.626
ГРНТИ 78.25.41

МЕТОДИКА ОЦЕНКИ КОМПЛЕКСА РАДИОЭЛЕКТРОННОГО ПОДАВЛЕНИЯ ПО ВОЗМОЖНОСТИ ВЕДЕНИЯ РАДИОРАЗВЕДКИ

А. К. Сагдеев, Д. С. Самаркин, И. Н. Алехин, Н. С. Новиков

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

Предварительным этапом радиоэлектронного подавления является проведение радиоразведки, причем, на чем большую дальность ведется радиоразведка, чем выше пропускная способность приемного тракта и выше вероятность разведки за заданное время, тем эффективнее будет осуществляться радиоэлектронное подавление.

радиоразведка, радиоэлектронное подавление

При выполнении оперативно-тактических расчетов эффективность подсистемы радиоразведки комплекса радиоэлектронного подавления (РЭП) целесообразно оценивать с использованием следующих ключевых показателей [1]:

– пропускной способностью $П_{рр}$(средним временем $\bar{T}$, необходимым для обнаружения источников радиоизлучения (ИРИ) в заданной полосе частот и изменения их параметров с качеством не ниже $P_{тр}$);
– вероятностью $P(M, \Delta T)$ разведки не менее заданного количества M ИРИ за интервал времени ΔT, выделенного на разведку;
– размерами рабочих зон пеленгования.

Так как, размеры рабочих зон пеленгования определяются исходя из тактико-технических характеристик средств радиоразведки и заранее могут быть определены, исходя из аппаратной документации, целесообразно будет рассмотреть методику определения пропускной способности подсистемы радиоразведки комплексов РЭП и методику определения вероятности разведки не менее заданного количества ИРИ за выделенное время [2].

Методика определения пропускной способности подсистемы радиоразведки комплексов РЭП

Физическая модель поиска и обнаружения, которая лежит в основе методики, состоит в следующем.

Приемнику разведки выделен участок диапазона поиска от Φ_{min} до Φ_{max} шириной $\Delta\Phi = \Phi_{max} - \Phi_{min}$. Весь участок разбит на интервалы, ширина которых соответствует полосе пропускания приемника разведки ΔF, при этом количество таких интервалов в выделенной полосе частот $N = \Delta\Phi/\Delta F$.

Имеются априорные сведения о загруженности частотного диапазона, выраженные коэффициентом загрузки частотного диапазона Kf, а для работающих радиолиний из этого участка известна априорная вероятность работы ИРИ заданной радиолинии P_R, численно выраженная отношением суммарного времени излучения ИРИ на этой частоте ко времени существования радиолинии. Приемник осуществляет поиск в панорамном режиме, перестраиваясь по участку со скоростью γ. При этом уровень сигнала ИРИ в точке приема зависит от многих факторов и, в частности, от тактическо-технических характеристик средств связи и характера распространения радиоволн, а действующее значение напряжения сигнал на входе преселектора разведприемника может быть найдено как $U_c = E_c * h_\partial$, где E_c – напряженность поля сигнала в точке приема, рассчитываемое по известным методикам, h_∂ – действующая длина антенны (например, для штыревой антенны $h_\partial = \frac{\lambda}{2\pi}\ \mathrm{tg}\frac{\pi h}{\lambda}$, где h – геометрическая длина антенны, λ – длинна волны сигнала ИРИ). Уровень шума определяется как электромагнитной обстановкой, так и внутренними шумами приемника и аппроксимируется действующим значением напряжения $U_{\text{ш}}$, пересчитанным к входу приемника (действующим на входе преселектора). Примем, что приемник линейный, т.е. отношение $q = U_c/U_{\text{ш}}$ при прохождении трактов основной селекции не изменяется.

Процесс энергетического обнаружения при перестройке приемника эквивалент обнаружению со сниженным значение q при работе на фиксированной частоте. Используя формулу Шеннона, можно показать, что

$$q_y = \begin{cases} \sqrt{(1+q^2)^R}\ 1, \text{где } R = \frac{\gamma}{\Delta F^2}\ \text{при}\ \frac{\Delta F}{\gamma}\ \tau_{\text{кор}} \\ q,\ \text{иначе} \end{cases}.$$

В существующих панорамных приемников разведки снижением отношения С/Ш практически можно пренебречь.

На изменение параметров обнаруженного сигнала ИРИ затрачивается среднее время τ_0 и обнаружение сигнала осуществляется по критерию Неймана-Пирсона [3]. При этом задается вероятность ошибочных обнаружений ИРИ (остановок поиска на шумовых всплесках – ложной тревоги) $P_{\text{лт}}$, ис-

ходя из которой, определяется уровень порога энергетического обнаружителя z_0.

Таким образом, дано:

– полоса частот, в которых ведется разведка $\Delta\Phi_{min}, \Delta\Phi_{max},\ \Delta\Phi = \Phi_{max} - \Phi_{min}$;
– ширина полосы пропускания приемника разведки ΔF;
– скорость перестройки панорамного приемника γ;
– время, необходимое для обнаружения и измерения параметров одного сигнала τ_0;
– априорная вероятность работы РЭС в одном частотном канале приемника P_R;
– коэффициент загрузки частотного диапазона Kf;
– вероятность ложной тревоги $P_{\text{лт}}$;
– требуемая вероятность разведки ИРИ $P_{\text{тр}}$.

Решение:

1. Определяют вероятность разведки любого ИРИ за один обзор выделенной полосы частот [4]:

$$P_{\text{р1}} = P_R * P_{\text{эо}} * P_{\text{изм}}, \quad (1)$$

где $P_{\text{эо}}$ – вероятность энергетического обнаружения сигнала при заданной вероятности ложной тревоги, которая для случая обнаружения детерминированных сигналов имеет вид:

$$P_{\text{эо}} = \int_{z_0}^{\infty} W(q)dq = 1 - \Phi\left[\frac{z_0}{q} - q\right],$$

$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(\frac{-t^2}{2}\right)dt$ – интеграл вероятности.

$P_{\text{изм}}$ – вероятность правильного измерения пеленга на ИРИ и определения его параметров, условная по факту обнаружения сигнала. На основе экспериментальных данных:

$$P_{\text{изм}} = exp\left[-3 * \left(\frac{U_{\text{ч}}^2}{U_{\text{с}}^2}\right)\right],$$

где $U_{\text{ч}}$ – чувствительность разведприемника.

