СПбГУТ)))

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

INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT

XIV Международная научно-техническая и научно-методическая конференция

«Актуальные проблемы инфотелекоммуникаций в науке и образовании»

АПИНО ICAIT

25-27 ИЮНЯ 2025

СБОРНИК НАУЧНЫХ СТАТЕЙ

ТОМ 1

APINO.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)

XIV МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ

25-27 июня 2025

Сборник научных статей

Том 1

Инфокоммуникационные сети и системы

Радиоэлектронные системы и робототехника

Информационные технологии и программная инженерия

Кибербезопасность

Сети связи специального назначения

Инновации для Арктики

СПб ГУТ)))

Санкт-Петербург

2025

УДК 001:061.3(082)
ББК 72
А 43

XIV Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2025). Сб. науч. ст. в 2 т. / Под. ред. А. В. Рабина; сост. А. Дзюбаненко, И. М. Татарникова. СПб.: СПбГУТ, 2025. Т. 1. 744 с.

Рецензент – доктор технических наук, профессор, 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, проректор по научной работе СПбГУТ (Россия)

Ответственный секретарь

Дзюбаненко А. А., кандидат технических наук, и. о. начальника управления организации научной работы и подготовки научных кадров 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., кандидат технических наук, доцент, первый проректор – проректор по учебной работе

Ответственный секретарь

Татарникова И. М., шеф-редактор Объединенной редакции рецензируемых научных изданий

Члены организационного комитета

Зайцев А. И., проректор по цифровой трансформации и административной работе

Дружков К. В., кандидат экономических наук, директор департамента экономики и финансов

Бобровский В. И., доктор технических наук, доцент, и.о. директора НИИ «Технологии связи»

Ивасишин С. И., кандидат технических наук, 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

Михеева В. А., заместитель начальника управления – начальник отдела рекламы

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

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

ISBN 978-5-89160-380-6 (Том 1)
ISBN 978-5-89160-379-0

© СПбГУТ, 2025

СОДЕРЖАНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ 11

Степанов А. Б. О развертывании гибридной сети связи в рамках Третьей Арктической технологической экспедиции СПбГУТ по побережью моря Лаптевых 11

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ 17

Абрамова Н. И., Лящук М. З. Требования автоматизированной системы управления к передаче информации 17

Авакян С. А., Бабанов З. Д., Кукунин Д. С., Максименко С. О. Система удаленного доступа к программируемым устройствам на базе микроконтроллеров: архитектура и результаты анализа 22

Антропова Л. А., Марочкина А. В., Санникова П. А. Предсказание инфаркта миокарда на основе федеративного обучения с использованием распределенных медицинских данных 27

Бабанов З. Д., Кукунин Д. С., Максименко С. О. Оптимизация RAID-систем с использованием кодирования Коши-Рида-Соломона и резистивной памяти с произвольным доступом 33

Багаев Е. С. Оценка точности первичных дальномерных измерений в БЛС IEEE 802.11az. Модели многолучевого радиоканала 39

Бадасян А. Н., Дементьев М. Е., Марочкина А. В., Юрьева А. С. Архитектурные основы Apache Kafka и пошаговое руководство по запуску 45

Бадасян А. Н., Дементьев М. Е., Марочкина А. В., Юрьева А. С. Архитектура и принципы работы REDIS: анализ однопоточной модели и механизмов кластеризации 50

Березина Ю. С., Перелыгин С. В. Светодиодные экраны и их элементы 57

Березкин А. А., Козлова А. И., Ченский А. А. Алгоритм оценки качества кадров FPV-видеопотока 63

Бурумбаев Д. И., Стремедловский А. В., Чупина В. А. К проблеме формирования исследовательской компетенции будущих инженеров 69

Бучатский А. Н., Лосев А. П. Математические методы преобразования и обработки информации в видеопоследовательностях на примере метрики расстояния Фреше 75

Васильев Н. А., Лещинский Б. С., Ситдиков Д. С. Проблемы сетевой архитектуры в эпоху двойного стека 81

Викулов А. С., Скоробогатова С. А. Исследование нагрузки в беспроводной сети IEEE 802.11 на временной площадке 86

Викулов А. С., Скоробогатова С. А. Анализ загрузки временного ресурса радиоканала стандарта IEEE 802.11 в различных условиях 92

Гольдштейн А. Б., Танашев С. Р. Анализ вероятностно-временных характеристик туннелей MPLS OVER QUIC в транспортных сетях B5G 98

Дунайцев Р. А., Светова А. В. Эффективность технологии MU-MIMO 104

Елагин В. С., Чипсанова Е. В. Разгрузка задач Интернета вещей в системах граничных вычислений со множественным доступом 109

Елисеев С. М. RAN SLICING для виртуальных операторов MVNO в сетях 5/6G 115

Задбоев В. А., Татаринов В. И., Ткачев Д. Ф. Организация ложного трафика в HONEYPOT-системах 119

Задбоев В. А., Татаринов В. И., Ткачев Д. Ф. Принципы маскировки заражённых файлов в HONEYPOT-системах 123

Качнов А. В., Прасолов А. А., Туманова Е. И. Исследование характеристик канала акустического трансформатора с учетом многократных переотражений от границ барьера 128

Книгиницкий Е. И., Кукунин Д. С. Построение асинхронного широкополосного канала точка-многоточие 134

Козлов А. А., Чикалов Н. В. К вопросу о синхронизации беспилотных летательных аппаратов и беспилотных транспортных средств, объединенных в единую систему (рой) 139

Корнюшкин Д. А., Крылов А. А. Многоуровневая система качественных данных на основе моделей искусственного интеллекта 145

Новиков Е. В., Шваков А. В. Оптимизация конструкции и технологии изготовления датчиков на основе изгибов оптического волокна на базе 3D моделирования 150

Павловская А. А., Павловский М. В., Фёдоров С. Л. Дипфейки на изображении: генерация, обнаружение и борьба 155

Павловская А. А., Павловский М. В., Фёдоров С. Л. Уменьшение вычислительной сложности моделей распознавания действий человека на изображении 161

Парамонов А. И., Хоанг Ф. Н. Анализ проблем масштабируемости в сетях Интернета вещей и стратегии их решения 168

Парамонов А. И., Хоанг Ф. Н. Модель гетерогенного Интернета вещей: архитектура, ключевые технологии и перспективы развития 174

Рютин К. Е. Оценка производительности и конфигурация проекта OpenWiFi на платформе LibreSDR 182

Рябиков Д. С. Экспериментальная апробация SDR платформы HackRF One в среде GNU Radio Часть 1 188

Рябиков Д. С. Экспериментальная апробация SDR платформы HackRF One в среде GNU Radio Часть 2 195

Семенов А. Б. Метод расчета предельной протяженности кабельного тракта с репитерами PoE 201

Хыа Х. К. Исследование точности первичных дальномерных измерений в сетях LTE в условиях отсутствия прямой видимости 207

Хыа Х. К. Исследование точности первичных дальномерных измерений в сетях LTE в условиях прямой видимости 213

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА 219

Акимов С. В., Верхова Г. В. Моделирование логических и топологических отношений между природно-техногенными геосистемами 219

Акимов С. В., Верхова Г. В. Сценарий установления отношений между агентами в децентрализованной киберфизической среде 223

Алли Р. А. Алгоритм meta-esprit для совместной оценки скорости и угла места целей в допплеровской локации 227

Арсирий А. И. Современные базовые методы исследования и визуализации структур квазикристаллов 233

Берестовский П. А., Воробьев П. В., Татаринов В. И. Особенности аппаратной и программной реализации SDR-модулей в БПЛА 239

Берестовский П. А., Воробьев П. В., Ткачев Д. Ф. Технические средства противодействия БПЛА и дальнейшие перспективы их развития 244

Бикбулатов В. Р., Негурица А. О., Чуднов А. М. Анализ помехоустойчивости приема двоичных псевдослучайных сигналов с использованием Δ-слоя неразличимости в условиях преднамеренных помех и гауссовского шума 248

Бойко И. А., Владыко А. Г., Горобцов И. А., Глушанков Е. И. Методы адаптивной обработки сигналов в гибридных сетях связи 254

Борисов С. В., Ланда А. Э., Остроумова Ю. С., Ханин С. Д., Шумаков П. П. К содержательному наполнению обучения физическим основам электроники 260

Борисов С. В., Ланда А. Э., Остроумова Ю. С., Ханин С. Д., Шумаков П. П. Проблемно-деятельностный подход к обучению физическим основам электроники: предпосылки использования и методико-технологическая разработка 266

Брагина А. Э., Чикалов Н. В. Разработка робототехнической омниплатформы для маневренного перемещения в ограниченном пространстве 272

Брагина А. Э., Чикалов Н. В. Разработка основных электронных узлов беспилотного летательного аппарата 277

Владыко А. Г., Глушанков Е. И., Горобцов И. А., Лялина А. Ж. Методы моделирования непрерывных каналов связи в гибридных сетях связи 282

Волынкин П. А. Модернизация мобильного робота ROBO-PICA элементами искусственного интеллекта 288

Глушанков Е. И., Суденкова А. В. Оценка точности фильтрации радионавигационных параметров 294

Елисеев Н. К. Выбор оптимального свёрточного кодера для решетчатой кодовой модуляции 301

Зайцева З. В. Разработка и создание виртуального лабораторного практикума по исследованию влияния потерь на характеристики реактивных фильтров 307

Зеленцов В. В., Калибабчук А. О. Синтез входного воздействия по требуемому тормозному усилию для моделирования электрогидравлического тормозного механизма 314

Коровин К. О., Межевов П. А. Анализ влияния количества направленных излучателей в кольцевой антенной системе на огибающую диаграммы направленности 320

Любимов А. Г. К вопросу применения процессного подхода к управлению распределенными производствами 324

Негурица А. О., Сазонов В. В. Синтез решающего правила приемника с Δ-слоем неразличимости псевдослучайных сигналов при некогерентном воздействии преднамеренных помех 329

Остроумова Ю. С., Ханин С. Д. Об информативности динамического подхода к анализу и применению транспортных свойств функциональных диэлектрических материалов с неупорядоченный структурой 335

Сидоркович Д. Р. Исследование алгоритмов линейной и нелинейной фильтрации сигналов в гидроакустическом канале связи 341

Сыроветник Д. С. Диаграммообразование антенной решетки в системе координатометрии близкорасположенных источников сигналов для подавления помех 345

Хренов А. А. Исследование влияния количества элементов антенной решетки на алгоритмы адаптации при воздействии мерцающих помех 351

Элентух А. В. Анализ возможности применения двойного экспоненциального распределения для вычисления порога обнаружения сигнала 357

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ 363

Арланцева Ю. А., Вивчарь Р. М., Дулаев Р. А., Зайчиков К. Д., Кульситова К. А., Пачин А. В., Шибаленков К. А. Концепция применения цифровых двойников для повышения эффективности управления спутниковой системой передачи данных 363

Васильев Н. А., Лещинский Б. С., Ситдиков Д. С. Анализ гидроакустических сигналов с помощью методов глубокого обучения 373

Васильев Н. А., Лещинский Б. С., Ситдиков Д. С. Интеграция знаний нейросетевых моделей без доступа к данным 378

Вивчарь Р. М., Гончаров В. А. Методика поиска корневых причин нарушений нормального функционирования гибридной сети 384

Владыко А. Г., Плотников П. В., Тамбовцев Г. И. Сравнительный анализ гибридных вычислительных архитектур в V2X-системах 389

Волошинов Д. В. Принцип Буйневича-Шестакова 394

Громов В. В. GNU COBOL – «мертвый язык» с большими возможностями 400

Громов В. В. «Архитектура информационных систем» как метод борьбы с шаблонами искусственного интеллекта 404

Губин А. Н., Литвинов В. Л., Филиппов Ф. В. Исследование методов распознавания зеленых зон городской инфраструктуры по аэрофотоснимкам 410

Губин А. Н., Литвинов В. Л., Филиппов Ф. В. Методы выявления конфабуляций в процессе инференса больших языковых моделей 416

Губин А. Н., Литвинов В. Л., Филиппов Ф. В. Определение размерности латентного слоя автоэнкодера на основе оценки дивергенции Кульбака-Лейблера 422

Давыдова Е. В., Федотов А. А., Мошак Н. Н. Формализация процесса установления IPSec-туннеля 428

Журавлев В. А. Применение технологий искусственного интеллекта в сельском хозяйстве зарубежных стран 434

Карпенко Д. Е., Курочка Д. Е. Обучение нейросетевой модели машинного зрения RT-DETRv2, для распознования специальной индивидуальной защиты 441

Кваша Н. В., Михайлик Е. А. Сравнение методов управления памятью в JVM с точки зрения производительности и экономики данных 447

Коровкина Е. В., Молоков Д. А. Исследование искусственного интеллекта в обработке больших данных 453

Котлова М. В., Лабковская Р. Я. Исследование проблемы формирования семантического ядра атрибуционных данных предметов в рамках централизованного учета Музейного фонда 457

Котлова М. В., Лабковская Р. Я. Формирование модели распределенной государственной системы учета музейных предметов 462

Лабковская Р. Я. Применение методов искусственного интеллекта для улучшения качества жизни людей с непереносимостью лактозы 467

Малахов В. Е. Сравнительный анализ результатов работы систем синтеза звуковых сигналов 472

Матюхина Т. В., Раковский О. В. Применение мультиагентных систем и искусственного интеллекта для системы контроля учебной деятельности университета 479

Медведев С. А. Два варианта минималистичной аксиоматизации исчисления высказываний 485

Медведев С. А. Использование Railroad-диаграмм для фиксации семантики 491

Медведев С. А. Расширения контекстно-свободных грамматик для описания формальных систем 497

Мошак Н. Н., Эль Сабаяр Шевченко Н. Интеллектуальные подходы к обеспечению QoS в мультисервисной архитектуре 5G 502

Плотников П. В. Анализ подходов к решению минимаксных задач размещения 506

Раковский О. В. Использование методов машинного обучения для выявления и предотвращения распространения фейковых новостей в интернет-пространстве 512

Раковский О. В. Обеспечение информационной безопасности в облачных вычислительных средах с применением искусственного интеллекта 518

Тарасов В. А. Применение элементов интеллектуализации в управлении информационной инфраструктурой 523

КИБЕРБЕЗОПАСНОСТЬ 527

Антонюк Е. А., Чечулин А. А. Применение источников данных матрицы MITRE ATTACK при поиске следов киберпреступлений 527

Билан В. В., Перов Р. А. Анализ уязвимостей в экосистеме беспилотных транспортных средств и предложения по их устранению 532

Билан В. В., Перов Р. А., Шевяков В. Д. Исследование системы управления и выявление слабых мест в управлении автономным транспортным средством 536

Билан В. В., Перов Р. А., Шевяков В. Д. Исследование текущих структур и методов обеспечения безопасности информации в сфере беспилотного транспорта 540

Бучин Д. Д., Лукашенок В. И., Николаева П. А. Методы обеспечения безопасности в системах интернета вещей 545

Ветошев В. О., Горда М. Д. К вопросу об использовании RAG при расследовании инцидентов ИБ 549

Виткова Л. А., Колинко И. П. Обнаружение аномалий в Веб-трафике с помощью моделей искусственного интеллекта 556

Герлинг Е. Ю., Коржик В. И. Стегосистема для видео с улучшенной скрытностью, использующая квантовый компьютер с целью ускорения процедуры вложения 562

Жернова К. Н. Визуализация данных безопасности на географических картах средствами языка Python 570

Жернова К. Н. Подходы к отбору признаков для визуализации данных безопасности 575

Зикратов И. А. Определение класса защищенности автоматизированной системы управления технологическими процессами на основе критерия минимума среднего риска 581

Ковальский И. В., Сычужников В. Б., Уралов М. А. Анализ взаимодействия между блоками в контексте определения угроз для автономных транспортных средств 587

Ковальский И. В., Сычужников В. Б., Уралов М. А. Анализ подходов информационной безопасности в сфере беспилотного транспорта 593

Красов А. В. Испытательная лаборатория вуза как пример отраслевого объекта критической информационной инфраструктуры, функционирующий в сфере науки 597

Красов А. В., Панков А. В., Ушаков И. А. Биометрическая аутентификация и система контроля доступа в сфере услуг телеприсутствия 603

Красов А. В., Ушаков И. А., Штеренберг С. И. Анализ атак типа отравления данных в сфере услуг телеприсутствия 608

Кушнир Д. В., Шемякин С. Н. О поиске невычетов 613

Кюнер А. П., Чечулин А. А. Активные методы сбора информации о мошенниках 618

Липатников В. А., Макаренко Д. В., Шевченко А. А. Механизм моделирования компьютерных атак на объект критической инфраструктуры 625

Лукашенок В. И., Николаева П. А., Таранущенко А. П. Безопасность встроенных сетей в автономных транспортных средствах с помощью протокола toucan 631

Лукашенок В. И., Николаева П. А., Таранущенко А. П. Происхождение уязвимостей и направления атак в области автономных транспортных средств 637

Майоров А. В. Модель представления данных о компьютерных инцидентах в государственных информационных системах 642

Михневич С. Ю., Семенович А. Ю., Тэт Н. Тестирование источника энтропии генератора случайных чисел на светодиоде 647

Панков А. В. Разработка модели данных для обнаружения аномалий в зашифрованном трафике 652

Попов А. А. Использование машинного обучения для эффективного анализа схожести трейсеров стека 658

Садовников В. Е., Саенко И. Б. Анализ эффективности шумовых искажений в защите сверточных нейронных сетей от итеративной состязательной атаки IGSM 663

Штеренберг С. И. Введение нового термина – «Интеллектуальный IDS» в отрасли защищенных систем связи 668

СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ 674

Волостных В. А., Задбоев В. А., Шевченко А. А. О выборе средств криптографической защиты информации 674

Гриднев В. А., Сагдеев А. К. Прелагаемые дополнения к программе подготовки специалистов по специальной связи в военном учебном центре с учетом опыта проведения СВО 680

Иваненко Т. А. Влияние качества учебно-методического обеспечения на мотивацию к занятиям физической культурой у студентов военного учебного центра технического университета 685

Иваненко Т. А. Формирование компетентности преподавателя-методиста как фактор совершенствования учебно-методического обеспечения процесса обучения студентов военного учебного центра 693

ИННОВАЦИИ ДЛЯ АРКТИКИ 699

Запайщиков А. В. О методах анализа сигналов на основе декомпозиции на эмпирические моды 699

Лебедева Н. П., Степанова А. Б. Исследование свойств параарамидных нитей под воздействием эксплуатационных факторов с использованием современного программного обеспечения 705

Степанов А. Б. Особенности построения сети передачи данных в деревне Летняя Золотица Архангельской области с применением УКВ приемопередатчиков АЛИСА-С 710

Степанова А. Б. Использование среды MATLAB для выполнения расчетов при исследовании свойств параарамидных нитей 715

Степанова А. Б. Обзор исследований свойств параарамидных нитей при воздействии низких температур 720

АВТОРЫ СТАТЕЙ 725

ПЛЕНАРНЫЕ ДОКЛАДЫ

УДК 621.39
ГРНТИ 49.13

О РАЗВЕРТЫВАНИИ ГИБРИДНОЙ СЕТИ СВЯЗИ В РАМКАХ ТРЕТЬЕЙ АРКТИЧЕСКОЙ ТЕХНОЛОГИЧЕСКОЙ ЭКСПЕДИЦИИ СПбГУТ ПО ПОБЕРЕЖЬЮ МОРЯ ЛАПТЕВЫХ

А. Б. Степанов

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

В июле 2024 года в пгт. Тикси участниками Третьей Арктической технологической экспедиции СПбГУТ по побережью моря Лаптевых в тестовом режиме была развернута гибридная сеть связи, которая позволила организовать видеоконференцсвязь между данным поселком (Республика Саха (Якутия)), г. Санкт-Петербург, г. Архангельск, г. Смоленск, г. Самара. При этом использовалось преимущественно отечественное оборудование, в том числе разработанное в СПбГУТ. Статья посвящена описанию основных особенностей развертывания данной гибридной сети связи, а также результатов испытания оборудования, включенного в ее состав. В заключении приводятся предлагаемые направления дальнейших исследований в интересах реализации Стратегии развития отрасли связи Российской Федерации на период до 2035 года.

гибридная сеть связи, экспедиция, Арктическая зона Российской Федерации, приемопередатчики, УКВ, КВ, спутниковая связь, автоматический портативный электроэнцефалограф

В декабре 2023 г. была утверждена Стратегия развития отрасли связи Российской Федерации на период до 2035 года [1]. Одной из важнейших задач, обозначенной в документе, является проведение исследований, ориентированных на гибридные сети связи. В связи с этим актуальными могут считаться исследования, направленные на разработку оборудования для гибридных сетей связи, а также их испытание в реальных условиях эксплуатации.

Как известно [2], Арктическая зона Российской Федерации характеризуется суровыми климатическими условиями, малой плотностью населения,

географическим положением на высоких широтах. Все это влияет на особенности организации электросвязи в данных регионах.

Под руководством автора данной работы разработано оборудование, предназначенное для применения в Арктической зоне Российской Федерации [3]. Оно прошло успешное испытание в рамках трех Арктических технологических экспедиций СПбГУТ: в пгт. Диксон (2022 г.), на Онежском полуострове (2023 г.), в пгт. Тикси (2024 г.). Основными задачами данных экспедиций были:

1. Проведение испытаний, ориентированных на ликвидацию цифрового неравенства на территории Крайнего Севера, а также на устойчивое развитие Арктической зоны Российской Федерации.

2. Проведение испытаний оборудования для гибридных сетей связи, развертывание фрагментов подобных сетей связи, а также развертывание в тестовом формате гибридной сети связи федерального уровня, объединяющей отдельные регионы Российской Федерации.

3. Проведение испытаний оборудования для обработки биомедицинских сигналов (автоматического портативного электроэнцефалографа), обработки сейсмических данных и пр.

Также в рамках экспедиций были проведены экологические исследования и съемки документальных фильмов.

Рассмотрим более подробно результаты Третьей Арктической технологической экспедиции СПбГУТ по побережью моря Лаптевых. Маршрут экспедиции: г. Санкт-Петербург, г. Якутск, Национальный парк «Ленские столбы», пгт. Тикси, мыс Быковский, пгт. Тикси, г. Якутск, ледник Булуус, г. Якутск, г. Санкт-Петербург. Основные исследования были проведены в пгт. Тикси. В экспедиции приняли участие 12 человек: руководитель экспедиции (автор данной работы), заместитель руководителя экспедиции, 10 студентов СПбГУТ. Продолжительность экспедиции – 17 дней (21.07.2024 г. – 06.08.2024 г.).

В конце июля 2024 г. в 1,5 км от пгт. Тикси в тестовом режиме была развернута гибридная сеть связи. При этом использовалось преимущественно отечественное оборудование, в том числе:

1. Разработанные под руководством автора данной статьи:

– энергоэффективные УКВ приемопередатчики АЛИСА-С [3] АТ1.1 (рис. 1, *а*) и ретрансляторы АЛИСА-С РТ1.1. Мощность данных устройств – 0,1 Вт. Тип антенны – штыревая. Максимальное расстояние между элементами сети составило 4 км;
– оборудование с встроенными датчиками, подключаемое к сети приемопередатчиков АЛИСА-С АТ1.1 и ретрансляторов АЛИСА-С РТ1.1 по радиоканалу;

– энергоэффективные УКВ приемопередатчики АЛИСА-С [3] АТ1.2 (рис. 1, *б*) и ретрансляторы АЛИСА-С РТ1.2. Мощность данных устройств – 2 Вт. Тип антенны – штыревая. Максимальная расстояние между однотипными элементами сети связи 16 км;
– автоматический портативный электроэнцефалограф «Катюша» (рис. 2), позволяющий выполнять регистрацию и анализ электроэнцефалограммы автоматически без участия врача-физиолога в неподготовленных помещениях [3–8]. Данное устройство обладает возможностью подключения к элементам гибридной сети связи за счет наличия Ethernet, Wi-Fi, Bluetooth, интерфейсов для подключения к КВ и УКВ радиомодемам, а также спутниковым терминалам связи [3].

2. Оборудование, сконструированное работниками СПбГУТ:
– анализатор сети радиосвязи;
– бортовой прибор системы идентификации БПЛА.

3. Оборудование компаний-партнеров СПбГУТ:
– носимый комплекс спутниковой связи «СНАРК-100Р» ГК «Рэйс-Коммуникейшн».
– учебная станция приема спутниковых данных «Вьюнок» компании ООО «Спутниковые инновационные космические системы».

4. Радиостанции отечественного производства, а также другое оборудование.

(*а*) (*б*)

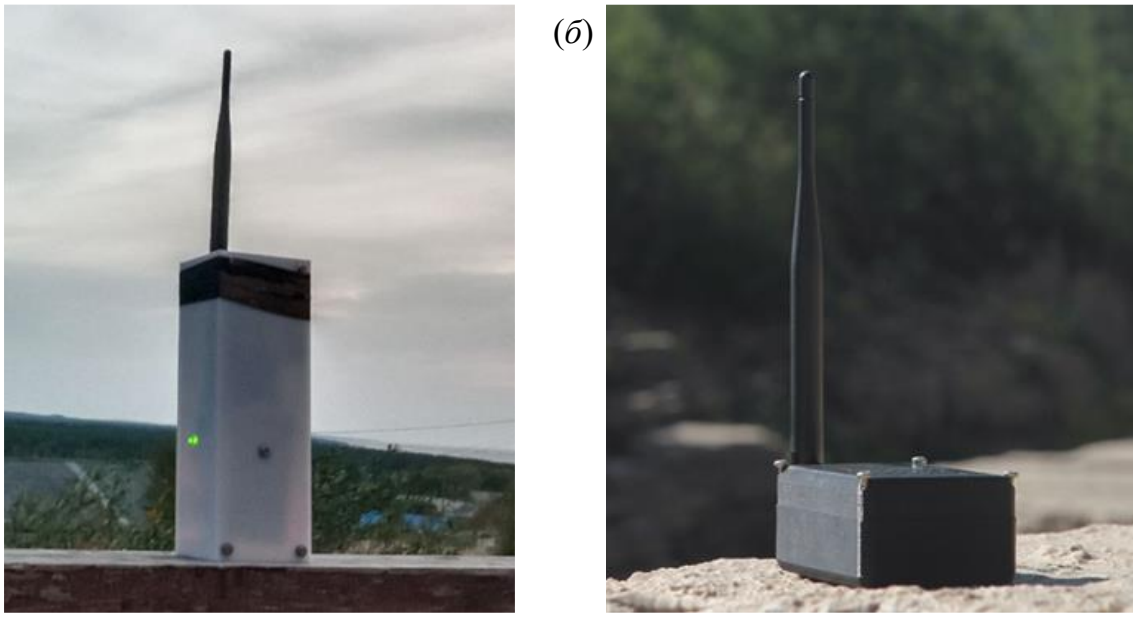


Рис. 1. Энергоэффективные приемопередатчики АЛИСА-С: (*а*) АТ1.1 и (*б*) АТ1.2

В единую сеть связи были включены устройства различных видов связи и организована видеоконференцсвязь между пгт. Тикси, г. Санкт-Петербург, г. Архангельск, г. Смоленск и г. Самара (рис. 3).

Третья Арктическая технологическая экспедиция СПбГУТ по побережью моря Лаптевых реализована Санкт-Петербургским государственным университетом телекоммуникаций им. проф. М. А. Бонч-Бруевича при поддержке Комитета по информационной политике, информационным технологиям и связи Государственной Думы Федерального Собрания Российской Федерации, Комитета Санкт-Петербурга по делам Арктики, Правительства Республики Саха (Якутия), Постоянного представительства Республики Саха (Якутия) при Президенте Российской Федерации в рамках Профессионального конкурса «Открываем Россию заново», организованного ВШЭ и АНО «Россия – страна возможностей», по программе Росмолодежи «Больше, чем путешествие».

Автором данной статьи запланирована серия арктических экспедиций, в рамках которых планируется провести научные исследования в интересах реализации Стратегии развития отрасли связи Российской Федерации на период до 2035 года.

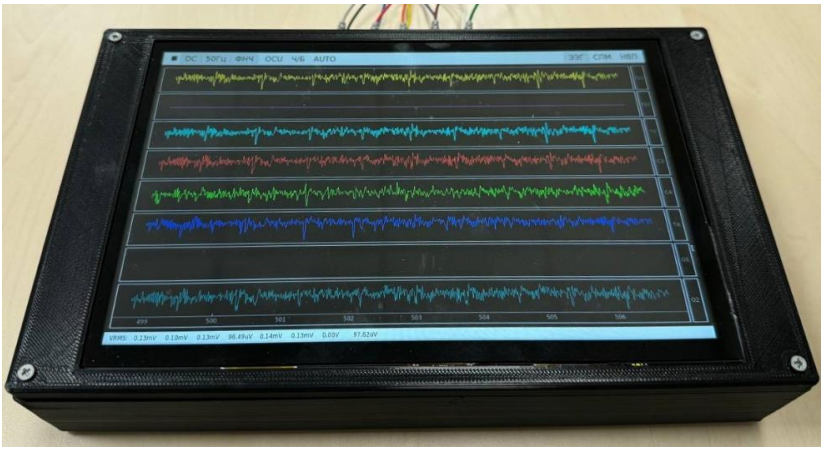


Рис. 2. Автоматический портативный электроэнцефалограф «Катюша» [3]

Четвертая Арктическая технологическая экспедиция СПбГУТ, посвященная 130-летию со дня изобретения радио, запланирована в деревню Летняя Золотица Архангельской области. Планируется проведение испытаний следующего оборудования, разработанного под руководством автора данной статьи: универсального КВ радиомодема, энергоэффективных УКВ приемопередатчиков и ретрансляторов АЛИСА-С, оборудования для терминала спутниковой связи низкоорбитальной группировки спутников, автома-

тического портативного электроэнцефалографа, портативной метеорологической станции и пр.

Рис. 3. Организация видеоконференцсвязи неподалеку от пгт. Тикси

Пятая Арктическая технологическая экспедиция СПбГУТ ожидается в пгт. Тикси (Республика Саха (Якутия)), где планируется развертывание полномасштабной сети приемопередатчиков и ретрансляторов АЛИСА-С. Также планируется испытание и других устройств, разработанных автором данной работы: портативного универсального КВ радиомодема при работе на расстояниях более 1000 км, автономных портативных терминалов спутниковой связи, обеспечивающих передачу тревожных сообщений в тундре в условиях полного отсутствия инфраструктуры и пр.

Шестая Арктическая технологическая экспедиция СПбГУТ запланирована на архипелаг Северная Земля. В рамках экспедиции планируется проведение испытаний оборудования, разработанного автором данной статьи в условиях нахождения и движения на ледоколе или плавучей платформе и при нахождении на территории на высоких широтах (около 80°): энергоэффективных приемопередатчиков и ретрансляторов АЛИСА-С, универсального портативного КВ радиомодема, терминала спутниковой связи, оборудования для организации связи, управления и контроля телеметрии беспилотных авиационных систем и пр.

Список используемых источников

1. Распоряжение Правительства Российской Федерации от 24 ноября 2023 года №3339-р об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года. Электронный ресурс: http://static.government.ru/media/files/Pc7fHuejbNvqv17b0RJNv0RIqTo20lUV.pdf, [дата обращения: 01.06.2025 г.].
2. Указ Президента Российской Федерации от 26.10.2020 г. №645 «О Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года». Электронный ресурс: http://www.kremlin.ru/acts/bank/45972, [дата обращения: 01.06.2025 г.].
3. Степанов А. Б. Разработка автоматического портативного электроэнцефалографа с возможностью интегрирования в Единую информационную систему Арктической зоны Российской Федерации. Электросвязь. 2024. № 12-2. С. 53-60.
4. Степанов А. Б. Автоматический портативный электроэнцефалограф. В сборнике: Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции. Санкт-Петербург, 2022. С. 150-153.
5. Степанов А. Б. Способ анализа электроэнцефалограмм. Патент на изобретение RU 2467384 C1, 20.11.2012. Заявка № 2011127377/08 от 28.06.2011.
6. Степанов А. Б. Автоматизированная система анализа электроэнцефалограмм. Патент на полезную модель RU 110632 U1, 27.11.2011. Заявка № 2011127360/14 от 28.06.2011.
7. Степанов А. Б., Козлов Д. В., Запайщиков А. В. Автономный портативный электроэнцефалограф на базе одноплатного компьютера Nvidia Jetson. Вестник Воронежского государственного технического университета. 2022. Т. 18. № 2. С. 77-85.
8. Степанов А. Б., Козлов Д. В. Программа, реализующая автоматический портативный электроэнцефалограф. Свидетельство о регистрации программы для ЭВМ RU 2022667973, 29.09.2022. Заявка № 2022667302 от 21.09.2022.

ON THE DEPLOYMENT OF A HYBRID COMMUNICATIONS NETWORK WITHIN THE FRAMEWORK OF THE THIRD ARCTIC TECHNOLOGICAL EXPEDITION OF SPBSUT ALONG THE COAST OF THE LAPTEV SEA

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

In July 2024 in the village Tiksi participants of the Third Arctic Technological Expedition of SPbSUT along the coast of the Laptev Sea deployed a hybrid communication network in a test mode, which made it possible to organize video conferencing between this village (Republic of Sakha (Yakutia)), St. Petersburg, Arkhangelsk, Smolensk, Samara. At the same time, mainly domestic equipment was used, including those developed at SPbSUT. The article describes the main features of the deployment of this hybrid communication network, as well as the test results of the equipment included in its composition. In conclusion, the proposed directions for further research are presented in the interests of implementing the Strategy for the Development of the Communications industry of the Russian Federation for the period up to 2035.

Key words: *hybrid communication network, expedition, Arctic zone of the Russian Federation, transceivers, VHF, HF, satellite communications, automatic portable electroencephalograph*

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И СИСТЕМЫ

УДК 621.396
ГРНТИ 49.33.29

ТРЕБОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ К ПЕРЕДАЧЕ ИНФОРМАЦИИ

Н. И. Абрамова, М. З. Лящук

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

В статье рассматривается процесс передачи в автоматизированной системе управления сообщений различных категорий по важности и срочности содержащейся информации. Сформулированы основные требования по времени доведения и достоверности передаваемой информации при определенном объеме передаваемых сообщений.

автоматизированная система управления, система передачи информации, время доведения, достоверность, сообщение, категория

Качественные сдвиги в формах и методах управления в военном деле предопределили необходимость постоянного совершенствования технической базы системы управления. и прежде всего, использования автоматизированных систем управления (АСУ). Автоматизированная система управления действует как человеко-машинная система – информация обрабатывается на вычислительных машинах, а принятие решения остается за человеком [1, с. 367-377]. Необходимым условием функционирования любой АСУ является осуществление надежного и оперативного обмена информацией между ее элементами [2, с. 5-17, 226-234].

В самом общем виде система, в которой реализуется автоматизированное управление, включает: внешнюю среду, объекты управления, управляющие объекты, устройства обработки информации (как правило, ЭВМ) и канал взаимодействия (рис. 1).

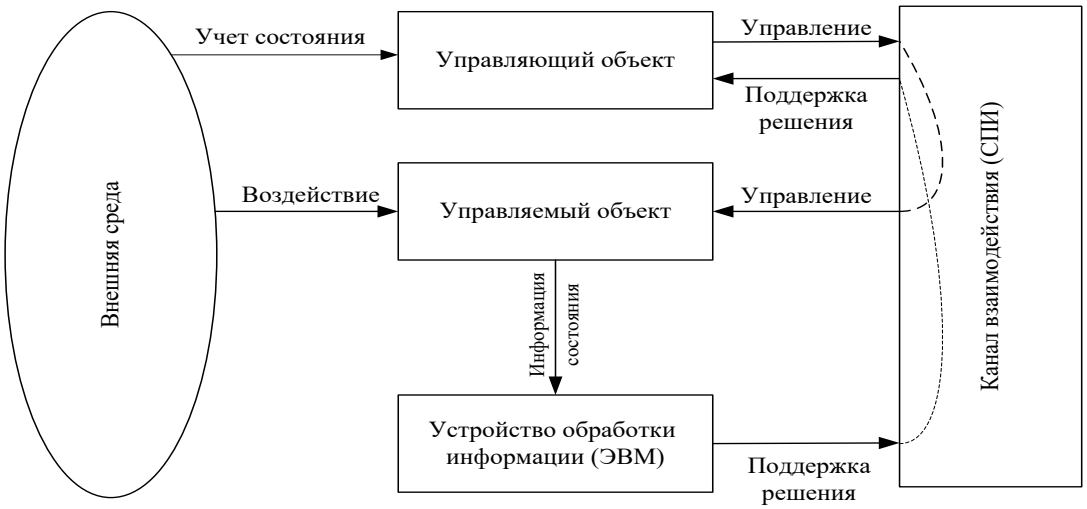


Рис. 1. Структура АСУ

Внешняя среда воздействует как на управляющие объекты, так и на объекты управления, изменяя их состояние. Состояние объектов управления, пройдя устройство обработки информации, поступает в управляющие объекты в виде информации «поддержки решения» для выработки управляющим устройством сигнала управления, который поступает на объекты управления, переводя их в новое состояние. Поэтому процесс управления состоит в следующем: внешняя среда, воздействуя на объекты управления, вызывает их изменение. В результате, управляющие объекты получают информацию состояния от устройства ее обработки для поддержки выработанного решения, которое переводит управляемые объекты в новое состояние.

В соответствии с этим важнейшим условием осуществления управления является обеспечение обмена информацией между объектами системы управления, которые в большинстве случаев находятся на значительном удалении друг от друга. Следовательно, основу любой системы обмена информацией составляет система передачи информации (СПИ). Для обеспечения процесса передачи информации создаваемая СПИ должна выполнять все требования, предъявляемые к процессу передачи.

Информация, передаваемая в системе управления в виде сообщений, неоднородна по своему содержанию и может быть разделена по группам важности и срочности информации, каждая из которых характеризуется определенным уровнем требований к процессу передачи. В случае важности информации к процессу передачи предъявляются требования по надежности доставки, а в случае срочности – требования по допустимой

задержке. По названным группам в АСУ различают сигналы оповещения и телеметрическую информацию, диалоговую и справочную информацию, общие донесения и распоряжения и обычную информацию. Соответствующие группы сообщений образуют категории срочности.

В таблице 1 даны ориентировочные требования к допустимой задержке ($T_{дов}$) и к достоверности передаваемой информации ($P_{ош}$), содержащей различные сведения, при определенном объеме ($V_с$) сообщений в битах.

ТАБЛИЦА 1. Ориентировочные требования к временным задержкам и достоверности информации при определенном объеме сообщений

№ п/п	Содержание информации	Время доведения $T_{дов}$(с)	Объем сообщения $V_с$(бит)	Вероятность потери и ошибки $P_{ош}$ (на знак сообщения)
1	Сигналы оповещения	1-10	5-10	10^{-9}-10^{-10}
2	Телеметрическая информация	1-10	100-1000	10^{-3}-10^{-5}
3	Диалог «человек-машина»	1-10	10-50000	10^{-6}
4	Справочная информация	10-100	1000-100000	10^{-6}
5	Обмен программами между ЭВМ	100-5000	1000-10000000	10^{-6}
6	Общие донесения и распоряжения	500-10000	500-10000	10^{-5}
7	Обычная информация	100000	1000-100000	10^{-3}-10^{-5}

В общем случае, требования к надежности передачи допускают различные вероятности ошибки и потери сообщения. Но при передаче сигналов оповещения СПИ должна обеспечивать практическую невозможность ошибочного приема или пропадания информации оповещения. В большинстве случаев значения допустимой ошибки и потери сообщений оповещения выбираются в пределах 10^{-9}-10^{-10} на знак первичного кода. В то же время для телеметрической информации допустимые значения вероятностей ошибки и потери сообщения могут быть различными. Это связано с тем, что при пропадании какого-либо из отсчетов измеряемого процесса последствия могут быть скомпенсированы за счет информации соседних отсчетов. Опыт эксплуатации ряда телеметрических систем в АСУ технологическими процессами показывает, что граничные значения вероятностей потери и

ошибки следует выбирать равными 10^{-3} и 10^{-5}, соответственно. Большинство систем широкого использования, ведущих передачу диалоговой и справочной информации, успешно функционируют при вероятности ошибки или потери сообщения порядка 10^{-6}.

Под общими донесениями и распоряжениями понимают смысловую информацию, которая передается между людьми при решении в системе управления задач, не подлежащих автоматизации. В настоящее время опыт в работе систем передачи такого рода информации, обеспечивающих приемлемое качество функционирования систем управления при вероятности потери или ошибки 10^{-5}. Другая обычная информация обеспечивает приемлемое качество функционирования систем управления при вероятности ошибки или потери сообщения, равной 10^{-3}-10^{-5}.

Множество сообщений, передаваемых в АСУ, делятся на подмножества – категории, к каждой из которых со стороны системы управления предъявляются идентичные требования. При этом, сообщениям каждой из категорий присваивается определенный ранг преимущества (приоритет), в соответствии с которым происходит обслуживание сообщений в СПИ. Кроме того, на принципы построения СПИ существенное влияние оказывает структура системы управления (централизованная, децентрализованная, комбинированная), определяющая в процессе управления взаимосвязь множества управляющих объектов и объектов управления. Система передачи информации, создаваемая в интересах системы управления, может строиться с учетом структуры управления или независимо от нее. Следовательно, в первом случае система передачи информации раскрывает структуру системы управления, а во втором случае структуру управления скрывает.

Обмен информацией между техническими устройствами, а также между техническими устройствами и человеком в АСУ осуществляется посредством сообщений данных. Данные не предназначены непосредственно для человека, как получателя информации. Осмысление данных человеком может происходить после их соответствующей обработки и представления в форме, удобной для их окончательного использования. Задача доставки данных по заданному адресу с обеспечением соответствующих качественных показателей по скорости, верности и надежности выполняется сетью передачи данных (СПД), передающей электрические сигналы, несущие информацию. Требования к СПД, если передача сообщений данных произво-

дится по каналам передачи данных, обычно касаются объемов поступающей на вход каналов информации (нагрузки), верности, надежности и сроков доставки (временной задержки), аналогичные требованиям к СПИ АСУ. Значения этих показателей в значительной степени различаются ввиду различий в назначении АСУ по разнообразию решаемых задач [2].

Список использованных источников

1. Малиновский С. Т. Сети и системы передачи дискретной информации и АСУ, М.: «Связь». 1979. 364 с.

2. Гойхман Э. Ш., Лосев Ю. И. Передача информации в АСУ. М.: «Связь». 1976. 280 с.

REQUIREMENTS OF THE AUTOMATED SYSTEM OF MANAGEMENT TO TRANSMIT INFORMATION

Abramova N., Lyashuk M.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

This paper discusses the process of transmitting messages of various categories in an automated management system, taking into account the importance and urgency of the information contained in the messages. The article formulates the main requirements for the time of delivery and the reliability of the transmitted information, taking into account the volume of transmitted messages.

Key words: *automated control system, information transmission system, delivery time, reliability, message, category*

УДК 004.771
ГРНТИ 50.41.23

СИСТЕМА УДАЛЕННОГО ДОСТУПА К ПРОГРАММИРУЕМЫМ УСТРОЙСТВАМ НА БАЗЕ МИКРОКОНТРОЛЛЕРОВ: АРХИТЕКТУРА И РЕЗУЛЬТАТЫ АНАЛИЗА

С. А. Авакян, З. Д. Бабанов, Д. С. Кукунин, С. О. Максименко

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

В настоящей работе представлена разработка системы удаленного доступа к программируемым устройствам, ориентированной на интеграцию в образовательные процессы технических вузов. Система сочетает эмуляцию микроконтроллеров (на базе QEMU) с управлением физическими устройствами (ESP32), что обеспечивает гибкость применения в условиях дистанционного обучения. Ключевым аспектом архитектуры является использование микросервисов и контейнеризации (Docker), позволяющих масштабировать систему при высокой нагрузке. Экспериментальные данные демонстрируют возможность обработки до 100 одновременных запросов с задержкой 1.2 секунды, а также повышение производительности на 40 % по сравнению с существующими аналогами.