2. Определяют требуемое количество обзоров выделенной полосы частот n для достижения заданной вероятности разведки ИРИ $P_{\text{тр}}$:

$$n = \frac{ln(1-P_{\text{тр}})}{ln(1-P_{\text{р1}})}. \quad (2)$$

3. Находят среднюю длительность однократного обзора выделенной полосы частот $\Delta\Phi$:

$$\bar{T}_1 = \frac{\Delta\Phi}{\Delta F} * P_{p1} * Kf + \frac{\Delta\Phi}{\Delta F} * \left(1 - Kf * P_{\text{р1}}\right) * \frac{\Delta F}{\gamma} = \\ = \frac{\Delta\Phi}{\Delta F}\left[P_{\text{р1}} * Kf * \left[\tau_0 - \frac{\Delta F}{\gamma}\right] + \frac{\Delta F}{\gamma}\right] \quad (3)$$

4. Определяют среднее время, необходимое для обнаружения ИРИ с требуемым качеством:

$$\bar{T} = n * \bar{T}_1 \quad (4)$$

И пропускную способность подсистемы разведки

$$\Pi_{\text{рр}} = \frac{Kf * P_{\text{тр}} * \frac{\Delta\Phi}{\Delta F}}{\bar{T}} \quad (5)$$

Методика определения вероятности разведки не менее заданного количества ИРИ за выделенное время

В условиях описанной выше модели ИРИ последовательность решения состоит в следующем:

1. Определяют количество обзоров выделенной полосы частот, произведенных приемником за определенный интервал времени ΔT, выделенный для ведения разведки:

$$k = \frac{\Delta T}{T_1}. \quad (6)$$

2. Определяют вероятность разведки любого ИРИ из заданного участка частот за время ΔT:

$$P_{\text{рк}} = 1 - (1 - P_{\text{р1}})^k, \quad (7)$$

где P_{p1} определено в соответствии с (1).

3. При допущении независимости работы ИРИ в своих каналах вероятность обнаружения m ИРИ за k просмотров выделенной полосы частот определяется выражением:

$$P(m, \Delta T) = C^m_{[Kf*N]} * P^m_{\text{рк}} * \left(1 - P_{\text{рк}}\right)^{[Kf*N]-m} \approx \\ \approx \frac{1}{\sqrt{2\pi * N * Kf * P_{\text{рк}} * \left(1 - P_{\text{рк}}\right)}} * e^{\frac{-(m - N*Kf*P_{\text{рк}})^2}{2*N*Kf*P_{\text{рк}}*\left(1-P_{\text{рк}}\right)}}, \quad (8)$$

где $C^m_{[Kf*N]}$ – количество сочетаний из $[Kf * N]$ по m – биноминальные коэффициенты [5].

4. Искомую вероятность разведки не менее M ИРИ за интервал времени ΔT находят как:

$$P(M, \Delta T) = 1 - \sum_{m=0}^{M-1} P(m, \Delta T) \quad (9)$$

Методика оценки дальности радиоразведки

Дальность разведки зависит от следующих факторов:

мощность передатчиков РЭС и характеристик применяемых противником антенно-фидерных систем (АФС);

условий распространения радиоволн;

характеристик приемных устройств и АФС средств разведки и определяется требуемым качеством разведки $P_{\text{тр}}$.

Применительно к УКВ диапазону на основании формулы Веденского дальность разведки ИРИ будет равна:

$$D_{\text{р}\,P_{\text{тр}}}(\text{км}) = \frac{0{,}047 * \sqrt[4]{P_c(\text{кВт}) * Gc * \left(h_0^2(\text{м}) + h_1^2(\text{м})\right) * \left(h_0^2(\text{м}) + h_2^2(\text{м})\right)}}{\sqrt{U_c(\text{в}) * \frac{\lambda(\text{м})}{h_{\partial}(\text{м})}}}, \quad (10)$$

где P_c – излучаемая мощность сигнала;

Gc – коэффициент усиления передающей антенны;

h_1, h_2 – высота подъема передающей и приемной антенны над поверхностью земли;

h_0 – минимальная эффективная высота антенны ($h_0 \approx 2 \div 4$м при вертикальной поляризации и $f_0 = 50$ МГц; $h_0 \leq 0.5$ м при горизонтальной поляризации и $f_0 = 50$ МГц), но не превысит пределов прямой видимости:

$$D_{\text{р}\,P_{\text{тр}}} = 0.5 * \lambda * \sqrt[4]{\frac{P_c * Gc * Gp * (\varepsilon^2 + (60 * \lambda * \sigma)^2}{Uc^2 / R_{\text{вх}}}}. \quad (11)$$

Выражение (11) справедливо для случая плоской земли:

$$D_{\text{р}}(\text{км}) \leq 20 * \lambda^{\frac{1}{3}}\,(\text{м}).$$

Используя выражения (10, 11), можно определить дальность радиоразведки в УКВ и КВ диапазонах соответственно. При этом вероятность обнаружения и измерения параметров принимаемого сигнала определяется из выражения (1). Следовательно, для обеспечения заданного качества ведения

радиоразведки $P_{тр}$, используя выражения (1, 2), определяются требуемое значение уровня входного сигнала U_c, а выражения (10, 11) позволяют вычислить дальность разведки для данного U_c.

Таким образом, получены основные расчетные соотношения для оценки возможности комплекса РЭП по ведению радиоразведки.

Список используемых источников

1. Кощеев А. В., Лашин Ю. Ф., Сагдеев А. К., Халепа С. Л. Вопросы конфликтологии в системах военного назначения // Научно-практический журнал. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки № 1-2 2022. С. 27-31.

2. Сагдеев А. К., Сидоренко Е. Н., Суюндукова А. А., Тихомиров Д. А. Применение теории игр для исследования радиоэлектронного конфликта // 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. 4. 708 с. С. 518-521.

3. Лукин К. И., Сагдеев А. К., Стахеев И. Г., Титова О. В. Содержательное описание модели конфликта информационно-телекоммуникационных систем специального назначения в киберпространстве // Научно-практический журнал. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки № 06/2 2022. С. 108-112.

4. Глушко А. В., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Методы повышения достоверности распознавания объектов при ведении технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. Р.В. Киричка; сост. А.А. Нестеров. СПб.: СПбГУТ, 2024. Т. 3. 846 с. С. 684-687.

5. Поляков А. А., Сагдеев А. К., Самаркин Д. С., Сидоренко Е. Н., Скрыков И. А. Входные данные для алгоритмической модели системы технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. Р. В. Киричка; сост. А. А. Нестеров. СПб.: СПбГУТ, 2024. Т. 3. 846 с. С. 754-757.

THE METHODOLOGY FOR EVALUATING THE COMPLEX OF ELECTRONIC SUPPRESSION OF THE POSSIBILITY OF CONDUCTING RADIO INTELLIGENCE

Sagdeev A., Samarkin D., Alekhin I., Novikov N.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The preliminary stage of electronic jamming is to conduct radio reconnaissance, and the longer the range of radio reconnaissance, the higher the throughput of the receiving path and the higher the probability of reconnaissance in a given time, the more effective electronic jamming will be.

Key words: *radio intelligence, electronic suppression*

УДК 623.626
ГРНТИ 78.25.41

МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОСТЕЙ КОМПЛЕКСА РЭП ПО РАДИОПОДАВЛЕНИЮ

А. К. Сагдеев, Д. С. Самаркин, И. Н. Алехин, Н. С. Новиков

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

Вероятность энергетической доступности целей радиопомех и вероятность подавления комплексом радиоэлектронного подавления заданного количества целей являются основными показателями методики оценки возможностей комплекса радиоэлектронного подавления по радиоподавлению.

радиоэлектронное подавление, вероятность радиоэлектронного подавления, энергетическая доступность

В оперативно – тактических расчетах при планировании применения комплекса РЭП и ведении радиоподавления (РП) используются следующие информационно – боевые показатели эффективности подсистемы подавления [1]:

– вероятность $P_{\text{энд}}^{Q}$ энергетической доступности (ЭНД) целей радиопомех заданного звена управления при воздействии помехой по Q каналам станции помех с временным уплотнением каналов;
– вероятность подавления комплексом РЭП $P_{\text{обсл}N}$ заданного количества N целей радиопомех;
– дальность подавления линии радиосвязи заданного звена управления Dn с заданным качеством $P_{\text{энд}_{\text{тр}}}$ (зона радиоподавления).