микроконтроллеры, кластеризация, микросервисы, балансировка нагрузки, Docker, образовательные технологии

Актуальность исследования определяется растущим спросом на дистанционные образовательные технологии [1], особенно в контексте ограниченного доступа к лабораторному оборудованию [2]. Современные учебные программы технических специальностей требуют практического взаимодействия с программируемыми устройствами, однако большинство доступных решений, таких как веб-симуляторы (например, WokWI [3]), не обеспечивают работы с физическими микроконтроллерами. Это существенно снижает эффективность обучения, так как студенты лишены возможности экспериментировать с реальным оборудованием.

Целью работы является создание универсальной платформы, объединяющей эмуляцию и прямое управление устройствами, что позволяет преодолеть ограничения существующих аналогов. Научная новизна исследования заключается в комбинировании технологий контейнеризации и кластеризации для распределения вычислительной нагрузки, а также в реализации механизмов автоматического восстановления при отказах узлов.

Архитектура системы (рис. 1) разделена на два взаимосвязанных модуля: клиентский веб-интерфейс и серверную инфраструктуру. Клиентская часть реализована в виде веб-приложения, включающего редактор кода с подсветкой синтаксиса (на базе библиотеки CodeMirror), динамическую панель для публикации лабораторных работ и консоль вывода результатов. Данный подход обеспечивает интуитивность взаимодействия, что критически важно для пользователей без глубоких технических знаний.

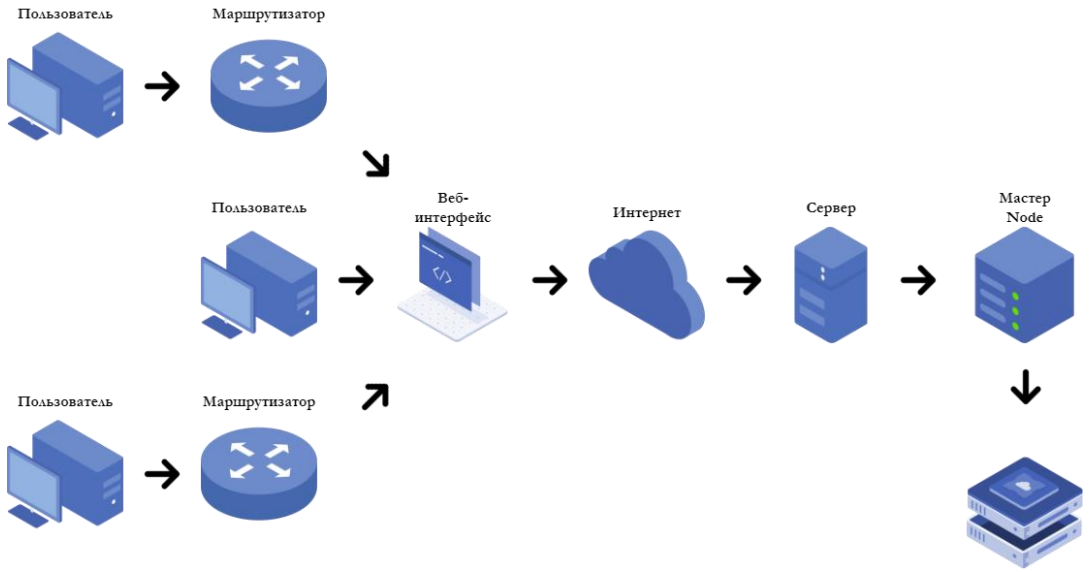


Рис. 1. Схема взаимодействия клиентского интерфейса, Master Node и Worker Nodes.

Серверная инфраструктура построена на микросервисной архитектуре [4], где центральную роль играет Master Node – модуль, разработанный с использованием фреймворка FastAPI (Python). Его функционал включает обработку HTTP-запросов, распределение задач между рабочими узлами (Worker Nodes) и мониторинг их состояния через периодические health-чеки. Рабочие узлы развернуты в изолированных Docker-контейнерах, что обеспечивает безопасность и стабильность системы. Каждый контейнер содержит либо эмулятор QEMU для виртуального взаимодействия, либо микропрограммы для управления физическими устройствами (ESP32) [5].

Взаимодействие между компонентами осуществляется через REST API (для связи клиента с Master Node) и протокол MQTT [6] (для обмена данными между Master Node и Worker Nodes). Сетевая изоляция реализована посредством Docker-сети (lab_net) с DNS-маршрутизацией, что минимизирует риски несанкционированного доступа.

Одним из ключевых аспектов системы является кластеризация устройств, направленная на оптимизацию обработки запросов. Как показано

на рис. 2, кластеры формируются на базе сетевых коммутаторов, объединяющих группы устройств под управлением Master Node. Алгоритм Round-Robin, используемый для распределения задач, обеспечивает равномерную нагрузку на узлы [7]. Например, при одновременной работе 50 пользователей Master Node последовательно направляет запросы на доступные Worker Nodes, что исключает перегрузку отдельных элементов системы.

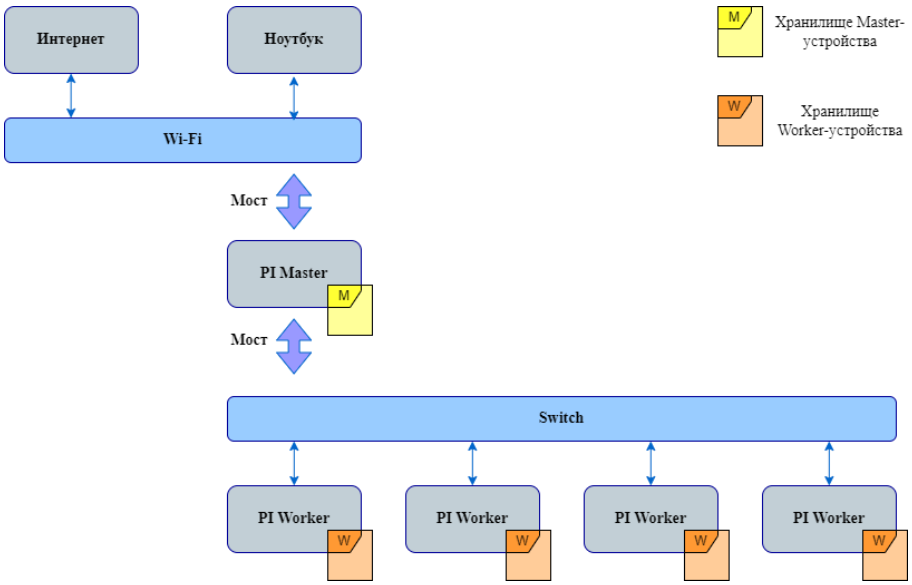


Рис. 2. Структура подключения устройств через сетевые коммутаторы

Экспериментальный кластер, собранный на базе плат ESP32, продемонстрировал прямую зависимость между количеством узлов и производительностью. Так, увеличение числа устройств с 3 до 6, позволило повысить скорость обработки запросов на 40 %, что подтверждает эффективность предложенного подхода.

Проведенный анализ рынка выявил существенные ограничения конкурирующих продуктов. Например, платформа WokWI, несмотря на удобный интерфейс, не поддерживает работу с физическими устройствами, что сужает ее применение в исследовательских целях. Решение Windows Remote Experience, разработанное Microsoft, хотя и позволяет управлять устройствами в локальной сети, требует ручной настройки для каждой платы и не предусматривает механизмов кластеризации. Проект esp-link, ориентированный на прошивку микроконтроллеров через MQTT, ограничен базовым функционалом и не поддерживает многопользовательский режим.

В отличие от аналогов, предложенная система обеспечивает комбинированное использование эмуляции и реального оборудования, автоматическое развертывание контейнеров через Docker Compose, а также гибкое

управление ресурсами за счет кластеризации. Эти особенности позволяют адаптировать систему как для учебных лабораторий, так и для исследовательских задач, требующих высокой надежности и масштабируемости.

Для оценки производительности системы проведены серии тестов, имитирующих реальные условия эксплуатации. Нагрузочное тестирование (рис. 3) показало, что при одновременной работе 100 пользователей средняя задержка обработки запросов составляет 1.2 секунды, что соответствует требованиям образовательных процессов. Тестирование отказоустойчивости подтвердило способность системы автоматически перенаправлять задачи при отключении узлов: время восстановления не превышало 0.8 секунды.

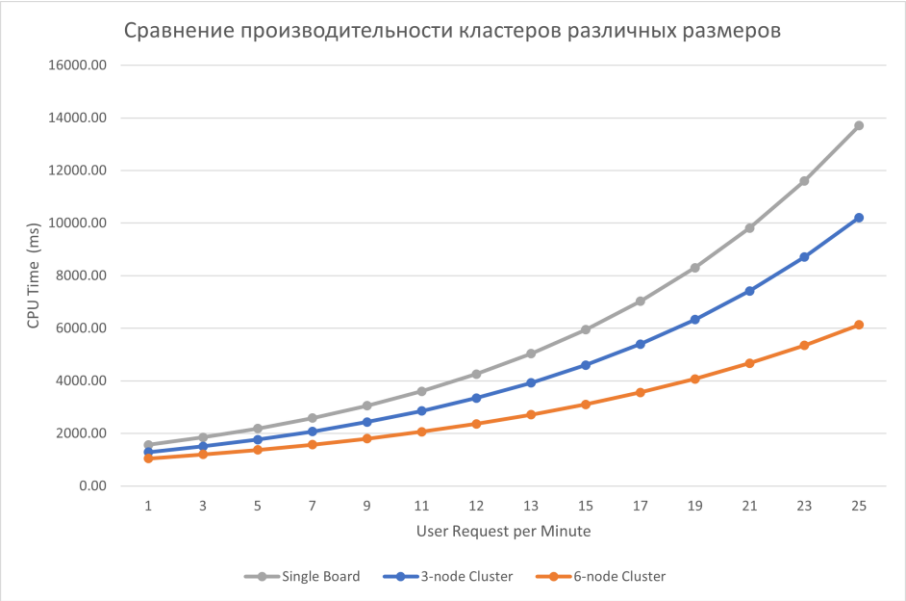


Рис. 3. Рост производительности при увеличении числа узлов

Сравнение с платформой WokWI выявило преимущество предложенного решения в скорости выполнения кода – разница составила 40 %, что обусловлено эффективным распределением нагрузки между узлами кластера. Эти результаты подтверждают, что комбинирование эмуляции и управления реальными устройствами в сочетании с кластеризацией позволяет преодолеть ключевые ограничения существующих аналогов.

Разработанная система удаленного доступа к программируемым устройствам представляет собой комплексное решение, объединяющее гибкость веб-интерфейса, надежность микросервисной архитектуры и эффективность кластеризации. Экспериментальные данные подтверждают ее способность обрабатывать высокие нагрузки с минимальными задержками, а также автоматически восстанавливаться при сбоях.

Перспективы дальнейших исследований включают интеграцию системы с облачными платформами (AWS, Azure) для глобального масштабирования, поддержку новых типов устройств (Raspberry Pi, STM32) и разработку методических материалов для внедрения в учебный процесс. Практическая значимость работы подтверждена успешным тестированием прототипа и положительными отзывами преподавателей, отметивших удобство взаимодействия и снижение зависимости от физического присутствия в лаборатории.

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.

Список использованных источников

1. Garefalakis M., Kamarianakis Z., Panagiotakis S. Towards a Supervised Remote Laboratory Platform for Teaching Microcontroller Programming // Information. 2024. № 15(4), 209. С. 1-23.

2. Abekiri N., Rachdy A., Ajaamoum M., Nassiri B., Elmahni L., Oubail Y. Platform for hands-on remote labs based on the ESP32 and NOD-red // Scientific African. 2023. № 19.

3. Wokwi: Building and Testing Embedded Projects. URL: https://wokwi.com (дата обращения 22.05.2025).

4. Qian Q., Ronghua X., Seyed Yahya N., Yu C. An Experimental Study on Microservices based Edge Computing Platforms // IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Toronto, ON, Canada: IEEE, 2020. С. 836-841.

5. Howard M., Bruce Irvin R. ESP32: QEMU Emulation Within a Docker Container // Proceedings of the Future Technologies Conference. - London, UK: Springer, 2023. С. 63-80.

6. MQTT Version 5.0 // Oasis Standard URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf (дата обращения 22.05.2025).

7. Richardson C. Microservice Patterns. Shelter Island, NY: Manning Publications, 2018.

REMOTE ACCESS SYSTEM FOR MICROCONTROLLER-BASED PROGRAMMABLE DEVICES: ARCHITECTURE AND ANALYSIS RESULTS

Avakyan S., Babanov Z., Kukunin D., Maksimenko S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This work presents the development of a remote access system for programmable devices, designed for integration within educational processes in technical universities. The system combines microcontroller emulation (based on QEMU) with physical device management (ESP32), providing application flexibility in remote learning environments. A key architectural aspect involves the utilization of microservices and containerization (Docker), enabling system scalability under high load conditions. Experimental results demonstrate the system's capability to handle up to 100 concurrent requests with a latency of 1.2 seconds, alongside a 40 % performance enhancement compared to existing solutions.
Key words: *microcontrollers, clustering, microservices, load balancing, Docker, educational technology*

УДК 615.1
ГРНТИ 14.05.01

ПРЕДСКАЗАНИЕ ИНФАРКТА МИОКАРДА НА ОСНОВЕ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ РАСПРЕДЕЛЕННЫХ МЕДИЦИНСКИХ ДАННЫХ

Л. А. Антропова, А. В. Марочкина, П. А. Санникова

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

Несмотря на многолетние достижения в кардиологии, сердечно-сосудистые заболевания сохраняют статус главной причины смертности во всем мире. Одним из ключевых направлений современных исследований является разработка инструментов, способных выявлять предрасположенность пациентов к инфаркту миокарда на минимальных сроках и с максимальной точностью. Традиционные подходы машинного обучения, основанные на централизованных наборах медицинских данных, сталкиваются с серьезными ограничениями, связанными с безопасностью и конфиденциальностью информации о пациентах. Федеративное обучение предлагает принципиально иной подход: обработка и обучение моделей осуществляются в локальных хранилищах данных, а централизованному серверу передаются только агрегированные обновления параметров моделей без доступа к самим сырым данным.

В настоящей статье рассматривается применение федеративного обучения для задачи прогнозирования риска инфаркта миокарда на обширном синтетически распределенном медицинском корпусе. В качестве базовых алгоритмов выбраны логистическая регрессия и метод опорных векторов, дополнительно исследованы методы ближайших соседей и деревья решений. Проведенное моделирование показало, что логистическая регрессия достигает высокой точности предсказания, метод опорных векторов демонстрирует сопоставимый результат, а методы с более высоким уровнем интерпретируемости уступают в среднем показателю точности. Особое внимание уделяется анализу сетевых затрат в рамках коммуникации между узлами федерации и центральным сервером, а также перспективам оптимизации протоколов защищенной агрегации и устранения утечек приватной информации.

федеративное обучение, предсказание инсульта, распределенные медицинские данные, машинное обучение, предсказательная аналитическая медицина

Кардиологические нарушения, в том числе острый инфаркт миокарда, ежегодно приводят к огромному числу летальных исходов, обусловливая потребность в эффективных стратегиях ранней диагностики и профилактики. В последние годы стремительное развитие методов машинного обучения и искусственного интеллекта породило ряд значимых достижений в области предиктивной медицины. Однако традиционные модели неизбежно

предполагают передачу и хранение медицинской информации в централизованном хранилище, что противоречит принципам защиты персональных данных и создает потенциальные риски нарушения конфиденциальности. Появление федеративного обучения стало ответом на эти вызовы: при сохранении локальных данных на серверах медицинских учреждений обеспечивается обучающий процесс моделей посредством обмена агрегированными обновлениями параметров, что минимизирует объем передаваемой информации и сохраняет ее приватность.

Федеративное обучение [1] представляет собой распределенную парадигму, в которой каждый узел федерации осуществляет локальную оптимизацию параметров модели по собственным данным и передает результирующие градиенты или веса на центральный сервер. Алгоритм агрегирует полученные параметры, формируя новую глобальную модель, и направляет ее обратно узлам. В результате достигается баланс между персонализацией моделей в каждом узле и общей обобщаемостью, при этом отсутствует необходимость централизованного хранения медицинских данных. Успешность такого подхода обусловлена сохранением ключевых характеристик локальных распределений и возможностью учета статистических особенностей каждого медицинского учреждения.

Для моделирования сценария федеративного обучения на медицинских записях был синтезирован набор данных [2], максимально приближенный к реальным условиям: электронные медицинские карты пациентов, содержащие демографические характеристики, анамнестические сведения, результаты лабораторных исследований, параметры жизненно важных функций и данные о принимаемых препаратах. Для обеспечения реалистичности распределения данные были сегментированы по нескольким виртуальным клиникам, каждая из которых хранила уникальную часть общего массива с некоторым перекрытием по признакам. Отдельное внимание уделялось качеству записей: минимальное количество пропусков, стандартизованные форматы представления результатов анализов и верифицированные алгоритмы анонимизации.

На рис. 1 продемонстрирована тепловая карта взаимосвязей между клиническими признаками, используемыми в задаче прогнозирования инфаркта миокарда. Визуализированная матрица отражает сложность структуры медицинских данных, подчеркивая наличие перекрестных влияний

между параметрами, что особенно важно при обучении моделей в условиях федеративной неоднородности.

Подготовительный этап [3] включал очистку от выбросов и ошибочных значений, заполнение пропусков с применением статистических методов имитаций, нормализацию числовых признаков и кодирование категориальных переменных. Для создания условий федеративного обучения централизованный массив данных был горизонтально разделен на несколько частей равного объема с учетом схожести распределений, что позволило воспроизвести влияние неоднородности клинических наборов на качество глобальной модели.

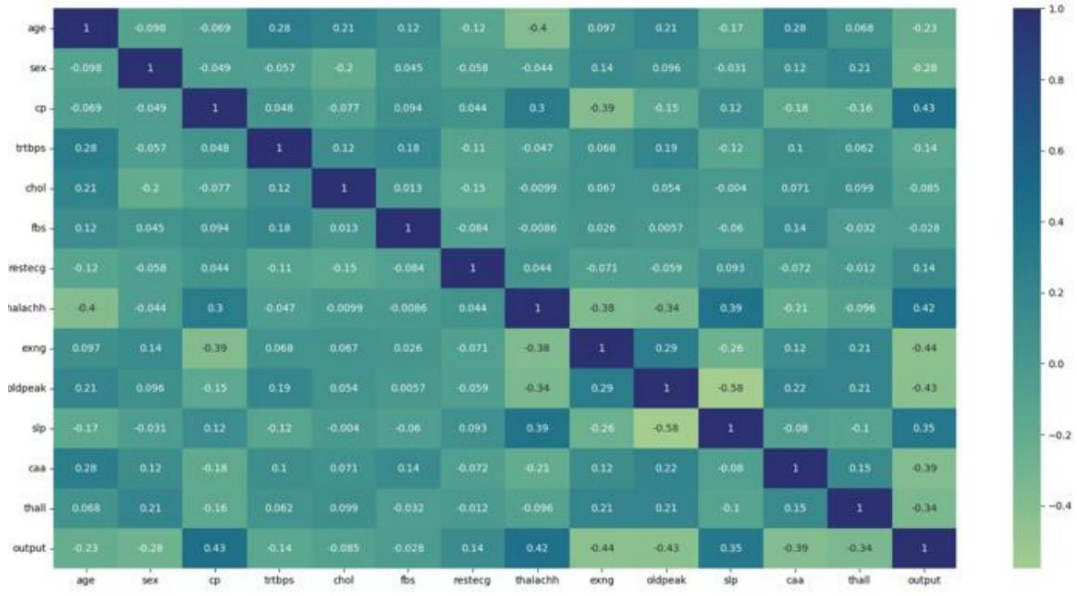


Рис. 1. Тепловая карта отношения заявленных в наборе данных параметров

В качестве основного алгоритма был выбран метод логистической регрессии [4] благодаря его простоте, интерпретируемости результатов и широкому применению в медицинских исследованиях. Вторая ключевая модель, метод опорных векторов [5], привлекла внимание своей способностью обрабатывать данные высокого размерного пространства и находить разделяющую гиперплоскость с максимальным зазором. В дополнение к ним рассмотрены метод ближайших соседей, обладающий интуитивной природой принятия решений на основе сходства с тренировочными точками, и модель деревьев решений, обеспечивающая наглядность принимаемых правил классификации.

Процесс обучения, показанный на рис. 2, условно разделен на две стадии: локальную и глобальную. Сначала каждый виртуальный узел осу-

ществляет локальную настройку параметров модели на своем подмножестве данных, рассчитывая обновления весов или градиентов. Затем центральный сервер объединяет результаты при помощи протокола безопасной агрегации, формируя новую глобальную модель [6, 7]. Цикл итераций повторяется до достижения сходимости. Для оценки качества глобальных моделей применялись традиционные метрики: точность классификации, сбалансированность precision – recall, др.

Модели продемонстрировали различную степень эффективности. Логистическая регрессия (LR) показала наивысшую точность прогнозирования, что свидетельствует об адекватности линейного подхода в задаче бинарной классификации риска инфаркта. Метод опорных векторов подтвердил свою применимость, уступив LR лишь незначительно. Метод ближайших соседей, несмотря на более простую архитектуру, обеспечил приемлемый уровень качества, однако из-за чувствительности к выбору гиперпараметра k его применение требует дополнительной настройки. Модель деревьев решений продемонстрировала наименьшую точность, но при этом обеспечила максимальную прозрачность критериев принятия решений, что представляется ценным в клиническом контексте.

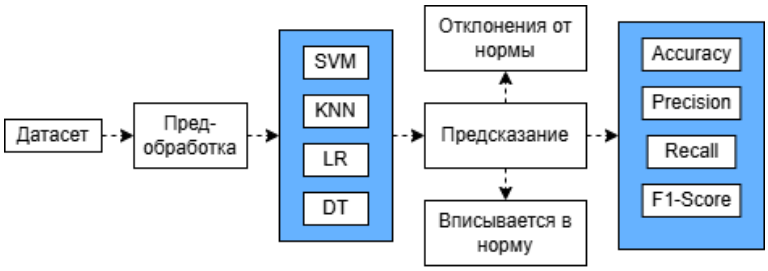


Рис. 2. Схема процесса обучения и оценки модели

Ключевым ограничением федеративного подхода оказалась нагрузка на сеть при постоянном обмене параметрами модели. Анализ распределения объемов передаваемых данных и частоты обновлений показал необходимость внедрения алгоритмов компрессии градиентов, уменьшения разрядности весов и адаптивного управления частотой агрегации. Применение техник квантования и спарсити-регуляризации может существенно снизить коммуникационные затраты без заметного ухудшения качества итоговой модели.

Для гарантии конфиденциальности медицинских записей рассмотрены методы дифференциальной приватности и криптографические протоколы защищенной агрегации. Дифференциальная приватность позволяет добав-

лять контролируемый шум к обновлениям параметров, сохраняя полезность модели, а защищенная агрегация гарантирует, что сервер не может восстановить индивидуальные градиенты узлов.

Проведенное исследование подтвердило высокий потенциал федеративного обучения для медицинских приложений, в частности для предсказания инфаркта миокарда. Важнейшие направления развития включают совершенствование протоколов коммуникации, расширение спектра приватных алгоритмов для специфических моделей, таких как логистическая регрессия и SVM, и интеграцию данных носимых устройств для повышения точности и актуальности прогнозов. Помимо технических аспектов, необходимо учитывать регуляторные требования и этические нормы, касающиеся обработки персональных медицинских данных.

Настоящая работа продемонстрировала возможность создания эффективных моделей прогнозирования инфаркта миокарда на основе федеративного обучения, сохраняя высокий уровень конфиденциальности и интерпретируемости результатов. Линейные модели, в частности логистическая регрессия, подтвердили свою надежность и применимость, а метод опорных векторов обеспечил сопоставимые показатели. Разработанные рекомендации по оптимизации коммуникации и механизмы приватности создают основу для последующих практических реализаций в рамках мультиинституционального сотрудничества.

Список используемых источников:

1. Brisbane W., Gibson A., and Campbell S. Federated learning: Architectures, models, and applications // IEEE Access. 2019. Vol. 7. PP. 78973-78984.

2. Rahman, R. (2021). Heart Attack Analysis & Prediction Dataset: A dataset for heart attack classification. [Kaggle]. URL: https://www.kaggle.com/datasets/johnsmith88/heart-disease-dataset (дата обращения 22.05.2025).

3. Shrivastava A., Kumar S., Naik N. S., and Bhatt T. A Novel Hybrid Model for Predictive Analysis of Myocardial Infarction using Advanced Machine Learning Techniques // in 2023 OITS International Conference on Information Technology (OCIT). 2023. PP. 381-386: IEEE.

4. M. Shouman, T. Turner, and R. Stocker, Using logistic regression to predict heart attacks // Medical Informatics and Decision Making. 2012. Vol. 12. № 1. PP. 143, 2012.

5. Lee, Y.-C. Application of support vector machines to corporate credit rating prediction // Expert Systems with Applications. 2007. Vol. 33(1). PP. 67-74.

6. Kanna R. K., Ambikapathy A., Brayyich M., Reddy V. V., and Nagpal A. Machine Learning Based Cardiovascular Detection Approach // in 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2023. Vol. 10. PP. 1487-1491: IEEE.

7. Ullah, F., Chen, X., Rajab, K., Reshan, A., Saleh, M., Shaikh, A., Hassan, M. A., Rizwan, M., & Davidekova, M. An efficient machine learning model based on improved features selections for early and accurate heart disease predication // Computational Intelligence and Neuroscience, 2022.

HEART ATACK PREDICTION VIA FEDERATED LEARNING UTILIZING DISTRIBUTED MEDICAL DATA

Antropova L., Marochkina A., Sannikova P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Despite decades of advancements in cardiology, cardiovascular diseases remain the leading cause of global mortality. A key focus of contemporary research is developing tools capable of identifying patient predisposition to myocardial infarction at the earliest stages with maximum accuracy. Traditional machine learning approaches, reliant on centralized medical datasets, face significant limitations concerning patient data security and privacy. Federated learning offers a fundamentally distinct paradigm: data processing and model training occur within local data repositories, with only aggregated model parameter updates transmitted to a central server–without exposing raw sensitive data.

This article investigates the application of federated learning for predicting myocardial infarction risk using an extensive synthetically distributed medical corpus. Logistic Regression and Support Vector Machines were selected as base algorithms; k-Nearest Neighbors and Decision Trees were additionally evaluated. Simulations demonstrated that Logistic Regression achieved high predictive accuracy, while Support Vector Machines delivered comparable performance. Methods offering higher interpretability exhibited lower average accuracy metrics. Particular emphasis is placed on analyzing network overhead associated with node-to-server communication within the federation, alongside prospects for optimizing secure aggregation protocols and mitigating privacy leakage.

Key words: *federated learning, myocardial infarction prediction, distributed medical data, machine learning, predictive analytics in medicine, privacy-preserving computation*

УДК 004.33
ГРНТИ 50.11.15

ОПТИМИЗАЦИЯ RAID-СИСТЕМ С ИСПОЛЬЗОВАНИЕМ КОДИРОВАНИЯ КОШИ-РИДА-СОЛОМОНА И РЕЗИСТИВНОЙ ПАМЯТИ С ПРОИЗВОЛЬНЫМ ДОСТУПОМ

З. Д. Бабанов, Д. С. Кукунин, С. О. Максименко

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

В данной работе исследуется возможность повышения производительности RAID-массивов, использующих твердотельные накопители, за счет применения помехоустойчивого кодирования на основе алгоритма Коши-Рида-Соломона. Традиционные методы кодирования на процессорном RAID-контроллере сталкиваются с ограничениями, связанными с вычислениями в полях Галуа и увеличением числа обращений к памяти. Предлагается решение, основанное на использовании резистивной памяти с произвольным доступом (ReRAM) для улучшения эффективности процесса кодирования. ReRAM может быть интегрирована как в RAID-контроллеры, так и в контроллеры твердотельных накопителей. В работе представлены порождающие матрицы, обеспечивающие возможность восстановления утраченных данных на накопителях с использованием памяти ReRAM.

резистивная память, RAID, SSD, твердотельные накопители, коды Рида-Соломона

Применяемые в RAID массивах методы хранения данных повышают устойчивость к потерям и скорость сервисного обслуживания. «Зеркалирование» и стирающее кодирование являются главными примерами таких методов. При этом наиболее распространенным среди стирающих кодов являются коды Рида-Соломона (RS) [1].

Кодирование Рида-Соломона, основанное на матрицах умножения, ставит под вопрос эффективность современных решений, основанных на процессорных вычислениях. Реализация матриц умножения включает в себя арифметические действия над конечными полями или полями Галуа (GF) [2]. Операции над полем GF (2^w), для битовых слов длины w, основываются на дискретных логарифмах. Алгоритм кодирования Коши-Рида-Соломона [3] переводит коды Рида-Соломона в коды использующие битовые слова единичной длины, заменяя неэффективное умножение матриц на операции XOR. Текущие решения, основанные на процессорных вычислениях, разделяют процесс кодирования на доступ к памяти и обработку данных, что ведет к множественному копированию данных в памяти и процессорах. В случае решений, основанных на GPU [3], этот процесс ускоряется чтением битовых матриц из постоянной памяти, а

данных из общей памяти. Однако, даже в таких решениях восстановление данных с помощью кодов Рида-Соломона является субоптимальным для RAID массивов из-за «задачи восстановления» [4]. Главным достоинством резистивной памяти с произвольным доступом в данной задаче является возможность проведения арифметических операций не зависимо от хранения данных. Благодаря новейшей архитектуре, основанной на перемычках, ReRAM может эффективно производить матричные сложения и умножения [5, 6].

Помимо хранения данных, часть ReRAM может быть использована для ускорения кодирования. Для уменьшения вычислительной нагрузки RAID-контроллера, нами предлагается использовать матрицы Коши-Вандермонда в качестве порождающей для кодирования, благодаря чему проверочные символы можно получить как результат операции XOR над всеми фрагментами данных. В случае единичного отказа, выжившие диски могут обратиться к ReRAM для восстановления утерянных данных через проведение операции XOR с первичными проверочными символами, а оставшиеся данные нужны лишь через строку.

RAID массивы используют избыточность для повышения отказоустойчивости, а проверочные символы генерируются RAID-контроллером. При хранении данных, частота единичных отказов куда выше, чем множественных: на единичные отказы приходится более 90 % всех отказов [7].

Коды Коши-Рида-Соломона используют битовые слова единичной длины, таким образом, времязатратные операции в полях GF (2^w) могут быть представлены в виде битовых XOR и AND в поле GF (2). Все фрагменты данных объединяются для генерации проверочных фрагментов путем умножений битовых векторов. Наборы фрагментов доставляются на диски независимо друг от друга, для большей отказоустойчивости.

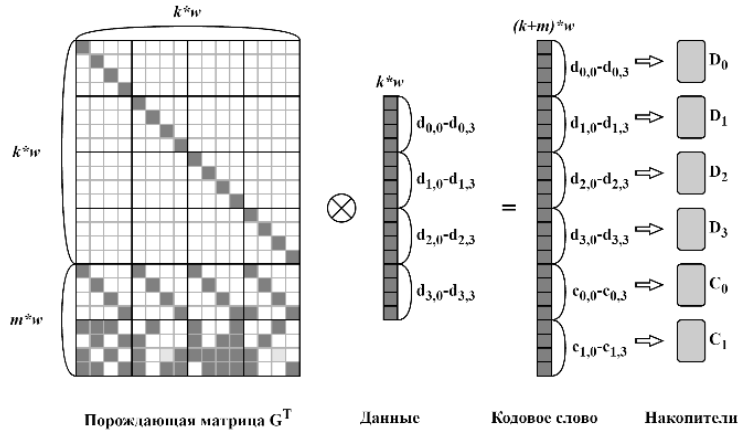


Рис. 1. Матрично-векторная форма кодирования Коши-Рида-Соломона

Нами выбрана ReRAM архитектура, основанная на перемычках размерности 16*8, где каждая ячейка является однобитовой SLC. Входное напряжение на каждую входную линию имеет два уровня (1 бит), так, чтобы выходные битовые линии имели 6 бит. В процессе кодирования нам понадобятся только нижние строки порождающей матрицы G^T, как показано на рисунке 1.

После доставки данных на RAID-контроллер, начинают работу два главных компонента системы: Менеджер Распределения и Генератор Проверочных символов. Процесс кодирования Коши-Рида-Соломона показан на рисунке 2. Фрагменты данных, распределенные Менеджером, кэшируются в ReRAM как в режиме хранения, так и в режиме вычислений. Нижние ($m * w$) строк порождающей матрицы будут расположены на перемычках, для ускорения вычислений при кодировании.

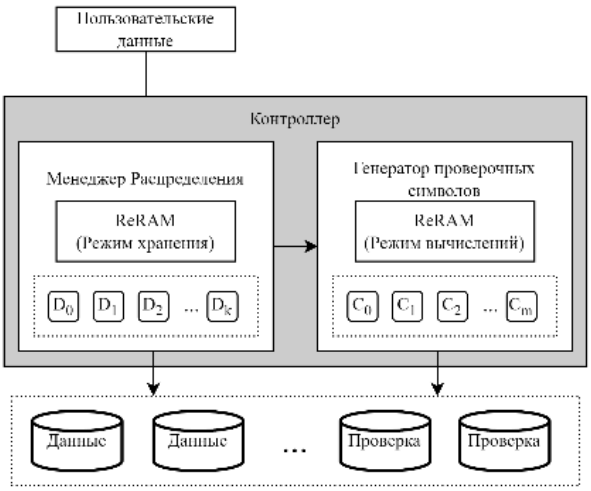


Рис. 2. Поток данных при кодировании Коши-Рида-Соломона

Традиционный путь восстановления единичных отказов требует построение матрицы декодирования, что несет большую вычислительную нагрузку. Более того, весь процесс восстановления проводится на RAID-контроллере, что не является эффективным при выполнении данных контролером задач обработки входящих-выходящих данных. При использовании предложенной порождающей матрицы Коши-Вандермонда процесс восстановления данных может быть распределен между накопителями за счет восполнения порождающей матрицы G^T. При этом каждый отдельный накопитель может использовать ReRAM контроллер без декодирования матрицы, как показано на Рисунке 3(b), или же традиционным методом как на рисунке 3(a).

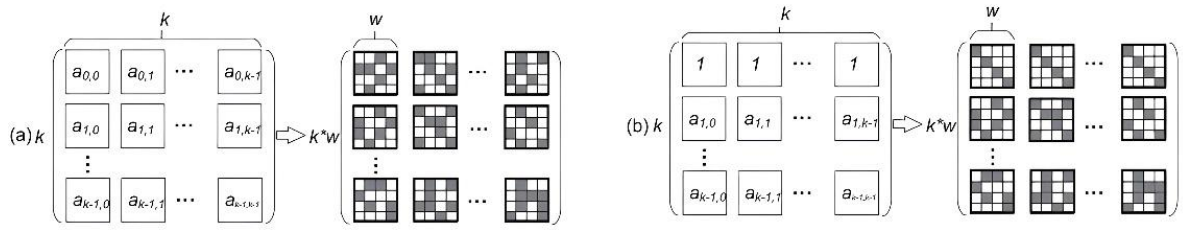
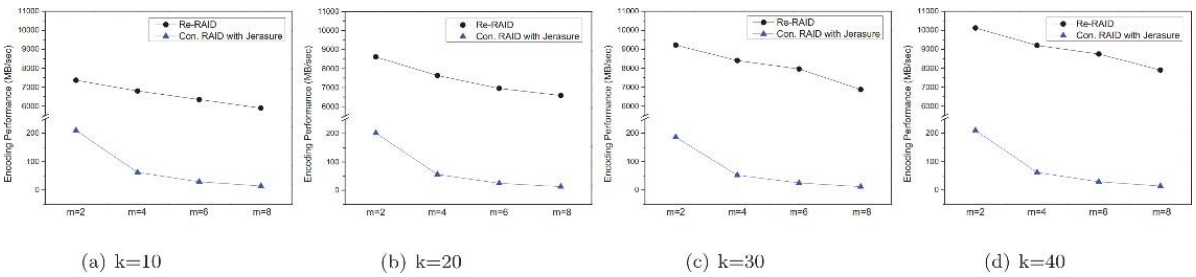


Рис. 3. (a) Традиционная матрица Коши в битовом представлении, (b) Переработанный код

Предложенная архитектура использует базовые принципы для восстановления множественных отказов - декодированная матрица умножается на выжившие фрагменты данных. Матрица Коши-Вандермонда всегда обратима [8], так что может быть использована и в данном случае. Наиболее многообещающим решением является взаимодействие ReRAM памяти и RAID-контроллера, где на контроллер ложатся задачи декодирования, а на ReRAM память задачи вычислений и восстановления данных.

В рамках эксперимента для проверки предложенной архитектуры RAID-контроллеры и накопители моделировались нами в NVsim [9]. Симулятор предоставляет функционал работы с периферией и кодированием на ReRAM перемычках. Конфигурации системы, которые были взяты за основу представлены в работах [10, 11].

Нами была исследована производительность при кодировании Коши-Рида-Соломона в сравнении с выделенным RAID-контроллером, основанным на процессорных вычислениях. В качестве симуляции решения процессорных вычислений был выбран Intel Q9550 с использованием библиотеки Jerasure [12]. Обычно производительность при кодировании Коши-Рида-Соломона связывают с размерностями матрицы k, m, w, размером пакета и размером буфера. Для достижения наиболее приближенных к реальности результатов, был выбран размер пакета в 8 Байт, из-за 64-битной архитектуры процессора. Мы изменяем параметры следующим образом: $k = 10, 20, 30, 40$; $m = 2, 4, 6, 8$. Размер буфера зафиксирован на отметке в 8 МБ. Для тестирования использовался входной видеофайл размеров 1.37 ГБ.



(a) k=10 (b) k=20 (c) k=30 (d) k=40

Рис. 4. Сравнения производительности при кодировании

На рисунке 4 показаны результаты кодирования. Стоит отметить, что производительность предложенной архитектуры достигает преимущества вплоть до 27 %, и показывает себя наилучшим образом при достижении максимума параметра *k*. Мы связываем это с уменьшением использования рядов слов в памяти ReRAM при повышении размерности.

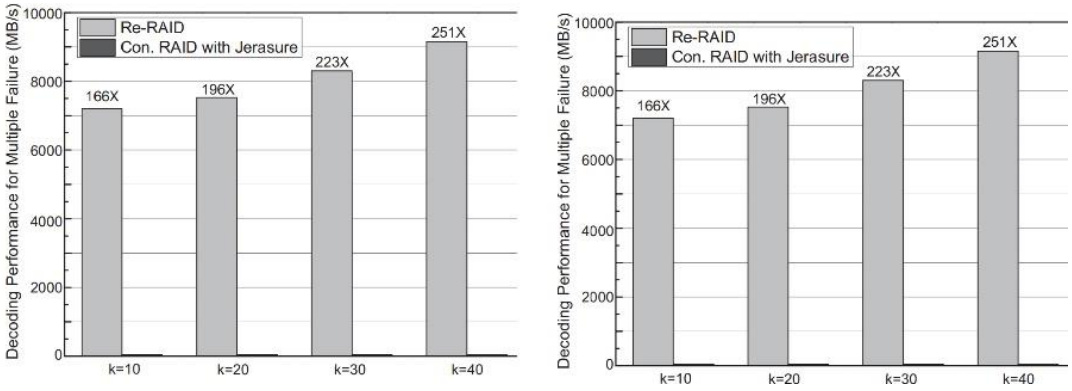


Рис. 5. (a) Производительность при декодировании единичных отказов, (b) Производительность при декодировании множественных отказов

Процесс восстановления единичных отказов на носителях мы воспроизводим путем кодирования видеоданных с параметрами k = 10, 20, 30, 40; m = 4. Рисунок 5(a) показывает производительность при декодировании. Можно заметить, что производительность предложенного решения выше вплоть до 44.6 раз. Наибольшая производительность так же достигается при наибольшем значении параметра *k*, из-за уменьшения использования рядов слов. На рисунке 5(b) показано сравнение общей производительности декодирования при множественных ошибках.

В данной работе была представлена новая архитектура для улучшения производительности кодирования Коши-Рида-Соломона в RAID массивах с использованием резистивной памяти с произвольным доступом для кодирования и хранения данных. Результаты симуляции показывают, что предложенная архитектура значительно улучшает производительность при кодировании и декодировании.

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1023031600087-9-2.2.4;2.2.5;2.2.6;1.2.1;2.2.3 в ЕГИСУ НИОКТР.

Список используемых источников

1. Dau H., Duursma I. M., Kiah H. M. and Milenkovic O. Repairing Reed-Solomon Codes with Multiple Erasures // in IEEE Transactions on Information Theory. 2018. Vol. 64. № 10. PP. 6567-6582.

2. Dickson L. E. Linear groups: With an exposition of the Galois field theory // Courier Corporation, 2003.

3. Liu C., Wang Q., Chu X. and Leung Y. -W. G-CRS: GPU Accelerated Cauchy Reed-Solomon Coding // in IEEE Transactions on Parallel and Distributed Systems. 2018. Vol. 29. № 7. PP. 1484-1498.

4. Sathiamoorthy M., Asteris M., Papailiopoulos D., Dimakis A., Vadali R., Chen S., Borthakur D. XORing Elephants: Novel Erasure Codes for Big Data // in Proceedings of the VLDB Endowment. 2013. № 6.

5. Han L. and et al. A novel reram-based processing-in-memory architecture for graph traversal, TOS, 2018.

6. Song L. and et al. Pipelayer: A pipelined reram-based accelerator for deep learning // in HPCA. IEEE, 2017.

7. Xiang L. and et al. Optimal Recovery of Single Disk Failure in RDP Code Storage Systems // SIGMETRICS, 2010.

8. Vavřín Z. Confluent cauchy and cauchy-vandermonde matrices // Linear algebra and its applications 1997. PP. 271–293.

9. Dong X., Xu C., Xie Y. and Jouppi N. P. NVSim: A Circuit-Level Performance, Energy, and Area Model for Emerging Nonvolatile Memory // in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2012. Vol. 31. № 7. PP. 994-1007.

10. Ramezani M., Elyasi N., Arjomand M., Kandemir M. T. and Sivasubramaniam A. Exploring the impact of memory block permutation on performance of a crossbar ReRAM main memory // 2017 IEEE International Symposium on Workload Characterization (IISWC), Seattle, WA, USA. 2017. PP. 167-176

11. Cho S., Park C., Oh H., Kim S., Yi Y., & Ganger G. Active disk meets flash: A case for intelligent SSDs // in Proceedings of the 27th International ACM Conference on Supercomputing. 2013. PP. 91-102.

12. Plank J. S., Simmerman S., Schuman C. D. Jerasure: A library in C/C++ facilitating erasure coding for storage applications-Version 1.2. // University of Tennessee, Tech. Rep, 2008.

OPTIMIZATION OF RAID SYSTEMS UTILIZING CAUCHY-REED-SOLOMON CODING AND RESISTIVE RANDOM-ACCESS MEMORY

Babanov Z., Kukunin D., Maksimenko S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This work investigates the potential for enhancing the performance of RAID arrays employing Solid-State Drives (SSDs) through the implementation of fault-tolerant coding based on the Cauchy-Reed-Solomon algorithm. Traditional encoding methods executed on the processor-based RAID controller encounter limitations associated with computations in Galois fields and increased memory access overhead. A solution is proposed, founded on the utilization of Resistive Random-Access Memory (ReRAM) to improve the efficiency of the encoding process. ReRAM can be integrated into both RAID controllers and SSD controllers. The work presents generator matrices that enable the recovery of lost data on storage devices utilizing ReRAM.

Key words: *resistive memory, RAID, SSD, solid-state drives, Reed-Solomon codes*

УДК 621.396.969
ГРНТИ 47.49.31

ОЦЕНКА ТОЧНОСТИ ПЕРВИЧНЫХ ДАЛЬНОМЕРНЫХ ИЗМЕРЕНИЙ В БЛС IEEE 802.11AZ. МОДЕЛИ МНОГОЛУЧЕВОГО РАДИОКАНАЛА

Е. С. Багаев

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

Статья посвящена исследованию моделей многолучевого радиоканала для задач высокоточного позиционирования в беспроводных локальных сетях IEEE 802.11az. Целью работы является определение влияния параметров многолучевого распространения на точность определения координат пользовательского устройства. Детально анализируются параметры модели, включая характеристики кластеров, временные задержки, угловые параметры и доплеровские сдвиги. Представлены характеристики и параметры различных модификаций канальных моделей для сценариев прямой и непрямой видимости.

стандарт 802.11az, позиционирование, беспроводные локальные сети Wi-Fi

Достижение дециметровой точности при определении местоположения пользовательского устройства в беспроводных локальных сетях (БЛС) усложняется при отсутствии прямой видимости, а также при многолучевом распространении сигнала [1, 2, 3]. Современные стандарты, такие как IEEE 802.11az [4], используют сложные модели радиоканала с целью минимизации ошибки позиционирования. Модель канала TGax [5], представляет собой эволюцию предыдущих моделей TGn [6] и TGac [7]. Предпосылками к ее появлению стала необходимость повышения эффективности работы БЛС в условиях высокой плотности устройств и сложные сценарии распространения сигнала в помещениях [8, 9].

В работе Салеха-Валенсуэлы [10] была предложена кластерная структура для описания процессов распространения сигнала, рисунок 1.

Было установлено, что в закрытых помещениях сигнал, приходящий к приемнику, состоит из множества отдельных лучей, каждый из которых проходит свой путь, включая как прямое распространение, так и множественные переотражения от объектов. Группы таких лучей впоследствии объединили в понятие «кластер». При физической интерпретации кластер характеризует случай отражения сигнала от крупного объекта, а отдельные лучи внутри кластера – отражения от деталей поверхности объекта [11].

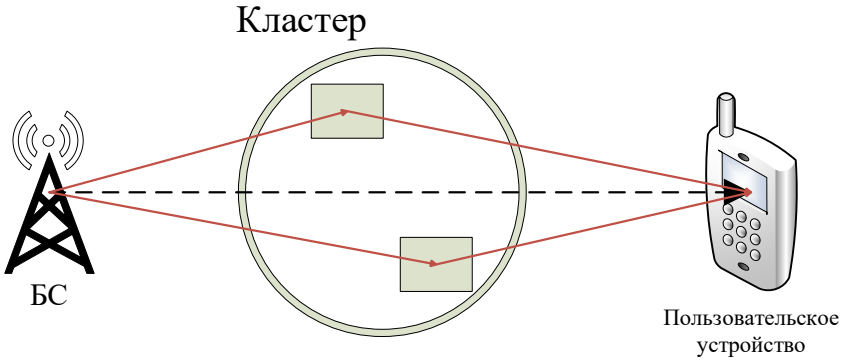


Рис. 1. Кластерная структура прихода МЛК

Импульсная характеристика модели канала Салеха-Валенсуэлы описывает отклик канала на дельта-импульс как двойную сумму по кластерам и лучам внутри каждого кластера [10]:

$$h(t) = \sum_{l=0}^{L} \sum_{k=0}^{K} a_{k,l} e^{j\theta_{k,l}} \delta\left(t - T_l - \tau_{k,l}\right), \quad (1)$$

где $a_{k,l}$ – амплитуда k-го луча в l-м кластере, $\theta_{k,l}$ – случайная фаза, T_l – время прихода первого луча l-го кластера, $\tau_{k,l}$ – задержка k-го луча относительно первого луча кластера, δ – дельта- функция Дирака.

На оценку точности первичных дальномерных измерений влияет и различие в сценариях прямой LoS (Line-of-Sight) и непрямой NLoS (Non-Line-of-Sight) видимости. Сценарий LoS возникает, если между базовой станицей БС и пользовательским устройством расстояние меньше, чем дистанция то точки прерывания BP (Breakpoint). Принимаемый сигнал на пользовательском устройстве в таком случае включает как LoS, так и NLoS компоненты, вызванные переотражениями сигнала. Сценарий NLos возникает, если расстояние между БС и пользовательским устройством больше, чем дистанция BP [12].

Модель TGax сохраняет подход, предложенный в работе Салеха-Валенсуэлы, при этом затухание энергии для кластеров и лучей в этой модели носит экспоненциальный характер. Также, для учета LoS и NLoS сценариев целесообразно использовать различные модификации, приведенные в [5]. В таблице 1 представлены виды моделей канала TGax. Каждый из этих видов предназначен для симуляции процесса передачи сигнала в определенных типах сред, что позволяет учитывать специфику распространения МЛК. Так, например, Модель A применяется для расчета в сценариях прямой видимости с минимальным количеством препятствий, а Модель F предназна-

чена для моделирования сред с плотным типом застройки, где имеют место множественные переотражения и преобладают NLoS сценарии.

Также, модель канала TGax позволяет учитывать скорость движения объектов в различных средах. В статичных средах, где скорость изменения положения объектов в пространстве мала, доплеровский сдвиг равен $f_d = 2{,}8$ Гц, а для динамичных сред f_d принимается равным 56 Гц.

ТАБЛИЦА 1. Профили задержки канала TGax

Параметр	Модель					
	A	B	C	D	E	F
Расстояние до точки прерывания, м	5	5	5	10	20	30
СКО задержки, нс	0	15	30	50	100	150
Максимальная задержка	0	80	200	390	730	1050
К-фактор, дБ	0	0	0	3	6	6
Количество отводов	1	9	14	18	18	18
Количество кластеров	1	2	2	3	4	6

На рисунке 2 показаны импульсные характеристики для различных профилей задержки.

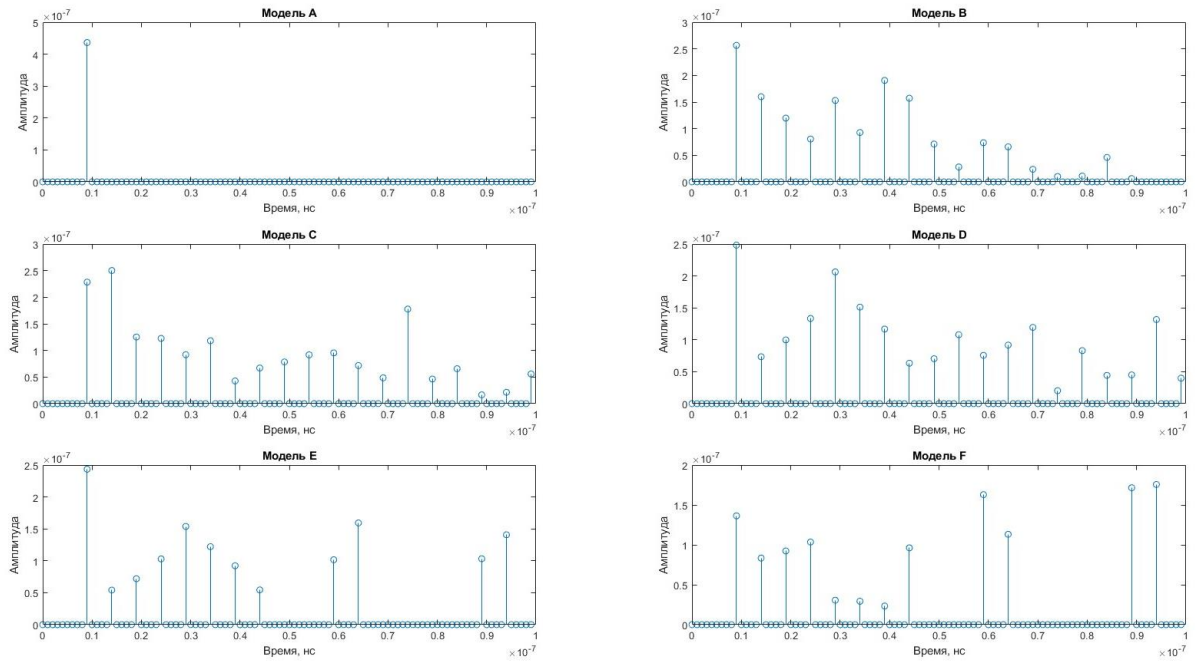


Рис. 2. Импульсные характеристики профилей задержки

Для оценки точности первичных дальномерных измерений для модели канала TGax при использовании различных модификаций в работе проведено имитационное моделирование (ИМ) по модели [13]. Характеристики профилей задержки, приведенные в таблице 1, используются для описания многолучевого канала. В ИМ рассматривается БЛС со следующими параметрами:

– ширина полосы пропускания = 20 МГц;
– количество приемных и передающих антенн = 1;
– количество пространственно-временных потоков = 1;
– количество БС = 3, количество пользовательских устройств = 1;
– значения отношения сигнал/шум SNR (Signal-to-Noise Ratio) = 10; 20 и 30 дБ;
– несущая частота 2.4 ГГц.

В ИМ происходит оценка времени прихода сигнала ToA (Time of Arrival) по алгоритму, описанному в [14]. Оценка точности первичных дальномерных измерений происходит после расчета разности между измеренным и истинным значением ToA. На рисунке 3 представлены результаты ИМ.

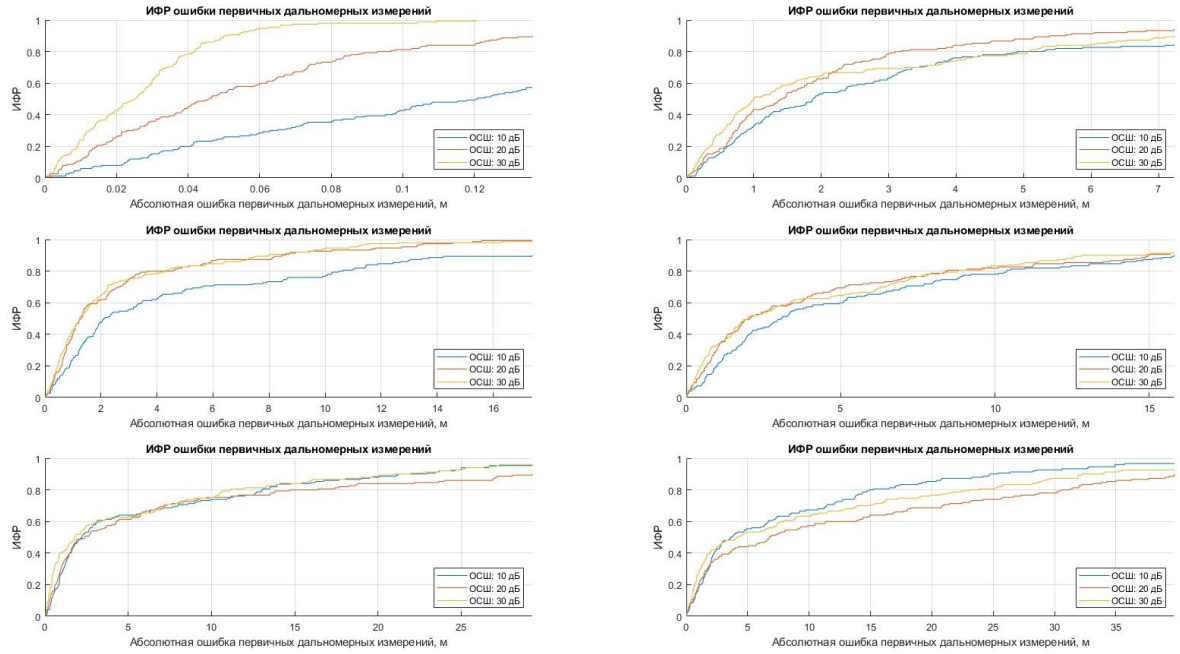


Рис. 3. Оценка точности первичных дальномерных измерений для различных профилей задержки

Результаты, представленные на рисунке 3, демонстрируют ухудшение точности измерений при переходе от простых сценариев распространения (Модель A) сигнала к более сложным (Модель F). Так, для Модели A

ошибка первичных дальномерных измерений не превышает нескольких десятков дециметров, тогда как для Модели F имеют место отклонения вплоть до 35 метров.

Полученные результаты подтверждают теоретические предсказания о влиянии многолучевости на точность позиционирования в стандарте IEEE 802.11az. Представленные результаты ИМ демонстрируют увеличение медианной ошибки, что подчеркивает критическую важность выбора адекватной модели канала и соответствующих алгоритмов компенсации для конкретных условий эксплуатации

Список используемых источников

1. Фокин Г. А. Достижение дециметровой точности позиционирования в гетерогенных сетях NR-Wi-Fi // 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. Т. 4, С. 542-547.

2. Багаев Е. С., Фокин Г. А Модели радиоканала для позиционирования в сетях стандарта IEEE 802.11az. 80-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио: сб. докладов. URL: https://conf-ntores.etu.ru/2025/ru/sbornik-dokladov/ (дата обращения 02.06.2025).

3. Фокин Г. А. Позиционирование в беспроводных локальных сетях Wi-Fi стандарта IEEE 802.11az Часть 1. Постановка задачи достижения дециметровой точности / Г. А. Фокин, Е. С. Багаев, Д. Е. Мещеряков // Первая миля. 2025. № 1(125). С. 50-56. DOI 10.22184/2070-8963.2025.125.1.50.56. EDN YKDPHX.

4. 802.11ax-2021. Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) S. IEEE, 2021.

5. IEEE 802.11ax Task Group. Channel Model Document. URL: https://www.ieee802.org/11/Reports/tgax_update.html (дата обращения 01.06.2025).

6. Erceg V., Schumacher, L., Kyritsi, P. TGn Channel Models. Vol 4. IEEE 802.11-03/940r4, 2004.

7. Breit G., Sampath H., Vermani S. TGac Channel Model Addendum. Vol. 12. IEEE 802.11-09/0308r12, 2010.

8. Фокин Г. А. Модель технологии сетевого позиционирования метровой точности 5G NR. Часть 1. Конфигурация сигналов PRS // Труды учебных заведений связи. 2022. Т. 8. № 2. С. 48–63.

9. Фокин Г. А. Модель технологии сетевого позиционирования метровой точности 5G NR. Часть 2. Обработка сигналов PRS // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 80–99.

10. Saleh A. A. M., Valenzuela R. A statistical model for indoor multipath propagation //IEEE Journal on selected areas in communications. 1987. Т. 5. №. 2. С. 128-137.

11. Meijerink A., Molisch A. F. On the physical interpretation of the Saleh–Valenzuela model and the definition of its power delay profiles // IEEE Transactions on Antennas and Propagation. 2014. Т. 62. № 9. С. 4780-4793.

12. Cao L. et al. Revisiting multi-user downlink in IEEE 802.11 ax: A designer’s guide to mu-mimo // arXiv preprint arXiv:2406.05913. 2024.

13. 802.11az Positioning Using Super-Resolution Time of Arrival Estimation. MathWorks. URL: https://www.mathworks.com/help/wlan/ug/802-11az indoor positioning using super resolution time of arrival estimation.html (дата обращения 09.06.2025).

14. Lee J. H. et al. Application of the Newton method to improve the accuracy of TOA estimation with the beamforming algorithm and the MUSIC algorithm // Progress in Electromagnetics Research. 2011. Т. 116. С. 475-515.

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Г. А. Фокиным

ANALYSIS OF THE RANGING METHOD FOR POSITIONING IN 802.11az NETWORKS

Bagaev E.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Positioning in Wireless Local Area Networks (WLANs) involves determining the location (DL) of a user device or a client station (STA) using the infrastructure of access points (APs) with known coordinates. Traditionally, in WLANs of the IEEE 802.11 working group standards, the fingerprinting method was used, which relied on preliminary collection of Received Signal Strength Indicator (RSSI) measurements, recording them in a database (DB) with coordinate binding, and then matching current measurements with those previously recorded in the DB. This method was characterized by high labor intensity in preparing the DB with radio maps of RSSI measurements received from APs and relatively low accuracy in estimating the coordinates of STA. With the advent of the 802.11az standard, which is specialized for high-precision positioning using the ranging method, achieving decimeter accuracy in estimating the coordinates of STA indoors becomes a practically achievable task. This paper analyzes the operation of the ranging method for positioning in 802.11az networks.

Key words: *802.11az standard, positioning, Wi-Fi wireless local network*

УДК 004.75
ГРНТИ 50.41.21

АРХИТЕКТУРА И ПРИНЦИПЫ РАБОТЫ REDIS: АНАЛИЗ ОДНОПОТОЧНОЙ МОДЕЛИ И МЕХАНИЗМОВ КЛАСТЕРИЗАЦИИ

А. Н. Бадасян, М. Е. Дементьев, А. В. Марочкина, А. С. Юрьева

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

В условиях стремительного роста объемов данных и требований к производительности распределенных систем, традиционные реляционные СУБД сталкиваются с рядом ограничений, связанных с высокой латентностью операций ввода-вывода и сложностью горизонтального масштабирования. В этой связи возрастает актуальность применения in-memory решений, среди которых Redis (Remote Dictionary Server) занимает ключевое место благодаря своей высокой скорости, низкой задержке и поддержке множества необходимых структур данных.

Redis, распределенные системы, отказоустойчивость, кеширование, NoSQL, СУБД, архитектура микросервисов

Изначально разработанный как высокоскоростное key-value хранилище, Redis эволюционировал в многофункциональную платформу обработки данных, поддерживающую сложные структуры (хеши, множества, сортированные наборы, потоки), транзакционные механизмы и продвинутые функции распределенных систем. Подобное многообразие функциональных возможностей породило широкий спектр архитектурных реализаций и применений в различных областях информационной среды [1].

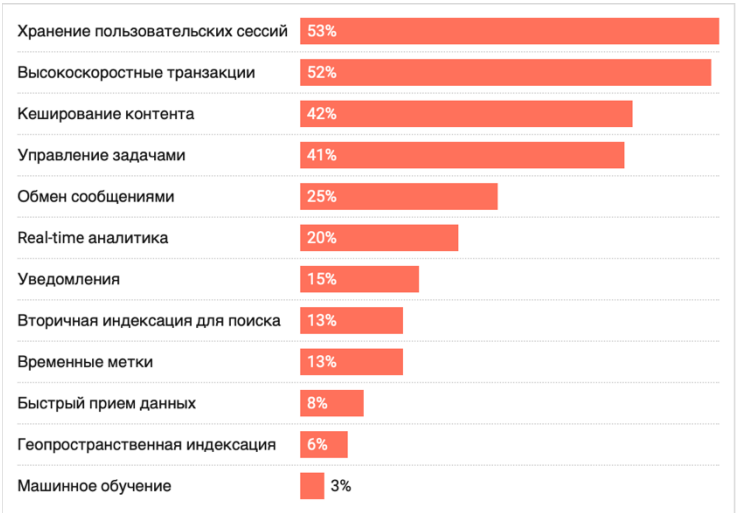


Рис. 1. Статистика основных вариантов использования Redis Enterprise среди 106 пользователей

В контексте современных распределенных систем особый интерес представляет анализ эффективности инструмента как средства кеширования данных (рис. 1). Парадоксальным образом, однопоточная модель выполнения команд, противоречащая современным тенденциям параллельных вычислений, становится ключевым преимуществом при обработке операций кеширования. Сравнения производительности (количества операций в секунду) с Redis-совместимой многопоточной in-memory системой Dragonfly демонстрируют, что в сценариях с многочисленными операциями GET и SET однопоточный Redis 7.0 Cluster опережает своего конкурента на 18-40 % [2].

Помимо результатов сравнительных тестов на производительность, подобное преимущество обуславливается рядом технических особенностей ядра Redis. Во-первых, полное отсутствие необходимости в механизмах синхронизации (блокировках, семафорах или атомарных операциях) исключает такие негативные явления как contention и false sharing, типичные для многопоточных сред. Во-вторых, строго последовательная обработка команд в рамках event-loop оптимальным образом соответствует паттернам доступа к кешированным данным, где значительную часть времени выполнения составляет ожидание сетевого I/O. Экспериментальные измерения показывают, что использование механизма конвейерной обработки команд (pipelining) в Redis позволяет существенно увеличить производительность системы. При выполнении теста на ноутбуке MacBook Air 11” с использованием пакета из 16 команд сервер с однопоточным Redis достигал скорости обработки 1536098 операций SET в секунду с медианной задержкой 0,479 мс и 1811594 операций GET в секунду с медианной задержкой 0,391 мс при общем объеме теста в 1000000 операций [3].

Концепция однопоточной обработки запросов в Redis представляет собой осознанное архитектурное решение, тесно связанное с подходом к горизонтальному масштабированию системы. В контексте Redis Cluster это реализуется через механизм шардирования (разделения данных), где каждый шард (фрагмент данных) представляет собой независимый однопоточный экземпляр Redis, отвечающий за определенный диапазон хеш-слотов. В Redis Cluster используется фиксированное количество – 16384 слотов, равномерно распределяемых между узлами-шардами. Вычисление номера слота для ключа данных сводится к следующей формуле:

$$s(k) = CRC16(k)\ mod\ 16384,$$

где $\mathrm{CRC16}$ – функция, вычисляющая хеш ключа данных по алгоритму CRC16/XMODEM [4].

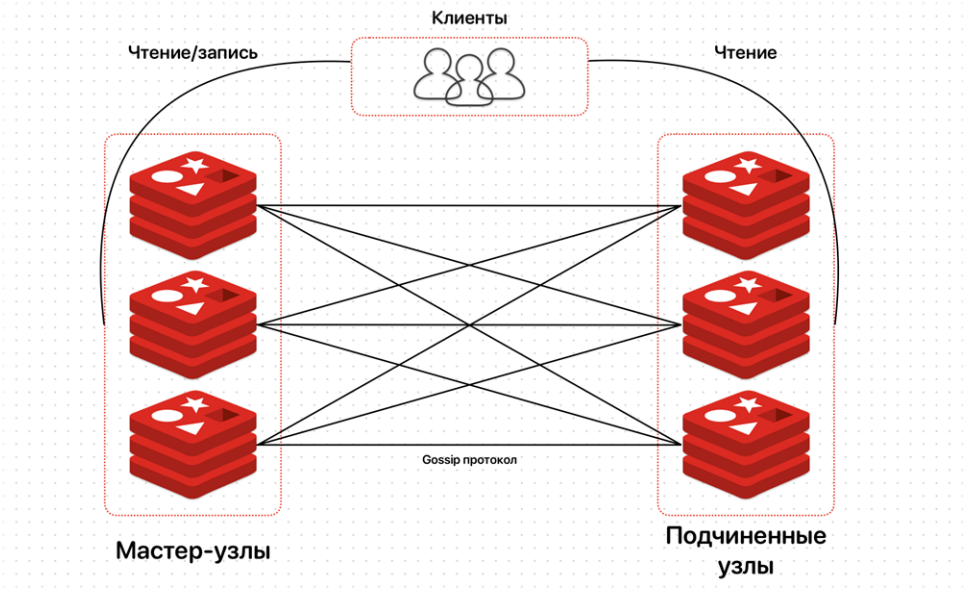


Рис. 2. Структура кластера Redis

Принцип работы кластера основан на частично децентрализованной архитектуре, где каждый узел хранит полную карту распределения слотов и может перенаправлять клиентские запросы к нужному шарду. Механизм эпидемического протокола Gossip обеспечивает синхронизацию метаданных между узлами, а алгоритм согласования изменений, схожий с Raft, гарантирует консистентность при выборе нового мастера для шарда. Каждый шард в Redis Cluster представляет собой логическую единицу масштабирования, состоящую из мастер-узла и одного или нескольких подчиненных узлов (реплик) (рис. 2), что обеспечивает отказоустойчивость при несущественных потерях в производительности.

Для выполнения фоновых задач, которые могут блокировать основной поток, кластер использует порожденные процессы – форки – которые создаются преимущественно для операций сохранения данных из оперативной памяти на диск (RDB-снимки и AOF-логи), работая по принципу copy-on-write для минимизации нагрузки на основной процесс [5].

Отказоустойчивость и распределенность в кластере обеспечивается асинхронной репликацией на уровне каждого шарда. Репликация данных происходит по следующему алгоритму: мастер-узел инициирует синхронизацию данных с подчиненным узлом через RDB-снимок (при отсутствии актуальных данных у подчиненного узла). Во время формирования и передачи RDB-снимка мастер-узел записывает в backlog-буфер команды, которые не были применены к данным на момент создания снимка. Затем недостающие

команды отправляются подчиненному узлу для завершения синхронизации данных. После синхронизации подчиненные узлы применяют недостающие команды к полученным в RDB-снимке данным, работают в режиме read-only и могут автоматически стать мастер-узлами при сбое текущего мастера. Для координации работы кластеров и отслеживания сбоев используется gossip-протокол, в котором содержится карта распределения слотов, состояние узлов и эпоха конфигурации для поддержания консистентности кластера.

В отличие от традиционных многопоточных СУБД, где увеличение производительности достигается за счет усложнения внутренней структуры отдельного процесса, Redis реализует принцип «один процесс – одно ядро процессора». Такой подход обеспечивает несколько ключевых преимуществ в условиях современных распределенных систем. Основная идея заключается в том, что масштабирование производительности достигается не за счет усложнения отдельного экземпляра Redis, а путем добавления новых независимых процессов-шардов. На практике это означает возможность запуска нескольких экземпляров Redis на одной физической или виртуальной машине – по количеству доступных вычислительных ядер. Каждый такой экземпляр функционирует как самостоятельный узел в составе кластера, отвечая за определенный сегмент данных и операций.

Горизонтальное масштабирование происходит с помощью добавления нового шарда в кластер и механизма решардинга (перераспределения слотов между узлами), позволяющего динамически добавлять или удалять узлы с минимальным влиянием на общую производительность системы.

Например, в исходном распределении кластер состоял из двух узлов-шардов: M1 и M2, каждый из которых отвечал за ключи с номерами 0-8191 и 8192-16383 соответственно. После добавления нового узла – M3 – происходит решардинг, перераспределяющий номера ячеек равномерно между тремя узлами: M1 отвечает за ключи с номерами 0-5460, M2 – за ключи с номерами 5461-10922, M3 – за ключи с номерами 10923-16383. Преимущества такого подхода заключаются в отсутствии необходимости повторного вычисления номеров всех ключей и в перемещении в новый узел-шард только тех данных, чьи номера вышли за перераспределенные границы других узлов.

Особую актуальность данный подход приобретает в контексте микросервисных архитектур, где критически важными становятся следующие характеристики: возможность оперативного увеличения мощности отдельных компонентов системы через добавление новых шардов, гарантированное

время отклика на запросы благодаря детерминированному распределению данных по слотам, простота управления вычислительными ресурсами за счет атомарности каждого шарда, а также устойчивость к отказам отдельных элементов благодаря репликации каждого фрагмента данных.

Таким образом, Redis утвердился как технологическая основа для построения распределенных отказоустойчивых систем, где однопоточная архитектура служит не ограничением, а инструментом эффективного горизонтального масштабирования через кластеризацию. Данное решение доказало свою производительность в сценариях высокой нагрузки. Однако тренд развития отрасли проявляется в появлении Redis-совместимых систем, которые, реализуя многопоточные модели, бросают вызов традиционной парадигме «один процесс – одно ядро», открывая новые направления для оптимизации.

Список используемых источников

1. Прия Балакришнан. Redis Enterprise для основной базы данных, хранения сеансов, высокоскоростных транзакций и многого другого. // Redis. URL: https://redis.io/blog/results-redis-enterprise-primary-database-session-store-high-speed-transactions/ (дата обращения 26.05.2025)

2. Шульман И., Готлиб Й., Оливейра Ф. 13 лет спустя – нужна ли Redis новая архитектура? // Redis. – URL: https://redis.io/blog/redis-architecture-13-years-later/ (дата обращения 25.05.2025)

3. Бенчмарк Redis // Redis. URL: https://redis.io/docs/latest/operate/oss_and_stack/management/ optimization/benchmarks/ (дата обращения 02.06.2025)

4. Документация Redis Cluster // Redis. URL: https://redis.io/docs/latest/operate/oss_and_stack/reference/cluster-spec/ (дата обращения 01.06.2025)

5. Комягин А. REDIS: такой простой и такой сложный // Хабр. URL: https://habr.com/ru/companies/stm_labs/articles/841792/ (дата обращения 02.06.2025).

REDIS ARCHITECTURE AND PRINCIPLES OF OPERATION: ANALYSIS OF THE SINGLE-THREADED MODEL AND CLUSTERING MECHANISMS

Badasyan A., Dementiev M., Marochkina A., Yurieva A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the rapid growth of data volumes and performance requirements for distributed systems, traditional relational DBMSs face a number of limitations related to high latency of I/O operations and complexity of horizontal scaling. In this regard, the relevance of in-memory solutions is increasing, among which Redis (Remote Dictionary Server) occupies a key place due to its high speed, low latency and support for a variety of required data structures.

Key words: *Redis, distributed systems, fault tolerance, caching, NoSQL, DBMS, microservices architecture*

УДК 004.75
ГРНТИ 50.41.25

АРХИТЕКТУРНЫЕ ОСНОВЫ APACHE KAFKA И ПОШАГОВОЕ РУКОВОДСТВО ПО ЗАПУСКУ

А. Н. Бадасян, М. Е. Дементьев, А. В. Марочкина, А. С. Юрьева

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

В условиях перехода к распределенным микросервисным архитектурам традиционные методы интеграции уступают брокерам сообщений, таким как Apache Kafka. Благодаря высокой пропускной способности, асинхронной доставке и горизонтальному масштабированию, Kafka незаменима для создания высоконагруженных и отказоустойчивых систем, работающих с потоками данных в реальном времени.

Apache Kafka, брокеры сообщений, горизонтальное масштабирование, микросервисы, архитектура

1. Введение

На начальных этапах разработки приложения часто используют монолитную архитектуру, при которой вся логика размещается на одном сервере. Такой подход уязвим с точки зрения безопасности и отказоустойчивости: сбой одного компонента может нарушить работу всей системы. Кроме того, монолитная архитектура ограничена пропускной способностью шины процессора и оперативной памяти – при высокой нагрузке это может привести к перегрузке и отказу системы.

По мере развития проекта возникает необходимость перехода к микросервисной архитектуре, в которой компоненты функционируют на изолированных серверах. Взаимодействие между серверами часто строится через протокол HTTP, что порождает ряд проблем: отсутствие гарантий безопасности передачи данных, синхронность операций и необходимость заранее знать адрес получателя.

В качестве альтернативы могут применяться брокеры сообщений – программные посредники, управляющие потоками сообщений между приложениями и обеспечивающие обмен данными, – такие как Apache Kafka. Такие решения обеспечивают гарантированную доставку сообщений, асинхронное взаимодействие сервисов и эффективное масштабирование за счет поддержки модели «один производитель – множество потребителей» [1].

2. Apache Kafka

Apache Kafka – распределенная потоковая платформа, обрабатывающая данные в реальном времени через несколько серверов, объединенных в кластер. Каждый сервер, или брокер сообщений, участвует в обработке потоков данных.

Основная функция Kafka – обмен сообщениями между производителями и потребителями, где каждый сервис может быть как производителем, так и потребителем в брокере сообщений. Для организации эффективного обмена данными, Kafka использует топики (topics) – категории или каналы данных, по которым группируются сообщения. Топики заменяют традиционные очереди сообщений и структурируют данные по темам.

Каждый топик делится на разделы (partitions) с целью параллельной обработки сообщений. Важно отметить, что порядок доставки сообщений сохраняется только внутри отдельного раздела, но не между разделами в рамках одного топика [2].

На рис. 1 изображена архитектура брокера Apache Kafka с 3 топиками и 2 партициями в каждой.

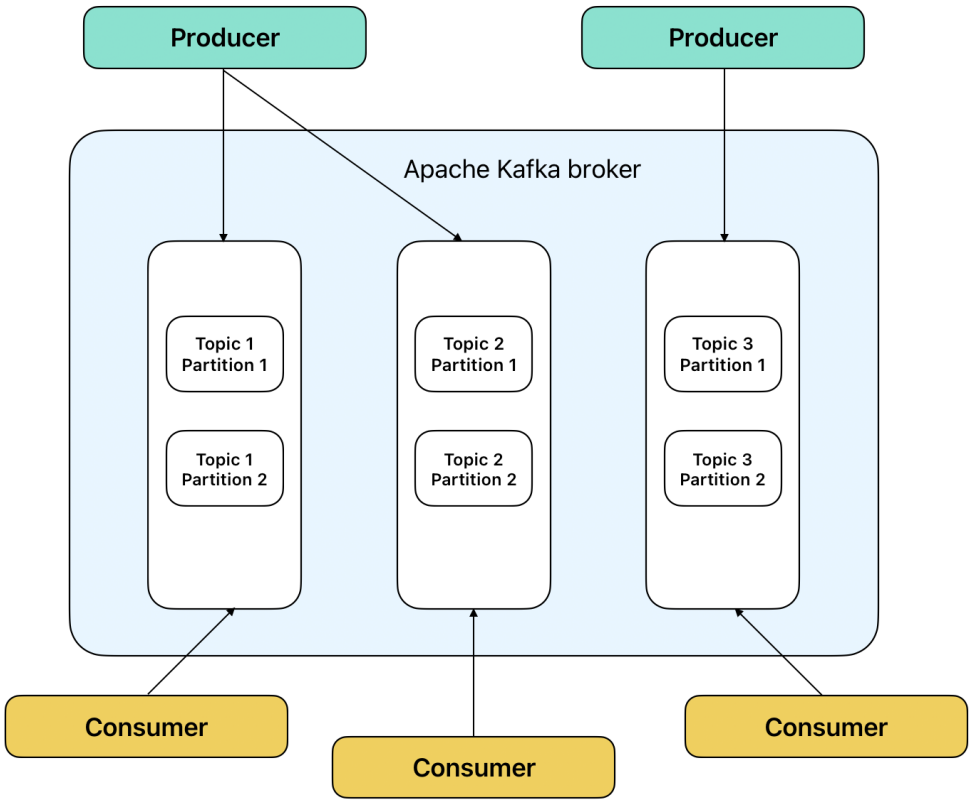


Рис. 1. Архитектура брокера в Apache Kafka

Для обеспечения правильного порядка получения сообщений необходимо направить их в один раздел. Это достигается при помощи ключа сообщения. Сообщения с одинаковым ключом всегда попадают в одну и ту же партицию, что гарантирует их строгий порядок при чтении из этой партиции. Сообщения без ключа (или с null-ключом) распределяются по партициям циклически (round-robin), что не гарантирует их упорядоченность относительно друг друга.

После записи каждое сообщение получает смещение (offset) – уникальный идентификатор, который позволяет потребителям продолжать чтение с последнего обработанного сообщения. В случае отключения сервиса, он сможет возобновить чтение с того места, где оно было прервано.

3. Гарантии доставки сообщений

Для обеспечения надежности каждая партиция реплицируется на различных брокерах. Каждый брокер в кластере Apache Kafka имеет уникальный идентификатор и управляет хотя бы одним разделом (партицией), что видно на рис. 2. Количество реплик (копий) партиции задается параметром Replication Factor. Для надежности доставки сообщения используется Partition Leader: лидер принимает сообщения, а реплики синхронизируются с ним. После подтверждения получения большинством реплик запись считается зафиксированной.

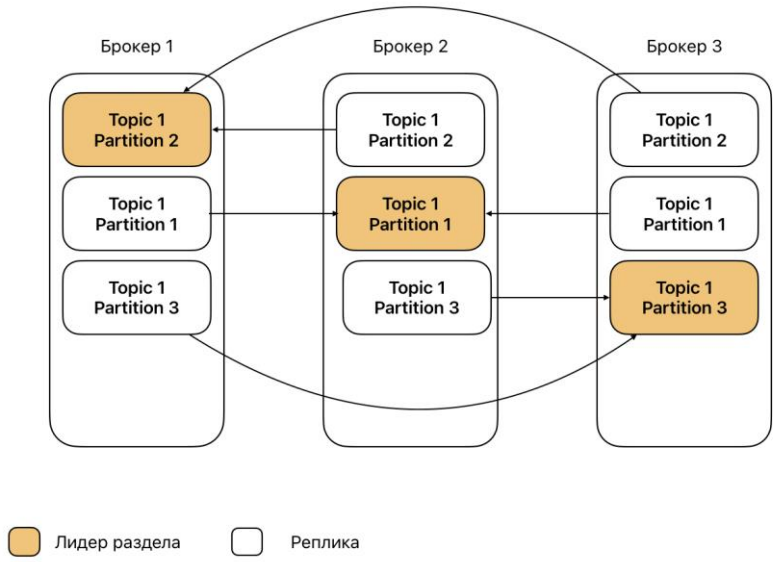


Рис. 2. Принцип репликации одной темы с тремя разделами и параметром Replication Factor равным трем

Функционирование Apache Kafka требует надежного и согласованного механизма для хранения и синхронизации метаданных. К метаданным относится информация о составе топиков и их конфигурациях, количество партиций в каждом топике, расположение лидеров (Partition Leaders) и их реплик (followers) для каждой партиции на конкретных брокерах.

До версии Kafka 2.8.0 управление метаданными и обеспечение консенсуса полностью зависело от Apache ZooKeeper – внешнего распределенного сервиса координации, ответственного за хранение состояния, выборы лидеров и отказоустойчивость кластера. Такая зависимость создавала значительные эксплуатационные сложности: требовала поддержки отдельного кластера ZooKeeper и усложняла администрирование и обновление всей системы.

Начиная с версии 2.8.0, Kafka представила режим KRaft (Kafka Raft Metadata Mode), полностью устраняющий зависимость от ZooKeeper путем переноса управления метаданными внутрь самого кластера.

В основе KRaft лежит алгоритм консенсуса Raft, разработанный для обеспечения согласованности состояния (метаданных Kafka) в распределенной системе даже при частичных сбоях узлов (брокеров). Raft гарантирует наличие единственного активного лидера (Controller) в каждый момент времени, который служит единым источником истины для метаданных [3].

Ключевым механизмом, обеспечивающим эту гарантию, является leader epoch (монотонно возрастающий номер при избрании нового Controller'a) предотвращает действия устаревших "зомби"-лидеров (устаревших лидеров, пытающихся записать данные после потери кворума), обеспечивая консистентность данных.

В KRaft брокеры выполняют роли: Controller (единственный лидер метаданных), Active Controller (голосующие члены кворума, хранят лог и подтверждают изменения) и Broker (наблюдатели, синхронизируют метаданные). Controller и Active Controller образуют кворум (большинство) для фиксации изменений, выборов нового Controller'a и поддержания согласованности.

Надежность передачи сообщений обеспечивается при помощи параметра конфигурации подтверждение (ack). Параметр ack определяет минимальное количество подтверждений, требуемое продюсером для признания записи успешно доставленной брокеру. Доступные значения параметра:

ack = none – Продюсер считает запись доставленной немедленно после отправки на брокер без ожидания подтверждения. Гарантии доставки отсутствуют.

ack = one – Продюсер ожидает подтверждения от лидера партиции о внесении записи в локальный лог. Обеспечивается базовый уровень надежности.

ack = all – Продюсер ожидает подтверждения от лидера и всех синхронизированных реплик партиции. Гарантируется максимальная надежность доставки[4].

Для распределения нагрузки на сервер и параллельной обработки партиций используются потребительские группы – логические объединения потребителей, где каждый участник группы закрепляется за отдельной партицией топика. Оптимальная производительность обеспечивается при равенстве числа потребителей количеству партиций [5].

Благодаря такой архитектуре Kafka обеспечивает высокую производительность, отказоустойчивость и масштабируемость, что делает ее ключевым компонентом в построении надежных распределенных систем.

4. Запуск Apache Kafka

Для работы с Apache Kafka, реализованной на платформе Java, необходимо предварительно установить Java Development Kit (JDK), доступный для загрузки на официальном сайте Oracle. Последовательность установки и запуска Kafka включает следующие этапы.

Установка и распаковка дистрибутива:

– $ tar -xzf kafka_2.13-4.0.0.tgz
– $ cd kafka_2.13-4.0.0

Инициализация и запуск брокера:

– $ KAFKA_CLUSTER_ID="$(bin/kafka-storage.sh random-uuid)"
– $echo $KAFKA_CLUSTER_ID
– $ bin/kafka-storage.sh format --standalone -t $KAFKA_CLUSTER_ID -c config/server.properties
– $ bin/kafka-server-start.sh config/server.properties

Остановка сервера:

– $ bin/kafka-server-stop.sh

После генерации идентификатора кластера необходимо сохранить его в конфигурационном файле server.properties. Это обеспечит корректную ра-

боту брокера при последующих запусках. После выполнения данной настройки для старта сервера будет достаточно единственной команды: bin/kafka-server-start.sh config/server.properties.

Для работы с топиками в Kafka используются следующие команды.

Создание топика:

– bin/kafka-topics.sh --bootstrap-server localhost:9092 --create --topic <имя_топика> --partitions <количество_партиций> --replication-factor <фактор_репликации>

Просмотр списка топиков:

– bin/kafka-topics.sh --bootstrap-server localhost:9092 --list

В качестве примера создадим 2 топика с 2 партициями. Для отправки данных в топик воспользуемся консольным продюсером.

Создание консольного продюсера:

– bin/kafka-console-producer.sh --bootstrap-server localhost:9092 --topic <имя_топика>

Создание консольного консьюмера:

– bin/kafka-console-consumer.sh --bootstrap-server localhost:9092 --topic \
– --partition -from-beginning

Параметр --from-beginning указывает на чтение с начала, а не с отступа. В качестве примера отправим в топик два сообщения, после чего подключим консьюмера и отправим еще два сообщения. На рис. 3 представлен результат.

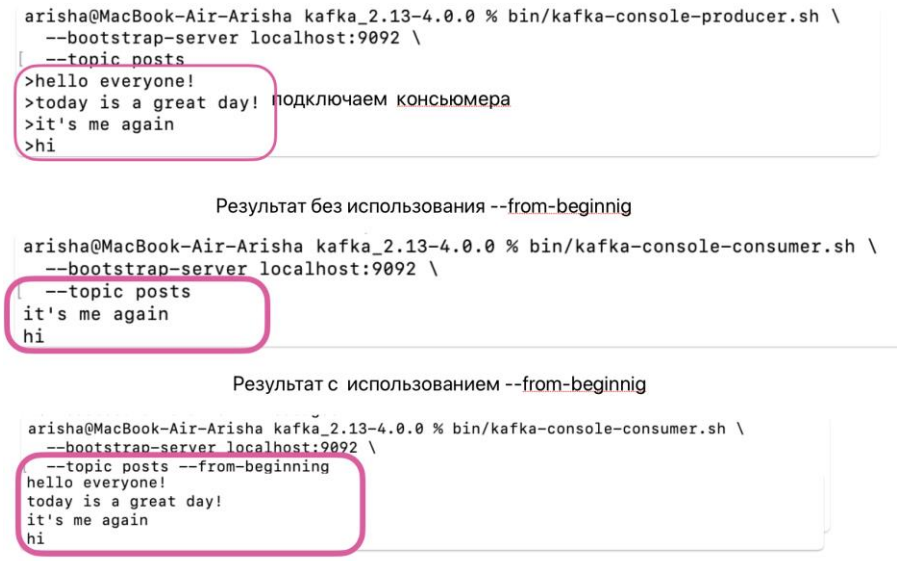


Рис. 3. Разница получения сообщений консьюмеров с параметром --from-beginning и без

5. Вывод

Apache Kafka – распределенная платформа для потоковой обработки данных, обеспечивающая гарантированную доставку сообщений и асинхронную обработку даже при экстремальных нагрузках. Ее архитектура гарантирует отказоустойчивость и эффективную горизонтальную масштабируемость. Kafka легко интегрируется в любую инфраструктуру благодаря поддержке множества языков программирования и развитому API. Совокупность всех перечисленных факторов делает Apache Kafka универсальным решением для построения распределенных систем.