Рассмотрим методику расчета указанных показателей.

Методика определения вероятности энергетической доступности целей радиопомех

Радиоподавление считается эффективным, когда на приемном конце обеспечивается отношение $(Pn/Pc)_{\text{вх}}$, превышающее Kn (Pn – мощность помехи, Pc – мощность сигнала, Kn – коэффициент подавления). Оценка эффективности может производиться на этапе планирования боевого применения комплекса и подготовки предложений командиру для принятия решения и непосредственно в процесс боевой работы [2].

В первом случае при проведении энергетических расчетов есть возможность говорить не о конкретных дистанциях связи и помех Dc и Dn, а только об ожидаемых средних значениях этих величин $\overline{Dc}$ и $\overline{Dn}$ в заданном звене управления. Эта информация добывается путем статистического моделирования боевых действий, для каждого звена управления и системы управления, строятся функции распределения Dc и определяются статистически характеристики m_{Dc} и σ_{Dc}^2 – математическое ожидание и дисперсия случайной величины Dc. Вследствие случайности пространственной конфигурации системы связи и данных о боевых позициях станций помех случайными будут также и Dn. Поэтому на этапе планирования мерой эффективности РП принимают не детерминированную величину – факт повышения $(Pn/Pc)_{\text{вх}} \geq Kn$, а вероятность этого события [3].

Во втором случае, при оценке эффективности РП в процессе боевой работы, мера эффективности определяется исходя из наличия разведывательной информации о целях радиопомех. При известном местоположении корреспондирующих абонентов линии радиосвязи (а следовательно, известных Dc и Dn) оценивают $(Pn/Pc)_{\text{вх}}$ и сравнивают с порогом Kn. При неизвестном местоположении хотя бы одного конца радиолинии, полагают случайной дальность связи Dc, а неизвестном местоположении обоих корреспондентов (но известной оперативно – тактической принадлежности цели, т.е. известных статистических характеристиках целей) – случайной также и Dn, и в этом случае используют вероятностную меру [4].

Существующие станции помех обладают повышенной пропускной способностью за счет временного уплотнения временных каналов. Известно, что в этом случае коэффициент подавления оказывается зависящим от количества Q выделенных на подавление целей помеховых каналов (скважности помехи), причем зависимость эта более существенная для аналоговых видов передач (так, для ЧТ сигнала при $Q = 4$ – непрерывное излучение - $Kn \approx 1{,}1$ а при $Q = 1$ – скважность равна четырем – $Kn \approx 2$, в то время как для ЧМ сигнала при $Q = 4$ $Kn \approx 1{,}5$, а при $Q = 1$ $Kn \approx 24$). Поэтому при энергетических расчетах мы будем учитывать это обстоятельство, используя обозначение Kn^Q для различных значений Q.

Уравнение радиоподавления для случая прицельной по частоте и поляризации помехи и равных КПД антенно-фидерных систем передатчиков связи и помех (с учетом замечания о Q) запишется в виде:

$$\left(\frac{Pn}{Pc}\right)_{\text{вх}} = \frac{GnPnGnptmnDc^2Vn}{GcPcGnptmcDn^2Vc} \geq Kn^Q, \quad (1)$$

где Gn, Gc – коэффициент усиления передающей антенны передатчиков помехи и сигнала соответственно;

Pn, Pc – мощность, подводимая к излучающей антенне передатчиков помехи и сигнала соответственно;

$Gnptmn, Gnptmc$ – коэффициент усиления антенны подавляемого приемника в направление передатчиков помехи и сигнала соответственно;

Vn, Vc – множитель ослабления на трассе распространения помехи и сигнала.

Отношение множителей ослабления в КВ диапазоне для наземных станций помех с учетом допущения об идентичности подстилающей поверхности на трассах сигнала и помех при распространении радиоволн земной волной $\frac{Vn}{Vc} \approx \frac{Dc^2}{Dn^2}$ (при соблюдении условия $Dc, n_{[\text{км}]} \leq 20\lambda^{\frac{1}{3}}_{[\text{м}]}$). В УКВ диапазоне $\frac{Vn}{Vc} \approx \frac{Dc^2 * hn^2}{Dn^2 * hc^2}$, где hn, hc – высота поднятия антенн передатчиков помехи и сигнала соответственно (при соблюдении условия $\frac{18h_{\text{прм}}h_{n,c[\text{м}]}}{\lambda_{[\text{м}]} * 10^3} \leq Dn, c_{[\text{км}]} \leq 4.12\left(\sqrt{h_{\text{прм}[\text{м}]}} + \sqrt{h_{n,c[\text{м}]}}\right)$).

Случайный характер $(Pn/Pc)_{\text{вх}}$ обусловлен случайностью отношения Dc/Dn, поэтому преобразуем (1) к виду (подставив выражение для Vn/Vc):

$$\frac{Dc}{Dn} \geq C(Q) \text{ где } C(Q) = \begin{cases} \left[\frac{Kn^Q PcGnptmcGc}{PnGnptmnGn}\right]^{\frac{1}{4}} \text{ для КВ} \\ \left[\frac{Kn^Q PcGnptmcGchc^2}{PnGnptmnGnhn^2}\right]^{\frac{1}{4}} \text{ для УКВ} \end{cases}, \quad (2)$$

а также заметим, что в этом случае:

$$P\text{энд}^Q = P\left\{\left(\frac{Pn}{Pc}\right)_{\text{вх}} \geq Kn^Q\right\} = P\left\{\frac{Dc}{Dn} \geq C(Q)\right\} = P\{Dc \geq C(Q) * Dn\} = \\ = P\{Dn * C(Q) - Dc \leq 0\}, \quad (3)$$

т.е. вероятность превышения отношением мощностей помехи и сигнала на входе подавляемого приемника коэффициента подавления будет равна вероятности того, что случайная величина $z = Dn * C(Q) - Dc$ не превзойдет нуля.

Таким образом, при оценке ЭНД цели радиопомех имеем три случая:

1. Известны Dc, Dn и $C(Q)$;

2. Известен коэффициент $C(Q)$;

3. Известны Dn и $C(Q)$.

В первом случае решение очевидно: $\frac{Dc}{Dn} \leqq C(Q)$.

Во втором случае рассмотрим случайные величины Dn и Dc. С достаточной степенью точности при расчетах можно предположить их независимость, а учитывая многофакторный, равнозначный характер событий, определяющих местоположение целей радиопомех, будем полагать закон распределения Dn и Dc нормальным [5]. Как известно из курса математики, линейная комбинация случайных величин $z = Dn * C(Q) - Dc$, имеющих нормальное распределение, также имеет нормальный закон, параметры которого для нашего случая записываются в виде:

математическое ожидание $m = C(Q) * m_{Dn} - m_{Dc}$, (4)

дисперсия $\sigma_2^2 = C(Q) * \sigma_{Dn}^2 - \sigma_{Dc}^2$, (5)

где m_{D*} и σ_{D*}^2 – математическое ожидание и дисперсия рассматриваемых расстояний.