Список используемых источников

1. Колосова А. Брокеры сообщений, или как происходит взаимодействие в рамках распределенной инфраструктуры // Хабр. 2022. URL: https://habr.com/ru/companies/ sberbank/articles/ 669456/ (дата обращения 22.04.2025).

2. Apache Kafka, Официальная документация URL: https://kafka.apache.org/ documentation/#gettingStarted (дата обращения 22.04.2025).

3. Guozhang Wang. Почему KRaft заменил ZooKeeper / пер. А. Сокол // Хабр. 2022. URL: https://habr.com/ru/companies/slurm/articles/685694/ (дата обращения 22.04.2025)

4. Аверина П., 5 вещей, о которых должен знать любой разработчик Apache Kafka // Хабр. 2022. URL: https://habr.com/ru/companies/slurm/articles/547264/ (дата обращения 22.04.2025).

5. Ушаков С. Что такое потребительские группы в Kafka и для чего они нужны. URL: https://kafka-school.ru/blog/kafka-groups/ (дата обращения 22.04.2025).

APACHE KAFKA ARCHITECTURAL BASICS AND STEP-BY-STEP STARTUP GUIDE

Badasyan A., Dementiev M., Marochkina A., Yurieva A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of the transition to distributed microservice architectures, traditional integration methods are inferior to message brokers such as Apache Kafka. Due to its high throughput, asynchronous delivery, and horizontal scaling capabilities, Kafka is an indispensable tool for creating highly loaded and fault-tolerant systems that work with real-time data flows.

Key words: *Apache Kafka, message brokers, horizontal scaling, microservices, architecture*

УДК 004.353.254.5
ГРНТИ 47.63.29

СВЕТОДИОДНЫЕ ЭКРАНЫ И ИХ ЭЛЕМЕНТЫ

Ю. С. Березина[1], С. В. Перелыгин[2]

[1] ООО «Вижен Сервис»
[2] Санкт-Петербургский государственный институт кино и телевидения

В статье рассмотрены структурные элементы светодиодного экрана, современные технологии производства светодиодов для LED-экранов, их особенности, достоинства и недостатки. Описана архитектура системы управления светодиодного экрана, обозначены этапы передачи сигнала от главного управляющего устройства к светодиодам.

светодиодные экраны, светодиодные дисплеи, DIP, SMD, COB, драйверы IC

Структура светодиодного экрана

Светодиодный экран – это экран, который использует светодиоды для формирования изображения.

Светодиодный экран состоит из отдельных блоков – светодиодных панелей, которые в профессиональной среде называют кабинетами (англ. cabinets). Размеры кабинетов могут достигать нескольких метров в длину и/или ширину. Каждый кабинет, в свою очередь, состоит из отдельных светодиодных модулей – более мелких единиц размерами, как правило, до нескольких десятков сантиметров. Светодиодный модуль состоит уже непосредственно из светодиодов, установленных на печатной плате, и необходимых для формирования и вывода изображения радиоэлементов [1]. На рис. 1 наглядно показана структура светодиодного экрана.

Светодиод – самая мелкая структурная единица светодиодного экрана. Каждый пиксель светодиодного экрана состоит из трех светодиодов – красного, зеленого и синего, т.е. представляет собой классический RGB-пиксель. В зависимости от того, какие светодиоды и с какой яркостью светятся в каждом пикселе, будет меняться видимый человеком цвет.

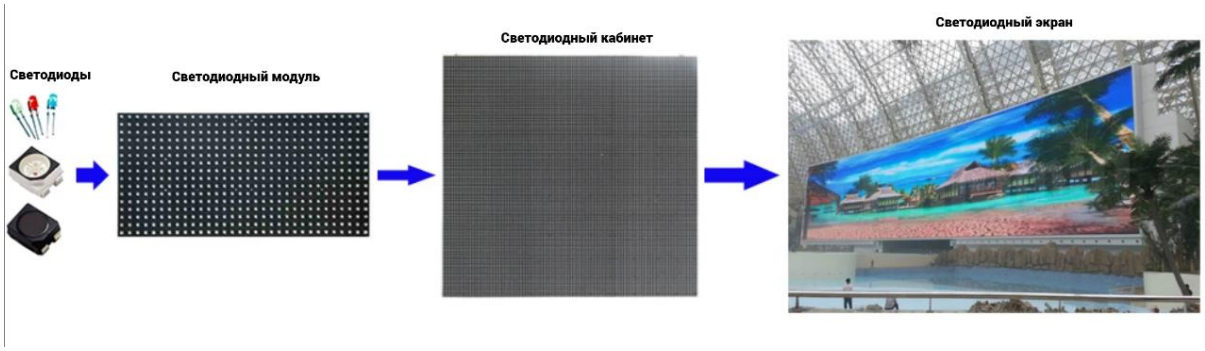


Рис. 1. Структура светодиодного экрана (на основе оригинала, взятого из [2])

Шаг пикселя (расстояние между двумя соседними пикселями) является одним из важнейших параметров любого светодиодного экрана и влияет на дистанцию просмотра изображения. Упрощенно можно сказать, что минимальная дистанция просмотра должна быть в 1 000 раз больше, чем шаг пикселя [3].

Светодиодный модуль представляет собой многослойную печатную плату, на которую устанавливаются светодиоды, радиоэлементы и микросхемы, необходимые для работы. Сама плата, как правило, устанавливается на специальный корпус, который обеспечивает ее защиту и позволяет крепить каждый модуль к металлическому профилю кабинета.

Кабинет – это рамная конструкция, на которую крепятся отдельные модули. В состав кабинета, помимо непосредственно конструкции для крепления и модулей, входит также вспомогательное оборудование, а именно: блоки питания, карты приема и пр. (например, система охлаждения), если оно требуется.

Технологии изготовления светодиодов

В настоящее время наиболее распространены следующие технологии: DIP (англ. dual in-line package) и SMD (англ. Surface Mounted Devices); также приобретают распространение GOB (англ. Glue On Board), COB (англ. Chip On Board) и MiP (англ. MicroLED In Package) светодиоды. В таблице 1 приведено сравнение данных технологий.

ТАБЛИЦА 1. Основные технологии производства светодиодов для экранов (на основе [4 - 8])

Название технологии	Конструкция светодиодов	min шаг пикселя	Недостатки	Преимущества
DIP	В колбе, выполняющей роль линзы, на катоде располагается кристалл светодиода, являющийся источником свечения. Кристалл с помощью анодного провода соединен с катодом	6 мм	- невозможность получить маленький шаг пикселя; - узкий угол обзора; - один корпус – один кристалл – один светодиод	- высокая надежность; - простота ремонта отдельных светодиодов; - устойчивость к воздействиям внешней среды; - долгий срок службы
SMD	Кристаллы светодиодов располагаются на подложке, в которую вмонтированы анод и катод; вся конструкция помещается в корпус, который сверху накрыт линзой	0,9 мм	- хрупкость отдельных светодиодов; - меньший срок службы по сравнению с DIP-светодиодами; - сложный ремонт отдельных светодиодов	- компактный размер; - низкая цена; - широкий угол обзора; - простота автоматизации производства; - кристаллы всех трех цветов в одном корпусе
COB	Кристаллы светодиодов располагаются не в корпусе, а непосредственно на подложке печатной платы	Менее 1 мм	- сложность ремонта – при выходе из строя одного пикселя необходимо менять весь модуль; - дороговизна	- высокое качество изображения; - стойкость к воздействиям окружающей среды и механическим повреждениям
GOB	SMD-светодиоды дополнительно покрываются компаундом, образовывающим защитный слой	1,5 мм	- сложность ремонта; - сложнее отвод тепла; - дороговизна	- стойкость к воздействиям окружающей среды и механическим повреждениям;
MiP	Основана на технологии MicroLED, но с дополнительным корпусированием. Микроскопические кристаллы светодиодов (до миллионов) располагаются на чипах, размещаемых в корпусах (размеры корпусов – сотни микрон). Корпуса устанавливаются на общую плату	0,3 мм	- дороговизна; - сложность производства; - сложность ремонта	- самый мелкий шаг пикселя из существующих на сегодняшний день для светодиодных экранов; - высокие параметры качества изображения

Архитектура светодиодного экрана

Светодиодный экран, являясь сложной технической системой, требует наличия специальной многоступенчатой системы управления.

Архитектура системы управления в общем виде показана на рисунке 2. Основные элементы системы управления приведены в таблице 2.

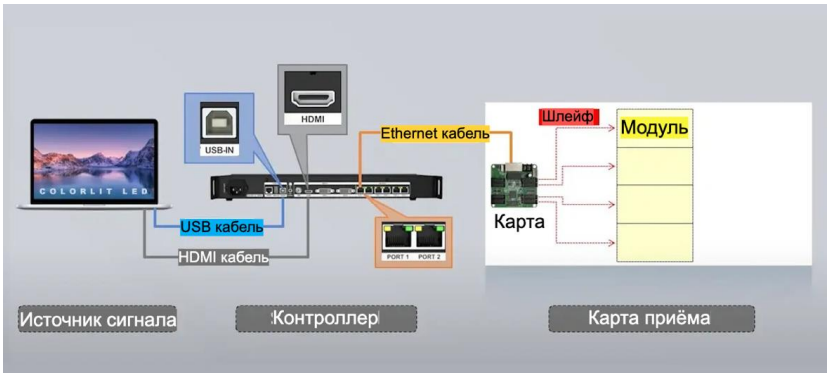


Рис. 2. Архитектура светодиодного экрана (на основе оригинала, взятого из [9])

ТАБЛИЦА 2. Элементы системы управления светодиодного экрана и их функции

Элемент	Назначение	Особенности	Объект управления
Управляющий сервер	Источник видеосигнала; главное управляющее устройство	Представляет собой ПК или сервер с установленным ПО для воспроизведения контента и управления экраном	Видеопроцессор и/или передающая карта (контроллер)
Видеопроцессор	Масштабирование видеосигнала; обработка сигнала	Может быть объединен с контроллером в одном устройстве (All-in-One устройства)	Передающая карта (контроллер)
Передающая карта (контроллер)	Передача сигнала с источника на экран, распределение изображения по кабинетам	Без видеопроцессора не сможет масштабировать сигнал, передача изображения «пиксель в пиксель». Может быть объединен с процессором в одном устройстве (All-in-One устройства)	Карты приема
Карта приема	Распределение изображения по модулям в пределах одного кабинета	1 карта приема = 1 кабинет. Для корректной работы необходим правильный файл конфигурации кабинета, где будут указаны используемые микросхемы	Микросхемы внутри модуля (декодер и IC-драйвер)
Декодер	Формирование построчной развертки в пределах одного модуля	Присутствует не во всех экранах. Некоторые IC-драйверы поддерживают формирование развертки непосредственно в микросхеме драйвера; в некоторых экранах развертка отсутствует	Строки или столбцы светодиодного модуля
IC-драйвер	ШИМ-управление яркостью свечения светодиодов в пределах одного модуля или его части	Число светодиодов, которыми одновременно может управлять один IC-драйвер, ограничено числом каналов драйвера	Отдельные светодиоды

Путь прохождения сигнала внутри экрана между кабинетами и модулями определяется конфигурацией кабинета и маппингом (англ. mapping) экрана, т.е. файлами, которые отражают в системе, как физически соединены модули и панели внутри экрана. Подробнее маппинг и конфигурация кабинета будут рассмотрены в соответствующей статье.

Заключение

Были рассмотрены основные структурные единицы светодиодного экрана от светодиодов к кабинетам. Настоящий обзор позволяет получить базовое представление о принципе работы как экрана в целом, так и его элементов.

Светодиодный экран является сложной системой с многоступенчатой системой управления, построенной по принципу иерархии. Для проектирования и эксплуатации систем на основе светодиодных экранов необходимо обладать глубокими теоретическими знаниями и постоянно развивать прикладные компетенции. Это позволит специалисту выбирать оптимальную конфигурацию системы для получения наилучшего качества изображения.

Список используемых источников

1. How LED Display Work: A Complete Guide for Beginners. URL: https://www.unit-led.com/how-led-display-work (дата обращения 12.06.2025).
2. What are the components of LED displays? URL: https://www.twleddisplay.com/blog/what-are-the-components-of-led-displays (дата обращения 14.06.2025).
3. Choosing the Best Pixel Pitch For Your LED Display . URL: https://www.assured-signage.com/choosing-the-best-pixel-pitch-for-your-led-display/ (дата обращения 10.06.2025).
4. COB vs GOB in LED Display. URL: https://www.eagerled.com/cob-vs-gob-in-led-display/ (дата обращения 10.06.2025).
5. Светодиоды DIP и SMD. В чем разница?. URL: https://www.rusimpuls.ru/about/publications/7704/ (дата обращения 10.06.2025).
6. Understanding the Differences Between DIP, SMD, and COB in LED Screen Installation. URL: https://www.novastar.tech/novastar-innovation/understanding-the-differences-between-dip-smd-and-cob-in-led-screen-installation/ (дата обращения 14.06.2025).
7. Micro LED: The Essence of MiP Packaging as the Upstream of COB. URL: https://www.minimicroled.com/mip-packaging-micro-led-2024-advances-cob/ (дата обращения 15.06.2025).
8. MicroLED: The Next Revolution In Display Technology. URL: https://blog.delmic.com/microled-revolutionary-technology (дата обращения 11.06.2025).
9. Comprehensive Guide to LED Display Connection. URL: https://www.colorlitled.com/led-display-connection/ (дата обращения 11.06.2025).

LED SCREENS AND THEIR ELEMENTS

Berezina I. [1], Perelygin S. [2]
[1] OOO Vision Service
[2] St. Petersburg State Institute of Cinema and Television

The article examines the structural elements of the LED screen, modern technologies for producing LEDs for LED screens, their features, advantages and disadvantages. The architecture of the LED screen control system is described, the stages of signal transmission from the main control device to the LEDs are designated.

Key words: *LED screens, LED displays, DIP, SMD, COB, IC drivers*

УДК 004.42, 004.021:004.932.2
ГРНТИ 50.41.25

АЛГОРИТМ ОЦЕНКИ КАЧЕСТВА КАДРОВ FPV-ВИДЕОПОТОКА

А. А. Березкин, А. И. Козлова, А. А. Ченский

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

При управлении от первого лица в рамках беспилотной авиационной системы видеопоток с камеры, установленной на беспилотном воздушном судне, передается на станцию внешнего пилота. Для понимания полетной обстановки и управления беспилотным воздушным судном данный видеопоток просматривает внешний пилот. Точность распознавания внешним пилотом полетной обстановки зависит от того, насколько близок видеопоток, восстановленный видеокодеком, к исходному. Качество восстановленных кадров видеопотока определяется степенью их близости к исходным кадрам. В настоящей работе представлен алгоритм, предназначенный для решения задачи оценки качества восстановленных кадров FPV-видеопотока.

качество, качество изображения, видеокодек, видеопоток, управление от первого лица, беспилотный летательный аппарат, беспилотное воздушное судно, беспилотная авиационная система, БПЛА

Введение

Как известно, беспилотная авиационная система (БАС) включает в себя ряд элементов, такие как беспилотное воздушное судно (БВС, также БПЛА – беспилотный летательный аппарат), станцию внешнего пилота, а также линии связи с землей и линии связи с бортом. Управление БВС от первого лица (FPV – first person view) осуществляется внешним пилотом (ВП) на основе видеопотока и телеметрических данных, поступающих со стороны камеры, установленной на БВС. Для передачи телеметрической информации могут применяться такие системы, как Remote ID [1] и разрабатываемая в СПбГУТ система идентификации БВС на основе DOA (digital objects architecture – архитектура цифровых объектов) [2]. Команды управления вводятся ВП на СВП. Для управления может применяться такие протоколы, как UranusLink, MAVCan, MAVLink [3].

Наибольшая полоса пропускания необходима для передачи видеопотока. Для ее уменьшения в настоящее время применяются техники кодирования (сжатия) кадров видеопотока видеокодеками. Традиционно для этих целей применяются видеокодеки стандартов AVC/H264, HEVC/H265, VP9

и AV1 [4]. Наиболее перспективной на сегодняшний день является технология сжатия FPV-видеопотока на основе нейросетевых кодеков, особенностью которых является низкая необходимая полоса пропускания [5–7]. Из недостатков данной технологии следует выделить заметные искажения восстановленных кадров.

Качество восстановления кадров видеопотока представляет собой степень искажения восстановленных кадров видеопотока относительно исходных. Оно определяется видеокодеком и его параметрами. Для оценки качества восстановления кадров видеопотока в настоящее время широко используются объективные метрики качества: *SSIM* (structural similarity – структурное сходство) и *PSNR* (peak sound to noise ratio – пиковое отношение сигнала к шуму) [8].

При оценке качества восстановления кадров видеопотока, сжатых стандартными кодеками, необходимо измерить среднее значение метрик качества для всех кадров видеопотока. Однако, такая оценка связана с рядом проблем:

– потери кадров видеопотока. Это приводит к зависаниям, артефактам кадров (при утрате I-кадра и поступлении P- и B-кадров) и при потере всех кадров за некоторый временной интервал (зависанию изображения на экране оператора).
– задержки кадров видеопотока. При передаче кадров видеопотока возникает задержка. Эта задержка приводит к тому, что при отображении кадров видеопотока и их съемке кадры, снятые на кодере и декодере, будут отличаться.

Данные проблемы приводят к тому, что при наличии потерь порядковые номера исходных и восстановленных кадров не будут соответствовать, а при наличии задержек не будут соответствовать моменты времени кадров. Потеря каждого кадра видеопотока приводит к уменьшению номера восстановленного кадра и, как следствие, порядковый номер не может быть использован для определения соответствия кадров. Задержка видеопотока представляет собой стохастическую величину. Следовательно, в общем случае задержка видеопотока даже при поправках не может быть использована для определения соответствия кадров.

Таким образом, возникает проблема синхронизации кадров видеопотока и устранения выбросов (артефактов, подвисаний изображения). В некоторых исследованиях [9] для синхронизации кадров видеопотока приме-

няется метрика *PSNR*, но в то же время алгоритмы и методы синхронизации подробно не рассматриваются. В других исследованиях [10] выполняется вставка кадров на базе информации о потерях, но это приводит к вычислению метрик между кадрами, которые не соответствуют друг другу, и как следствие искажению результата. В настоящей работе предлагается алгоритм для оценки качества кадров, восстановленных стандартными видеокодеки, с учетом синхронизации исходных и восстановленных кадров.

Алгоритм

Пусть с БВС на СВП с применением некоторого стандартного кодека передается тестовый видеопоток интенсивностью *FPS* кадров в секунду, длительность которого составляет *sec* секунд. Тогда исходные кадры видеопотока повторяются с периодом $per = sec \times FPS(\text{кадров})$.

Пусть уровень потерь кадров видеопотока в канале информационного обмена оценивается как *loss* %. Тогда период повторения восстановленных кадров видеопотока будет приблизительно равен

$$per^* \approx per \times loss/100(\text{кадров}).$$

Схема алгоритма представлена на рис. 1.

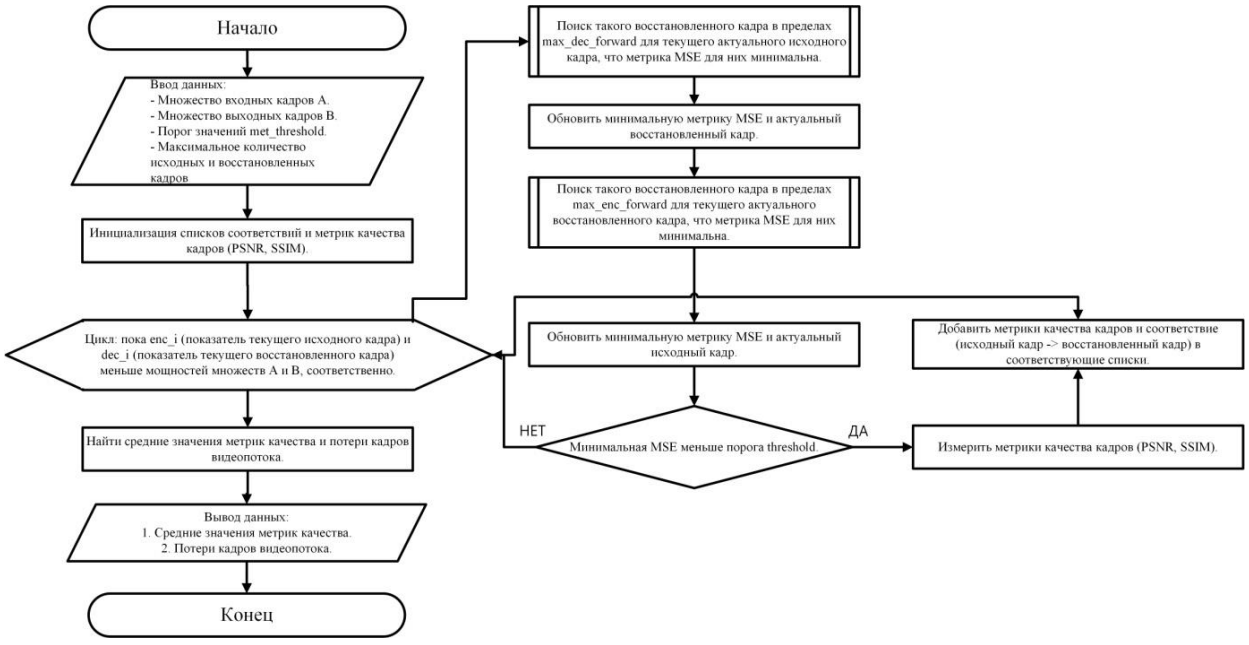


Рис. 1. Обобщенная схема алгоритма

Алгоритм базируется на ряде предпосылок:

1. Есть такое множество исходных кадров видеопотока A_i такое, что метрика качества *met* (в частности, может применяться *MSE* [8]) восстановленного кадра b_i с кадрами из данного множества равна и минимальна.

2. Элементы множества A_i представляют собой кадры, взятые из множества исходных кадров A с периодом *per*.

3. Существует такое множество восстановленных кадров видеопотока B_i, что метрика качества *met* исходного кадра a_i с кадрами из данного множества приблизительно равна и минимальна. Полное равенство достигается в том случае, если восстановленные кадры одного и того же типа (I, P, B) и при P и B – одного порядкового номера при отсчете от предыдущего I-кадра.

Элементы множества B_i представляют собой кадры, которые отбираются из множества восстановленных кадров B каждые *pb* кадров, причем $pb \approx per$ * представляет собой стохастическую величину.

На вход алгоритма поступают множества исходных и восстановленных кадров A и B, порог метрики *met_threshold* и максимальные количества исходных и восстановленных кадров для анализа *max_enc_forward* и *max_dec_forward*.

1. Инициализация *cur_enc_i* и *cur_dec_i* как 0.

2. Инициализация *max_enc_i* и *max_dec_i* как мощности множеств A и B соответственно.

3. Инициализация списков: соответствий *assoc_list* и финальных метрик (например, *psnr_list* и *ssim_list*).

4. Цикл с предусловием: $cur_enc_i < max_enc_i$.

   4.1. Получение значений *met* между *cur_enc_frame* и элементами множества B с индексами [*cur_dec_i*; max(*cur_dec_i* + *max_dec_forward*; *max_dec_i*)] кадров видеопотока. Значению *min_met* присваивается минимальное значение *met*, а *cur_dec_i* – индекс соответствующего элемента множества B.

   4.2. Инициализация $cur_dec_frame = b_{cur_dec_i}$.

   4.3. Нахождение минимального значения *min_met* между *cur_dec_frame* и элементами множества A с индексами [*cur_enc_i*; max(*cur_enc_i* + *max_enc_forward*; *max_enc_i*)] кадров видеопотока. *cur_enc_i* – индекс соответствующего элемента множества A.

   4.4. Присваивание $cur_enc_frame = a_{cur_enc_i}$.

4.5. Если *met* > *met_threshold*, то считается, что соответствие не найдено. Переход на следующую итерацию.

4.6. Добавление кортежа (*cur_enc_i*, *cur_dec_i*) в *assoc_list*.

4.7. Нахождение метрик качества между *cur_enc_frame* и *cur_dec_frame* и добавление их в соответствующие списки.

5. Нахождение потерь кадров видеопотока *floss* как отношение длины списка *assoc_list* к мощности множества *A*.

6. Нахождение средних значений метрик качества.

7. Вывод *floss* и средних значений метрик качества.

На выходе алгоритма: средние значения метрик качества (*PSNR*, *SSIM*), потери кадров видеопотока.:

Заключение

Оценка качества восстановления кадров FPV-видеопотока связана с проблемой синхронизации кадров, возникающей вследствие потерь и задержек передачи кадров по каналу информационного обмена.

В настоящей работе представлен алгоритм, выполняющий синхронизацию кадров видеопотока на основе метрики качества *MSE* (допускаются альтернативные метрики) и проводящий оценку качества. Полученный результат позволяет оценивать и сравнивать методы кодирования видеопотока: видеокодеки с установленными параметрами. Выполнение алгоритма привело к увеличению значения метрик качества *PSNR* и *SSIM* кадров, восстановленных стандартными кодеками, при испытаниях передачи видеопотока по геостационарной системе спутниковой связи «Ямал-601».

В программной реализации алгоритма предлагается: поступление на вход программы вместо множеств кадров *A* и *B* директорий исходных и восстановленных кадров; кеширование прочитанных кадров кодера и декодера.

Научная статья подготовлена в рамках прикладных научных исследований СПбГУТ, регистрационный номер 1024032900105-1-2.2.4;2.2.5;2.2.6 в ЕГИСУ НИОКТР.

Список используемых источников

1. Belwafi K., Alkadi R., Alameri S. A., Al Hamadi H., Shoufan A. Unmanned aerial vehicles' remote identification: A tutorial and survey // IEEE Access. 2022. T. 10. C. 87577–87601.

2. Ченский А. А., Березкин А. А. Разработка программного обеспечения для нагрузочного тестирования систем идентификации и мониторинга беспилотных летательных аппаратов // Актуальные проблемы инфотелекоммуникаций в науке и образовании:

Сборник научных статей XIII Международной научно-технической и научно-методической конференции в 4 т., Санкт-Петербург, 27–28 февраля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2024. С. 101–106.

3. Khan N. A., Jhanjhi N. Z., Brohi S. N., Nayyar A. Emerging use of UAV's: secure communication protocol issues and challenges // Drones in smart-cities. Elsevier, 2020. С. 37–55.

4. Layek M. A., Thai N. Q., Hossain M. A., Thu N. T., Tuyen L. P., Talukder A., Huh, E. N. Performance analysis of H. 264, H. 265, VP9 and AV1 video encoders // 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2017. С. 322–325.

5. Ченский А. А., Березкин А. А., Киричек Р. В., Захаров А. А. Исследование методов латентного сжатия видеопотока при FPV управлении беспилотными системами // Электросвязь. 2024. № 6. С. 46–56.

6. Ченский А. А., Березкин А. А., Киричек Р. В., Захаров А. А. Исследование методов квантования латентного пространства вариационного автокодировщика для кадров FPV видеопотока. Часть I // Электросвязь. 2024. № 6. С. 58–64.

7. Ченский А. А., Березкин А. А., Киричек Р. В., Захаров А. А. Исследование конфигураций нейросетевых кодеков для адаптивной системы сжатия кадров FPV-видеопотока при управлении беспилотными системами. Часть I. Методика // Электросвязь. 2024. № 9. С. 42–51.

8. Martinez-Rach M., López O., Pinol P., Malumbres M. P., Oliver J. A study of objective quality assessment metrics for video codec design and evaluation // Eighth IEEE International Symposium on Multimedia (ISM'06). IEEE, 2006. С. 517–524.

9. González N., Solera M., Ruiz F., Gijón C., Toril M. A quality of experience model for live video in first-person-view drone control in cellular networks // Computer Networks. 2023. Т. 237. С. 110089.

10. Klaue J., Rathke B., Wolisz A. Evalvid–a framework for video transmission and quality evaluation // Computer Performance Evaluation. Modelling Techniques and Tools: 13th International Conference, TOOLS 2003, Urbana, IL, USA, September 2-5, 2003. Proceedings 13. Springer Berlin Heidelberg, 2003. С. 255–272.

ALGORITHM FOR ESTIMATION OF FPV VIDEO STREAM FRAMES, QUALITY

Berezkin A., Kozlova A., Chenskiy A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the first-person control of an unmanned aircraft system, the video stream from the camera mounted on the unmanned aircraft is transmitted to the external pilot's station. In order to understand the flight environment and control the unmanned aircraft, this video stream is observed by the external pilot. The accuracy of the external pilot's recognition of the flight situation depends on the closeness of the video stream reconstructed by the video codec to the original video stream. The quality of the reconstructed video stream frames is determined by the degree of their closeness to the original frames. This paper presents an algorithm, designed to solve the problem of estimating the quality of reconstructed video stream frames.

Key words: *quality, quality estimation, video codec, standard video codec, video stream, first person control, unmanned aerial vehicle, unmanned aircraft system, algorithm, software.*

УДК 378.14
ГРНТИ 14.35.07

К ПРОБЛЕМЕ ФОРМИРОВАНИЯ ИССЛЕДОВАТЕЛЬСКОЙ КОМПЕТЕНЦИИ БУДУЩИХ ИНЖЕНЕРОВ

Д. И. Бурумбаев, А. В. Стремедловский, В. А. Чупина

Уральский технический институт связи и информатики (филиал) Сибирского государственного университета телекоммуникаций и информатики
Уральский государственный педагогический университет

Цель работы – провести аналитический обзор научной литературы по проблеме формирования исследовательской компетенции будущего инженера. Исследовательская компетенция представлена с позиции ее дескрипторного наполнения, особое внимание уделено развитию инженерного мышления, исследовательской культуры, созданию образовательных сред.

инженерное образование, исследовательская компетенция, развитие мышления, исследовательская культура, организационно-педагогические условия

В настоящее время большое внимание со стороны государства уделяется вопросам инженерного образования. Одним из примеров является программа «Приоритет-2030», ключевой задачей которой является процесс поддержки вузов в подготовке кадров и проведении исследований для обеспечения технологического лидерства Российской Федерации [1]. Другим примером поддержки инженерного образования со стороны государства является федеральный проект «Передовые инженерные школы», в котором «студенты создают инновационные разработки для реального сектора экономики, чтобы внести вклад в развитие технологического суверенитета нашей страны» [2].

Поддержка инженерного образования со стороны государства свидетельствует об острой необходимости в инженерах, которые, обладая исследовательской компетенцией, способны проводить научные исследования и решать нестандартные задачи в своей отрасли. Однако для подготовки таких специалистов недостаточно содействия государства, необходимо обновление методологических, методических и организационно-педагогических основ формирования исследовательской компетенции.

Понятие исследовательской компетенции в инженерном образовании подразумевает способность к поиску решения творческих задач и предпола-

гает наличие у будущего инженера соответствующих знаний, умений, практического опыта и личностно-профессиональных качеств. Все четыре дескриптора исследовательской компетенции нашли отражение в научных исследованиях. Ряд авторов отмечает, что для современного инженера важным является сформированность компетенций, которые позволят решать постоянно меняющиеся креативные инновационные задачи, творчески подходить к их анализу и проработке, восполнять недостающие знания самоподготовкой и непрерывным повышением своей квалификации. Они предлагают две модели формирования таких компетенций: практико-ориентированное образование и работа в научно-образовательных центрах, отмечая, что работоспособность данных моделей зависит от различных условий, поэтому при проектировании образовательного процесса необходимо учитывать специфику отрасли, уровень образование, потребности обучающихся [3]. Исследовательскую компетенцию инженера отличают особые личностные качества: самостоятельность, ответственность, самоорганизация, инженерное мышление, творческое начало в инженерной деятельности, для чего их необходимо формировать не только в рамках учебной дисциплины, но и отдельно через программу воспитания [4]. Также в научных исследованиях поднимается тема формирования исследовательской компетенции в условиях определенной отрасли, когда компетенция начинает формироваться при проведении первых экспериментов на общих курсах технических дисциплин, что развивает у студента творческое мышление, самостоятельность и другие личностно-профессиональные качества [5]. Важность исследовательской компетенции в инженерном образовании подчеркивается работодателями, подавляющее большинство которых считает, что исследовательская компетенция влияет как на профессиональное развитие, так и на личностное. Авторы исследования подчеркивают, что компоненты исследовательской компетенции могут отличаться в зависимости от отрасли и заказа работодателя, но есть ее общие составляющие: умение работать с технической и научной литературой, критическое мышление, умение создавать прототипы, проводить эксперимент [6].

Большое внимание при формировании исследовательской компетенции уделяется развитию мышления будущего инженера. В ряде работ утверждается, что он должен обладать не только комплексом универсальных и профессиональных компетенций, но и глубокими фундаментальными знаниями, инновационным мышлением, быть мотивированным на непрерыв-

ное самообразование. Подчеркивается, что для развития такого мышления студента необходимо привлекать к математическому моделированию [7]. Другие авторы предлагают возможности использования элементов STEM и STEAM, где STEM подразумевает использование научно-исследовательский действия для закрепления знаний и умений, а подход STEAM добавляет направление Art – искусство, в результате чего помимо технических и инженерных компетенций формируются компетенции креативного и критического мышления [8].

С исследовательской компетенцией инженера неразрывно связан культурный компонент, влияющий на ее формирование, творческая составляющая, которой пока еще уделяется недостаточно внимания при подготовке инженеров. В свою очередь, инженерное творчество имеет социальную значимость, так как общество нуждается в новаторских решения, которые способствуют научно-техническому прогрессу [9]. В других работах отмечается, что исследовательская культура является одним из ключевых факторов для решения социальных проблем и развития технологий в целях улучшения качества жизни современного общества, что инженеры, способные проводить исследования, самостоятельно разрабатывать инновационные решения и умело применять передовые достижения на практике, являются более востребованными на рынке труда [10]. Размышляя об исследовательской культуре инженера, некоторые авторы считают, что изменения в системе высшего образования, направленные на повышение качества и результативности образовательного процесса, не коснулись вопросов, связанных с формированием ценностно-поведенческих установок будущих инженеров. Поэтому предлагается добавить нравственный компонент исследовательской культуры в образовательные программы, чтобы у инженеров формировалась не только исследовательская культура, но и нравственный компонент как неотъемлемая часть данной культуры [11].

Рассуждая о проблеме формирования исследовательской компетенции, нельзя обойти вниманием организационно-педагогические и дидактические условия, в которых данный процесс становится более результативным, что подтверждается рядом научных работ. В своих исследованиях авторы поднимают проблему развития мотивации будущих инженеров к научно-техническому творчеству, к участию в инновационно-производственных и технологических процессах, проектной деятельности, что требует обновления образовательной среды вуза, дидактики, педагогических методов [12, 13].

Особое внимание уделяется методу проектов, благодаря которому формирование исследовательских компетенций специалиста технического направления осуществляется посредством проектно-исследовательской деятельности, которая должна быть связана с решением межотраслевых проблем, формирующих прикладные знания, а важным условием организации такой работы является взаимодействие с предприятием, чтобы студенты могли ознакомиться с его производственными процессами [14].

Одним из важнейших условий современного образования является организация цифровой образовательной среды, которая для формирования исследовательской компетенции будущего инженера играет ключевую роль. В этом аспекте заслуживает внимательного рассмотрения концепция формирования исследовательской компетенции с помощью двух методов: проектного и исследовательского, в рамках которых каждый обучающийся учится формировать гипотезы, исследовать интересующие его вопросы, критически мыслить. При формировании такой компетенции отдельное внимание уделяется информационным технологиям, которые позволяют делать процесс обучения более интерактивным, персонализированным и увлекательным, создают условия для личностного и интеллектуального роста каждого обучающегося [15]. Другим примером является использование информационных технологий, формирующих инженерное мышление средствами 3D-технологий. Авторы технологии подчеркивают, что Индустрия 4.0 и приоритеты цифрового общества определяют требования к инженерам будущего, который должен обладать такими компетенциями: готовность и способность к исследовательской работе, креативность, интеллектуальные навыки, ответственность [16].

В процессе подготовки инженера-исследователя одним их главных является условие сетевого взаимодействия государства, работодателя и университета. Важной задачей формирования технологического суверенитета страны является качество инженерных кадров, способных решать нестандартные задачи, генерировать инновационные идеи в условиях трансформации технологий, науки и производства, поэтому для подготовки выпускника инженерного образования с исследовательским потенциалом необходима тесная работа инженерных вузов, научных организаций и отраслевых предприятий [17].

Таким образом, на основании проведенного анализа можно сделать вывод, что формирование исследовательской компетенции в инженерном об-

разовании зависит от большого количества условий и факторов: отрасль подготовки выпускников, требования профессиональных стандартов и работодателей, специально организованные образовательные среды, согласованность действия государства, работодателей и вузов.

Список используемых источников

1. Программа «Прииоритет-2030». // URL: https://национальныепроекты.рф/new-opportunities/uchitsya-v-vedushchikh-vuzakh-i-zanimatsya-naukoy/ (дата обращения 06.05.2025).

2. Федеральный проект «Передовые инженерные школы». // URL: https://национальныепроекты.рф

3. Галиновский А. Л. Компетентностный портрет специалиста в новых моделях инженерного образования / А. Л. Галиновский, Ю. В. Баданина, В. А. Моисеев // Вестник Пермского национального исследовательского политехнического университета. Проблемы языкознания и педагогики. 2017. № 3. С. 139-149. DOI 10.15593/2224-9389/2017.3.12.

4. Данилаев Д. П. Воспитание профессионально значимых качеств в системе инженерного образования / Д. П. Данилаев, Н. Н. Маливанов // Высшее образование в России. 2024. Т. 33. № 1. С. 87-105. DOI 10.31992/0869-3617-2024-33-1-87-105.

5. Тютяев А. В. Формирование исследовательских компетенций у студентов нефтегазового профиля в техническом университете / А. В. Тютяев, В. Н. Михелькевич, Я. В. Малолеткова // Современные проблемы науки и образования. 2023. № 5. С. 51. DOI 10.17513/spno.32931.

6. Федорова М. А. Представление работодателя о значимых научно-исследовательских компетенциях выпускников инженерных вузов / М. А. Федорова, М. В. Цыгулева // Вестник Сибирского института бизнеса и информационных технологий. 2017. № 3(23). С. 89-96.

7. Голубева Н. В. Инженерное образование: на пути к профессионализму / Н. В. Голубева // Перспективы науки. 2020. № 2(125). С. 127-131.

8. Вахитова Е. И. Использование элементов STEM и STEAM в профессиональном обучении при подготовке бакалавров технического профиля / Е. И. Вахитова, А. А. Федорова // Вопросы педагогики. 2019. № 2. С. 20-22.

9. Моргунова С. Б. К вопросу о феномене культуры творческой деятельности будущего инженера / С. Б. Моргунова, Ю. М. Гришаева // Материалы ежегодной Международной заочной научно-практической конференции. 2021. № 4. С. 69-76.

10. Бакаев А. А. Актуальность формирования и содержание исследовательской культуры будущего инженера / А. А. Бакаев // Primo Aspectu. 2024. № 3(59). С. 34-38. DOI 10.35211/2500-2635-2024-3-59-34-38.

11. Лебедева, Н. А. Нравственный компонент исследовательской культуры студентов технического вуза / Н. А. Лебедева, Л. П. Белю // Современные проблемы науки и образования. 2024. № 6. С. 75. DOI 10.17513/spno.33832.

12. Минин М. Г. Формирование компетенции инженерного изобретательства на примере студентов элитного технического образования НИ ТПУ / М. Г. Минин, Д. С. Денчук // Инженерная педагогика. Том 1, Выпуск 17. Москва: Московский автомобильно-дорожный государственный технический университет (МАДИ), 2015. С. 154-159.

13. Власова Е. А. Подготовка инженера-исследователя технического вуза в условиях интеграции научно-образовательной деятельности в партнерстве с отраслевыми предприятиями / Е. А. Власова, В. С. Попов // Мир науки. Педагогика и психология. 2024. Т. 12. № 3.

14. Тарасова, Е. Н. К вопросу организации проектно-исследовательской деятельности студентов в инженерном вузе / Е. Н. Тарасова, О. Ю. Хацринова // Управление устойчивым развитием. 2021. № 1(32). С. 109-115.

15. Носков, Н. Г. Реализация процесса формирования проектно-исследовательских компетенций в инженерном культурно-образовательном пространстве на практике / Н. Г. Носков // Вестник Пермского государственного гуманитарно-педагогического университета. Серия № 1. Психологические и педагогические науки. 2024. № 2. С. 61-68. DOI 10.24412/2308-717X-2024-2-61-68.

16. Суворова Т. Н. Особенности формирования инженерного мышления средствами 3D-технологий / Т. Н. Суворова, Е. А. Мамаева // Научно-методический электронный журнал «Концепт». 2020. № 8. С. 71-86. DOI 10.24411/2304-120X-2020-11058.

17. Горшкова, О. О. Подготовка конкурентоспособного выпускника, обладающего исследовательским потенциалом, в инновационной интегрированной среде инженерного вуза / О. О. Горшкова // Современные наукоемкие технологии. 2022. № 1. С. 128-132. DOI 10.17513/snt.39021.

TOWARDS THE PROBLEM OF FORMING THE RESEARCH COMPETENCE OF FUTURE ENGINEERS

Burumbaev D., Stremidlovsky A., Chupina V.
Ural Technical Institute of Communications and Informatics (branch) of the Siberian State University of Telecommunications and Informatics
Ural State Pedagogical University

The purpose of the work is to conduct an analytical review of the scientific literature on the problem of forming the research competence of a future engineer. Research competence is presented from the perspective of its descriptive content, special attention is paid to the development of engineering thinking, research culture, and the creation of educational environments.

Key words: *engineering education, research competence, development of thinking, research culture, organizational and pedagogical conditions*

УДК 004.932.2
ГРНТИ 28.23.15

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ПРЕОБРАЗОВАНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТЯХ НА ПРИМЕРЕ МЕТРИКИ РАССТОЯНИЯ ФРЕШЕ

А. Н. Бучатский, А. П. Лосев

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

Математические алгоритмы работы с видеопоследовательностями имеют значительное влияние на работу с пространственной и временной информацией. Управление передачей данных типов информации является приоритетной задачей записи и воспроизведения видеопоследовательностей, а также алгоритмов преобразования видео. Задача эффективной передачи видеоинформации по каналам связи дополнительно актуализируется в рамках современных форматов видеопоследовательностей высокого разрешения, а также видеопоследовательностей с панорамным изображением и расширенным динамическим диапазоном. В работе рассмотрены основные математические алгоритмы детектирования и преобразования пространственной и временной информации на примере метрики расстояния Фреше между видеопоследовательностями.

пространственная и временная информация, расстояние Фреше, фильтр Собеля, цветовое пространство

Математические методы обработки изображений – основа передачи и хранения видеопоследовательностей в цифровом виде. Алгоритмы анализа и преобразования видеоинформации позволяют осуществлять задачи сжатия, поиска объектов, предобработки, а также анализа видеопотока при помощи искусственных нейронных сетей. Также, математические методы позволяют экономить скорость цифрового потока видеоинформации при хранении и передаче видео.

Основой представления видеоинформации с цветом является попиксельная передача значений индивидуальных каналов цвета, где каждый пиксель содержит информацию о канале зеленого, красного и синего цвета в целочисленных значениях от 0 до 255, если используется 8-битное представление видео и цветовое пространство RGB. Визуализация изображения при помощи данного цветового пространства является наиболее применимой на конечных устройствах (например, жидкокристаллические дисплеи) и позво-

ляет получить любой цвет посредством комбинации трех каналов базовых цветов, однако для цифровых преобразований используется представление видеоинформации в пространстве YCbCr, в связи с большей применимостью данного цветового пространства к алгоритмам кодирования, а также в связи с большей чувствительностью человеческих органов зрения к изменениям яркости, чем к изменениям цвета [1]. Цветовое пространство YCbCr в качестве основного информационного канала использует коэффициент яркости, вычисляемый как взвешенное усреднение для RGB-изображения по формуле 1:

$$y = k_r R + k_g G + k_b B \quad (1)$$

где k – весовой множитель для каждого из каналов цвета, утверждаемый для различных стандартов цифрового телерадиовещания Международным союзом электросвязи (МСЭ). Согласно рекомендациям МСЭ для систем телевидения высокой четкости [2], расчет сигнала яркости производится по формуле 2:

$$E'_Y = 0{,}2126E'_R + 0{,}7152E'_G + 0{,}0722E'_B \quad (2)$$

Алгоритмы сжатия, преобразования и извлечения видеоинформации используют яркость сегментов изображения в качестве основного источника информации, что повышает важность данных компонент видеопотока. Для вычисления пространственной и временной информации в видео используются фильтры Собеля с различными ядрами для свертки по горизонтали и по вертикали [3]. Матрицы ядер для свертки размера 3×3 по горизонтали K_x и по вертикали K_y представлены в формуле 3:

$$K_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix}, K_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} \quad (3)$$

соответственно, интенсивности яркости пикселя изображения a_{ij}, который расположен на строке i и столбце j и обработан фильтром Собеля по горизонтали (I_x) и по вертикали (I_y), вычисляются по формуле 4:

$$I_x = \sum_{k=1}^{3}\sum_{m=1}^{3} K_{x,km} b_{km}\,, I_y = \sum_{k=1}^{3}\sum_{m=1}^{3} K_{y,km} b_{km} \quad (4)$$

что позволяет найти результирующую яркость пикселя (I) по формуле 5:

$$I = \sqrt{I_x^2 + I_y^2} \quad (5)$$

Фильтр Собеля позволяет формировать представление о границах яркости благодаря оконному методу сканирования изображения, что позволяет находить границы объектов и отдельные зоны интереса внутри изображения. Пример работы фильтра Собеля представлен на рисунке 1:

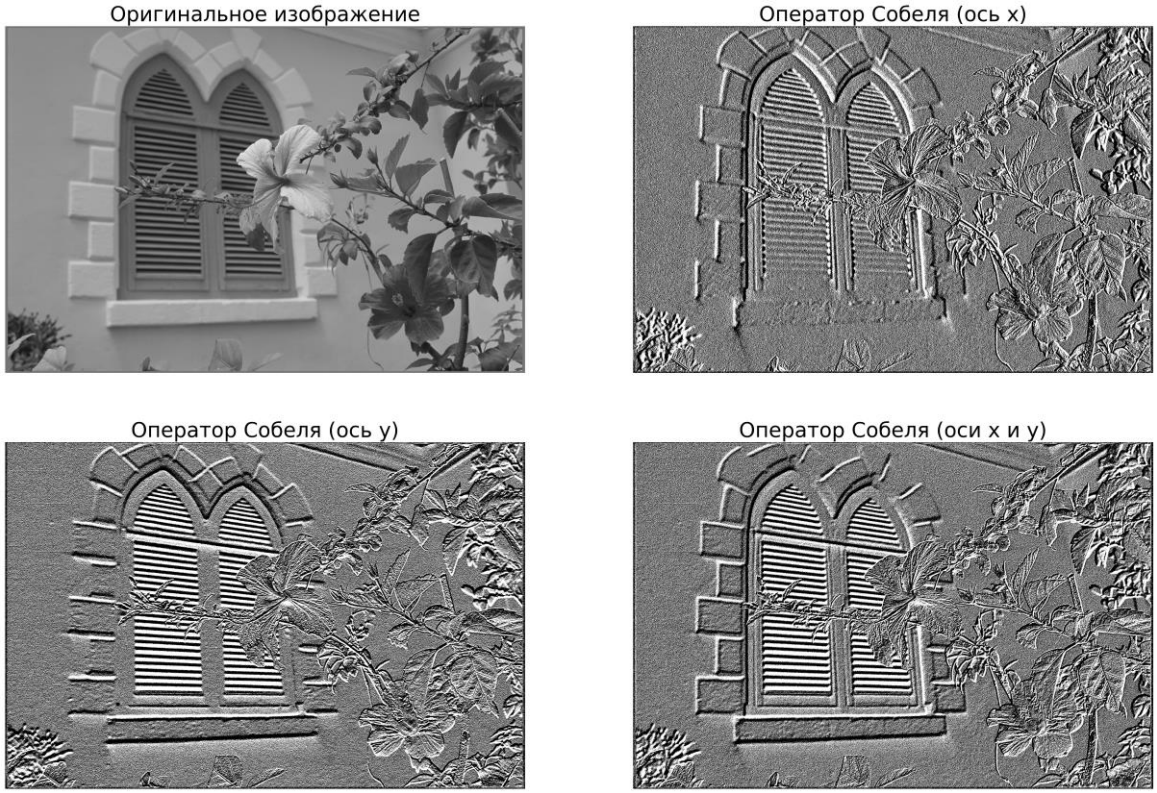


Рис. 1. Исходное изображение и изображения после обработки фильтром Собеля

Подход оконного сканирования изображений фильтром Собеля позволяет получать пространственную информацию (SI) для видеофайла из N кадров как вычисления максимума от стандартного отклонения покадровых значений яркости, в соответствии с формулой 6:

$$SI = \max_{0 \le n \le N-1} \left\{ \operatorname*{std}_{\substack{1 \le i \le W-2 \\ 1 \le j \le H-2}} [I_{sum}] \right\} \quad (6)$$

где I_{sum} является результирующим значением яркостей после работы фильтра Собеля [4]. Значение временной информации (TI) рассчитывается на основе разниц в видоизменениях кадров $F_n \in F_0, F_1, \ldots, F_{N-1}$ и отражено в формуле 7:

$$TI = \max_{1\le n\le N-1}\left\{\operatorname*{std}_{\substack{0\le i\le W-1\\0\le j\le H-1}}\left[F_n - F_{n-1}\right]\right\} \quad (7)$$

Подходы анализа информации при помощи представления последовательности кадров как набора математически извлеченных признаков используется и на данный момент при объективной оценке качества результатов работы генеративных искусственных нейронных сетей. Примером данного подхода является метрика оценки расстояния Фреше. Так как генеративная нейронная сеть [5] использует распределение данных как источник результирующей генерации, то разница между реальным нормальным распределением P_R и нормальным распределением P_G, определенным нейронной сетью, является метрикой соответствия результатов генерации реальным данным. Однако, с учетом отсутствия единых распределений при реальной работе нейронной сети, при оценке работы используют начальное расстояние Фреше, рассчитываемое между P_R и P_G соответственно по формуле 8:

$$d(P_R, P_G) = min_{X,Y}\, E\,|X - Y|^2 \quad (8)$$

где X и Y являются общими совокупностями случайных переменных в распределениях P_R и P_G соответственно [6]. С учетом того, что оба распределения являются многомерными гауссовскими распределениями, данное выражение расстояния Фреше затруднительно рассчитать для общих случаев, правая часть формулы 8 преобразуется в соответствии с выражением из формулы 9 для расчета общих случаев расстояния Фреше:

$$|\mu_R - \mu_G|^2 + Tr\left(\Sigma_R + \Sigma_G - 2(\Sigma_R\Sigma_G)^{\frac{1}{2}}\right) \quad (9)$$

Выражение 9 является расстоянием Фреше для генеративных моделей нейронных сетей, в котором μ_R и μ_G являются средними значениями реальных и сгенерированных данных, а Σ_R и Σ_G – ковариации распределений P_R и P_G соответственно. Расчет данных параметров позволяет объективно оценить генерации видеоинформации, выполняемые нейронной сетью.

Несмотря на использование расстояния Фреше при оценке генеративных моделей, недавние исследования выявили несоответствия корреляции метрики с субъективным восприятием человека. Исследователи, анализировавшие работу метрики, установили, что расстояние Фреше наиболее чув-

ствительно к искажениям в пространственной и временной области одновременно (в соответствии с расчетом пространственной и временной информации по формулам 6 и 7), что приводит к повышению значений метрики при возникновении видимых искажений в видеопоследовательности.

В качестве практического эксперимента был проведен расчет метрики расстояния Фреше на наборе данных UCF101 [7], содержащем размеченные видеопоследовательности человеческих действий. Метрика рассчитывалась при помощи программного кода, доступного на основе исследования [8] на программном ресурсе GitHub. Расчет метрики проводился для двух используемых моделей генеративных нейронных сетей: VideoMAE и I3D. Результаты практического тестирования представлены в таблице 1.

ТАБЛИЦА 1. Значения метрики расстояния Фреше для используемых генеративных моделей

Используемая модель	Значение метрики видеорасстояния Фреше
VideoMAE	1064.7018
I3D	3384.3443

В рамках проведенного исследования были рассмотрены частные случаи использования математических алгоритмов для анализа и обработки изображений: анализ изображений при помощи фильтра Собеля, расчет пространственной и временной информации, оценка качества генеративных моделей искусственных нейронных сетей при помощи расстояния Фреше. Математические алгоритмы преобразования визуальной информации являются необходимым инструментом в эксплуатации, исследованиях и разработке в области компьютерного зрения, генерации видео и видеокодеков, однако сами алгоритмы также нуждаются в непрерывном совершенствовании и проверке с точки зрения соответствия человеческому восприятию.

Список используемых источников

1. Тропченко А. Ю. Методы сжатия изображений, аудиосигналов и видео: Учебное пособие / А. Ю. Тропченко, А. А. Тропченко. СПб: Университет ИТМО, 2009. 109 с.

2. МСЭ-R. Рек. BT.709-6 Значения параметров стандартов ТВЧ для производства программ и международного обмена программами. 2015. URL: https://www.itu.int/rec/R-REC-BT.709 (дата обращения 05.07.2025).

3. Доманов Е. В. Анализ качества работы фильтра Собеля на различных форматах изображения / Е. В. Доманов // Научный альманах. 2016. № 11-2(25). С. 308-311. DOI 10.17117/na.2016.11.02.308.

4. Robitza W. и др. Impact of Spatial and Temporal Information on Video Quality and Compressibility // 2021 13th International Conference on Quality of Multimedia Experience (QoMEX). Montreal, QC, Canada: IEEE, 2021. С. 65–68.

5. Goodfellow I. J. и др. Generative Adversarial Networks. 2014. URL: https://arxiv.org/abs/1406.2661 (дата обращения 05.07.2025).

6. Unterthiner T. и др. Towards Accurate Generative Models of Video: A New Metric & Challenges. 2019. URL: https://arxiv.org/abs/1812.01717 (дата обращения 05.07.2025).

7. Soomro K., Zamir A. R., Shah M. UCF101: A Dataset of 101 Human Actions Classes From Videos in The Wild. 2012. URL: https://arxiv.org/abs/1212.0402 (дата обращения 05.07.2025).

8. Ge S. и др. On the Content Bias in Fréchet Video Distance. 2024. URL: https://arxiv.org/abs/2404.12391 (дата обращения 05.07.2025).

MATHEMATHICAL METHODS OF INTERACTION WITH SPATIAL AND TEMPORAL INFORMATION IN THE VIDEO SEQUENCES WITH THE EXAMPLE OF FRECHET VIDEO DISTANCE METRIC

Buchatskiy A., Losev A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Mathematical algorithms for interaction with video sequences have a strong impact on an operation with the spatial and temporal information. The management of the transmission for these types of information is the prior task for video data recording and playback, and for various video transformation tasks. The goal of the effective transmission of video information through the communication channels is prioritizing significantly nowadays, with the distribution of high-resolution videos, high dynamic range and pan view. This work is dedicated to the mathematical algorithms for detection and transformation of spatial and temporal information with the example of Frechet Video Distance.

Key words: *spatial and temporal information, Frechet Video Distance, Sobel filter, color space*

УДК 004.738.5.057.4
ГРНТИ 20.15.05

ПРОБЛЕМЫ СЕТЕВОЙ АРХИТЕКТУРЫ В ЭПОХУ ДВОЙНОГО СТЕКА

Н. А. Васильев, Б. С. Лещинский, Д. С. Ситдиков

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

Широкое распространение Network Address Translation как временного решения проблемы исчерпания адресов IPv4 привело к системному нарушению принципа сквозного взаимодействия (end-to-end), что стало препятствием для развития децентрализованных сетевых архитектур. Введение Carrier-Grade Network Address Translation усилило эти проблемы, вызвав рост задержек, снижение надежности и невозможность прямого соединения между узлами. Переходные технологии IPv6 лишь частично компенсируют ограничения, не устраняя фундаментальных архитектурных проблем. IPv6 предлагает решение, обеспечивая адресное пространство практически неограниченного масштаба, сквозную маршрутизацию и встроенные механизмы безопасности. Переход на IPv6 представляется необходимым условием для масштабируемого, децентрализованного и надежного интернета нового поколения.

Network Address Translation (NAT), Carrier-Grade NAT (CGNAT), IPv6, Double NAT, DS-Lite, NAT64/DNS64, 464XLAT, IoT, безопасность сетей, WebRTC

Протокол IPv4, разработанный в 1980-х годах, стал основой современного интернета. Однако ограниченное адресное пространство (всего 4,3 миллиарда уникальных IP-адресов) уже к 1990-м годам стало серьезным ограничением, особенно в условиях роста числа подключенных устройств. Для решения проблемы дефицита был внедрен механизм Network Address Translation (NAT), изначально задуманный как временное решение, позволяющее нескольким устройствам использовать один внешний IP-адрес. Со временем NAT стал стандартом де-факто, однако его широкое применение породило ряд технических, архитектурных и организационных проблем, затрудняющих развитие цифровой инфраструктуры будущего.

Одной из наиболее значимых проблем является нарушение модели end-to-end взаимодействия – одного из фундаментальных принципов интернета, согласно которому любой узел должен иметь возможность напрямую обмениваться данными с любым другим узлом без участия промежуточных элементов. NAT скрывает внутренние устройства за общим IP-адресом, что де-

лает невозможным установление входящих соединений без дополнительных механизмов проброса портов или протоколов обхода, таких как STUN, TURN и ICE [1].

Эта проблема особенно остро проявляется в следующих случаях:

1. Double NAT – когда два уровня трансляции накладываются друг на друга, например, домашний маршрутизатор за модемом провайдера, работающим в режиме NAT [2]. Это вызывает проблемы с подключением в онлайн-играх, VoIP-звонках и P2P-сетях.

2. Carrier-Grade NAT (CGNAT) используется провайдерами для распределения одного внешнего IP-адреса между тысячами пользователей. CGNAT делает невозможным хостинг сервисов, точную геолокацию и стабильные голосовые/ видео соединения [2].

Кроме того, NAT создает лишь иллюзию безопасности, поскольку не обеспечивает шифрования данных, аутентификации или защиты приложений. Особенно уязвимы устройства IoT, часто подключаемые за CGNAT и имеющие слабые механизмы безопасности. Такие устройства могут быть объединены в ботнеты и использоваться для DDoS-атак.

Для обеспечения совместимости между IPv4 и IPv6 были разработаны различные переходные механизмы [3]:

1. DS-Lite (Dual-Stack Lite) – позволяет IPv6-устройствам взаимодействовать с IPv4-ресурсами через инкапсуляцию и централизованную трансляцию. Недостатками являются увеличенный overhead от туннелирования и отсутствие поддержки multicast.

2. NAT64/DNS64 – позволяет IPv6-клиентам обращаться к IPv4-сервисам, синтезируя AAAA-записи. Однако несовместим с протоколами, где IPv4-адреса жестко закодированы в payload (например, SIP, FTP без ALG).

3. 464XLAT – использует двойную трансляцию: stateless SIIT на клиенте и stateful NAT64 на стороне провайдера. Подходит для мобильных сетей, но усложняет диагностику и управление.

Несмотря на свою практическую ценность, эти технологии остаются временными мерами и сохраняют зависимость от IPv4-инфраструктуры.

Причины замедленного перехода к IPv6:

1. Инерция провайдеров, особенно региональных и небольших, которые предпочитают использовать NAT вместо масштабного обновления инфраструктуры.

2. Отсутствие спроса со стороны конечных пользователей, которые не замечают разницы между IPv4 и IPv6 при использовании большинства сервисов.

3. Сложность обновления legacy-оборудования и программного обеспечения, поддерживающего исключительно IPv4.

Механизм NAT создает серьезные препятствия для реализации новых сетевых парадигм:

1. P2P-сети и mesh-инфраструктуры требуют равноправного доступа к каждому узлу сети. При использовании NAT устройство не имеет собственного публичного IP-адреса, что делает невозможным установление прямого соединения.

2. WebRTC и VoIP сталкиваются с необходимостью использования посредников (TURN-серверов), что увеличивает задержки и снижает качество связи.

3. IoT и edge computing требуют уникальности IP-адреса для управления, диагностики и безопасности. Отсутствие такового делает затруднительным обслуживание и мониторинг устройств.

4. Блокчейн-сети и децентрализованные хранилища (IPFS, Filecoin и др.) зависят от возможности прямого взаимодействия между участниками. NAT вынуждает полагаться на центральные серверы, что противоречит сути децентрализации.

IPv6 предоставляет практически неограниченное количество уникальных адресов (порядка $3{,}4\times10^{38}$), что позволяет вернуть интернету истинную end-to-end модель взаимодействия. Преимущества IPv6 включают:

1. Упрощенная маршрутизация и отсутствие необходимости в NAT.

2. Поддержка распределенных систем, P2P-сетей, mesh-сетей и децентрализованных вычислений.

3. Повышенный уровень безопасности благодаря встроенным протоколам Secure Neighbor Discovery (SEND) и Cryptographically Generated Addresses (CGA) [4].

Успешные примеры внедрения IPv6 демонстрируют Азиатско-Тихоокеанский регион и Северная Америка, где доля IPv6-готовых пользователей превысила 50 %. В APNIC-регионе (включая Японию, Индонезию, Вьетнам и Индию) показатель IPv6-capable составляет около 50,2 %, что обусловлено активной политикой отказа от CGNAT в мобильных сетях и широким распространением IPv6-технологий среди операторов. В Северной

Америке (регион ARIN) уровень IPv6-доступа достигает 52–54 %, в том числе благодаря политике крупных провайдеров (Comcast, Verizon) и корпоративных сетей. Эти регионы уже демонстрируют снижение задержек, улучшение стабильности P2P-соединений и рост доступности современных децентрализованных приложений. Карта распространенности IPv6 пользователей по странам представлена на рисунке 1.

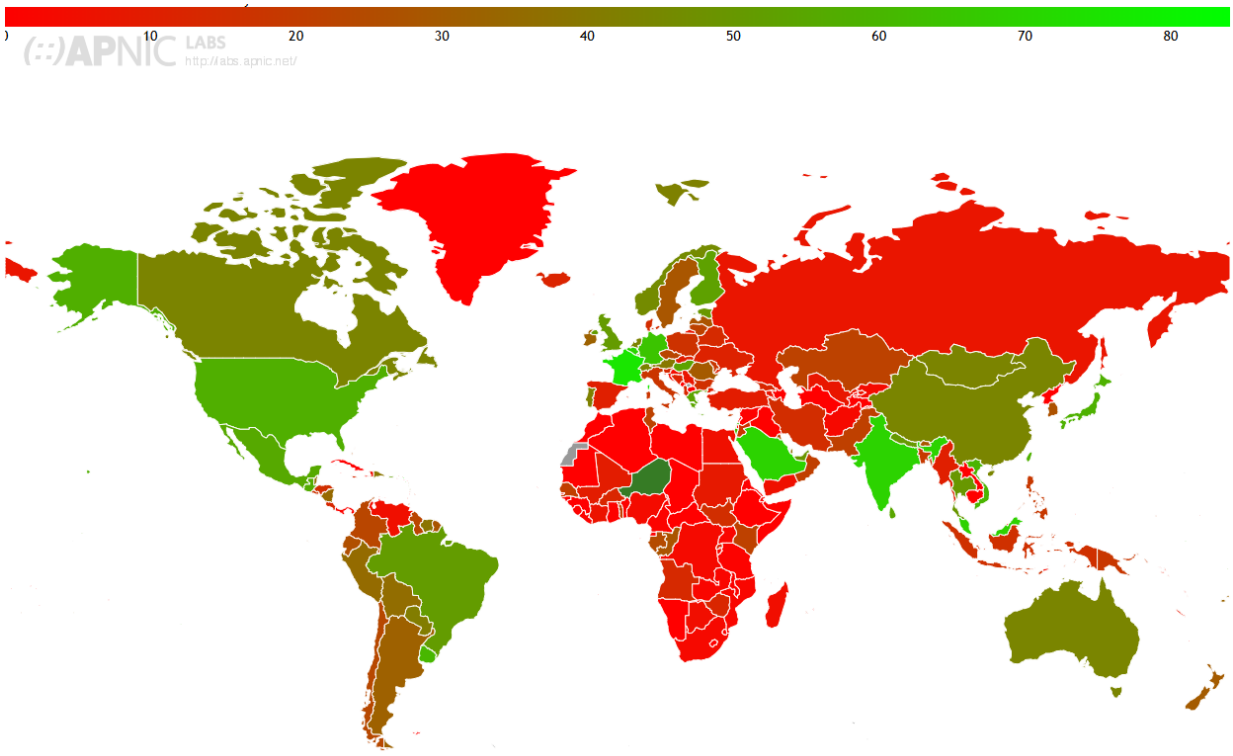


Рис. 1. Уровень доступности IPv6 у пользователей по странам и регионам (май–июнь 2025) – по данным APNIC Labs [5].

NAT, изначально задуманный как временное решение для экономии IPv4-адресов, сегодня стал серьезным препятствием на пути развития современных и перспективных сетевых технологий. Он нарушает принцип end-to-end взаимодействия, снижает прозрачность и управляемость сетевой инфраструктуры, ограничивает возможности децентрализованных систем и повышает риски безопасности.

Переход к IPv6 – это не просто техническая необходимость, но и стратегический шаг в сторону более открытой, масштабируемой и безопасной цифровой инфраструктуры. Хотя инерция рынка и инфраструктурные барьеры замедляют этот процесс, дальнейшее развитие интернета нового поколения невозможно без отказа от NAT и массового внедрения IPv6.

Список используемых источников

1. Swer D. Let's talk about CGNAT and IPv6, again // URL: https://blog.apnic.net/2025/05/13/lets-talk-about-cgnat-and-ipv6-again (дата обращения 01.05.2025).
2. Kanaris O., Pouwelse J. Mass Adoption of NATs: Survey and experiments on carrier-grade NATs // URL: arXiv preprint arXiv:2311.04658. 2023 (дата обращения 01.05.2025).
3. Hamdou M. et al. Classification of IPv6 Transition Mechanisms using Multiple-Criteria Decision-Making //Engineering, Technology & Applied Science Research. 2025. Т. 15. № 3. С. 22960-22968.
4. Najjar F., Bsoul Q., Al-Refai H. An analysis of neighbor discovery protocol attacks // Computers. 2023. Т. 12. № 6. С. 125.
5. APNIC Labs. IPv6 Capability by Region. URL: https://stats.labs.apnic.net/ipv6 (дата обращения 01.05.2025).

NETWORK ARCHITECTURE CHALLENGES IN THE DUAL-STACK ERA

Vasiliev N., Leshchinsky B., Sitdikov D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The widespread use of Network Address Translation as a temporary solution to the IPv4 address exhaustion problem resulted in a systemic breakdown of end-to-end connectivity, which became an obstacle to the development of decentralized network architectures. The introduction of Carrier-Grade Network Address Translation exacerbated these problems by increasing latency, reducing reliability, and preventing direct connectivity between nodes. IPv6 transition technologies only partially compensate for these limitations without addressing the fundamental architectural problems. IPv6 offers a solution by providing an address space of virtually unlimited scale, end-to-end routing, and built-in security mechanisms. The transition to IPv6 appears to be a prerequisite for a scalable, decentralized, and reliable next-generation Internet.

Key words: *Network Address Translation (NAT), Carrier-Grade NAT (CGNAT), IPv6, Double NAT, DS-Lite, NAT64/DNS64, 464XLAT, IoT, network security, WebRTC*

УДК 004.725.5
ГРНТИ 49.33.29

АНАЛИЗ ЗАГРУЗКИ ВРЕМЕННОГО РЕСУРСА РАДИОКАНАЛА СТАНДАРТА IEEE 802.11 В РАЗЛИЧНЫХ УСЛОВИЯХ

А. С. Викулов, С. А. Скоробогатова

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

В статье представлены результаты лабораторных измерений характеристик загрузки временного ресурса канала беспроводной локальной сети стандарта IEEE 802.11 при различных сценариях с разным числом уникальных идентификаторов беспроводной сети на один радиоканал, а также с различным количеством точек доступа. Авторы преследовали сугубо практическую цель – продемонстрировать влияние различных условий на характеристики беспроводной среды. Для ряда практических сценариев показана целесообразность их применения в реальных проектных задачах.

Wi-Fi, загрузка канала, Channel Utilization, beacon-кадр

Введение

Сети Wi-Fi стандарта IEEE 802.11 [1], требуют эффективного управления различными типами ресурсов, среди которых можно в некотором смысле выделить спектральный, временной и энергетический.

Спектральный ресурс включает в себя частотные диапазоны и номера каналов. Временной связан с управлением доступом и передачами (OFDMA, TWT, MAC-уровень). Энергетический отражает мощность сигнала, влияющую на стабильность и дальность связи.

При этом в Wi-Fi сетях особенно важно учитывать временной ресурс, поскольку он отражает степень занятости радиоканала и играет важнейшую роль в обеспечении производительности и стабильности соединения. Временная загрузка канала зависит от множества факторов: количества одновременно активных клиентов, типа трафика, механизма доступа, объема служебного трафика и др.

Целью данной работы является анализ загрузки временного ресурса радиоканала в беспроводных сетях стандарта IEEE 802.11 при различных условиях и разработка рекомендаций по оптимальному планированию ресурсов в сетях стандарта IEEE 802.11ax. Для достижения этой цели поставлены следующие задачи: провести лабораторные измерения загрузки радио-

канала в диапазонах 2,4 и 5 ГГц с разным количеством точек доступа и уникальных SSID, оценить влияние длительности beacon-кадров и режима совместимости с устаревшим стандартом IEEE 802.11b на загрузку канала, сравнить теоретические и экспериментальные данные по загрузке временного ресурса и на основе полученных результатов разработать рекомендации по минимизации загрузки временного ресурса радиоканала.

Постановка эксперимента

Лабораторные исследования проводились с использованием следующего оборудования:

1. Экранирующая камера, предназначенная для защиты от электромагнитных помех.

2. Программно-аппаратный комплекс для анализа Wi-Fi среды – Ekahau AI Pro и измерительное устройство Ekahau Sidekick 2.

3. Двухдиапазонная точка доступа с поддержкой IEEE 802.11a/b/g/n/ac/ax, встроенными антеннами и схемой MIMO 3×2:2.

Несмотря на отсутствие активных клиентов, beacon-кадры существенно влияют на загрузку временного ресурса канала [2]. Длительность передачи одного beacon-кадра варьируется в зависимости от режима работы и версии стандарта [3]. Для минимизации нагрузки на канал и улучшения производительности обычно рекомендуется ограничивать число SSID в инфраструктуре не более чем четырьмя [4].

В ходе эксперимента проводилась последовательная настройка различных количеств SSID на точке доступа. Измерение загрузки канала (Channel Utilization) осуществлялось с помощью программно-аппаратного комплекса Ekahau AI Pro, что позволило зафиксировать зависимость между числом SSID и уровнем загруженности беспроводного канала.

Результаты экспериментов

В одном из экспериментов, представленном на рисунке 1, на спектре можно увидеть загрузку канала при шести точках доступа, каждая из которых транслирует по 16 уникальных SSID. Точки передают исключительно служебный трафик в виде beacon-кадров, при этом активных клиентских устройств в сети нет. В таких условиях загрузка канала достигает 38 %.

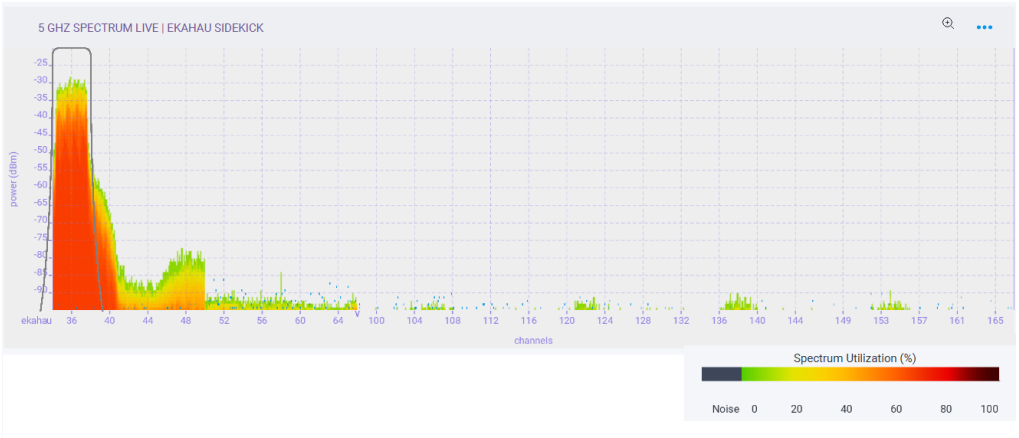


Рис. 1. Временная загрузка канала при трансляции beacon-кадров от 6 точек доступа в диапазоне 5 ГГц

Измерения проводились в диапазонах 5 ГГц и 2,4 ГГц при следующих условиях.

В диапазоне 5 ГГц использовался канал 36 с шириной 20 МГц и мощностью 100 мВт. Результаты показали, что одна точка доступа с одним SSID загружает канал примерно на 1 %, тогда как шесть точек с 16 SSID создают повышенную нагрузку на канал, достигая 38 %. Результаты представлены на графике ниже (рисунок 2). Хорошо видно, что чем больше точек доступа и SSID, тем выше нагрузка на временной ресурс. Причем зависимость близка к линейной.

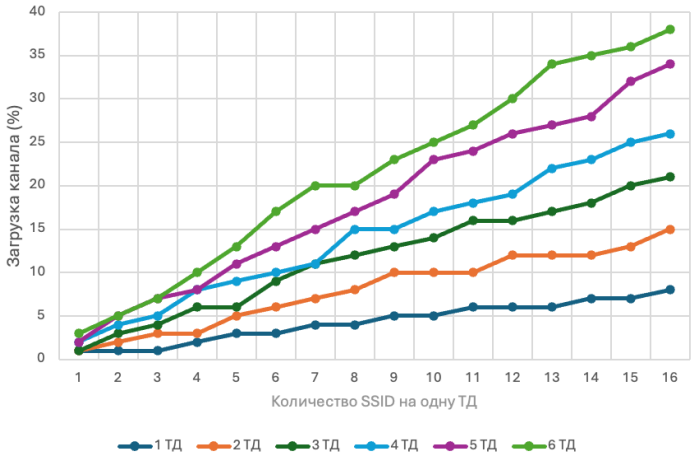


Рис. 2. Зависимость загрузки радиоканала от количества SSID и числа точек доступа в диапазоне 5 ГГц

Аналогичные измерения в диапазоне 2,4 ГГц (канал 1, ширина 20 МГц, мощность 100 мВт) показали сопоставимые результаты (рисунок 3). Это подтверждает, что ключевым фактором, влияющим на загрузку канала, является не частотный диапазон, а количество активных точек доступа и SSID.

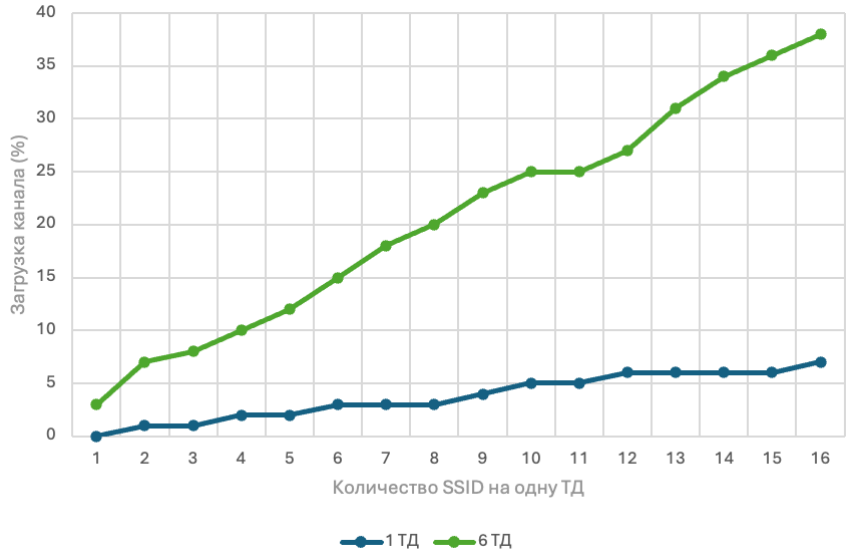


Рис. 3. Зависимость загрузки радиоканала от количества SSID и числа точек доступа в диапазоне 2,4 ГГц

При активации опции обратной совместимости с устаревшим стандартом IEEE 802.11b длительность передачи beacon-кадра значительно увеличивается. Это приводит к росту времени занятости канала и, соответственно, к увеличению загрузки радиоканала. В эксперименте, когда шесть точек доступа работали на одном канале в диапазоне 2,4 ГГц с включенным режимом совместимости с 802.11b, загрузка канала достигала практически 100 % (рисунок 4).

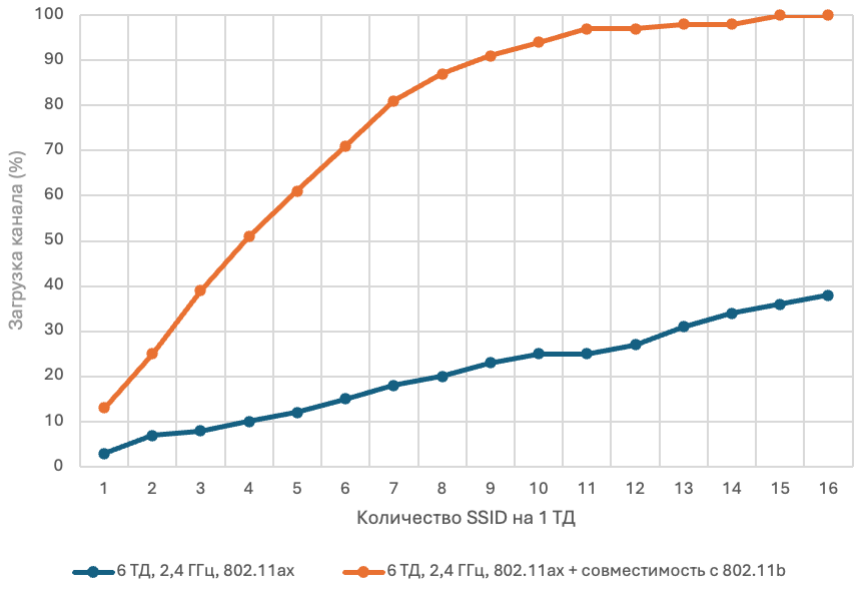


Рис. 4. Влияние режима совместимости с IEEE 802.11b на загрузку радиоканала

Теоретическая оценка загрузки временного ресурса радиоканала

Для теоретической оценки загрузки радиоканала была использована формула (1), учитывающая количество точек доступа, число SSID на каждую точку, длительность одного beacon-кадра и интервал между передачами beacon-кадров.

$$CU = \frac{N_{AP} * N_{SSID} * T_{beacon}}{T_{interval}} * 100\ \%, \quad (1)$$

где CU – channel utilization,

N_{AP} – число точек доступа,

N_{SSID} – число SSID на каждую точку,

T_{beacon} – длительность одного beacon-кадра,

$T_{interval}$ – интервал между beacon-кадрами.

В ходе эксперимента длительность одного beacon-кадра составляла 360 микросекунд, а интервал между beacon 102,4 миллисекунды. Полученные результаты измерений при работе шести точек доступа в диапазоне 5 ГГц в режиме 802.11ax соотносятся с теоретическими расчетами достаточно хорошо. Например, при 16 SSID на каждую точку доступа измеренная загрузка составила 38 %, тогда как расчетное значение 33,8 %.

Выводы

В работе были выполнены измерения использования временного ресурса канала при стандартной частоте передачи beacon-кадров.

Показано, что использование режима совместимости с 802.11b в современных Wi-Fi сетях недопустимо из-за резкого роста загрузки канала.

Полученные результаты демонстрируют зависимость загруженности эфира от числа точек доступа и количества SSID, работающих на одном канале.

Также подтверждено, что частотный диапазон (2,4 или 5 ГГц) не влияет на загрузку при прочих равных условиях, что соответствует теоретическим ожиданиям.

Из результатов можно оценить рекомендуемое максимальное число SSID. В условиях сети высокой плотности (high density) число SSID должно быть минимально возможным, чтобы не перегружать эфир.

Список используемых источников

1. IEEE 802.11ax-2021. IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN.

2. SSIDS overhead effect on channel utilisation // WiFi Professionals. 23 авг. 2018. URL: https://wifiprofessionals.com/2018/08/ssids-overhead-effect-on-channel-utilisation/ (дата обращения 28.07.2025).

3. 802.11 Mgmt: Beacon Frame // Mrncciew Blog. 8 окт. 2014. URL: https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame/ (дата обращения 31.07.2025).

4. Cisco Wireless LAN Controller (WLC) Configuration Best Practices // Cisco Systems. 26 янв. 2018. URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-6/b_Cisco_Wireless_LAN_Controller_Configuration_Best_Practices.html#concept_D28BDEBC0B7E49A39781FEA9AA4F516F (дата обращения 31.07.2025).

ANALYSIS OF TIME RESOURCE UTILIZATION IN THE IEEE 802.11 RADIO CHANNEL UNDER VARIOUS CONDITIONS

Vikulov A., Skorobogatova S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper presents the results of laboratory measurements on the time resource utilization characteristics of the IEEE 802.11 wireless local area network channel across various scenarios. These scenarios differ in terms of the number of unique wireless network identifiers sharing a single radio channel, as well as the number of access points deployed. The authors aim to demonstrate the practical impact of varying conditions on wireless environment performance. For a range of realistic scenarios, the study highlights the applicability of these findings in real-world network design and deployment.

Key words: *Wi-Fi, channel utilization, time resource load, beacon frame*

УДК 004.725.5
ГРНТИ 49.33.29

ИССЛЕДОВАНИЕ НАГРУЗКИ В БЕСПРОВОДНОЙ СЕТИ IEEE 802.11 НА ВРЕМЕННОЙ ПЛОЩАДКЕ

А. С. Викулов, С. А. Скоробогатова

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

В данной работе представлены результаты измерений и анализа статистики по сессиям в беспроводной локальной сети стандарта IEEE 802.11, развернутой в рамках временной инсталляции на площадке с высокой нагрузкой. Основная цель исследования заключается в описании ключевых характеристик анализируемого трафика, которые могут быть полезны для решения задач планирования сети в аналогичных условиях. Авторы рассмотрели такие параметры, как длительность сессий, распределение клиентских устройств по диапазонам, активность пользователей, и некоторые другие.

Wi-Fi, IEEE 802.11, статистический анализ, длительность сессий, распределение нагрузки

Введение

Создание беспроводной локальной вычислительной сети (БЛВС) стандарта IEEE 802.11 [1] с заданным качеством обслуживания невозможно без системного проектного подхода. В рамках решения проектной задачи по созданию БЛВС необходимо принимать во внимание множество факторов. Среди них можно выделить следующие:

1. Бизнес-задачи и ключевые сетевые сервисы. Здесь важно обозначить какую задачу должна решать сеть и какие сервисы являются приоритетными.

2. Масштаб и тип препятствий, особенности помещений (офисы, склады, конференц-залы и др.), источники возможных помех.

3. Расчетная мощность излучения ТД, тип антенн, частотные диапазоны, нормативные ограничения на уровень мощности.

4. Особенности монтажа и расстановки ТД. Высота установки, ориентация антенн, избегание избыточного перекрытия зон покрытия и помех.

5. Состав клиентских устройств (КУ). Определение основных моделей КУ, их функциональных возможностей и чувствительности (принцип most important, least capable [2]).

Таким образом очень часто в проектной практике возникает задача оценить качественный состав клиентских устройств и основной сценарий использования среды передачи. И если ответ на первый вопрос можно в ряде случаев дать заранее, опираясь на бизнес-требования к БЛВС, то второй вопрос почти всегда решается оценочно. В последнем случае помощь может оказать историческая статистика по клиентским устройствам в таких же или близких по масштабу и решаемым задачам беспроводным сетям. Ранее [3] такой анализ уже проводился авторами для ряда площадок (гостиницы, офисы и др.). Спустя несколько лет, принимая во внимание смену поколения стандарта мы поставим перед собой задачу проанализировать сравнить актуальные на сегодняшний день данные о клиентских устройствах в сетях Wi-Fi публичного доступа и сделать выводы, применимые для решения проектных задач.

Постановка задачи и описание анализируемой площадки

С точки зрения оценки нагрузки на БЛВС, важнейшим параметром является число одновременно активных КУ, которое можно оценить на основе опыта или экспертных оценок, учитывая специфику объекта и сценарии использования сети.

Для более точного прогноза можно использовать статистический анализ аналогичных БЛВС. Для этого необходимо собрать данные о длительности клиентских сессий, т.е. сколько времени устройства активно обмениваются данными. Требуется определить функцию распределения длительности сессий. Для достоверного анализа нужна большая выборка данных, полученных из реальных БЛВС с похожими условиями.

Правильная оценка числа одновременно активных КУ позволяет:
– планировать нагрузку на точки доступа;
– избежать перегрузок и деградации качества связи;
– обеспечить стабильную работу сети даже при пиковых нагрузках.

На рассматриваемой площадке площадью 7000 м² в рамках решения бизнес-задачи по организации БЛВС на время проведения мероприятия развернута временная инфраструктура БЛВС из 62 двухдиапазонных точек доступа (схема 2×2 MIMO, стандарты IEEE 802.11a/b/g/n/ac/ax) с равномерным размещением, частично на штативах. Сеть предназначалась для обслуживания до 3000 посетителей.

Результаты анализа

По результатам анализа работы БЛВС было зафиксировано 1428 клиентских устройств, из которых 975 подключались в диапазоне 5 ГГц, 481 в 2,4 ГГц, а 28 использовали оба диапазона. Для минимизации эффектов механизма band-steering (автоматического перевода устройств между диапазонами) были задействованы раздельные SSID для каждого частотного диапазона.

На рисунке 1 приведена гистограмма, иллюстрирующая распределение КУ по частотным диапазонам.

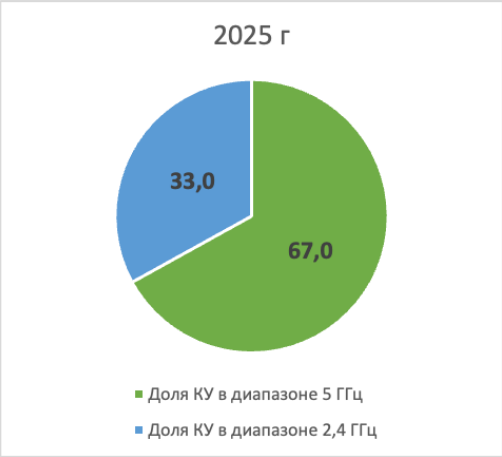


Рис. 1. Распределение КУ по частотным диапазонам

На основании статистических данных, за три дня работы исследуемой временной беспроводной сети процентное соотношение смещается в пользу 5 ГГц диапазона, что объясняется поддержкой современными устройствами стандарта IEEE 802.11a IEEE 802.11ax. Подобное изменение также можно объяснить тем, что в исследуемой БЛВС применялись раздельные SSID для каждого диапазона, то есть выбор диапазона осуществлялся непосредственно на стороне клиента.

В работе [4], основанной на анализе более чем 226 тысяч сессий, 83,4 % сессий приходилось на диапазон 2,4 ГГц, в то время как 5 ГГц составлял лишь 16,6 % (рисунок 2, второй столбец). Это связано с широкой распространенностью клиентских устройств, ориентированных на работу в диапазоне 2,4 ГГц. Несмотря на то, что стандарт 802.11n поддерживает оба диапазона, преобладание 2,4 ГГц можно объяснить как техническими ограничениями устройств, так и особенностями конфигурации анализируемой в работе беспроводной сети.