Для нормального распределения вероятность события $P\{z \leq 0\}$ может быть найдена через интеграл вероятности $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{c} dt$ следующим образом:

$$P_{\text{энд}}^{Q} = 1 - \Phi\left(\frac{m_z}{\sigma_z}\right). \quad (6)$$

При использовании выражения (6) следует учитывать следующие свойства интеграла вероятности:

$$\Phi(-z) = 1 - \Phi(z), \Phi(+\infty) = 1, \Phi(0) = 0.5.$$

В третьем случае учтем, что Dn – величина детерминированная, поэтому $m_{Dn} = Dn, \sigma_{Dn} = 0$ и для оценки вероятности ЭНД можем использовать выражение (1.6) с параметрами:

$$m_z = C(Q) * Dn - m_{Dc}, \sigma_z^2 = \sigma_{Dc}^2. \quad (7)$$

Таким образом, получены исходные выражения для оценки энергетической доступности целей радиопомех [6].

Методика определения вероятности радиоподавления заданного количества целей радиопомех

Оценить количество целей, которое способен подавить комплекс РЭП, возможно, если известны вероятности ЭНД $i-$й конкретной цели $P_{\text{энд}i}^{Qi}$ в режиме ее Q_i канального подавления. При этом естественно, необходимо

учитывать, что при наличии K станций помех исходное число каналов РП $M = K * q$, где q – количество возбудителей в станции данного типа. Эти каналы распределяются (каким-либо образом) по N заданным целям радиопомех, обеспечивая, при этом, вероятность РП $i-$ й цели $P_{\text{энд}i}^{Qi}$. При этом, вероятность РП заданного количества целей для выбранного варианта распределения помеховых каналов может быть рассчитана как

$$P\text{обсл}_N = \frac{1}{N}\sum_{i=1}^{N} P_{\text{энд}i}^{Qi} \quad (8)$$

при условии $\sum_{i=1}^{N} Q_i = M$.

Очевидно, что при $N > M$ тем большее количество целей может быть охвачено помехами, чем меньше каналов будет выделено на каждую цель. Однако увеличение пропускной способности влечет возрастание скважности помехи и, следовательно, возрастает коэффициент подавления Kn^Qи уменьшается вероятность ЭНД $P_{\text{энд}t}^{Q}$. Таким образом, существует оптимальный баланс между количеством обслуживаемых целей и вероятность ЭНД, при котором обеспечивается максимум эффективность комплекса РЭП. Это – задача подсистемы управления – задача оптимизации целераспределения помехового ресурса по заданному количеству целей.

Список используемых источников

1. Кощеев А. В., Лашин Ю. Ф., Сагдеев А. К., Халепа С. Л. Вопросы конфликтологии в системах военного назначения // Научно-практический журнал. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки № 1-2 2022. С. 27-31.

2. Сагдеев А. К., Сидоренко Е. Н., Суюндукова А. А., Тихомиров Д. А. Применение теории игр для исследования радиоэлектронного конфликта // 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. 4. 708 с. С. 518-521.

3. Лукин К. И., Сагдеев А. К., Стахеев И. Г., Титова О. В. Содержательное описание модели конфликта информационно-телекоммуникационных систем специального назначения в киберпространстве // Научно-практический журнал. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки № 06/2 2022. С. 108-112.

4. Лукин К. И., Сагдеев А. К., Стахеев И. Г., Титова О. В. Обоснование использования боевых кибернетических систем в информационном противоборстве // Научно-практический журнал. Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки № 06/2 2022. С. 105-107.

5. Глушко А. В., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Методы повышения достоверности распознавания объектов при ведении технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII

Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. Р.В. Киричка; сост. А.А. Нестеров. СПб.: СПбГУТ, 2024. Т. 3. 846 с. С. 684-687.

6. Поляков А. А., Сагдеев А. К., Самаркин Д. С., Сидоренко Е. Н., Скрыков И. А. Входные данные для алгоритмической модели системы технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. Р.В. Киричка; сост. А.А. Нестеров. СПб.: СПбГУТ, 2024. Т. 3. 846 с. С. 754-757.

METHODOLOGY FOR ASSESSING THE CAPABILITIES OF THE RAP COMPLEX FOR RADIO SUPPRESSION

Sagdeev A., Alekhin I., Novikov N., Samarkin D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The probability of energy availability of radio interference targets and the probability of suppression of a set number of targets by an electronic suppression system are the main indicators of the methodology for assessing the capabilities of an electronic suppression system for radio suppression.

Key words*: electronic suppression, probability of electronic suppression, energy availability*

УДК 621.391
ГРНТИ 49.33.29

ПРЕОБРАЗОВАНИЯ И ПЕРЕДАЧА ДАННЫХ В ТРАКТАХ И КАНАЛАХ СИСТЕМЫ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

В. В. Сазонов

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

Передача данных между хостами нередко требует более высокой надежности, большей скорости и достоверности, что обусловлено невозможностью логического контроля ее человеком в процессе преобразования их в трактах и каналах системы связи. Многообразие технических средств (хостов) используемых при построении системы связи специального назначения характеризуется еще большим количеством возможных вариантов построения трактов и каналов передачи данных. Детальное рассмотрение вариантов преобразования данных в трактах и каналах системы связи специального назначения позволит выполнить возрастающие требования к передаче данных.

данные, хост, преобразование данных, передача данных, тракт передачи данных, система связи специального назначения.

Известно [1], что основное отличие передачи данных от телеграфной и других видов связи заключается в том, что получателем или отправителем данных является хост, а не человек. Передача данных между хостами, нередко требует более высокой надежности, большей скорости и достоверности, что обусловлено невозможностью логического контроля ее человеком в процессе преобразования их в трактах и каналах системы связи.

Многообразие технических средств (хостов), используемых при построении системы связи специального назначения, характеризуется еще большим количеством возможных вариантов построения трактов и каналов передачи данных.

Целью статьи является раскрыть особенности преобразований и передачи данных в трактах и каналах системы связи специального назначения.

Для анализа преобразования и передачи данных в системе связи специального назначения тракт передачи данных удобно представить в виде, как показано на рис. 1. Рассматривая преобразования и передачу данных между двумя хостами 4А и 4Б, тракт и каналы системы связи представим совокупностью блоков сопряжения и распределения блоков данных 3А, 3Б и m ка-

налами передачи данных (6). Каналы передачи данных содержат устройства защиты от ошибок 2А, 2Б и дискретные каналы связи (5). Дискретные каналы связи (5) состоят из устройств преобразования сигналов 1А, 1Б и физических каналов. Взаимодействие между элементами (4А÷4Б) осуществляется через формально определенные логические и (или) физические границы, называемые интерфейсами. Следует отметить, что каждый из элементов (4А÷4Б) поддерживает интерфейсы двух типов.

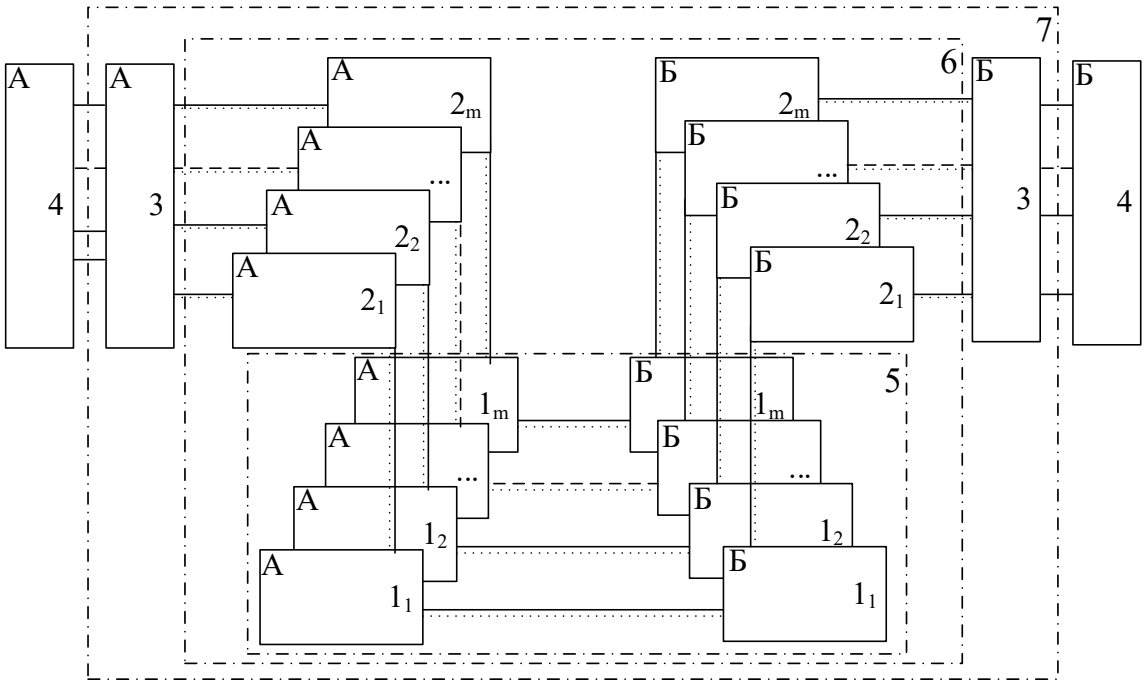


Рис. 1 Структура тракта передачи данных системы связи специального назначения (1_1÷1_m – устройства преобразования сигналов, 2_1÷2_m – устройства защиты от ошибок, 3 – блок сопряжения и распределения, 4 – хост, 5 – дискретные каналы связи, 6 – каналы передачи данных, 7 – тракты передачи данных)

Во-первых, это интерфейсы услуг с выше и нижележащими уровнями «своей» иерархии средств (4А-3А, 3А-2А, 2А-1А; 1Б-2Б, 2Б-3Б, 3Б-4Б), реализация которых может быть, как программной, программно-аппаратной так и аппаратной. Чем ниже по уровню, тем аппаратная составляющая ярче выделена и наоборот, чем выше по уровню, тем больше выделена программная составляющая.

Например, в тракте передачи данных специального назначения на уровне дискретного канала связи, устройства преобразования сигналов (1_1А÷1_mА ∩ 1_1Б÷1_mБ) могут взаимодействовать с физическими каналами через стыки (интерфейс) STM-1, E3, E2, E1, Ethernet, RS-232, RS-485, C1 (C1-ТГ, C1-ТФ, C1-ТЧ, C1-ФЛ) [2, 3].

Во-вторых, это одноранговый интерфейс со средствами взаимодействия другой стороны, расположенными на том же уровне иерархии (4А-4Б, 3А-3Б, 2А-2Б, 1А-1Б). Этот тип интерфейса называют протоколом [4, 5].

Например, в тракте передачи данных специального назначения на уровне канала передачи данных в устройствах защиты от ошибок (2_1А÷2_mА ∩ 2_1Б÷2_mБ) реализуется один из видов помехоустойчивого кодирования для повышения достоверности преобразования и передачи данных.

В основу всех методов обеспечения достоверности преобразования, распределения и передачи данных в трактах и каналах систем связи специального назначения положен принцип совместного использования корректирующих (помехоустойчивых) кодов и системных способов учитывающих наличие или отсутствие каналов обратной связи.

Способ преобразования, распределения и передача данных в трактах и каналах системы связи с точки зрения использования каналов передачи данных при наличии каналов обратной связи может быть реализовано в двух режимах или их комбинациях:

Информационной обратной связи (канал обратной связи используется для передачи принятого блока данных обратно в анализирующее устройство блока сопряжения и распределения данных передающей стороны (3А), которое после сравнения, переданного и принятого блоков принимает решение о повторении ранее переданного блока или о передаче очередного блока полученной от хоста (4А));

Решающей обратной связи (блок сопряжения и распределения данных приемной части (3Б) по сигналам решающего устройства декодера ($2Б_1$÷$2Б_m$) принимает решение о выдаче блока данных в хост получателя (при приеме без ошибок) или их стирании и переспросе).

Способ преобразования, распределения и передачи данных в трактах и каналах системы связи с точки зрения использования каналов передачи данных при отсутствии каналов обратной связи может быть реализовано в трех режимах или их комбинациях:

– параллельная передача блоков данных одновременно по всем m каналам;
– поочередная передача блоков данных по всем m каналам в соответствии с установленным порядком;
– передача блоков данных по одному лучшему из m каналов.

Таким образом, использование корректирующих (помехоустойчивых) кодов, системных способов повышения достоверности, стандартизированных стыков (интерфейсов) при построении цепочек преобразования и пере-

дачи данных в каналах и трактах системы связи специального назначения обеспечит выполнение возрастающих требований к передаче данных.

Список используемых источников

1. Теоретические основы сетей передачи данных военного назначения: Учебник / Под ред. В. В. Вовк и И. Б. Паращука. СПб.: ВАС, 2024. 252 с.

2. Иванов В. Г. Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи / В. Г. Иванов. Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2018. 214 с.

3. Особенности информационно-технического взаимодействия элементов сетей связи и передачи данных специального назначения / В. В. Зубакин, Д. К. Назаров, В. В. Сазонов, А. С. Сальников // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей XII Международной научно-технической и научно-методической конференции: в 4 т., Санкт-Петербург, 28 февраля – 01 2023 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. С. 771-774

4. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. СПб.: Питер, 2020. 1080 с.: ил.

5. Воробьев С. П., Давыдов А. Е., Ефремов В. В., Курносов В. И. Инфокоммуникационные сети: энциклопедия. Том 1: Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологий / Под ред. С. П. Воробьева. Изд. 2-е, перераб. и доп. СПб.: Наукоемкие технологии, 2019. 739 с.

DATA CONVERSION AND TRANSMISSION IN COMMUNICATION SYSTEM PATHS AND CHANNELS SPECIAL PURPOSE

Sazonov V.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Data transmission between hosts, often requires higher reliability, higher speed and reliability, which is due to the impossibility of logical control of its human in the process of their transformation in the paths and channels of the communication system. The variety of technical means (hosts) used in the construction of a special-purpose communication system is characterised by an even greater number of possible options for the construction of paths and channels of data transmission. The detailed consideration of variants of data transformation in paths and channels of the special purpose communication system will allow to fulfil the increasing requirements to data transmission.