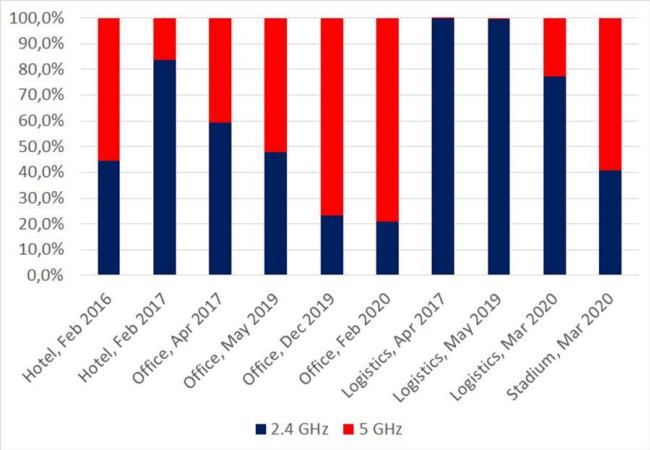


Рис. 2. Данные на разных площадках с 2016 по 2020 год

Следующим параметром анализа стала длительность клиентских сессий. Сессии продолжительностью 0 секунд были исключены из анализируемой выборки. Более 68 % всех сессий имели длительность менее 15 минут, что указывает на преобладание кратковременных подключений.

Для аппроксимации распределения можно использовать гамма-распределение. Оно хорошо подходит для моделирования неотрицательных, непрерывных величин, особенно при наличии асимметричного распределения.

Формула для функции плотности вероятности гамма-распределения:

$$f(x) = \begin{cases} \frac{1}{\Gamma(\alpha)\beta^{\alpha}} x^{\alpha-1} e^{-\frac{x}{\beta}}, x > 0 \\ 0, \qquad\qquad x \leq 0 \end{cases}, \tag{1}$$

где: $\Gamma(\alpha)$ – гамма-функция (обобщенный факториал),

α – параметр формы (shape),

β – параметр масштаба (scale),

x – переменная (середина интервала)

Функция распределения для гамма-распределения. Это интеграл от функции плотности и показывает вероятность того, что случайная величина будет меньше или равна значению x:

$$F(x) = \int_0^x \frac{1}{\Gamma(\alpha)\beta^{\alpha}} t^{\alpha-1} e^{-\frac{t}{\beta}} dt \tag{2}$$

Параметры гамма-распределения

Форма (α): 0.349. Значение меньше 1 указывает на резкий спад плотности вблизи нуля и длинный "хвост" (много коротких сессий и мало длительных).

Масштаб (β): 50.69. Большой масштаб означает высокую вариативность длительности сессий.

Аппроксимация приведена на рисунке 3.

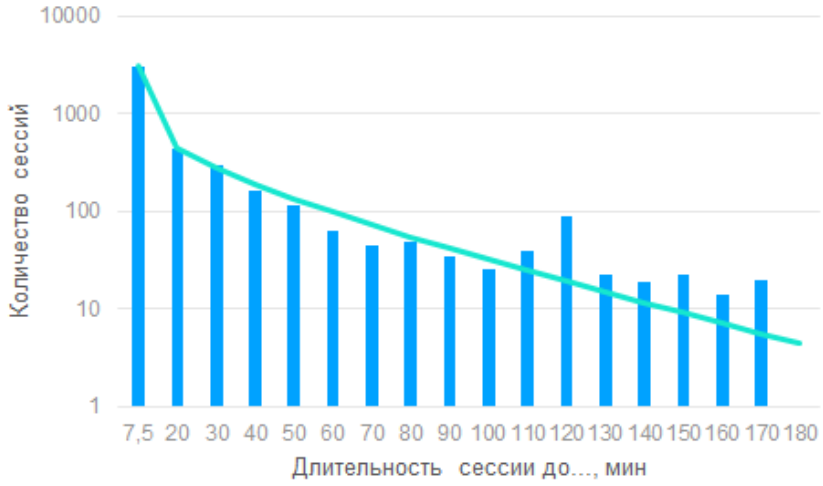


Рис. 3. Аппроксимация распределения длительности клиентских сессий

По сравнению с ранее собранными данными [4], где имело место более равномерное распределение длительностей с преобладанием средних сессий, можно отметить, что здесь наблюдается распределение длительности сессий с выраженным пиком в диапазоне 0-7 минут, быстрым спадом после 7 минут. Это может указывать на рост доли коротких подключений и снижение количества средних по продолжительности сессий.

Выводы

1. В данной работе были проанализированы клиентские сессии в высоконагруженной беспроводной сети стандарта IEEE 802.11 на временной площадке с большой плотностью пользователей.

2. В полученных результатах преобладали короткие сессии, что отражает выраженное асимметричное распределение.

3. Для аппроксимации собранных данных было использовано гамма-распределение с подобранными параметрами формы и масштаба. Это позволило получить модель, отражающую характеристики нагрузки.

4. При сравнении актуальных данных на момент 2025 года с данными 10-летней давности можно наблюдать рост коротких сессий и снижение ко-

личества средних. Это может отражать изменения поведения пользователей, а также характерно для

БЛВС на временной площадке с высокой проходимостью пользователей.

5. Для обеспечения стабильной работы БЛВС в условиях высокой плотности пользователей, аналогичных исследуемой площадке, полученные результаты могут быть использованы для прогнозирования нагрузки, планирования ресурсов сети и оптимизации ее работы.

6. В работе была подтверждена тендецния роста количества клиентских устройств, работающих в диапазоне 5 ГГц.

Список используемых источников

1. IEEE 802.11ax-2021. IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN

2. Викулов А. С., Парамонов А. И. Формализация требований к характеристикам сети IEEE 802.11 на основе предварительного обследования // Инновационное приборостроение. 2023. Т. 2. № 1. С. 43–53. DOI: 10.31799/29490693-2023-1-43-53.

3. Викулов А. С., Парамонов А. И. Исследование клиентского состава в сети беспроводного доступа // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ. 2017. Т. 2. С. 136-139.

4. Paramonov, A., Vikulov, A., Scherbakov, S. (2017). Practical Results of WLAN Traffic Analysis. In: Smart Spaces, and Next Generation Networks and Systems. ruSMART NsCC NEW2AN 2017. Lecture Notes in Computer Science, vol 10531. Springer, Cham. https://doi.org/10.1007/978-3-319-67380-6_68 (дата обращения 01.05.2025).

A STUDY OF NETWORK LOAD IN AN IEEE 802.11 WIRELESS NETWORK DEPLOYED AT A TEMPORARY INSTALLATION SITE

Vikulov A., Skorobogatova S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper presents the results of measurements and statistical analysis of sessions in an IEEE 802.11 wireless local area network deployed during a temporary installation at a high-traffic site. The main objective of the study is to characterize key features of the analyzed traffic that can aid network planning under similar conditions. The authors examined parameters such as session duration, distribution of client devices across frequency bands, user activity, and several other factors.

Key words: *Wi-Fi, IEEE 802.11, statistical analysis, session duration, load distribution*

УДК 654.153
ГРНТИ 49.33.29

АНАЛИЗ ВЕРОЯТНОСТНО-ВРЕМЕННЫХ ХАРАКТЕРИСТИК ТУННЕЛЕЙ MPLS OVER QUIC В ТРАНСПОРТНЫХ СЕТЯХ B5G

А. Б. Гольдштейн, С. Р. Танашев

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

В статье представлен формализованный анализ вероятностно-временных характеристик туннелей MPLS over QUIC в транспортных сетях шестого поколения (6G). Исследование развивает ранее предложенную концепцию использования MPLS over QUIC как основы для построения защищенных, адаптивных и масштабируемых туннелей передачи данных. Основное внимание уделено моделированию задержек и джиттера в системе последовательно соединенных сетевых узлов с учетом процессов сцепления и фрагментации пачек пакетов. Применена модель ARMA для прогнозирования временных флуктуаций в туннеле, а также предложен метод прогнозирования перегрузок с использованием AI/ML-инструментов. Полученные результаты позволяют точно оценивать вероятность SLA-нарушений и оптимизировать выбор маршрутов в реальном времени, что особенно актуально для критичных сервисов B5G, таких как URLLC.

сети Beyond 5G, транспортная сеть, MPLS-over-QUIC, ARMA, AI/ML

Развитие архитектуры транспортных сетей пятого поколения и выше требует не только внедрения новых протоколов передачи и маршрутизации, но и фундаментального пересмотра методов анализа и управления временными характеристиками сетевого трафика [1]. Настоящая статья посвящена углубленному анализу вероятностно-временных характеристик туннелей с учетом таких процессов, как сцепление и фрагментация пачек пакетов, проходящих через последовательные сетевые узлы, а также влияние этих процессов на джиттер, средние задержки и вероятность нарушения соглашения об уровне обслуживания.

Архитектурная модель туннеля MPLS over QUIC

В современных транспортных сетях B5G все большее внимание уделяется технологии MPLS over QUIC, сочетающей в себе преимущества мультипротокольной коммутации по меткам (MPLS) и транспортного протокола QUIC, ориентированного на минимизацию задержек и встроенное шифрование.

Инкапсуляция MPLS-потоков в QUIC создает зашифрованные туннели с низким временем установления соединения (один RTT) и встроенными средствами управления перегрузкой, что делает технологию особенно актуальной для нестабильных или небезопасных сред передачи (например, LEO-спутников или публичных Wi-Fi) [2].

Очереди в туннеле: сцепление и фрагментация пачек

Схематично такой туннель можно представить как цепочку последовательно соединенных сетевых узлов, каждый из которых моделируется как система массового обслуживания с буферизацией, – как наземных, так и неназемных – через которые проходит трафик от граничного узла источника до граничного узла получателя (рис. 1).

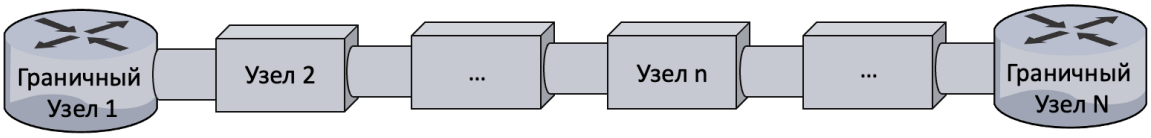


Рис. 1. Последовательные очереди в туннелях MPLS over QUIC

Особую сложность представляет учет группового поведения пакетов, выражающегося в двух феноменах: сцеплении и фрагментации пачек.

Согласно модели, впервые рассмотренной в работах Ле Галля [3], на любом узле n > 1 возможна ситуация, при которой последний пакет предыдущей пачки k − 1 и первый пакет текущей пачки k поступают с минимальным интервалом, и на данном узле они рассматриваются как единый поток. В результате происходит сцепление пачек, представляемое на рисунке 2.

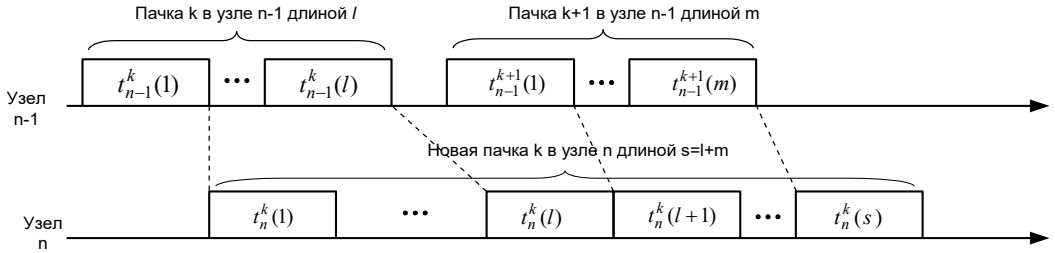


Рис. 2. Сцепление пачек *k-1* и *k* в узле *n*

Такое поведение характерно для сетей с высокой загрузкой и нерегулярными задержками в предыдущих звеньях, где относительное положение пакетов может меняться. Сцепленные пачки продолжают обрабатываться

совместно на последующих узлах, формируя крупные агрегированные группы, что, в свою очередь, влияет на латентность, джиттер и вероятность перегрузки.

Противоположный процесс наблюдается на втором узле (то есть первом узле после граничного входа), если длительность обслуживания соседних пакетов внутри пачки различается. Пусть в момент обслуживания пакета j поступает следующий пакет j + 1, но его время обслуживания оказывается значительно выше. Если второй узел пуст, то он начинает обрабатывать j, пока j + 1 еще обрабатывается на первом. В результате пачка разделяется, и на выходе второго узла появляются две независимые части, как показано на рисунке 3.

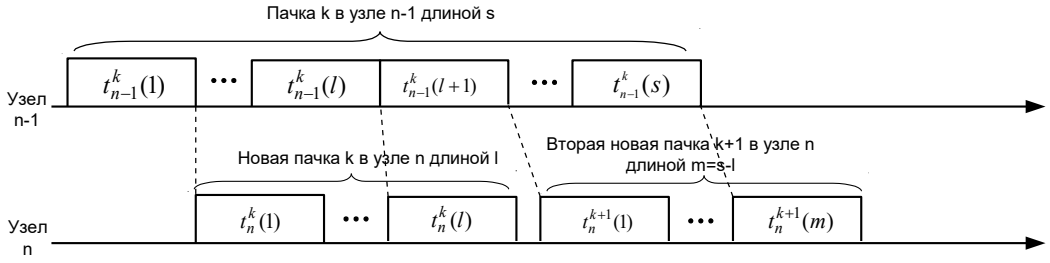


Рис. 3. Фрагментация пачки k

Характеристика задержек в туннеле

Основной вероятностно-временной характеристикой является случайная величина задержки D_t, определяемая как общее время прохождения пакета через последовательность узлов от источника до получателя [4]. Эта величина может быть декомпозирована:

$$D_t = \sum_{n=1}^{N} d_{n,t}$$

где $D_{n,t}$ – задержка на n-м узле в момент времени t, зависит от:

– поступающего интервала пакетов;
– состояния очереди в момент t;
– наличия сцепления или фрагментации пачек.

Таким образом, каждая задержка $D_{n,t}$ определяется не только локальным состоянием узла, но и задержками на предыдущих узлах, т.е. имеется выраженная авторегрессионная зависимость:

$$d_{n,t} = f(d_{n-1,t-1}, d_{n-2,t-2}, \dots) + \varepsilon_t$$

Для описания таких зависимостей применима модель ARMA(p, q) – авторегрессионная модель скользящего среднего, позволяющая выразить текущее значение случайной величины через ее прошлые значения и предыдущие шумы:

$$X_t = c + \sum_{i=1}^{p} \varphi_i X_{t-i} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j} + \varepsilon_t$$

где X_t – наблюдаемое значение (задержка D_t или джиттер);

c – постоянная составляющая;

φ_i – коэффициенты авторегрессии (поведения прошлых значений);

θ_j – коэффициенты скользящего среднего (учитывают инерцию предыдущих флуктуаций);

ε_t – белый шум, отражающий случайные флуктуации.

Модель ARMA/ARIMA позволяет предсказывать поведение туннеля во времени, что особенно важно при построении SLA-критичных маршрутов (например, URLLC) и при необходимости динамического реагирования на потенциальные перегрузки, а также обучать AI/ML-агенты на исторических данных трафика.

AI/ML-модель прогнозирования и оптимизации туннелей в реальном времени

Транспортная сеть B5G требует прогнозирования перегрузок и оптимизация маршрутов на основе анализа вероятностно-временных характеристик, сформированных в предыдущих разделах. Использование моделей машинного обучения (ML) и распределенного искусственного интеллекта (AI) позволяет превратить транспортную сеть в самообучающуюся адаптивную систему.

Предположим, что в некоторый момент времени t на основе предыдущей истории работы сети H_t (в которую входят, например, значения задержки, джиттера, уровня потерь) необходимо оценить вероятность возникновения перегрузки O_t в одном из туннелей:

$$P(O_t/H_t) = f(H_t/\theta)$$

где $P(O_t/H_t)$ – условная вероятность перегрузки в момент *t*,

$f(H_t/\theta)$ – функция, параметризованная обучаемым вектором θ,

H_t={Dt−1,Dt−2,… } – временной ряд характеристик туннеля,

$O_t \in \{0,1\}$ – бинарный индикатор перегрузки.

В качестве f могут выступать логистическая регрессия, деревья решений, рекуррентные нейросети (LSTM), сверточные автоэнкодеры или другие ML-модели. Критически важно, что входными признаками в эти модели могут служить значения задержек, полученные из ARMA-предсказаний, что обеспечивает слияние аналитических и обучаемых подходов. Для предсказания задержек и потерь в конкретном туннеле может использоваться обученная модель ARMA или ее обобщение – ARIMA. Предсказанное значение задержки $\widehat{D}_{t+1}$ и вероятность SLA-нарушения становятся основанием для принятия решений маршрутизатором или AI-агентом о смене пути:

$$\widehat{D}_{t+1} = c + \sum_{i=1}^{p} \varphi_i D_{t-i} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j}$$

Если $\widehat{D}_{t+1} > D_{SLA}$, где D_{SLA} – пороговое значение, заданное соглашением об уровне обслуживания, производится динамическое переключение маршрута или перестроение MPLS-меток и QUIC-туннеля.

Выводы

В данной работе представлен формализованный подход к анализу и управлению туннелями MPLS over QUIC в транспортных сетях B5G, а также предложено динамическое управление перегрузками и оптимизация маршрутов с использованием AI/ML-моделей. Интеграция MPLS, QUIC, вероятностных моделей и технологий машинного обучения позволяет формировать самоадаптирующуюся интеллектуальную транспортную инфраструктуру, отвечающую требованиям будущих B5G-сетей.

Список используемых источников

1. Кучерявый А. Е., Гольдштейн Б. С. Сети связи пост-NGN. СПб: БХВ-Петербург, 2013. 160 с.

2. Araniti G., Iera A., Pizzi S., and Rinaldi F. Towards 6G Non-Terrestrial Networks. IEEE Network. Volume: 36, Issue: 1, January/February, 2022.

3. Гольдштейн А. Б Модели и методы эксплуатационного управления телекоммуникационными сетями // Журнал «Электросвязь». М. 2017. № 2.

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

PROBABILISTIC AND TEMPORAL CHARACTERISTICS ANALYSIS OF MPLS OVER QUIC TUNNELS IN B5G TRANSPORT NETWORKS

Goldstein A., Tanashev S.
Saint Petersburg State University of Telecommunications named after Prof. M. A. Bonch-Bruevich

This paper presents a formalized analysis of the probabilistic and temporal characteristics of MPLS over QUIC tunnels in sixth-generation (6G) transport networks. The study develops a previously proposed concept of using MPLS over QUIC as a foundation for constructing secure, adaptive, and scalable data transmission tunnels. Special attention is given to modeling delays and jitter in a system of sequentially connected network nodes, taking into account packet bundling and fragmentation processes. An ARMA model is applied to predict temporal fluctuations within the tunnel, and a method for forecasting congestion using AI/ML tools is proposed. The results obtained enable accurate estimation of SLA violation probabilities and real-time route optimization, which is especially relevant for critical B5G services such as URLLC.

Key words: *Beyond 5G networks, transport network, MPLS-over-QUIC, ARMA, AI/ML*

УДК 004.732
ГРНТИ 49.43.29

ЭФФЕКТИВНОСТЬ ТЕХНОЛОГИИ MU-MIMO

Р. А. Дунайцев, А. В. Светова

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

В статье представлены результаты исследования эффективности объединения пользователей в группы MU-MIMO. Выявлены факторы, влияющие на группировку устройств. Приведены рекомендации по расположению Wi-Wi роутера для достижения максимальной эффективности использования технологии многопользовательского множественного входа/множественного выхода.

MU-MIMO, IEEE 802.11ax, Wave 2, Wi-Fi роутер

Впервые технология многопользовательского множественного входа/множественного выхода (Multi-User Multiple-Input/Multiple-Output, MU-MIMO) увидела свет в 2015 году во второй волне устройств спецификации IEEE 802.11ac (Wave 2) и далее получила развитие в IEEE 802.11ax и IEEE 802.11be. Очевидно, что данная технология оказала заметное влияние на динамику рынка [1], заставляя потребителей заменять старое оборудование на новое. Но так ли эффективна передача данных с MU-MIMO в домашней сети, где клиентских устройств не так много? Ведь главное преимущество технологии MU-MIMO в использовании нескольких пространственных потоков для отправки данных группе пользователей одновременно в отличие от обычных Wi-Fi роутеров с однопользовательским MIMO [2].

Был проведено исследование с целью узнать от чего зависит объединение в одну группу устройств при передаче данных с MU-MIMO. Эксперименты выполнялись посредством изменения расстояния и угла между пользовательскими устройствами, для выявления зависимости объединения в группы устройств от месторасположения. Исследование проводилось в учебной аудитории 523 второго учебного корпуса СПбГУТ по адресу пр. Большевиков, д. 22. Использовались следующие устройства: Wi-Fi роутер TP-Link Archer AX73, планшет Lenovo Tab4 8 Plus (схема MIMO 1x1:1),

планшет Lenovo Tab P11 (схема MIMO 1x1:1) и Wi-Fi адаптер ASUS USB-AC53 Nano (схема MIMO 2x2:1). Перехват трафика проводился с помощью программы Omnipeek, а для поиска пакетов в перехваченном трафике использовалась программа Wireshark.

Настройки Wi-Fi роутера показаны на рис. 1, из которых следует, что передача велась в частотном диапазоне 5 ГГц в канале 40 с шириной 20/40 МГц.

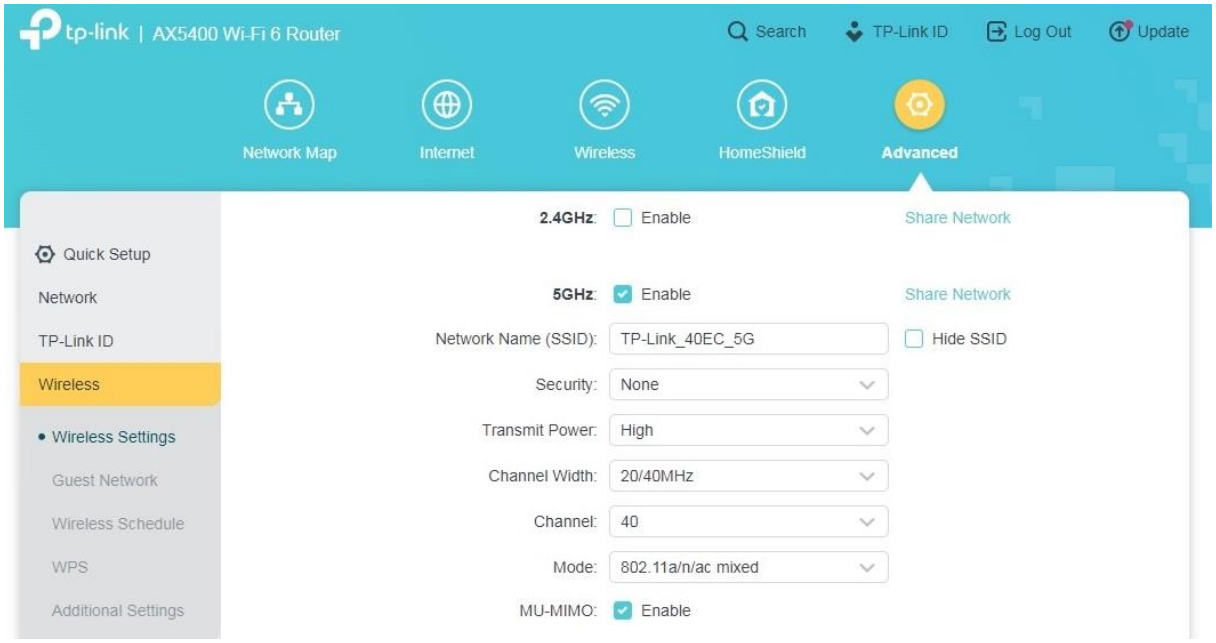


Рис. 1. Настройки Wi-Fi роутера TP-Link Archer AX73

В ходе первого эксперимента Wi-Fi роутер находился в неподвижном положении во втором ряду на первой парте, планшет Lenovo Tab 4 8 Plus (User A) также не менял своего положения и находился в первом ряду на первой парте, а планшет Lenovo Tab P11 (User B) и ноутбук с Wi-Fi адаптером ASUS USB-AC53 Nano (User C) вместе перемещались по рядам. Результаты эксперимента представлены на рис. 2.

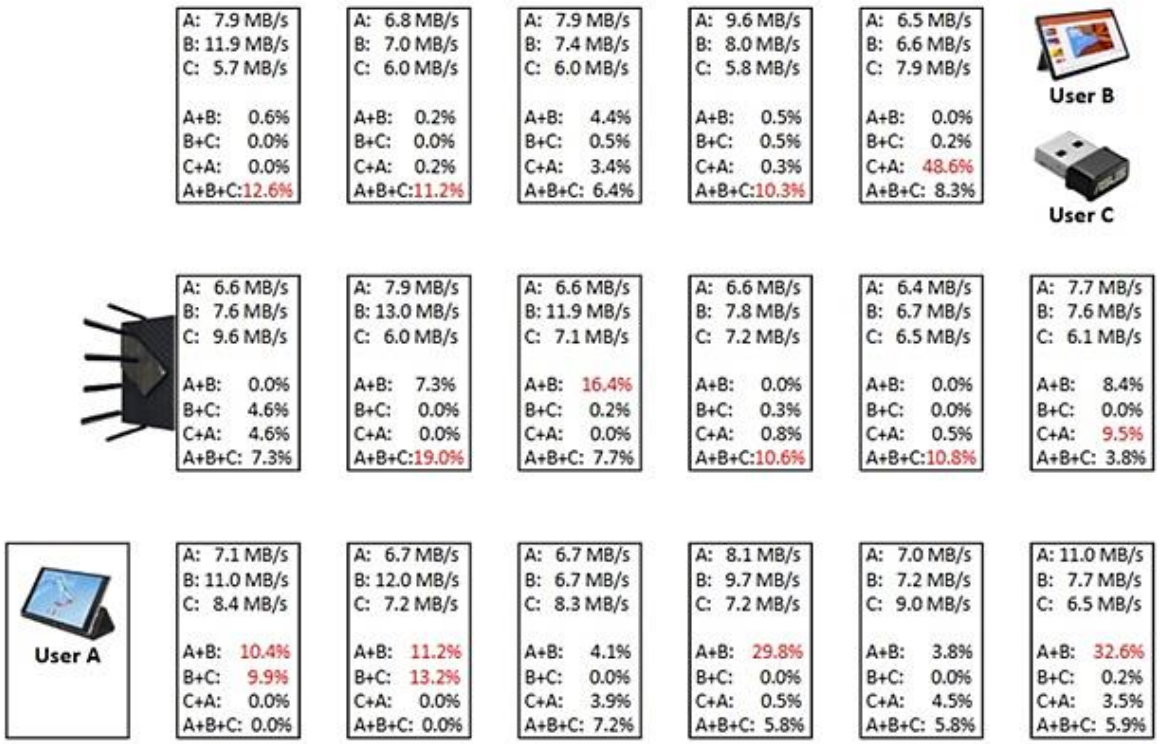


Рис. 2. Карта расположения устройств (эксперимент 1)

Самые высокие проценты объединения отмечаются для тех групп, в которых эффективность MU-MIMO была максимальной. Как можно заметить, наилучшие результаты достигаются, когда в одной группе объединяются клиенты с минимальным взаимным влиянием на сигналы друг друга [3]. Это подтверждается тем, что именно определенные группы получали максимальные проценты успешного объединения (выделены красным на рис. 2). В группе, где пользователи находятся слишком близко друг к другу (User B и User C), эффективность MU-MIMO уменьшается. Это ведет к уменьшению вероятности успешного совмещения клиентов в одну группу и, как следствие, снижению прироста суммарной скорости.

Далее Wi-Fi роутер повернули на 90° по часовой стрелке. Разворот Wi-Fi роутера изменяет пространственную ориентацию антенн. Предположительно устройства, которые раньше находились в области максимального покрытия, должны были оказаться в зоне меньшего сигнала, и наоборот. Результаты, представленные на рис. 3, свидетельствуют о том, что даже при сохранении одинакового расстояния между устройствами, изменение положения антенн может повлиять не только на уровень сигнала, но и на степень взаимных помех, тем самым воздействуя на процесс формирования групп MU-MIMO.

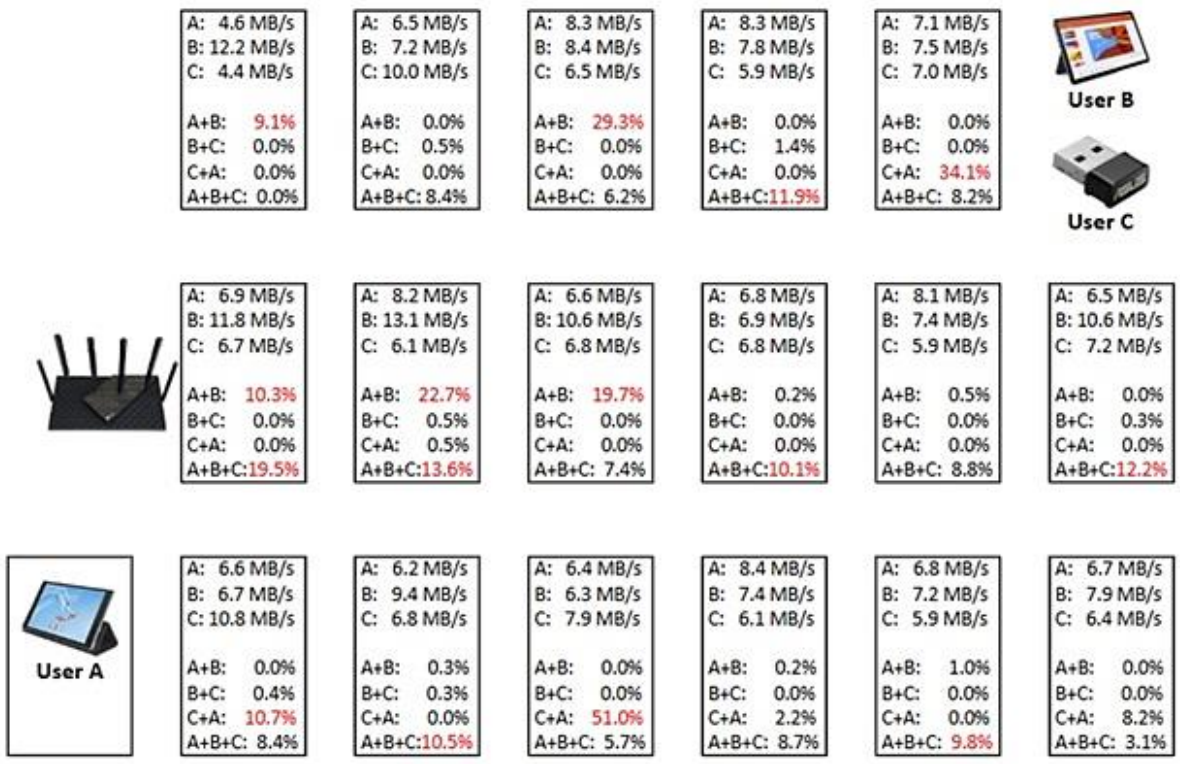


Рис. 3. Карта расположения устройств (эксперимент 2)

Результаты проведенного исследования показали, что применение MU-MIMO позволяет улучшить качество обслуживания пользователей за счет одновременной передачи данных нескольким клиентским устройствам. Практические испытания выявили, что эффективность MU-MIMO в значительной степени зависит от расположения пользовательских устройств, а также конфигурации и ориентации антенн Wi-Fi роутера. Полученные в ходе работы выводы могут быть использованы при проектировании и внедрении современных Wi-Fi сетей в различных областях, требующих высокой производительности и надежности беспроводных соединений.

Список используемых источников

1. Светова А. В., Дунайцев Р. А. Технология MU-MIMO в сетях стандарта IEEE 802.11ac // 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. Т. 1.С. 428–432.

2. Стандарт 802.11ac Wave 2: MU-MIMO и другие возможности. Самый полный FAQ по новому стандарту // URL: https://asp24.ru/novosti-asp24-ru/standart-802.11ac-wave-2-mu-mimo-i-drugie-vozmozhnosti.-samyy-polnyy-faq-po-novomu-standartu (дата обращения 09.06.2025).

3. MU-MIMO Grouping For Real-time Applications/Hannaneh B. Pasandi, Tamer Nadeem Hadi Amirpour // URL: https://arxiv.org/abs/2106.15262 (дата обращения 09.06.2025).

EFFICIENCY OF MU-MIMO TECHNOLOGY

Dunaytsev R., Svetova A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the results of a study on the efficiency of combining users into MU-MIMO groups. The factors influencing the grouping of devices are identified. Recommendations are given on the location of the router to achieve maximum efficiency of using the multi-user multiple input/multiple output technology.

Key words: *MU-MIMO, IEEE802.11ax, Wi-Fi router, IEEE802.11ac*

УДК 004.7
ГРНТИ 49.33.29

РАЗГРУЗКА ЗАДАЧ ИНТЕРНЕТА ВЕЩЕЙ В СИСТЕМАХ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ СО МНОЖЕСТВЕННЫМ ДОСТУПОМ

В. С. Елагин, Е. В. Чипсанова

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

Разгрузка задач приобретает все большую популярность благодаря тому, что оконечные устройства могут разгружать вычислительные задачи на облачные платформы или системы граничных вычислений со множественным доступом, тем самым значительно сокращая время выполнения задач и продлевая срок службы аккумулятора оконечного устройства.

разгрузка задач, интернет вещей, граничные вычисления со множественным доступом, искусственный интеллект, сеть радиодоступа

Введение

Развитие Индустрии 4.0 и умных городов привело к быстрому расширению масштабов Интернета вещей (IoT) [1]. Новые требования к инновациям значительно увеличили вычислительную нагрузку на оконечные устройства, особенно приложения IoT, которые включают функции искусственного интеллекта (ИИ) [2,3]. Однако вычислительная мощность и энергоснабжение оконечного устройства (ОУ) лимитированы из-за ограничений производственного процесса, стоимости и емкости аккумулятора. Это приводит к ограниченному применению ОУ. Появление технологии разгрузки вычислений предоставляет новые возможности для решения таких проблем [4]. ОУ могут разгружать вычислительные задачи на облачные платформы или сети периферийных вычислений, тем самым значительно сокращая время выполнения задач и продлевая срок службы аккумулятора ОУ [5].

Разгрузка задач IoT в сценарии MEC имеет свои особенности, которые отличаются от других сценариев применения. Во-первых, устройствам IoT необходимо разгружать более ресурсоемкие задачи из-за очень ограниченной вычислительной мощности. Во-вторых, разгрузка задач в сценариях применения IoT требует оптимизации энергопотребления ОУ для продления времени работы устройства из-за ограничений емкости аккумулятора.

В-третьих, IoT имеет больший масштаб сети (например, умные города). Это приводит к огромному количеству ОУ и граничных вычислительных узлов в сети. Поэтому очень сложно найти оптимальное решение для принятия решений о разгрузке задач. Кроме того, вычислительные задачи IoT сильно разнородны из-за различных аппаратных систем и разнообразных программных приложений. Мобильность устройств в некоторых сценариях применения IoT также очень высока (например, Интернет транспортных средств, где необходимо учитывать даже миграцию задач). В совокупности эти факторы делают процесс разгрузки задач в Интернете вещей крайне сложным и предъявляют особенно высокие требования к производительности. Все это приводит к тому, что механизмы разгрузки задач в Интернете вещей должны комплексно учитывать множество целей оптимизации, а не просто улучшать конкретную метрику производительности.

Актуальный метод для систем MEC-IoT

Механизм разгрузки задач на основе искусственного интеллекта – это стратегия, использующая технологии искусственного интеллекта, такие как машинное обучение, для принятия разумных решений о распределении вычислительных задач в распределенной вычислительной среде. Эти механизмы используют алгоритмы искусственного интеллекта для анализа различных факторов, включая состояние сети, возможности устройства и предпочтения пользователя, для определения оптимальной стратегии разгрузки. Основным преимуществом механизмов разгрузки на основе ИИ является их способность адаптироваться к изменяющимся условиям и неопределенностям, обеспечивая принятие решений в режиме реального времени и с учетом контекста. Более того, крупномасштабные сети и массивные устройства часто требуют автоматизированных и интеллектуальных процессов принятия решений.

Подводя итог, можно сказать, что классическая математическая оптимизация обеспечивает оптимальность благодаря строгим моделям, но испытывает трудности с масштабируемостью и динамическими средами Интернета вещей. Оптимизация Ляпунова, делающая акцент на устойчивости, адаптивна, но может быть сложной. Эвристические подходы обеспечивают скорость и адаптивность, но приводят к неоптимальным решениям. Теория игр моделирует стратегические взаимодействия, предлагая равновесные решения, но может требовать больших вычислительных ресурсов. Подходы на основе ИИ развиваются очень быстро. Они обладают высокой адаптивностью и способны

решать сложные задачи оптимизации выгрузки задач. На рисунке 1 сравниваются различные подходы к выгрузке задач в различных таксономиях технологий с точки зрения адаптивности, накладных расходов, возможностей многокритериальной оптимизации, способности поддерживать крупномасштабные системы Интернета вещей и множества параметров.

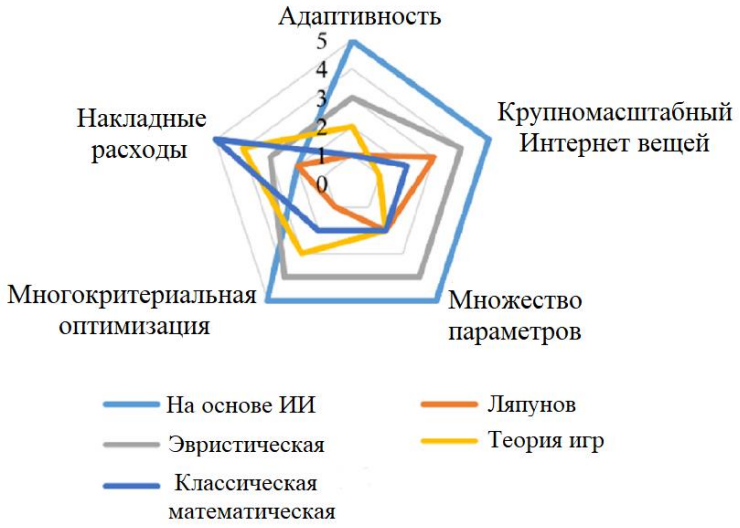


Рис. 1. Разгрузка задач в MEC

ТАБЛИЦА 1. Метрики производительности и их актуальность

Метрика	Актуальность
Эффективность разгрузки	Важна для оценки самой архитектуры MEC, но редко используется как основная метрика в современных исследованиях
Задержка	Метрики производительности, связанные со временем, играют ключевую роль в оценке эффективности разгрузки вычислений в сетях MEC. Возможность минимизировать задержку и оптимизировать временные аспекты разгрузки, выполнения и отклика задач критически важна для различных приложений реального времени, чувствительных к задержкам
Энергопотребление	Крайне важно для автономных IoT-устройств с ограниченным питанием (например, сенсоры, носимая электроника). Эта метрика важна, но часто рассматривается в паре с задержкой
Затраты ресурсов	Важно для операторов и бизнес-моделей, но не всегда является критичной для технических исследований
Точность	Степень правильности или соответствия результата вычислений, обработки данных или предоставления сервиса ожидаемым или эталонным значениям. Метрика важна для задач, связанных с анализом данных, но не всегда напрямую связана с разгрузкой вычислений

Опираясь на данные таблицы 1, большинство современных приложений IoT критичны к задержке: управление в реальном времени, безопасность. MEC внедряется именно для минимизации задержки, если сравнивать его с облаком. Ведущие публикации и стандарты (IEEE, Elsevier, Springer, ITU) используют задержку как основную метрику для оценки эффективности MEC-IoT. Второй по значимости метрикой идет энергопотребление, особенно для автономных устройств. Соответственно, самой значимой и актуальной для рассмотрения метрикой является задержка.

ТАБЛИЦА 2. Методы искусственного интеллекта для уменьшения задержки для сетей радиодоступа в системах MEC-IoT

Метод	Преимущества	Ограничения
Q-learning [6]	Не требует модели среды и платежной информации других устройств	Игнорирует мобильность оконечных устройств
DQN [7]	Поддержка многоадресной сети	Перегрузка системы не учитывается
PDS-learning [8]	Поддерживает оптимизацию как онлайн, так и офлайн выгрузки	Игнорирование динамической масштабируемости вычислительной мощности MEC
DDQN [9]	Высокая безопасность выгружаемых данных	Недостаточное внимание к оптимизации выгрузки между оконечными устройствами
DDPG [10]	Балансировка нагрузки между узлами MEC	Игнорирует мобильность оконечных устройств

Согласно таблице 2, наиболее актуальным методом из представленных является метод DDPG, исходя из следующих наблюдений:

– балансировка нагрузки между узлами MEC: это критически важно для сценариев IoT, где много устройств, нагрузка непостоянна, и где важно избегать перегрузки отдельных узлов;
– глубокое обучение: позволяет адаптироваться к сложным и динамичным условиям MEC-IoT;
– масштабируемость: метод хорошо подходит для распределенных систем с большим количеством устройств.

Заключение

В данной статье был проведен анализ современных подходов к разгрузке вычислительных задач в системах MEC-IoT.

Особое внимание уделялось сравнению различных методов разгрузки, включая классические математические, эвристические, игровые и, особенно, методы на основе искусственного интеллекта. Было показано, что именно методы ИИ, и, в частности, алгоритмы глубокого обучения, обладают наибольшей адаптивностью и способностью эффективно работать в динамичных и масштабируемых средах MEC-IoT.

На основании анализа преимуществ и ограничений существующих методов, а также с учетом актуальных метрик производительности, таких как задержка и энергопотребление, наиболее перспективным для современных MEC-IoT систем был выбран метод DDPG. Он обеспечивает балансировку нагрузки между узлами MEC и хорошо масштабируется для работы с большим количеством устройств, что критически важно для IoT-сценариев.

Список используемых источников

1. Gupta B. B., Quamara M. An overview of Internet of Things (IoT): architectural aspects, challenges, and protocols // Concurrency Comput. Pract. 2020. Ex. 32 (21).

2. Bakar K. B. A., Zuhra F. T., Isyaku B., Sulaiman S.B. A review on the immediate advancement of the internet of things in wireless telecommunications // IEEE Access 11. 2023. 21020–21048.

3. Sobin C. C. A survey on architecture, protocols and challenges in IoT // Wireless Pers. Commun. 2020. 112 (3). PP. 1383–1429.

4. Yousefpour A., Ishigaki G., Gour R., Jue J.P. On reducing IoT service delay via fog offloading // IEEE Internet Things J. 2018. 5 (2). PP. 998–1010.

5. Jin X., Hua W., Wang Z., Chen Y. A survey of research on computation offloading in mobile cloud computing // Wireless Network. 2022. 28 (4). PP. 1563–1585.

6. Wang Y., Yang J., Guo X., Qu Z. A game-theoretic approach to computation offloading in satellite edge computing // IEEE Access 8. 2020. PP. 12510–12520.

7. Yang X., Luo H., Sun Y., Zou J., Guizani M. Coalitional game-based cooperative computation offloading in MEC for reusable tasks // IEEE Internet Things J. 2021. 8 (16). PP. 12968–12982.

8. Hu S., Li G. Dynamic request scheduling optimization in mobile edge computing for IoT applications // IEEE Internet Things J. 2020. 7 (2). PP. 1426–1437.

9. Heidari A., Navimipour N.J., Jamali M.A.J., Akbarpour S. A hybrid approach for latency and battery lifetime optimization in IoT devices through offloading and CNN learning // Comput. Inf. Syst. 2023. 39. PP. 100899.