Key words: *data, host, data conversion, data transmission, data path, special purpose communication system*

АВТОРЫ СТАТЕЙ

АБРАМЕНКО Георгий Тимофеевич — аспирант кафедры безопасности информационных технологий Национального исследовательского университета ИТМО, gtabramenko@itmo.ru

АВДЕЕВ Максим Сергеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, maxim.avdeev.2001@bk.ru

АГЕЙЧИК Никита Олегович — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ageichik.no@sut.ru

АКИМОВ Сергей Викторович — кандидат технических наук, доцент, и.о. заведующего кафедрой систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, akimov.sv@sut.ru

АКСЕНОВ Кирилл Дмитриевич — генеральный директор ООО «Пространство интеллектуальных решений», научный сотрудник МГТУ им. Н. Э. Баумана, младший научный сотрудник Кубанского государственного технологического университета, axenov.kir@gmail.com

АЛЕХИН Илья Николаевич — студент военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, uvc@sut.ru

АЛЛЕНОВ Денис Сергеевич — начальник группы Департамента информационных систем Министерства обороны российской Федерации, соискатель ученой степени кандидата наук Военной академии связи им. Маршала Советского Союза С. М. Буденного, guritt_23@mil.ru

АЛЛИ Рашид Амидуевич — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alli.ra@sut.ru

АЛЬБАДР Ходр Баракат — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного,khodr.badr@gmail.com

АЛЬОТУМ Юсеф Мохаммед Абд Аллх — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alotum.umaa@sut.ru

АНТОНЮК Евгений Артурович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, evgeniy-antoniuk@rambler.ru

АСТАХОВ Михаил Романович — сотрудник Академии Федеральной службы охраны Российской Федерации, krispykroz@mail.ru

БАБКОВ Иван Николаевич — кандидат технических наук, доцент, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, babkov.in@sut.ru

БАРАНОВ Дмитрий Алексеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, bda@yandex.ru

БЕЛОВ Станислав Михайлович — ассистент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bsm@sut.ru

БЕЛОУС Константин Владимирович — кандидат технических наук, доцент, доцент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bk@sut.ru

БЕСЕДИН Максим Дмитриевич — младший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, vasn2020@mail.ru

БОБРОВСКИЙ Андрей Владимирович — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bobrovskii.av@sut.ru

БОЙКО Игорь Андреевич — ассистент кафедры радиотехники Санкт–Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, boiko.ia@sut.ru

БОЛДЫРЕВ Егор Алексеевич — магистрант группы ФП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, boldyrev.ea@sut.ru

БОРИСОВ Сергей Валерьевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, borisov1.sv@sut.ru

БОРИСОВ Сергей Викторович — кандидат технических наук, доцент, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, borisov.sv@sut.ru

БОЯРИНЦЕВ Александр Игоревич — старший преподаватель кафедры экспериментальной физики Уральского федерального университета им. первого Президента России Б. Н. Ельцина, a.i.boiarintsev@urfu.ru

БУДАРНЫЙ Глеб Сергеевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, budarnyi.gs@sut.ru

БУДКО Павел Александрович — доктор технических наук, профессор, ученый секретарь ПАО «Интелтех», budkopa@inteltech.ru

БУСНЮК Андрей Олегович — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fizika.ffp@sut.ru

ВАГАНОВ Александр Валерьевич — старший преподаватель кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vaganov.av@sut.ru

ВАСИЛЬЕВ Никита Алексеевич — кандидат технических наук, заместитель начальника отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, vasn2020@mail.ru

ВЕРХОВА Галина Викторовна — доктор технических наук, профессор, профессор кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, verkhova.gv@sut.ru

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, ra1alo@mail.ru

ВОЛЫНКИН Павел Александрович — кандидат технических наук, доцент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, volynkin.pa@sut.ru

ВОРОБЬЕВ Павел Владимирович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, gsg.1991@mail.ru

ВТОРЫХ Виталий Станиславович — аспирант кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vtorykh.vs@sut.ru

ВУ Тхе Зует — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vu.tz@sut.ru

ГАВРИЛОВ Илья Вячеславович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, ilya_vch@pisem.net

ГАЛУШКО Иван Витальевич — младший научный сотрудник научно-исследовательского отдела-4 научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, ivan16111999@yandex.ru

ГВОЗДКОВ Игорь Вячеславович — старший преподаватель кафедры систем обработки данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gvozdkov.iv@sut.ru

ГЛУХОВ Николай Иванович — заведующий лабораторией кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glukhov_nikolay@sut.ru

ГЛУШАНКОВ Евгений Иванович — доктор технических наук, профессор кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glushankov.ei@sut.ru

ГЛУШКО Артем Вячеславович — полковник, начальник кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glushko@sut.ru

ГОРБАЧЕВ Павел Николаевич — сотрудник Академии Федеральной службы охраны Российской Федерации, png@acdem.msk.rsnet.ru

ГОРДА Максим Дмитриевич — аспирант Санкт-Петербургского Федерального исследовательского центра Российской академии наук, gordamd@ya.ru

ГРИДНЕВ Василий Александрович — подполковник запаса, преподаватель кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gridnev@sut.ru

ГРУЗДЕВ Дмитрий Анатольевич — начальник учебной части – заместитель начальника кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gruzdev.da@sut.ru

ГУЩИН Илья Сергеевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, gushilya@gmail.com

ДЕМИДОВ Георгий Александрович — студент группы ИКТЗ-16 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, demidov.ga@sut.ru

ДЕРКАЧ Алексей Евгеньевич — адъюнкт кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, alder2000@inbox.ru

ДЕТКОВА Вера Михайловна — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича detkova.vm@sut.ru

ДОЛМАТОВА Ольга Александровна — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, dolmatova.oa@sut.ru

ДРЕПА Владислав Евгеньевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drepa.ve@sut.ru

ЖЕРНОВА Ксения Николаевна — кандидат технических наук, старший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zhernova@comsec.spb.ru

ЗАГОРЕЛЬСКИЙ Владимир Валерьевич — преподаватель цикла фельдъегерско-почтовой связи кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zagorelsky.vv@sut.ru

ЗАДБОЕВ Вадим Александрович — младший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, zadboev89@mail.ru

ЗАЙЦЕВ Дмитрий Александрович — аспирант кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaitsev.da@sut.ru

ЗАЙЦЕВА Зинаида Викторовна — кандидат технических наук, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaitch@sut.ru

ЗЕЛИЧЕНОК Игорь Юрьевич — аспирант, младший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zelichenok@comsec.spb.ru

ЗНОБИЩЕВ Роман Сергеевич — подполковник, начальник цикла проводной электросвязи кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, znomishchev@sut.ru

ИВАНИЩЕВА Елизавета Федоровна — аспирант кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivanisheva.ef@sut.ru

ИВАНОВ Василий Геннадиевич — доктор военных наук, председатель Военно-научного комитета Главного управления связи Вооруженных Сил Российской Федерации, доцент, guritt_23@mil.ru

ИВАНОВ Денис Вадимович — кандидат технических наук, доцент института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого, ivanov_dv@spbstu.ru

ИВАНЦОВ Дмитрий Сергеевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, dima_ivantsov91@mail.ru

ИЗОТОВ Даниил Юрьевич — аспирант кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А Бонч-Бруевича, izotov.du@sut.ru

ИЗРАИЛОВ Константин Евгеньевич — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, konstantin.izrailov@mail.ru

КАЛИНИКИН Никита Алексеевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, xorsst@gmail.com

КИРИКОВ Николай Дмитриевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, taleofmorfey@gmail.com

КИСЕЛЁВ Николай Николаевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kiselev.nn@sut.ru