10. Huang L., Bi S., Zhang Y. J.A. Deep reinforcement learning for online computation offloading in wireless powered mobile-edge computing networks // IEEE Trans. Mobile Comput. 2020. 19 (11). PP. 2581–2593.

TASK OFFLOADING IN INTERNET OF THINGS SYSTEMS WITH MULTI-ACCESS EDGE COMPUTING

Elagin V., Chipsanova E.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Task offloading is becoming increasingly popular, as end devices can offload computational tasks to cloud platforms or multi-access edge computing (MEC) systems, thereby significantly reducing task execution time and extending the battery life of the end device.

Key words: *task offloading, Internet of Things, multi-access edge computing, artificial intelligence, radio access network*

УДК 004.722
ГРНТИ 49.33.29

RAN SLICING ДЛЯ ВИРТУАЛЬНЫХ ОПЕРАТОРОВ MVNO В СЕТЯХ 5/6G

С. М. Елисеев

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

Ключевые технологические решения, заложенные в сетях 5/6G, такие как виртуализация сетевых функций NFV и Network Slicing, привнесли принципиально новые подходы и модели к построению виртуальных мобильных операторов. Разделение сети на логические виртуальные сегменты позволяет запускать MVNO в большом количестве при высоких скоростях внедрения и минимальных затратах. Как и в сетях предыдущих поколений, одной из основных целей опорных операторов PMNO является максимально эффективное использование подсистемы радиодоступа. В данной работе описывается задача оптимизации распределения ресурсов сети радиодоступа между логическими сегментами (RAN Slicing) с учетом различных требований MVNO к параметрам качества обслуживания и соглашениям SLA.

MVNO, 5G, 6G, Network Slicing, RAN, QoS

Технологии логического сетевого разделения Network Slicing и виртуализации сетевых функций NFV позволили базовым опорным операторам PMNO 5/6G проектировать и внедрять мобильных виртуальных операторов MVNO на основе выделенных сетевых сегментов [1,2].

Network Slicing обеспечивает реализацию сервисов, изоляцию и поддержку многопользовательской среды на общей сетевой инфраструктуре, выполняя логическое и физическое разделение сетевых ресурсов для достижения различных требований к параметрам качества обслуживания. Реализация разделения сети задумана как сквозная функция, которая включает в себя базовую сеть (Core Network, CN) и сеть радиодоступа (Radio Access Network, RAN).

Наиболее ограниченным участком для мобильных операторов всех поколений является радиодоступ. MVNO на базе Network Slicing впервые в сетях 5/6G получили инструменты для индивидуального конфигурирования сети в подсистеме RAN [2]. Для PMNO RAN Slicing открыл ряд новых задач для оценки и планирования использования радиоспектра в целях достижения максимальной эффективности с учетом предоставления сервисов с раз-

личными параметрами QoS. При этом особую роль в данном планировании играют сетевые сегменты для MVNO.

Ключевым фактором RAN Slicing для MVNO является то, что сетевые сегменты виртуальных операторов должны быть полностью независимы друг от друга.

Опорный оператор PMNO должен проводить распределение радиоресурсов, обеспечивая при этом строгую и полную изоляцию сегментов MVNO. Комплексную задачу планирования и оптимизации радиоресурсов для MVNO можно составить из следующих компонентов:

1. Обеспечение QoS, описанных в SLA между MVNO и опорным оператором для максимального количества пользователей MVNO во временном слоте в рамках сетевого сегмента. В частности, при максимальной загрузке радиоспектра обеспечить минимальные требования SLA для максимально возможного числа абонентов MVNO.

2. Изоляция сетевого сегмента. Сегмент радиоресурса должен быть предоставлен только одному абоненту MVNO.

3. Динамическое использование схем модуляций и технологий радиодоступа 5/6G для эффективного использования радиоресурса. Например, MIMO (Multiple-Input and Multiple-Output) или CoMR (Coordinated Multipoint)

Минимальным элементом ресурса радиодоступа, который может быть предоставлен пользователю, является ресурсный блок (Resource Block, RB) [3]. Цель PMNO – наиболее рационально распределять ресурсные блоки между пользователями, обеспечивая при этом заявленные параметры QoS. Оптимальное использование RB приведет к увеличению числа абонентов, обслуживаемых в одном временном интервале, как следствие, увеличению числа MVNO.

Скорость передачи данных для пользователя определяет выбранная для него схема модуляции и кодирования MCS (Modulation and Coding Scheme) [4].

Дополнительным условием для учета при RAN Slicing выступает состояние канала между абонентом и базовой станцией 5/6G. Для передачи информации о канале, пользовательское устройство отправляет отчет CQI (Channel Quality Indicator) через регулярные интервалы, определяемые PMNO [5]. При решении задачи оптимизации CQI позволяет планировать

загрузку сети радиодоступа в условиях динамического состояния канала, наиболее близко к реальным сценариям.

Узел сети управления RAN представлен в виде архитектуры Software Defined - Radio Access Network (SD-RAN), где управление и оркестровка реализованы как программно-определяемая сеть SDN. Функционально его можно разделить на контроллер и планировщик (рис. 1).

Управление сетевыми сегментами, в частности подсистемой RAN, со стороны PMNO и MVNO производится через стек SMF (Slice Management Function), который состоит из функций управления сервисами CSMF (Communication Service Management Function), сетевыми сегментами NSMF (Network Slice Management Function) и подсетями сетевых сегментов NSSMF (Network Slice Subnet Management Function) [2, 6].

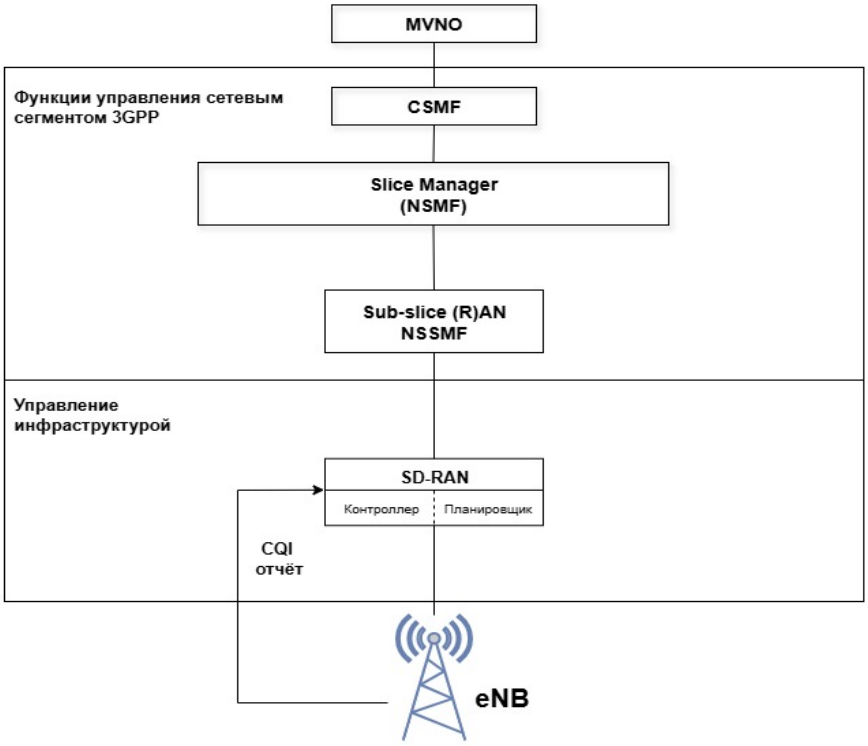


Рис 1. Функции управления RAN Slicing

Исходными критериями для планирования ресурсов радиодоступа для MVNO выступают параметры QoS, которые закладывает виртуальный оператор. За основу можно взять минимальную скорость передачи данных для пользователя MVNO, которая зависит от количества выделенных ресурсных блоков RB и выбранного уровня MSC в единицу времени. В свою очередь, выбор уровня MSC зависит от условий транспортного канала, информация о которых передается в отчетах CQI.

Математическому описанию, анализу и синтезу алгоритмов для оптимизации распределения ресурсов сети радиодоступа на основе описанных вводных будут посвящены последующие работы.

Список используемых источников

1. Елисеев. С. М., Гольдштейн Б. С. Мобильные виртуальные операторы в сетях 5G. Модели и архитектура // Системы синхронизации, формирования и обработки сигналов. М., 2025. Т. 16. № 3. С. 4-8.

2. Елисеев С. М., Гольдштейн А. Б. Технологические подходы к построению виртуальных мобильных операторов MVNO в сетях 5G // 65 Научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025), сборник научных статей: в 3-х т. Санкт-Петербург, 2025. С. 79-84.

3. 3GPP TS 38.211 V18.5.0 (2025-01) Physical channels and modulation. URL: https://www.etsi.org/deliver/etsi_ts/138200_138299/138211/18.05.00_60/ts_138211v 180500p.pdf (дата обращения 12.04.2025).

4. 3GPP TS 38.214 V16.2.0 (2020-07) Physical layer procedures for data. URL: https://www.etsi.org/deliver/etsi_ts/138200_138299/138214/16.02.00_60/ts_138214v160200p.pdf (дата обращения 12.04.2025).

5. 3GPP TS 38.521-4 V16.7.0 (2021-04) User Equipment (UE) conformance specification; Radio transmission and reception. URL: https://www.etsi.org/deliver/etsi_ts/138500_138599/138522/16.07.00_60/ts_138522v160700p.pdf (дата обращения 12.04.2025).

6. 3GPP TS 28.533 V15.0.0 (2018-10) Management and orchestration; Architecture framework. URL: https://www.etsi.org/deliver/etsi_ts/128500_128599/128533/15.00.00_60/ts_128533v 150000p.pdf (дата обращения 12.04.2025).

Статья представлена научным руководителем, профессором кафедры ИКС СПбГУТ, доктором технических наук Гольдштейном А. Б.

RAN SLICING FOR VIRTUAL MVNO OPERATORS IN 5/6G NETWORKS

Eliseev S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Key technological solutions incorporated into 5/6G networks, such as network function virtualization NFV and Network Slicing, have brought fundamentally new approaches and models to building virtual mobile operators. Dividing the network into logical virtual segments allows launching MVNOs in large numbers at high implementation speeds and minimal costs. As in previous generation networks, one of the main goals of PMNO operators is the most efficient use of the radio access subsystem. This paper describes the problem of optimizing the distribution of radio access network resources between logical segments (RAN Slicing) taking into account various MVNO requirements for quality of service parameters and SLA agreements

Key words: *MVNO, 5G, 6G, Network Slicing, RAN, QoS*

УДК 004.031.2
ГРНТИ 49.01.85

ОРГАНИЗАЦИЯ ЛОЖНОГО ТРАФИКА В HONEYPOT-СИСТЕМАХ

В. А. Задбоев, В. И. Татаринов, Д. Ф. Ткачев

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

В статье рассматриваются методы организации ложного трафика с использованием honeypot-подсистем различной степени интерактивности. Описаны подходы к интеграции таких систем в корпоративную инфраструктуру, включая использование облачных технологий, программных средств автоматизации и виртуализации.

honeypot, ложный трафик, кибербезопасность, кибератаки, автоматизация, IDS/IPS, Suricata, Ossec, User Mode Linux.

Актуальность: с развитием цифровых технологий растет и сложность кибератак. Традиционные средства защиты, такие как брандмауэры и системы обнаружения вторжений, не всегда способны своевременно выявить продвинутые угрозы. В этой связи все большее внимание уделяется активным методам защиты, одним из которых является использование honeypot-систем. Они представляют собой ложные среды, предназначенные для привлечения и анализа действий злоумышленников. Особый интерес представляет организация ложного трафика, который позволяет повысить реалистичность подделки и увеличить эффективность обнаружения атак.

Honeypot-системы представляют собой специально созданные ложные среды, предназначенные для привлечения атакующих с целью мониторинга их действий и извлечения ценных данных о методах кибератак [1]. Основная цель внедрения таких подсистем заключается не только в отслеживании активности угроз, но и в предоставлении информации для последующего анализа и улучшения механизмов защиты. Исследования показывают, что использование honeypot-систем позволяет эффективно собирать данные о сложных многоэтапных кибератаках [1].

Одним из ключевых подходов к созданию реалистичного ложного трафика является использование User Mode Linux (UML). Эта технология позволяет создавать копии оригинальных сетей в пользовательском пространстве хостовой операционной системы, исключая нежелательные побочные эффекты, такие как перекрестные помехи между honeypot-системами [2-3].

Для автоматизации генерации ложного трафика могут применяться программные решения:

– Suricata – open-source система обнаружения угроз с возможностью глубокого анализа пакетов (DPI);
– Ossec – система мониторинга безопасности и активного реагирования на угрозы с модульной архитектурой.

Примером успешной реализации является проект, в котором honeypot был интегрирован перед сетью для отслеживания и блокировки SSH-атак на порту 22. Для анализа данных использовались облачные решения AWS и Kubernetes, где логи атак сохранялись в DynamoDB с временем жизни записи в семь дней. За две недели тестирования система показала 100 % доступность и высокую производительность [4].

Однако вышеперечисленные способы с готовыми решениями могут пригодится только для больших компаний, так как они требуют обработку больших данных за короткие сроки. Поэтому для небольших организаций существуют упрощенные способы при создании ложного трафика, которые достаточно настроить на местном оборудовании.

Для развертывания ложного трафика достаточно имитировать [5]:

1. Активность реальных пользователей в системе, шаблон скрипта представлен на рис. 1, ими могут быть: веб-запросы посещения страниц, авторизации, отправки форм и так далее.

```
import requests
import time
session = requests.Session()
login_data = {
    "username": "user123",
    "password": "pass123"
}
response = session.post("http://your-app/login", data=login_data)
for _ in range(5):
    response = session.get("http://your-app/dashboard")
    print(f"Посетил dashboard → {response.status_code}")
    time.sleep(30)
```

Рис. 1. Скрипт для генерации веб-запросов

2. Трафик между сервисами для поддержки фоновой коммуникации между компонентами системы.

– простые HTTP-запросы между микросервисами: «curl -X POST http://api-service/users --data '{"name": "Alice"}'»;
– TCP/UDP-трафик: «echo "GET /status" | nc internal-db-server 8080»;
– скрипт на Python для постоянной эмуляции трафика, представленный на рис. 2:

```python
import socket
import time

while True:
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
        try:
            s.connect(("internal-service", 9000))
            s.sendall(b"ping")
            data = s.recv(1024)
            print("Ответ от сервиса:", data.decode())
        except Exception as e:
            print("Ошибка подключения:", str(e))
    time.sleep(60)
```

Рис. 2. Скрипт для эмуляции трафика

3. Использование фальшивых DNS/DHCP/SMB/HTTP сервисов.

Как и в настоящей сети в ложной необходимо добавить обслуживающие сервера для предоставления доступа между устройствами, так как статическая маршрутизация является явным признаком ложной сети.

4. Фальшивые логи и метаданные для симуляции обновляемых файлов, так как если зараженные файлы будут устаревшими, то для нарушителя они не будут представлять какой-либо ценности. Для данной цели можно написать генератор на Python представленный на рис. 3.

```python
import random
import datetime

users = ["admin", "user1", "support"]
ips = ["192.168.1.10", "192.168.1.11", "10.0.0.5"]

for _ in range(20):
    user = random.choice(users)
    ip = random.choice(ips)
    timestamp = datetime.datetime.now().strftime("%b %d %H:%M:%S")
    print(f"{timestamp} server sshd[1234]: Accepted password for {user} from
{ip}")
```

Рис. 3. Скрипт для генерации логов

Все скрипты рекомендуется настроить на автоматическую работу через сервис Cron, например: «*/5****/usr/bin/python3/path/to/ service_traffic.py».

Заключение

Таким образом, организация ложного трафика в honeypot-системах требует комплексного подхода, включающего использование современных технологий, программных решений и учета аппаратных ограничений. Интеграция таких систем позволяет значительно повысить уровень защищенно-

сти информационных ресурсов и сделать инфраструктуру более устойчивой к современным киберугрозам. Однако дальнейшие исследования должны быть направлены на оптимизацию производительности и снижение затрат на внедрение honeypot-систем, а также на развитие интеграции с машинным обучением и облачными платформами.

Список используемых источников

1. Липатников, В. А., Задбоев В. А., Мелехов К. В. 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: Изд-во Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2024. С. 112-114.

2. Задбоев В. А., Липатников В. А., Мелехов К. В., Шевченко А. А. Система контроля безопасности сети передачи данных. Патент № 2834591 C1 Российская Федерация; заявитель и правообладатель федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации. заявл. 29.09.23; опубл. 11.02.2025.

3. Задбоев В. А., Липатников В. А., Мелехов К. В., Шевченко А. А. Способ защиты информационно-вычислительной сети от вторжения. Патент № 2839562 C1 Российская Федерация; заявитель и правообладатель федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации. заявл. 27.02.24; опубл. 06.05.2025.

4. Задбоев В. А., Шевяков В. Д., Беседин М. Д., Садовников В. Е. Использование технологий блокчейн для обеспечения информационной безопасности // Современные тенденции развития фундаментальных и прикладных наук: материалы VIII всерос. науч.-практ. конф., Брянск, 25 янв. 2025 г. С. 529-532.

5. Липатников В. А., Шевченко А. А., Мелехов К. В., Задбоев В. А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37-49. DOI 10.31799/1684-8853-2025-2-37-49. EDN:PVFXDP.

ORGANIZING FALSE TRAFFIC IN HONEYPOT SYSTEMS

Zadboev V., Tatarinov V., Tkachev D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article discusses methods for organizing false traffic using honeypot subsystems of varying degrees of interactivity. Approaches to integrating such systems into corporate infrastructure are described, including the use of cloud technologies, automation software, and virtualization.

Key words: *honeypot, false traffic, cybersecurity, cyber attacks, automation, IDS/IPS, Suricata, Ossec, User Mode Linux*

УДК 004.031.2
ГРНТИ 49.01.85

ПРИНЦИПЫ МАСКИРОВКИ ЗАРАЖЕННЫХ ФАЙЛОВ В HONEYPOT-СИСТЕМАХ

В. А. Задбоев, В. И. Татаринов, Д. Ф. Ткачев

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

Honeypot-системы играют важную роль в обеспечении кибербезопасности информационно-вычислительных сетей, позволяя выявлять и анализировать внешние атаки. Одним из ключевых элементов такой системы являются зараженные файлы, которые должны быть тщательно созданы и замаскированы под реальные данные компании. В данной статье рассматриваются основные подходы к разработке таких файлов, способы их внедрения в сеть, а также техники маскировки для повышения достоверности honeypot-системы. Особое внимание уделено вопросам безопасности, эмуляции реального поведения в системе и предотвращения распознавания системы как ловушки.

honeypot, система обнаружения вторжений, кибербезопасность, зараженные файлы, маскировка данных, триггер, анализ кибератак, защита информационных систем, мониторинг сетевой активности

Актуальность: Honeypot-системы играют важную роль в современной кибербезопасности, особенно при защите информационно-вычислительных сетей (ИВС) от внешних вторжений. Их основное предназначение – привлечь внимание злоумышленников, создав для них иллюзию успешного вторжения. На деле же происходит сбор информации о методах и инструментах атаки самого злоумышленника. Однако для повышения эффективности такой системы недостаточно просто имитировать уязвимости. Одним из ключевых элементов является создание и маскировка зараженных файлов, под видом настоящих и ценных для потенциального злоумышленника.

Процесс создания зараженных файлов начинается с тщательного анализа типичного поведения пользователя внутри ИВС. Специалисты по безопасности собирают данные о том, какие форматы файлов чаще всего используются сотрудниками, где они обычно хранятся, какие названия предпочитаются, а также какова структура содержимого таких документов. На основе этих данных создаются файлы, которые визуально и функционально напоминают настоящие документы, отчеты, архивы или другие данные, доступные в корпоративной среде. Например, это могут быть документы Microsoft Office (Word, Excel), PDF-файлы, исполняемые файлы или архивы с паролем [1].

После того как такие файлы подготовлены, в них внедряются специальные триггеры – небольшие фрагменты кода, позволяющие зафиксировать факт взаимодействия с файлом. Триггеры могут быть реализованы в виде скриптов, запускаемых при указанных обстоятельствах, например при открытии файла [2].

Маскировка зараженных файлов заключается в их визуальном и структурном соответствии реальным данным. Файл должен выглядеть как настоящая рабочая информация, то есть может содержать таблицы, графики, текстовые блоки, логотипы компании, реалистичные заголовки и внутреннюю структуру. Это позволяет повысить доверие к нему со стороны злоумышленника. Для усиления эффекта правдоподобности можно использовать имена сотрудников, даты, проекты, названия отделов. Если есть потребность использовать настоящие сведения о компании, то для этого достаточно использовать открытые сведения, например имена начальства или основные задачи представленной организации. Также можно имитировать конфиденциальную информацию, например, финансовые отчеты, паспорта сотрудников или номера банковских карт. Все вышеперечисленные процессы необходимы для удержания злоумышленника в ИВС для сбора сведений о его действиях [3].

Еще одним важным аспектом является местонахождение файлов в структуре ИВС [4]. Зараженные файлы должны находиться в соответствующих им директориях, иметь соответствующие права доступа, быть частью логической структуры сети. Кроме того, файлы должны быть размещены в разных сегментах сети [5] для увеличения вероятности их обнаружения, как представлено на рис. 1.

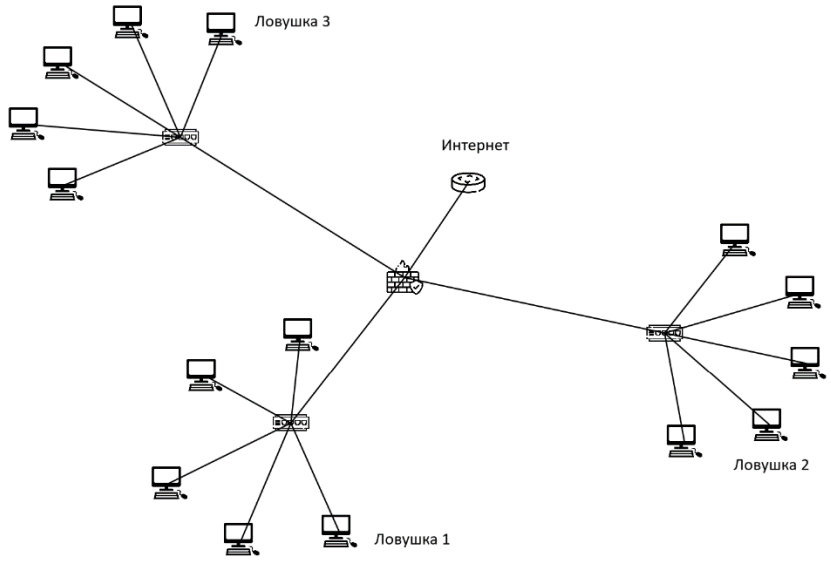


Рис. 1. Схема ИВС с внедренными ловушками

Ниже представлены примеры реализации зараженных файлов:

1. Документ Word под названием «Финансовый_отчет_2024.docx», который выглядит как настоящий отчет бухгалтерии компании и хранится, соответственно, по пути «\server\finance\reports». В нем присутствует таблица с данными по доходам и расходам, графики, логотип компании и подпись главного бухгалтера, а в свойствах документа могут присутствовать реалистичные метаданные, представленные на рис. 2, например: автор, дата последнего изменения, ключевые слова.

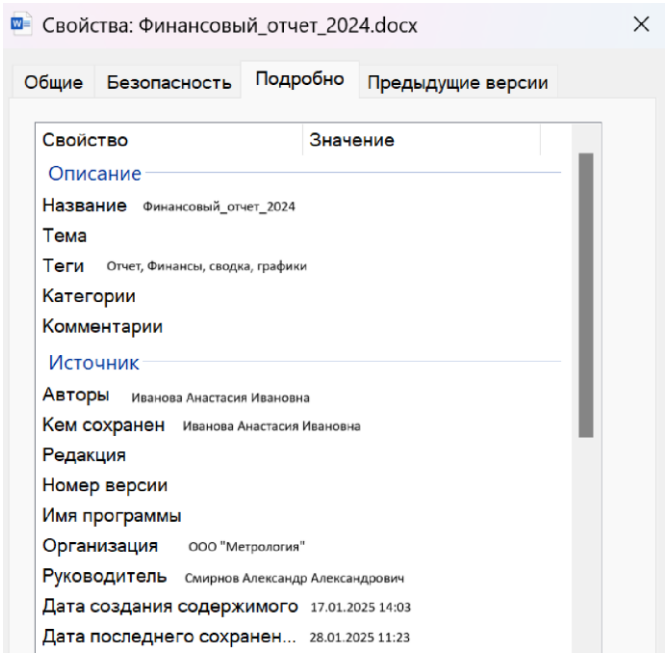


Рис. 2 Метаданные в документах

2. ZIP-архив, защищенный паролем (специально простым (например «12345»). Архив может называться по-разному в зависимости от местоположения, например в папке «\server\HR\employees\backup» он будет называться как резервные копии данных сотрудников, в котором для правдоподобности будут храниться сгенерированные списки, представленные на рис. 3.

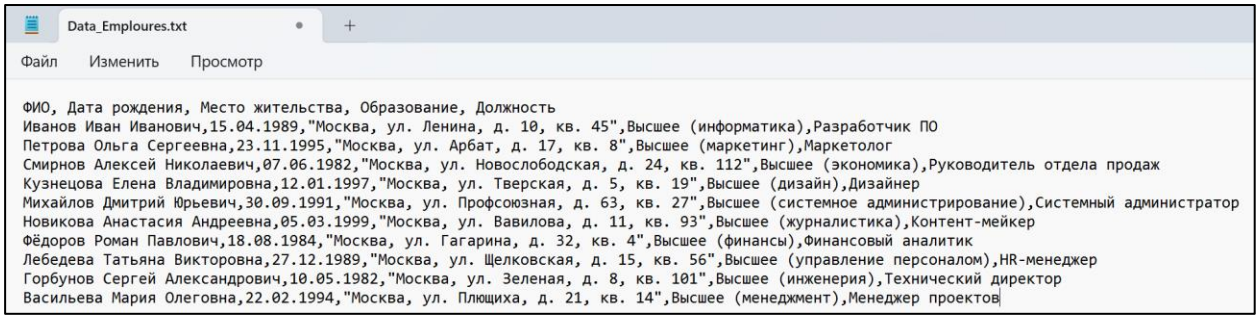


Рис. 3 Сгенерированная база данных сотрудников

Также стоит отметить, что зараженные файлы в honeypot-системе не должны влиять на состояние сети и не влиять на работу пользователей, если они находятся в первоначальной ИВС, так как цель таких файлов – детектировать попытки проникновения и собирать информацию о нарушителе, а не наносить вред. Поэтому все встроенные триггеры тщательно изолируются и не имеют возможности распространяться за пределы ловушки, если это не подразумевает иных действий. Это достигается с помощью строгих ограничений на сетевые подключения и постоянного мониторинга состояния файлов. Все действия, производимые злоумышленником над такими файлами, записываются и анализируются для дальнейшего использования в расследованиях и улучшении уровня защиты сети.

Для еще большей достоверности могут применяться различные методы обфускации кода для снижения вероятности обнаружения антивирусными программами и системами обнаружения вторжений злоумышленника.

Кроме того, файлы необходимо постоянно обновлять для сохранения актуального вида, для это можно создать скрипты с механизмами самообновления. Это особенно важно в долгосрочных honeypot-системах, где злоумышленник может вернуться к атаке спустя длительное время.

Заключение

Создание и маскировка зараженных файлов в honeypot-системе – это сложный процесс, требующий понимания как технической стороны атак, так и поведения реальных пользователей. Правильно реализованные и замаскированные файлы повышают эффективность ловушки, позволяя собирать ценные данные о методах кибератак, а также своевременно выявлять и реагировать на угрозы. Такие файлы становятся не просто приманкой, а важным элементом системы раннего предупреждения и анализа киберугроз.

Список используемых источников

1. Липатников В. А., Шевченко А. А., Мелехов К. В., Задбоев В. А. Метод активной защиты объектов критической информационной инфраструктуры от кибератак на основе прерывания процесса воздействия нарушителя // Информационно-управляющие системы. 2025. № 2(135). С. 37-49. DOI 10.31799/1684-8853-2025-2-37-49. EDN:PVFXDP.

2. Задбоев В. А., Липатников В. А., Мелехов К. В., Шевченко А. А. Система контроля безопасности сети передачи данных. Патент № 2834591 C1 Российская Федерация; заявитель и правообладатель федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Со-

ветского Союза С. М. Буденного» Министерства обороны Российской Федерации. заявл. 29.09.23; опубл. 11.02.2025.

3. Задбоев В. А., Липатников В. А., Мелехов К. В., Шевченко А. А. Способ защиты информационно-вычислительной сети от вторжения. Патент № 2839562 C1 Российская Федерация; заявитель и правообладатель федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации. заявл. 27.02.24; опубл. 06.05.2025.

4. Лимонцев Д. С., Задбоев В. А., Садовников В. Е. Уровень защищенных сокетов в сети и веб-безопасности // Инновационные исследования молодых ученых и проблемы Индустрии 4.0: Сборник научных статей по материалам конференции, Санкт-Петербург, 29 марта 2024 года. СПб.: Военная академия связи им. Маршала Советского Союза С. М. Буденного, 2024. С. 23-29. EDN:LOOYDP.

5. Задбоева Н. А., Задбоев В. А., Садовников В. Е. Программа визуализации информационной сети. Свидетельство о государственной регистрации программы для ЭВМ № 2025663608 Российская Федерация / Н. А. Задбоева, В. А. Задбоев; заявитель и правообладатель Задбоева Н. А. № 2025663608; заявл. 24.05.2025: опубл. 28.05.2025.

PRINCIPLES OF MASKING INFECTED FILES IN HONEYPOT SYSTEMS

Zadboev V., Tatarinov V., Tkachev D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Honeypot systems play an important role in ensuring cybersecurity of information and computing networks, allowing to detect and analyze external attacks. One of the key elements of such a system are infected files, which must be carefully created and disguised as real company data. This article discusses the main approaches to developing such files, methods of their introduction into the network, as well as disguise techniques to increase the reliability of the honeypot system. Particular attention is paid to security issues, emulation of real behavior in the system and prevention of recognition of the system as a trap.

Key words: *honeypot, intrusion detection system, cybersecurity, infected files, data masking, trigger, cyber attack analysis, information system protection, network activity monitoring*

УДК 534.2
ГРНТИ 49.03.05

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК КАНАЛА АКУСТИЧЕСКОГО ТРАНСФОРМАТОРА С УЧЕТОМ МНОГОКРАТНЫХ ПЕРЕОТРАЖЕНИЙ ОТ ГРАНИЦ БАРЬЕРА

А. В. Качнов, А. А. Прасолов, Е. И. Туманова

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

В статье показаны результаты моделирования амплитудно-частотной (АЧХ) и фазочастотной (ФЧХ) характеристик тракта акустического трансформатора. Рассматривается степень влияния переотражений на изменение свойства сигнала, проходящего через барьер. Проведен анализ зависимостей АЧХ и ФЧХ от размеров барьера и частоты информационного сигнала. Полученные результаты показывают, что переотражения вызывают появление резонансных пиков и провалов в АЧХ, что существенно влияет на качество передачи сигнала. Работа имеет практическое значение для реализации приемопередающих трактов акустического трансформатора

акустический трансформатор, ультразвуковая связь, переотражения, обработка сигналов, структурно-неоднородный канал

Передача информации через металлические барьеры с использованием ультразвуковых колебаний является одним из наиболее перспективных направлений для обеспечения беспроводных каналов связи в условиях, когда традиционные методы, основанные на передаче электромагнитных волн, оказываются неэффективными или невозможными [1-2]. Практической реализацией такого подхода является акустический трансформатор, структурная схема которого представлена на рис. 1.

В реальных условиях распространения ультразвуковых колебаний в твердых телах возникают многократные переотражения от границ барьера, неоднородностей и внутренних дефектов материалов. Переотражения приводят к формированию сложной интерференционной картины [3], которая оказывает существенное влияние на форму АЧХ и ФЧХ. Изучение этого влияния имеет фундаментальное значение для формирования требований к построению приемо-передающих устройств акустического трансформатора. Комплексный анализ изменения передаточной характеристики канала необходим также для разработки методов компенсации эха и адаптивной обработки сигналов в реальных устройствах.

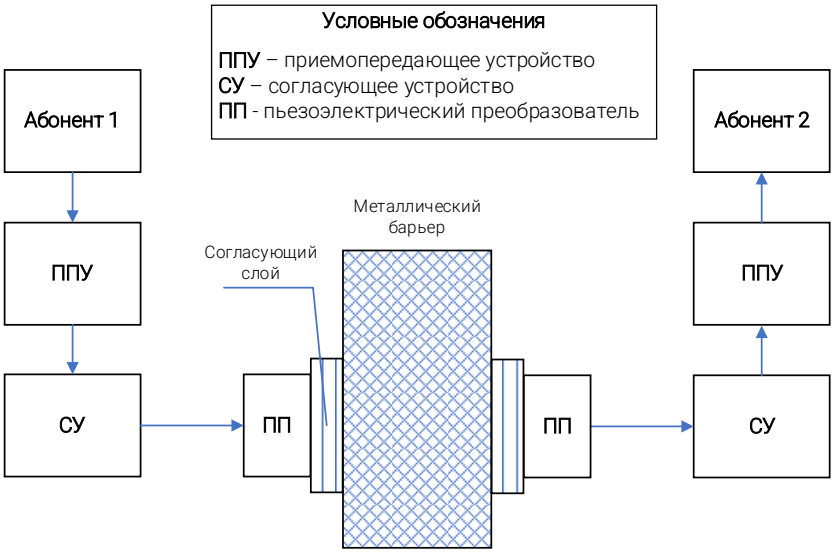


Рис. 1. Структурная схема акустического трансформатора

Настоящая работа является продолжением серии исследований, посвященных возможности применения акустического трансформатора в составе донных станций [4] комплекса морской сейсморазведки и мониторинга «КРАБ» [5].

1. Модель канала акустического трансформатора

В качестве модели канала акустического трансформатора будем рассматривать бесконечный плоскопараллельный барьер, выполненный из алюминия.

Для дальнейшего исследования введем следующие обозначения:

α – коэффициент затухания ультразвуковых колебаний в металле,

V – коэффициент отражения от границ барьера,

d – толщина образца,

c – скорость звука в барьере,

$k = \omega/c = 2\pi f/c$ – волновое число.

Пусть на пьезоэлектрический преобразователь подается гармонический сигнал U_0 с единичной амплитудой. Тогда на выходе барьера амплитуда ультразвукового импульса, без учета переотражений, будет описываться выражением:

$$U_1 = U_0 e^{-\alpha d} e^{jkd}$$

После прохождения в прямом направлении часть сигнала отражается от нижней границы образца и проходит в обратном направлении. Это же явление справедливо и для верхней границы образца. Таким образом часть сигнала будет отражаться от границ барьера и складываться с прямым сигналом. Результирующую комплексную амплитуду выходного сигнала в таком случае целесообразно описать как суперпозицию всех переотраженных сигналов от границ барьера:

$$U_{\text{вых}} = U_1 + U_2 + \cdots + U_n + \cdots,$$

где

$$U_2 = U_0 V^2 e^{-3\alpha d} e^{3jkd};$$
$$U_3 = U_0 V^4 e^{-5\alpha d} e^{5jkd} \ldots$$

После подстановки и проведения элементарных математических операций получим уравнение [6], описывающее комплексную амплитуду ультразвукового импульса, прошедшего плоскопараллельный барьер бесконечной ширины с учетом многократных переотражений:

$$U_{\text{вых}} = U_0 \frac{e^{-\alpha d} e^{jkd}}{1 - V^2 e^{-2\alpha d} e^{2jkd}}$$

С учетом вышесказанного, очевидно, что амплитудно-частотная характеристика представляет собой модуль $U_{\text{вых}}$, а фазочастотная характеристика – аргумент $U_{\text{вых}}$.

2. Исходные данные для моделирования

Для моделирования характеристик канала будем использовать параметры, указанные в таблице 1.

ТАБЛИЦА 1. Численные значения параметров моделирования

Параметр	Единицы измерений	Алюминий
Толщина образца, d	мм	1; 30
Скорость звука в барьере, c	м/с	6 320
Коэффициент затухания, α	Нп/м	3.50
Коэффициент отражения от границы, V	-	0.9
Диапазон исследуемых частот, f	кГц	10 … 500

3. Результаты моделирования

На первом этапе проведем симуляцию влияния переотражений для алюминиевого барьера толщиной 1 мм. Выбор толщины обусловлен наличием лабораторного стенда испытаний, в котором толщина барьера аналогична модели. Исследуемый диапазон выбран таким образом, чтобы попасть в рабочую полосу имеющего пьезоэлектрического преобразователя с резонансной частотой 40 кГц, установленного на лабораторном стенде.

На рис. 2 представлен график АЧХ (синяя линия) и ФЧХ (красная линия) алюминиевого барьера. Анализ графика показывает, что учет многократных переотражений оказывает существенное влияние на амплитуду выходного сигнала и она оказывается значительно выше входного единичного воздействия.

Вторым этапом проводилось моделирование распространения ультразвуковых колебаний через барьер, размеры которого соответствуют толщине корпуса донной станции системы КРАБ. На рис. 3 представлены АЧХ (синяя линия) и ФЧХ (красная линия) барьера толщиной 30 мм.

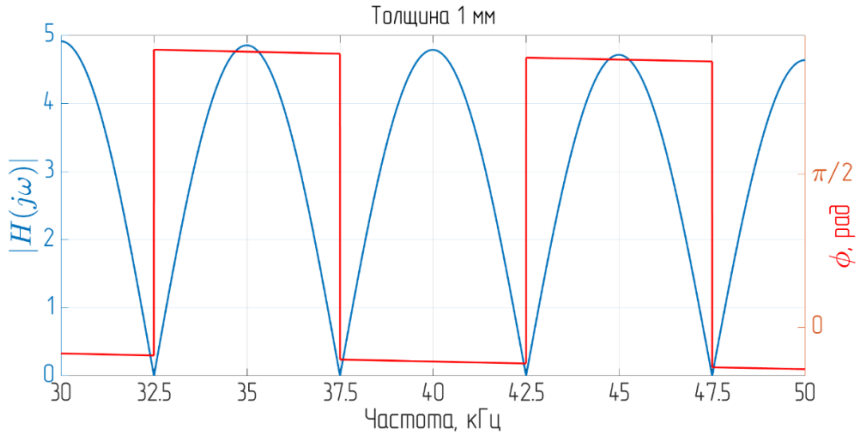


Рис. 2. АЧХ и ФЧХ алюминиевого барьера толщиной 1 мм

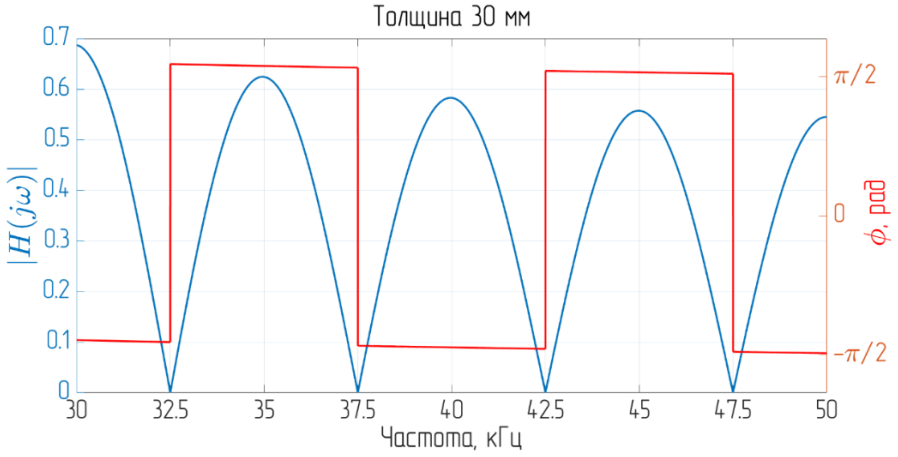


Рис. 3. АЧХ и ФЧХ алюминиевого барьера толщиной 30 мм

На рис. 4 представлены АЧХ канала передачи в расширенном диапазоне частот для разных толщин барьера.

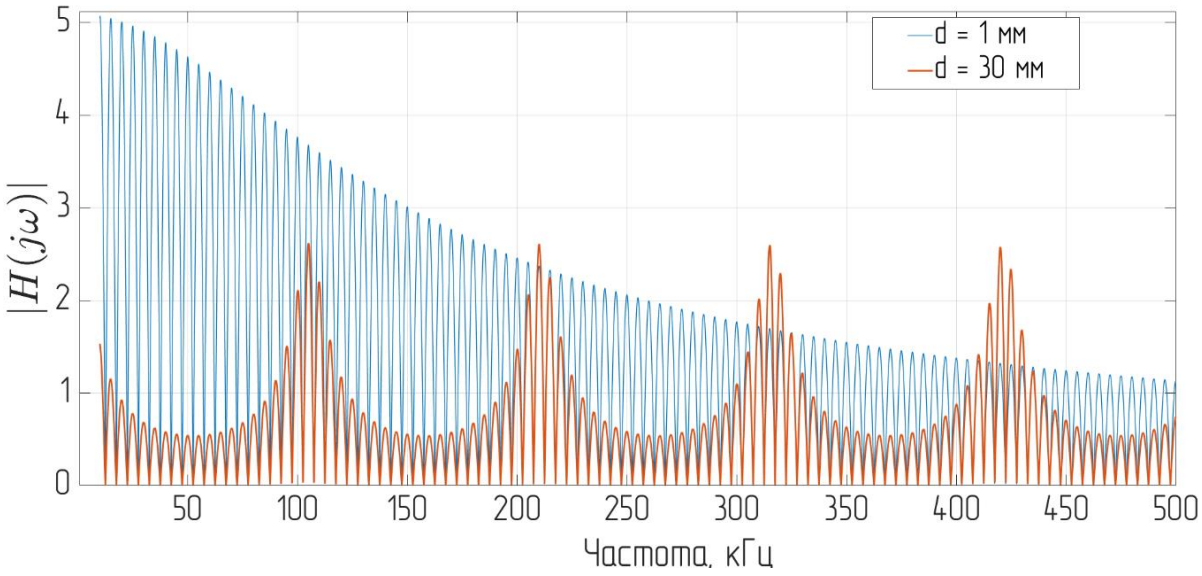


Рис. 4. АЧХ алюминиевого барьера в расширенном диапазоне частот

По итогам моделирования можно сделать вывод о том, что канал акустического трансформатора имеет ярко выраженный частотно-селективный характер с нулями передаточной функции, отстоящими друг от друга на 5 кГц. С увеличением толщины образца преобладающим фактором становиться затухание ультразвуковых волн, также необходимо учитывать образующийся набег фаз между прямым и переотраженными сигналами. Кроме того, с увеличением толщины барьера появляются пики АЧХ, обусловленные интерференцией сигнала, которые можно использовать в целях повышения эффективности передачи.

Дальнейшим направлением исследований является анализ применимости различных видов модуляции для использования в канале акустического трансформатора.

Список используемых источников

1. Исаев А. В., Глухов А. Ю., Петров С. А. Беспроводной способ и система передачи энергии и информации посредством ультразвука в упругой среде. Пат 2809996 C1 Российская Федерация; Правообладатель Российская Федерация, от имени которой выступает Государственная корпорация по атомной энергии «Росатом», Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт автоматики им. Н. Л. Духова» № 2022132726: заявл. 13.12.2022: опубл. 21.12.2023. 34 с.

2. Василенко А. В., Дикарев А. В., Дмитриев С. М., Кубкин В. А. Способ и система беспроводной передачи энергии и информации. Пат. 2693536 С1 Российская Федерация; Правообладатель Общество с ограниченной ответственностью "Лаборатория подводной связи и навигации" № 2018143899: заявл. 11.12.2018: опубл. 03.07.2019. 12 с.