КОВЦУР Максим Михайлович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kovcur.mm@sut.ru

КОКИН Сергей Алексеевич — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kokin.sa@sut.ru

КОНДРАШОВ Захар Константинович — кандидат физико-математических наук, генеральный директор АО «НИИМА «Прогресс», info@i-progress.tech

КОПАЧЕВ Артем Юрьевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, artemy12121212@mail.ru

КОПЫЛОВ Сергей Александрович — кандидат технических наук, сотрудник Академии Федеральной службы охраны Российской Федерации, gremlin.kop@mail.ru

КОРОВИН Константин Олегович — кандидат физико-математических наук, доцент, заведующий кафедрой радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korovin.ko@sut.ru

КОРОТИН Владимир Евгеньевич — кандидат технических наук, доцент кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korotin.ve@sut.ru

КОСЫРЕВ Александр Вячеславович — кандидат технических наук, адъюнкт кафедры технического обеспечения связи и автоматизации Военной академии связи им. Маршала Советского Союза С. М. Буденного, sashka13rup@mail.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ivkote@comsec.spb.ru

КОТОВ Григорий Андреевич — магистрант группы ФП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kotov.ga@sut.ru

КОЩЕНКО Кристиан Борисович — сотрудник Академии Федеральной службы охраны Российской Федерации, s.kop@acdem.msk.rsnet.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Krasov.AV@sut.ru

КУБАЛОВА Анна Рудольфовна — кандидат технических наук, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kubalova.ar@sut.ru

КУДРЯВЦЕВА Юлия Александровна — младший научный сотрудник научно-исследовательского отдела-4 научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Zhule4ka16@mail.ru

КУЗЕНОВ Сергей Ризабекович — кандидат технических наук, старший преподаватель кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fizika.ffp@sut.ru

КУШНИР Дмитрий Викторович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kushnir.dv@sut.ru

КЮНЕР Андрей Павлович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, kunerandrey@mail.ru

ЛАВРЕНТЬЕВ Владимир Владимирович — аспирант, младший научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, vvlavrentiev@yandex.ru

ЛАНДА
Александр Эдуардович
кандидат технических наук, доцент,
доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, landa.ae@sut.ru

ЛАУТА
Олег Сергеевич
доктор технических наук, доцент, начальник научно-исследовательского Военной академии связи им. Маршала Советского Союза С. М. Буденного, vasn2020@mail.ru

ЛЕВШУН
Дмитрий Сергеевич
кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, levshun.d@iias.spb.su

ЛЕЩИНСКИЙ
Богдан Сергеевич
адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, dnr_1910@mail.ru

ЛИВШИЦ
Александр Иосифович
доктор физико-математических наук, профессор,
профессор кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, livshits@sut.ru

ЛИКАРЬ
Александр Иванович
старший преподаватель кафедры систем обработки данных Санкт-Петербургского политехнического университета Петра Великого, likar_a@mail.ru

ЛИКОНЦЕВ
Алексей Николаевич
кандидат технических наук, доцент кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Likontsev.an@sut.ru

ЛИПАТНИКОВ
Валерий Алексеевич
доктор технических наук, профессор, старший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛУКОНИН
Кирилл Алексеевич
курсант факультета радиосвязи Военной академии связи им. Маршала Советского Союза С. М. Буденного, kirill.lukonin2004@gmail.com

ЛУКЬЯНЕНКО
Дмитрий Иванович
оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, dli99@bk.ru

ЛЮБИМОВ
Александр Геннадьевич
кандидат технических наук, доцент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lyubimov.ag@sut.ru

МАКАРОВ Алексей Алексеевич — магистрант группы ФП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makarov2.aa@sut.ru

МАКАРОВ Леонид Михайлович — кандидат технических наук, доцент кафедры автоматизации и робототехники Санкт Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makarov.lm@sut.ru

МАКОГОН Василий Петрович — доктор технических наук, старший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, mak229@rambler.ru

МАНАЕНКО Сергей Сергеевич — кандидат технических наук, доцент, старший преподаватель кафедры радиосвязи Военной академии связи им. Маршала Советского Союза С. М. Буденного, manaenkoss@mail.ru

МАНЬКО Иван Денисович — аспирант группы ФОА-140011 Уральского федерального университета им. первого Президента России Б. Н. Ельцина, i.d.manko@urfu.ru

МАРЧЕНКОВ Алексей Алексеевич — старший преподаватель цикла фельдъегерско-почтовой связи кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marchenkov.aa@sut.ru

МИХАЙЛОВ Василий Дмитриевич — ассистент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mvd@sut.ru

МИХАЙЛОВ Владимир Павлович — начальник отдела Департамента информационных систем Министерства обороны российской Федерации, соискатель ученой степени кандидата наук Военной академии связи им. Маршала Советского Союза С. М. Буденного, guritt_23@mil.ru

МОРОЗОВ Владислав Олегович — сотрудник Академии Федеральной службы охраны Российской Федерации, mvo@yandex.ru

МУРАЧЕВ Григорий Игоревич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, grigoriy.m99@mail.ru

НАЛИМОВ Константин Георгиевич — аспирант института компьютерных наук и кибербезопасности Санкт-Петербургского политехнического университета Петра Великого, nalimov1984@mail.ru

НЕГУРИЦА Артем Алексеевич — капитан, адъюнкт научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Art_18_02_1995@mail.ru

НИКИТИН Юрий Александрович — кандидат технических наук, старший научный сотрудник, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikitin.ua@sut.ru

НОВИКОВ Никита Сергеевич — студент военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ОСТРОУМОВА Юлия Сергеевна — доктор педагогических наук, доцент, заведующий кафедрой биологической и медицинской физики Военно-медицинской академии им. С. М. Кирова, sinklit@mail.ru

ПАВЛОВ Федор Федорович — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fizika.ffp@sut.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pantuhin.oi@sut.ru

ПАРФЕНОВ Михаил Сергеевич — майор, адъюнкт научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, mikhail.parfenov.88.88@bk.ru

ПЕРЕВОЗНИК Юрий Яковлевич — кандидат педагогических наук, доцент кафедры систем обработки данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, perevoznik.uy@net.sut.ru

ПЕРЕДИСТОВ Евгений Юрьевич — кандидат технических наук, доцент, заведующий кафедрой физики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, peredistov.eu@sut.ru

ПЕРМЯКОВ Андрей Александрович — аспирант кафедры систем автоматизации и робототехнки Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, permyakov.aa@sut.ru

ПЕТРИВ Роман Богданович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, petriv@sut.ru

ПОВЗНЕР Александр Александрович — доктор физико-математических наук, профессор кафедры физики Уральского федерального университета им. первого Президента России Б. Н. Ельцина, a.a.povzner@urfu.ru

ПОПОВ Андрей Иванович — кандидат технических наук, доцент кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, Adpopovai@yandex.ru

ПОПОВ Данил Сергеевич — магистрант группы РТ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, popov.ds@sut.ru

ПОПУГАЕВ Даниил Георгиевич — техник кафедры систем автоматизации и робототехники, студент группы ИСТ-261 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pdg@sut.ru

ПРОКОФЬЕВ Павел Александрович — ассистент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, prokofev.pa@sut.ru

РОМАНЮК Полина Романовна — сотрудник Академии Федеральной службы охраны Российской Федерации, s.kop@academ.msk.rsnet.ru

РОЩУПКИНА Полина Анатольевна — сотрудник Академии Федеральной службы охраны Российской Федерации, sda33@academ.msk.rsnet.ru

САГДЕЕВ Александр Константинович — кандидат технических наук, доцент кафедры радиорелейной и тропосферной связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sagdeev@sut.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, ibsaen@comsec.spb.ru

САЗОНОВ Виктор Викторович — кандидат технических наук, доцент, докторант кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, vmktor-sazonov@yandex.ru

САМАРКИН Денис Сергеевич — начальник цикла, старший преподаватель кафедры радиорелейной и тропосферной связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, samarkin@sut.ru

САХАРОВ Дмитрий Владимирович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, saharov.dv@sut.ru

СВЕЧНИКОВ Дмитрий Александрович — кандидат технических наук, доцент, сотрудник Академии Федеральной службы охраны Российской Федерации, sda33@academ.msk.rsnet.ru

СЕДЫШЕВ Эрнест Юрьевич — кандидат технических наук, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sedyshev.eu@sut.ru

СЕМКИНА Маргарита Руслановна — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, semkinamargarita931@gmail.com

СИМОНИНА Ольга Александровна — кандидат технических наук, доцент, доцент кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, olga.simonina@sut.ru

СИТДИКОВ Дмитрий Сергеевич — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, dima.sitdikov.99@mail.ru

СКОРЫХ Марк Андреевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skorykh.ma@sut.ru

СЛЕДЕВСКИЙ Константин Николаевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, sledevskiykn@mail.ru

СЛЁТОВ Максим Алексеевич — студент группы N4255c Санкт-Петербургского национального исследовательского института ИТМО, sletovo@mail.ru

СМИРНОВ Сергей Николаевич — доктор технических наук, профессор кафедры защиты информации Московского государственного технического университета им. Н. Э. Баумана, mr.nikkis@mail.ru

СМОЛЬЯНИНОВ Алексей Сергеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, sda33@academ.msk.rsnet.ru

СОЛДАТЕНКО Ярослав Геннадьевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, sokoltyp@gmail.com

СПИЦИН Олег Леонтьевич — кандидат военных наук, старший преподаватель кафедры Военной академии связи им. Маршала Советского Союза С. М. Буденного, mzsp@bk.ru

СТАХЕЕВ Иван Геннадиевич — кандидат технических наук, доцент, заведующий базовой кафедрой специальных средств связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича / Ведущий научный специалист ОАО «Супертел» staheev.ig@sut.ru

СУДЕНКОВА Анастасия Вячеславовна — студент группы РТ-11 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича

ТАКШЕЕВ Артем Дмитриевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, artyom.taksheev@gmail.com

ТАРАСЕНКО Станислав Евгеньевич — младший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, s.tar.my@mail.ru

ТИТКОВ Илья Евгеньевич — старший оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, ilyatitkov25@gmail.com

ТКАЧЕВ Дмитрий Федорович — подполковник, кандидат технических наук, начальник научно-исследовательского отдела-3 Военной академии связи им. Маршала Советского Союза С. М. Буденного, dimas.portnoy@inbox.ru

ТКАЧЁВ Михаил Андреевич — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного

ТРУХМАНОВ Игорь Романович — оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, truhmanovigor@yandex.ru

ТУХБАТУЛЛИНА Эвелина Фанилевна — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, Tuxbatullina2003@mail.ru

УРВАНЦЕВА Наталья Львовна — кандидат технических наук, доцент, доцент кафедры физики Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, urvanceva.nl@sut.ru

УШАКОВ Игорь Александрович — кандидат технических наук, доцент, и. о. заведующего кафедрой информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakov.ia@sut.ru

ФАМ Конг Куен — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fam.kk@sut.ru

ФЕДОРОВ Павел Николаевич — кандидат технических наук, старший научный сотрудник научно-исследовательского отдела-4 научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Fedorovpn1@yandex.ru

ФЕДОРОВ Сергей Игоревич — ассистент, инженер, аспирант кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fedorov1.si@sut.ru

ФУКАЛОВ Владислав Александрович — Оператор научной роты Военной академии связи им. Маршала Советского Союза С. М. Буденного, vladfukalov@yandex.ru

ХАНИН Самуил Давидович — доктор физико-математических наук, профессор, профессор кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khanin.sd@sut.ru

ХОХЛОВ Константин Олегович — кандидат физико-математических наук, доцент кафедры экспериментальной физики Уральского федерального университета им. первого Президента России Б. Н. Ельцина, k.o.khokhlov@urfu.ru

ХРУЩЕВ Иван Алексеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, hia@yandex.ru

ХУШЕЯ Кусай Ибрагим Махмуд — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, qusai2024@mail.ru

ЧАБАНЕНКО Виктор Вячеславович — главный эксперт группы Департамента информационных систем Министерства обороны Российской Федерации, соискатель ученой степени кандидата наук Военной академии связи им. Маршала Советского Союза С. М. Буденного, guritt_23@mil.ru

ЧЕРКАШИН Артем Игоревич — ассистент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cherkashin.ai@sut.ru

ЧЕРНЫШОВ Александр Сергеевич — аспирант кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chernyshov.as@sut.ru

ЧЕРТОВСКИХ Иван Алексеевич — сотрудник Академии Федеральной службы охраны Российской Федерации, s.kop@academ.msk.rsnet.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент, ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, andreych@bk.ru

ЧУДНОВ Александр Михайлович — доктор технических наук, профессор, профессор кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, chudnow@yandex.ru

ШАБАНОВ Александр Павлович — аспирант кафедры систем автоматизации и робототехники, преподаватель кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aps@sut.ru

ШАРИКОВ Павел Иванович — кандидат технических наук, старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sharikov.pi@sut.ru

ШАРИХИНА Юлия Валерьевна — кандидат физико-математических наук, доцент кафедры физики Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, sharihina.uv@sut.ru

ШАШКИН Владислав Сергеевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shashkin.vs@sut.ru

ШЕВЧЕНКО Александр Александрович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shevchenko.aa@sut.ru

ШЕМЯКИН Сергей Николаевич — кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sehemakin.sn@sut.ru

ШТЕРЕНБЕРГ Станислав Игоревич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shterenberg.si@sut.ru

ШУМАКОВ Павел Петрович — кандидат технических наук, доцент, заведующий кафедрой электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shumackov_pp@sut.ru

ЮЖАКОВА Анна Алексеевна — адъюнкт кафедры технического обеспечения связи и автоматизации Военной академии связи им. Маршала Советского Союза С. М. Буденного, anutikaaa@mail.ru

ЯРОВОЙ Роберт Владимирович — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Nadzar@yandex.ru

65-Я НАУЧНО-ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА, НАУЧНЫХ РАБОТНИКОВ И АСПИРАНТОВ (НТК ППС 2025)

Сборник научных статей
Том 2

Научное издание

Верстка
М. О. Мотыгина
Корректура
Д. Н. Яшугин
Дизайн логотипа Г. И. Юрьев
Подписано в печать 25.06.2025
Объем 35,33 усл.-печ. л.

Объединенная редакция рецензируемых научных изданий СПбГУТ
193232 СПб., пр. Большевиков, 22, корп. 1



СПбГУТ)))