3. Бреховских Л. М., Годин О. А. Акустика слоистых сред. М.: Наука. Гл. ред. физ-мат. лит., 1989. 416 с. ISBN 5-02-014155-0.

4. Качнов А. В., Кропанина А. А. Формирование требований к системе беспроводной передачи данных и электроэнергии сейсмических донных станций комплекса «краб» // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024): Сборник лучших докладов V Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей. В 2-х томах, Санкт-Петербург, 03–05 декабря 2024 года. СПб.: СПбГУТ, 2025. С. 159-163. EDN:OBXNXM.

5. Рогинский К. А., Ильинский Д. А., Ганжа О. Ю. Сейсморазведка в транзитной зоне. Опытно-промышленные испытания системы "КРАБ-400" (этап 3) // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2021. Т. 13, № 5. С. 611-624. DOI 10.21821/2309-5180-2021-13-5-611-624. EDN:URZHUE.

6. Иванов А. Н. Математическое моделирование процессов распространения акустических волн в структурно-неоднородных средах: дис. … канд. техн. наук: 01.04.06 / Иванов Андрей Николаевич. Владивосток, 2008, 141 с.

INVESTIGATION OF THE CHARACTERISTICS OF AN ACOUSTIC TRANSFORMER CHANNEL CONSIDERING MULTIPLE REFLECTIONS FROM BARRIER BOUNDARIES

Kachnov A. V., Tumanova E. I., Prasolov A. A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article presents the results of modeling the amplitude-frequency (AFC) and phase-frequency (PFC) characteristics of an acoustic transformer channel. The degree of influence of multiple reflections on changes in the properties of a signal passing through a barrier is considered. An analysis of the dependence of the AFC and PFC on the barrier dimensions and the frequency of the information signal has been carried out. The obtained results show that multiple reflections cause the appearance of resonance peaks and dips in the AFC, which significantly affects the quality of signal transmission. This work has practical significance for the implementation of transmitting and receiving paths of an acoustic transformer.

.

Key words: *Acoustic transformer, ultrasonic communication, multiple reflections, signal processing, structurally inhomogeneous channel*

УДК 621.391
ГРНТИ 47.05.03

ПОСТРОЕНИЕ АСИНХРОННОГО ШИРОКОПОЛОСНОГО КАНАЛА ТОЧКА-МНОГОТОЧИЕ

Е. И. Книгиницкий, Д. С. Кукунин

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

Работа посвящена исследованию модели канала передачи данных с применением технологии расширения спектра последовательностями максимальной длины. Исследуется модель канала передачи один ко многим на физическом уровне, рассматриваются различные типы модуляции несущей.

М-последовательность, фантомный канал, асинхронная передача

Введение

В предыдущей работе [1] было проведено моделирование канала передачи данных с самосинхронизацией [2, 3, 4, 5] на канальном уровне. Данная работа посвящена развитию модели в виде моделирования физического уровня. В ходе работы исследуется шумозащищенность канала при частотной (ЧМ) и дифференциальной фазовой (ДФМ) модуляциях, а также при различных параметрах системы.

Описание модели

Модель системы строится в программном пакете SciLab и, как и прежде, состоит из двух основных узлов: источника радиосигнала и приемника. К задачам источника, описанным в прошлой статье, добавляется задача модуляции сигнала. На приемной стороне соответственно появляется необходимость демодуляции принятого сигнала.

В качестве видов модуляции применены эффективные с точки зрения пик-фактора виды: частотная манипуляция (ЧМ) и дифференциальная фазовая манипуляция (ДФМ).

Обработанный сигнал S на канальном уровне представляет собой набор из $(p^k–1)*2*N_p$ чипов, где N_p – количество сигнальных пар. Каждый из чипов имеет значение от $–p^{k–1}$ до $p^{k–1}$. Это означает, что для передачи сигнала необходимо p^k+1 возможных частотных или фазовых уровней.

На физическом уровне сигнал представляет собой последовательность значений, характеризующих мгновенное значение напряженности электрического поля. При скорости передачи чипов F_m и частоте несущей F_0, каждый чип состоит из F_0/F_m периодов несущей. По теореме Котельникова для описания каждого чипа необходимо не менее $4*F_0/F_m$ отсчетов.

Для надежности выбрано количество отсчетов на чип, равное $N_t=10*F_0/F_m$. При этом временной шаг составляет $dt=1/(10*F_0)$.

При ЧМ формирование сигналов состоит из следующих этапов. Сначала формируются все возможные p^k+1 вариантов чипов в виде набора нормированных напряжений по временным отсчетам:

$$U_n(t) = exp\ (i * 2\pi * (F_0 + n * dF) * t),$$

где F_0 – частота несущей, dF – единичная девиация частоты, n – все возможные значения чипов (от $-p^{k-1}$ до p^{k-1}), t – набор временных отсчетов $(0..N_t-1)*dt$.

Далее для каждого Un рассчитывается фазовый набег к концу чипа. Это необходимо для обеспечения неразрывности фазы.

$$Ph_n = (F_0 + n * dF) * N_t * dt/2\pi.$$

Результирующий сигнал будет иметь состав:

$$U_r = [U_{S_1}, U_{S_2} * exp(i * Ph_{S_1}), U_{S_3} * exp(i * (Ph_{S_1} + Ph_{S_2})), \dots, U_{S_j} * exp\left(i * \sum_{m=1}^{j-1} Ph_{S_m}\right), \dots]$$

На приемной стороне каждый отсчет делится на значение несущей U_0 в этот же момент и из полученной величины вычисляется натуральный логарифм. В результате получается набор фазовых сдвигов относительно несущей. Из-за частотного сдвига в период каждого чипа фазовый сдвиг линейно меняется и по наклону прямой можно определить частотный сдвиг, а следовательно уровень чипа сигнала S.

При фазовой манипуляции вычисляются только U_0 и Ph_0. А затем составляется результирующий сигнал:

$$U_r = [U_0 * exp\left(i * 2\pi * \frac{S_1}{p^k + 1}\right),$$
$$U_0 * ex\,p\left(i * 2\pi * \frac{S_1 + S_2}{p^k + 1} + i * Ph_0\right), \dots,$$
$$U_0 * ex\,p\left(i * 2\pi * \frac{\sum_{m=1}^{j} S_m}{p^k+1} + i * Ph_0 * (j-1)\right), \dots].$$

При демодуляции каждый отсчет также делится на значение несущей U_0 в этот момент и вычисляется натуральный логарифм. Полученные значения фаз усредняются по N_t отсчетов на чип. Разность фаз между соседними чипами соответствует величине чипа исходного сигнала с точностью до 2π и коэффициента (p^k+1).

Кроме того, к каждому отсчету сигнала на физическом уровне добавляется шум типа АБГШ:

$$U_{nz} = A_{nz} * exp(i * Ph_{nz}),$$

где A_{nz} – случайная амплитуда с нормальным распределением со средним значением 0 и дисперсией 1/SNR, SNR – отношение сигнал/шум, Ph_{nz} – случайная фаза в диапазоне от 0 до 2π.

Также на этапе физического сигнала рассчитывается спектр сигнала и его ширина по уровню –12 дБ.

В результате моделирования получены некоторые зависимости плотности ошибок при передаче данных и плотности ошибок по отдельным чипам. Таким образом можно сравнить поведение канала при обоих видах модуляции (рис. 1 и 2).

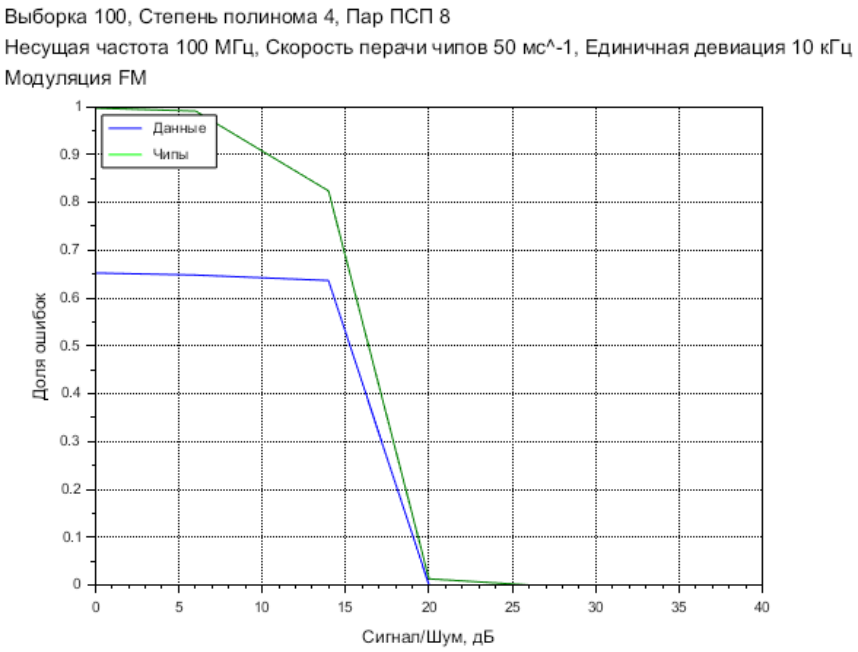


Рис. 1. Чувствительность плотности ошибок к отношению сигнал/шум при ЧМ

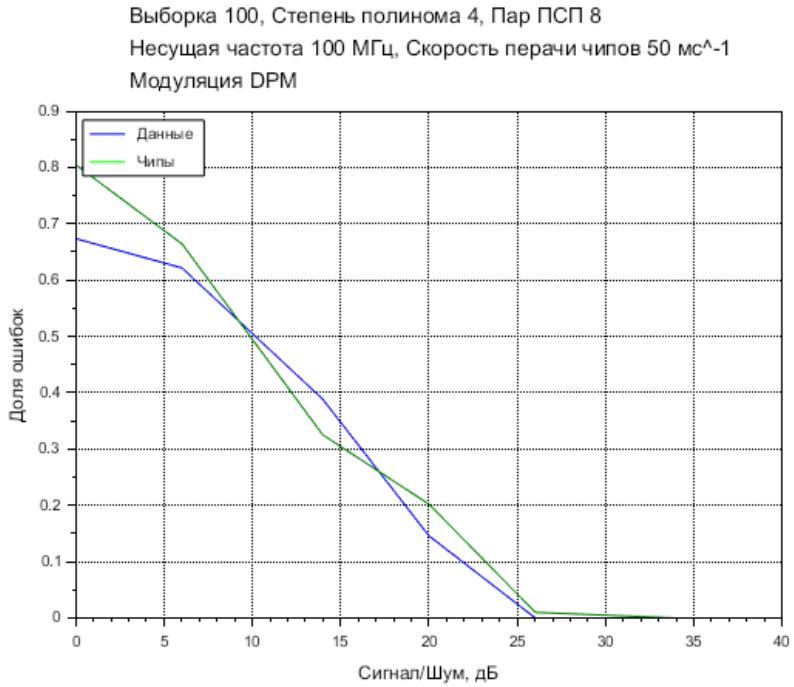


Рис. 2. Чувствительность плотности ошибок к отношению сигнал/шум при ДФМ

Стоит, однако, отметить, что сравнение не совсем корректно из-за наличия у ЧМ дополнительного измерения в виде частотной девиации (рис. 3).

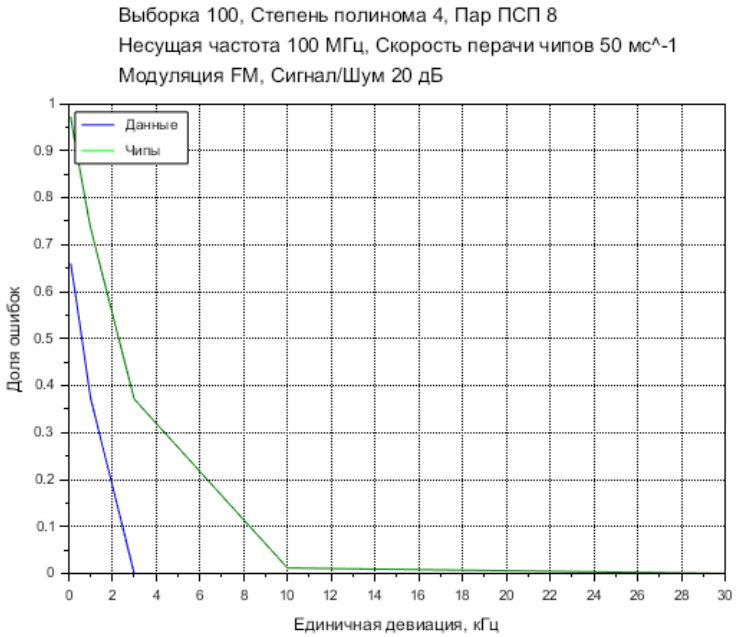


Рис. 3. Чувствительность плотности ошибок к величине единичной девиации при ЧМ

Заключение

В результате моделирования была построена модель, описывающая канал асинхронной передачи данных один ко многим на физическом уровне в присутствие АБГШ. Дальнейшим развитием модели является внедрение эффектов узкополосных помех и многолучевого распространения сигнала.

Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2025-005, "Прикладные научные исследования в области создания и развития систем телеметрии, управления и связи для беспилотных авиационных систем на период до 2030 года с учетом импортозамещения" (регистрационный номер ПТНИ: 1024032900105-1).

Список используемых источников

1. Бобровский В. И., Кукунин Д. С., Книгиницкий Е. И. Моделирование самосинхронизирующейся системы передачи данных; 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. 1. 775 с.

2. Kukunin D., Berezkin A., Kirichek R. Asynchronous Address System Using Code Division Based on Maximum Length Sequences // Proceedings of International Conference on Information, Control, and Communication Technologies (ICCT, Astrakhan, Russian Federation, 03–07 October 2022). IEEE, 2022. DOI:10.1109/ICCT56057.2022.9976772

3. Кукунин Д. С., Березкин А. А., Киричек Р. В., Елисеева К. А. Асинхронная передача данных с использованием многослойных ортогональных структур в системах с кодовым разделением каналов // Электросвязь. 2023. № 1. С. 26–35. DOI:10.34832/ELSV2023.38.1.003. EDN:HNTXND.

4. Кукунин Д. С., Когновицкий О. С., Березкин А. А., Киричек Р. В. Перспективы использования рекуррентных последовательностей в современной телекоммуникационной среде. СПб.: СПбГУТ, 2023. 289 с.

5. Когновицкий О. С. Широкополосные сигналы данных с расширением спектра прямой последовательностью и их характеристика //Труды учебных заведений связи. 2016. Т. 2. № 1. С. 82-89.

BUILDING AN ASYNCHRONOUS BROADBAND DOT-ELLIPSIS CHANNEL

Kniginickii E., Kukunin D.
The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

The article is devoted to the study of the data transmission channel model using the technology of spectrum spreading with maximum length sequences. The model of a one-to-many transmission channel at the physical level is investigated, and various types of carrier modulation are considered.

Key words: *M-sequence, phantom channel, asynchronous transmission*

УДК 621.39
ГРНТИ 47.41

К ВОПРОСУ О СИНХРОНИЗАЦИИ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ И БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ, ОБЪЕДИНЕННЫХ В ЕДИНУЮ СИСТЕМУ (РОЙ)

А. А. Козлов, Н. В. Чикалов

Научно-исследовательский институт «Рубин»

В данной статье приводится анализ проблем, возникающих в сетях связи при отсутствии надежного способа синхронизации, при объединении беспилотных летательных аппаратов и беспилотных транспортных средств в единый рой с общим управлением. Особое внимание уделяется способам решения данных проблем, поиску новых инженерных решений, анализу существующих тенденций.

Работа включает в себя обзорную характеристику проблемы потери сигнала в спутниковых сетях связи, используемых для координации дронов, анализ способов устранения, актуальных на сегодняшний день.

Целью статьи является поиск и исследование путей достижения удовлетворительной точности синхронизации в сетях связи, используемых для координации и управления беспилотниками. Результаты могут быть использованы для разработки и модернизации беспилотных летательных аппаратов и беспилотных транспортных средств нового поколения, способных взаимодействовать как единая система (рой) с подключением минимального количества операторов и высокой степенью автономности.

сигналы синхронизации, беспилотные летательные аппараты, беспилотные транспортные средства, частотная синхронизация.

Введение

В настоящее время одним из самых перспективных направлений разработки являются беспилотные летательные аппараты и беспилотные транспортные средства (БЛА и БТС в дальнейшем). Рынок БЛА, применение которых приходится для задач коммерческого сектора экономики Российской Федерации, растет на более чем 60 % в год. К 2028 году рост достигнет 81 миллиарда рублей [1]. В данный момент активно изучаются способы организации и управления БЛА и БТС в единую систему (рой). Компания L3Harris представила свою новую разработку: Система Amorphus, которая позволяет управлять одному пользователю тысячами различных устройств с помощью интуитивно понятного интерфейса управления. Для того, чтобы

БЛА могли эффективно автономно функционировать, им необходима единая система времени [2].

Основная часть

Существующие решения предлагают получение меток времени с систем спутниковой навигации таких как GPS, ГЛОНАСС, Beidou. В настоящее время данный подход позволяет добиться хороших результатов, однако возникают ситуации, в которых сигнал со спутника теряется и в таком случае точность всей системы способна значительно упасть. К потере сигнала с источника единого времени могут привести: плохая погода, средства радиоэлектронной борьбы, спуфинг (подмена данных, полученных со спутника), поломки антенны и приемника сигнала. Чтобы рой БЛА и БТС мог эффективно автономно функционировать в условиях потери спутникового сигнала, предлагается ввести дополнительное средство поддержки, оснащенное модулем синхронизации. Данное средство способно поддерживать определенную точность единого времени без спутникового сигнала в течении длительного периода. Распространять метку времени предлагается посредством радиоканала.

Данное решение позволит с одного устройства поддерживать синхронизацию времени у всего роя до конца полетного задания или же до возобновления сигнала с системы спутниковой навигации.

В роли средства поддержки может выступать любые БЛА и БТС, несущие на себе прецизионные термостатированные кварцевые генераторы, необходимые для поддержания достаточной точности внутреннего времени, которое, в случае потери сигнала, раздается остальному рою посредством радиоканала.

Подобная модернизация способна существенно повысить точность синхронизации роя БЛА или БТС, точность принятия решений, основанных на едином времени и усилить защиту от воздействия негативных факторов, описанных выше.

В качестве полетного контроллера в различных современных БЛА используются чипы архитектуры ARM от компании STMicroelectronics [3].

Согласно измерениям, представленным ниже на рисунке 1, ошибка временного интервала (ОВИ) внутренних часов микроконтроллера STM32 H743ZI2 превышает 5 с, что говорит о сильной рассинхронизации единого времени при объединении данных устройств в единую систему [4].

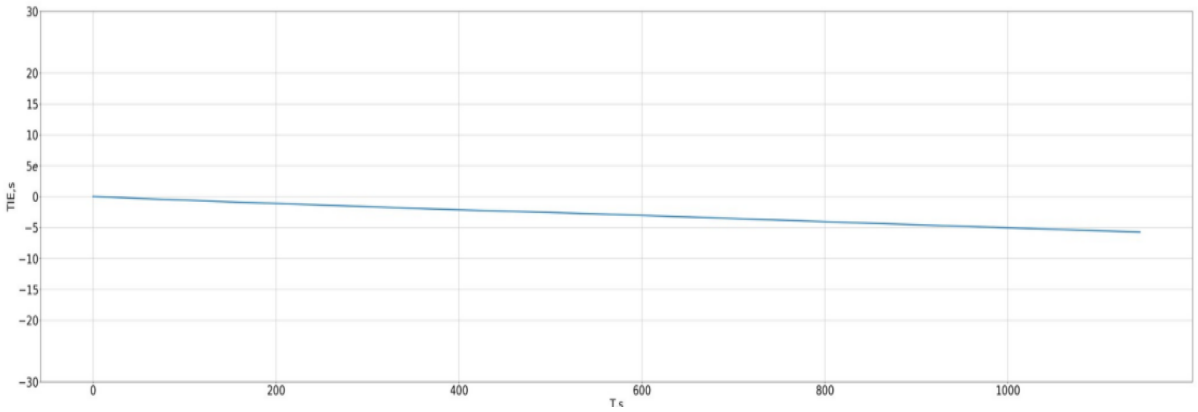


Рис. 1. ОВИ сигнала внутренних часов STM32

Ниже представлен график (рис. 2) ОВИ сигнала метки времени, который был снят с приемника системы ГЛОНАСС. На нем видно, что ОВИ сигнала времени находится в пределах [+200·10-9; -200·10-9].

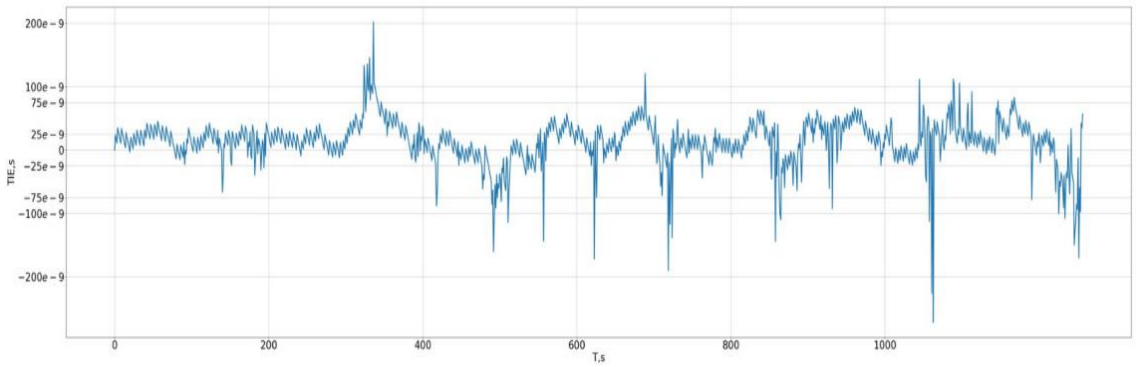


Рис. 2. ОВИ сигнала времени системы ГЛОНАСС

В ходе исследования путей решения проблемы синхронизации БЛА и БТС был разработан и протестирован макет, состоящий из двух полетных контроллеров, которые были соединены посредством радиоканала. Один из них был оснащен системой синхронизации, разработанной для поддержания единого точного времени в условиях потери спутникового сигнала. Структурная схема макета представлена ниже (рис. 3).

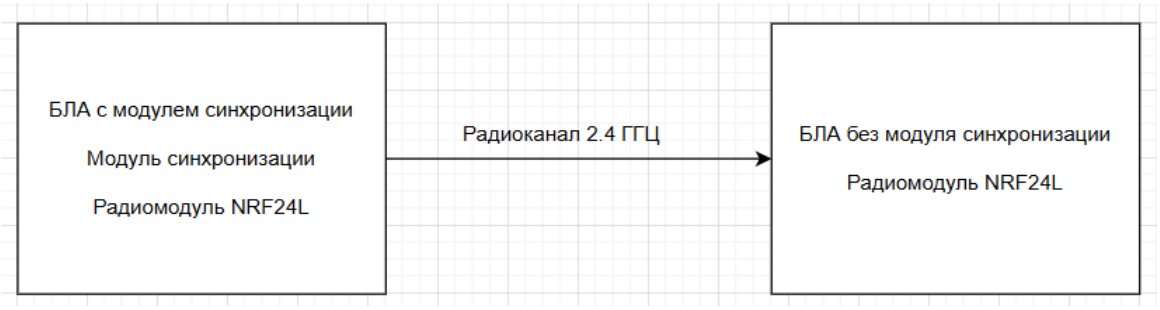


Рис. 3. Структурная схема макета

После создания искусственных условий, при которых получение сигнала со спутниковой навигационной системы стало невозможно, были проведены измерения ОВИ сигнала внутренней метки времени БЛА с модулем синхронизации, который осуществлял подстройку внутреннего времени в течение длительного времени. На графике ниже изображены результаты измерений ОВИ метки времени, которую формирует модуль синхронизации при переходе в режим удержания.

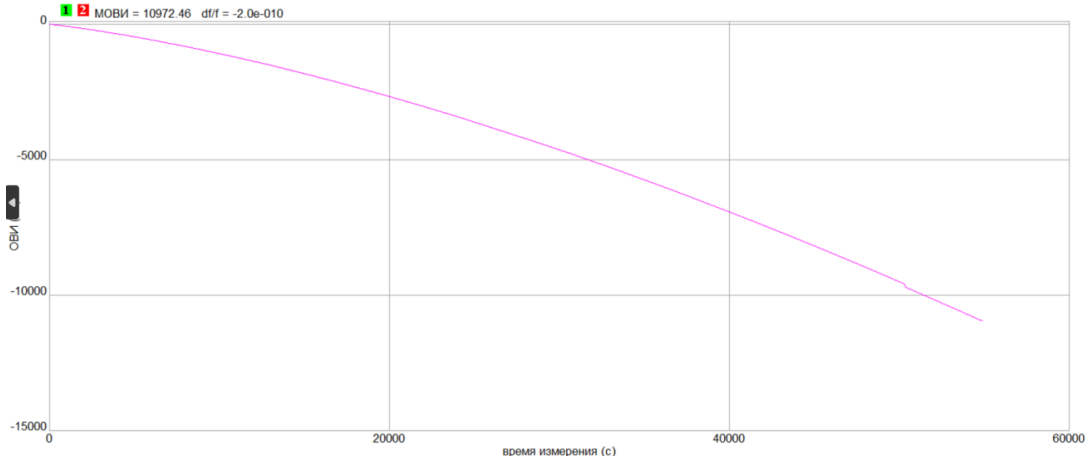


Рис. 4. ОВИ сигнала времени БЛА, оснащенного модулем синхронизации

На графике (рис. 4) ниже представлены измерения ОВИ сигнала времени БЛА без модуля синхронизации, получающего метку времени от устройства, оснащенного предлагаемым модулем. В результате наблюдаемая ОВИ находится в пределах [+15·10-3; -30·10-3].

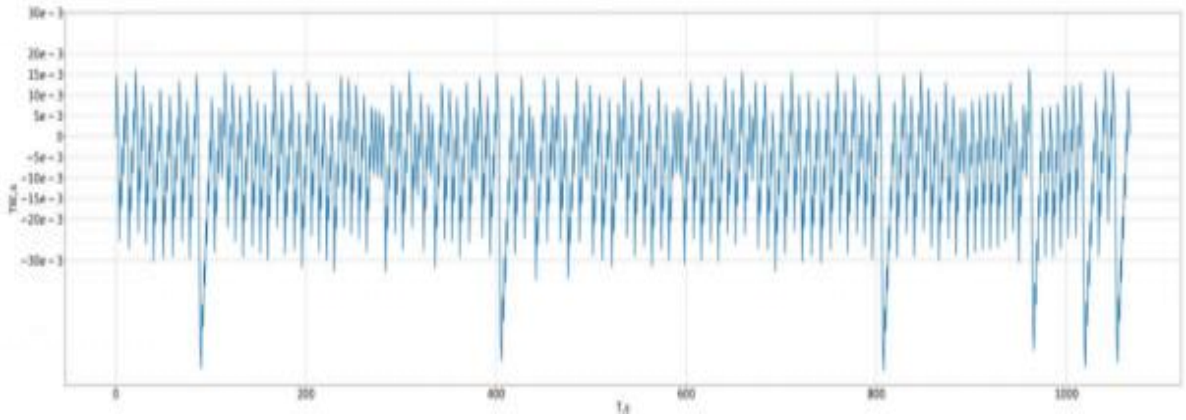


Рис. 5. ОВИ сигнала времени БЛА, подключенного по радиоканалу к устройству с модулем синхронизации

Низкая точность установки метки времени на ведущем устройстве связана с тем, что ведущее устройство программно ведет и корректирует вре-

менную шкалу. При добавлении методов аппаратной обработки метки времени точность возрастет [5].

Выводы

– для улучшения синхронизации БЛА и БТС, объединенных в единую систему, необходимо использовать прецизионные термостатированные кварцевые генераторы на одном или нескольких устройствах для обеспечения возможности раздачи метки времени в условиях отсутствия сигналов от спутниковой группировки;
– наличие модуля синхронизации позволяет БЛА и БТС эффективно автономно выполнять полетное задание в условиях отсутствия спутникового сигнала;
– в роли средства синхронизации могут выступать любые БЛА и БТС, оснащенные модулями синхронизации, и при этом выступать эталоном для всех остальных устройств, объединенных в единую систему, передавая сигнал синхронизации посредством радиоканала.

В рамках настоящей статьи было проведено исследование, посвященное проблеме синхронизации БЛА и БТС, объединенных в один рой устройств. В настоящее время предлагается оснащать несколько устройств в рамках роя модулем синхронизации для повышения эффективности автономного выполнения полетных заданий в условиях отсутствия спутникового сигнала.

Список используемых источников

1. Рынок гражданских беспилотных аппаратов: объем, динамика и сценарии применения беспилотников в отраслях экономики // РосТелеком. URL: https://ai.gov.ru/knowledgebase/tekhnologii-i-produkty-ii/2024_rynok_graghdanskih_bespilotnyh_apparatov_obyem_dinamika_i_scenarii_primeneniya_bespilotnikov_v_otraslyah_ekonomiki_rostelekom/, свободный. (Дата обращения 19.02.2025).

2. Микроконтроллеры полетного контроллера: разновидности и применение // ProfPV. URL: https://profpv.ru/mcu-poletnogo-kontrollera-raznovidnost/ (дата обращения 19.02.2025).

3. Собственный рой беспилотников возможно ли? // Robotrends. URL: https://robotrends.ru/pub/1603/sobstvennyy-roy-bespilotnikov---vozmozhno-li, (дата обращения 19.02.2025).

4. Микроконтроллеры полетного контроллера: разновидности и применение // ProfPV. URL: https://profpv.ru/mcu-poletnogo-kontrollera-raznovidnost/ (дата обращения 19.02.2025).

5. Improved RSA with Enhanced Security on STM32 84MHz // Researcher. URL: https://discovery.researcher.life/article/improved-rsa-with-enhanced-security-on-stm32-

84mhz/78928f8aa8ea3ffb9d359ecf21f91417?utm_source=chatgpt.com (дата обращения 19.02.2025).

6. Бакланов И. Г. Технологии измерений первичной сети. Ч. 2. Системы синхронизации в B-ISDN, ATM. М.: ЭКО-ТРЕНДЗ, 2000. 149 с. Гл. 1.1. С. 6–8.

Статья представлена ученым секретарем диссертационного совета АО "НИИ "РУБИН", кандидатом технических наук, доцентом Ю. В. Саниным

ON THE ISSUE OF SYNCHRONIZATION OF UNMANNED AERIAL VEHICLES AND UNMANNED VEHICLES UNITED INTO A SINGLE SYSTEM (SWARM)

Kozlov A., Chikalov N.
Research Institute "Rubin"

This article provides an analysis of the problems that arise in communication networks in the absence of a reliable synchronization method when unmanned aerial vehicles and unmanned vehicles are combined into a single swarm with common control. Particular attention is paid to ways to solve these problems, search for new engineering solutions, and analysis of existing trends.

The work includes an overview of the problem of signal loss in satellite communication networks used to coordinate drones, an analysis of the methods for eliminating it that are relevant today.

The purpose of the article is to find and study ways to achieve satisfactory synchronization accuracy in communication networks used to coordinate and control drones. The results can be used to develop and modernize new generation unmanned aerial vehicles and unmanned vehicles capable of interacting as a single system (swarm) with the connection of a minimum number of operators and a high degree of autonomy.

Key words: *synchronization signals, unmanned aerial vehicles, unmanned vehicles, frequency synchronization*

УДК 681.5
ГРНТИ 28.23.25

МНОГОУРОВНЕВАЯ СИСТЕМА КАЧЕСТВЕННЫХ ДАННЫХ НА ОСНОВЕ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Д. А. Корнюшкин, А. А. Крылов

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

В эру цифровых технологий высокое качество данных приобретает решающее значение для функционирования и продуктивности автоматизированных систем кибербезопасности, механизмов предотвращения мошенничества и алгоритмов искусственного интеллекта. Применение интегрированных кроссплатформенных систем управления качеством данных, оснащенных системой многоэтапного мониторинга, от фундаментального анализа статистики и базовой верификации достоверности до углубленного выявления отклонений, контроля целостности и синтеза искусственных наборов данных, позволяет обеспечить всестороннюю оценку состояния данных. Всеохватывающий подход к процессу управления качеством включает создание четкой политики действий, внедрение передовых технологических решений, унификацию стандартов обработки, регулярный аудит показателей и повышение квалификации сотрудников. Инвестиционная деятельность в улучшение качества данных приобретает ключевое стратегическое значение ввиду постоянного увеличения объема обрабатываемой информации и роста сложности внешних киберугроз.

многоуровневые системы качественных данных, архитектура кроссплатформенной системы качества данных, искусственный интеллект

В условиях современной цифровой экономики информация стала важнейшим стратегическим активом предприятий, обеспечивающим базу для обоснованного принятия управленческих решений, точного моделирования рыночных тенденций, разработки инноваций и эффективной защиты информационных ресурсов. Однако достоверность конечных выводов в значительной степени зависят от качества первичных данных. Низкое качество данных влечет искажение результатов анализа, снижение производительности автоматизированных систем обработки информации, финансовые потери и ущерб репутации организации. Особую значимость этот аспект приобретает в области информационной безопасности, противодействия мошенничеству и обучения моделей искусственного интеллекта, поскольку именно данные являются фундаментом для идентификации угроз, моделирования пользовательского поведения и автоматизации процессов принятия

решений. Ошибочность или недостоверность данных способна привести к пропуску критически значимых предупреждающих признаков, увеличению частоты ложных срабатываний, снижению доверительности аналитических инструментов и формирования неправильных выводов [2].

Необходимость кроссплатформенных систем качества данных

Обеспечение строгого соблюдения высоких стандартов качества данных требует реализации многоуровневых систем мониторинга, обладающих несколькими уровнями детальной оценки. Общая структура такой системы изображена на рисунке 1, представляющем пятиступенчатую архитектуру, обеспечивающую комплексный контроль качества данных посредством специализированных модулей.

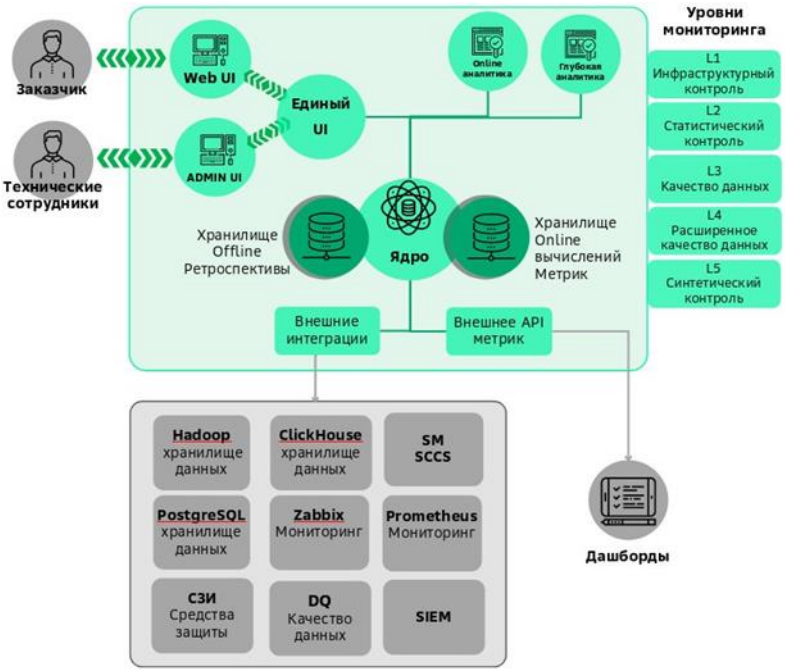


Рис. 1. Архитектура кроссплатформенной системы качества данных

1. Уровень инфраструктурного контроля. На первом уровне, обозначаемом как L1, осуществляется мониторинг состояния аппаратного и программного обеспечения, на котором работает система. Здесь отслеживаются такие параметры, как загрузка процессора, использование оперативной памяти, состояние сети и другие технические показатели [3]. Этот уровень обеспечивает стабильную работу инфраструктуры, предотвращая сбои и выявляя потенциальные проблемы на ранних стадиях.

2. Уровень статистического контроля. Второй уровень, L2, выполняет функции сбора и анализа статистических данных, таких как количество запросов, время отклика, объем обрабатываемых данных и другие метрики, связанные с производительностью системы [4].

3. Уровень качества данных. На третьем уровне, L3, проводится анализ качества данных, которые поступают и обрабатываются системой. На данном уровне особое внимание уделяется аспектам точности, согласованности и актуальности данных. Данный уровень выявляет и устраняет ошибки, обеспечивая тем самым защиту аналитических процессов от некорректных исходных сведений [5].

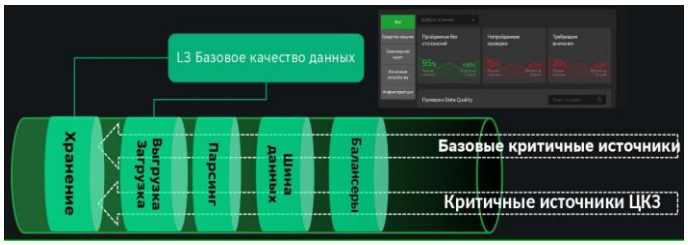


Рис. 2. Блок-схема уровня качества данных

4. Уровень расширенного контроля качества данных. На четвертом уровне, L4, проводится расширенный анализ качества данных с использованием продвинутых методов машинного обучения и алгоритмов [6].

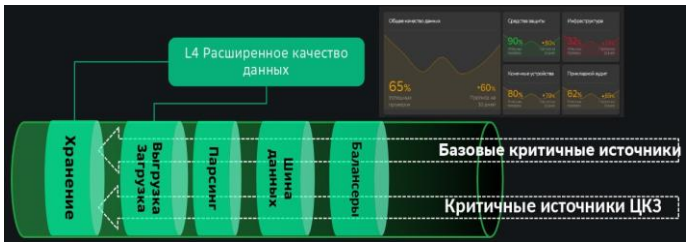


Рис. 3. Блок-схема расширенного контроля данных

5. Уровень синтетического контроля. На пятом уровне, L5, используется синтетические данные для тестирования и оценки системы. Синтетические данные создаются искусственно для проверки работы системы в различных сценариях. Этот уровень позволяет проверять корректность работы систем при различных сценариях [7].

Преимущества кроссплатформенных систем

Кроссплатформенные системы качества данных позволяют решить следующие задачи:

1. Единая платформа для сбора, хранения и обработки данных независимо от формата и типа источника.

2. Автоматизация процесса мониторинга и коррекции данных, снижение влияния человеческого фактора.

3. Возможность интеграции с различными системами корпоративного уровня, включая ERP, CRM и BI-решения.

4. Использование продвинутых методик очистки и нормализации данных, позволяющих выявлять аномалии и устранять дублирование.

5. Поддержка масштабируемости и адаптивность к изменениям структуры данных.

Заключение

Обеспечение соответствия высоким стандартам качества данных представляет собой важную задачу современных информационных систем, решение которой возможно путем реализации многоуровневых систем мониторинга. Предложенная пятиступенчатая архитектура позволяет эффективно контролировать качество данных на различных уровнях детализации, обеспечивая всестороннюю оценку ключевых характеристик данных. Специализированные модули позволяют проводить мониторинг качества данных на разных стадиях их жизненного цикла, выявлять отклонения и оперативно реагировать на изменения условий внешней среды. Предложенный подход обладает рядом преимуществ, среди которых возможность точной настройки критериев оценки качества, высокая степень автоматизации процесса мониторинга и возможность интеграции с существующими информационными системами предприятия. Результаты проведенных исследований подтверждают эффективность предложенной архитектуры и открывают перспективы для дальнейших разработок в области управления качеством данных. В дальнейшем планируется совершенствование предлагаемого подхода за счет расширения функционала модуля мониторинга, увеличения числа поддерживаемых типов данных и повышения производительности всей системы в целом. Дальнейшие исследования позволят создать универсальную платформу для эффективного управления качеством данных, способствующую достижению высоких стандартов качества данных в рамках любых корпоративных IT-инфраструктур.

Список используемых источников

1. Бурый А. С., Погодин И. М. Оценка качества больших данных. Часть 1. Основные понятия и метрики // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 3(78). С. 49–58. / Buryi A. S., Pogodin I. M. Assessment the Quality of Big Data. Part 1. Basic concepts and metrics. Information and Economic Aspects of Standardization and Technical Regulation. 2024; 3 (78): 49–58.

2. Бурый А. С., Погодин И. М. Оценка качества больших данных. Часть 2. Модели данных // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 4(79). С. 24–32. / Buryi A.S., Pogodin I.M. Assessment the Quality of Big Data. Part 2. Data Models. Information and Economic Aspects of Standardization and Technical Regulation. 2024; 4 (79): 24–32.

3. Ватьян А. С., Гусарова Н. Ф., Добренко Н. В. Системы искусственного интеллекта. СПб: Университет ИТМО, 2022. 186 с. URL: 3142.pdf.

4. Лопатин И. Н., Многоуровневые системы качественных данных на основе моделей искусственного интеллекта: проблемы и решения / И. Н. Лопатин // Информационно-экономические аспекты стандартизации и технического регулирования | 1/2025 (82) – Режим доступа: mnogourovnevye-sistemy-kachestvennyh-dannyh-naosnove-modeley-iskusstvennogo-intellekta-problemy-i-resheniya.pdf.

5. Бирачева, Е. А., Семенцова, Н. А., & Сутормин, В. В. (2018). Анализ больших данных и прогнозирование с помощью искусственного интеллекта. Информационные технологии и вычислительные системы, 4(1), 9-15.

6. Аманова А., Гарагулов А., Гурбанов Х. Влияние больших данных (Big Data) на бизнес-процессы // Вестник науки. 2025. № 1(82). Т. 2. С. 34–38.

7. Курочкин А. А., Боженко Е. С., Шевченко Д. А. Вызовы и перспективы применения больших данных в стратегическом управлении // Экономика и управление: проблемы, решения. 2025. Т. 4. № 3. С. 55–61. DOI: 10.36871/ek.up.p.r.2024.03.06.007.

MULTI-LEVEL QUALITATIVE DATA SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE MODELS

Kornyushkin D., Krylov A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In today's digital era, high data quality is critical to the operation and productivity of automated cybersecurity systems, fraud prevention mechanisms and artificial intelligence algorithms. The application of integrated cross-platform data quality management systems equipped with multi-stage monitoring systems, from fundamental statistical analysis and basic validation to in-depth outlier detection, integrity monitoring and synthesis of artificial datasets, provides a comprehensive assessment of data health. An all-encompassing approach to the quality management process includes the creation of clear action policies, implementation of advanced technological solutions, harmonisation of processing standards, regular auditing of indicators and staff development. Investing in data quality is of key strategic importance given the ever-increasing volume of information processed and the growing sophistication of external cyber threats.

***Key words**: multi-level quality data systems, cross-platform data quality system architecture, artificial intelligence*

УДК 681.7.08
ГРНТИ 59.41.71

ОПТИМИЗАЦИЯ КОНСТРУКЦИИ И ТЕХНОЛОГИИ ИЗГОТОВЛЕНИЯ ДАТЧИКОВ НА ОСНОВЕ ИЗГИБОВ ОПТИЧЕСКОГО ВОЛОКНА НА БАЗЕ 3D МОДЕЛИРОВАНИЯ

Е. В. Новиков, А. В. Шваков

Белорусская государственная академия связи

В Белорусской государственной академии разработан ряд методов оценки параметров различных видов физических воздействий, основанных на регистрации эффектов, сопровождающих макро- и микроизгибы оптического волокна. Использование 3D моделирования в этих работах позволяет уже на этапе проектирования проверить функционирование датчиков и облегчает выбор их параметров.

оптическое волокно, макро- и микроизгиб, датчик, 3D модель

Сфера применения информационно-измерительных систем, базирующиеся на волоконной оптике, постоянно расширяется, что обусловлено рядом уникальных свойств, которые присущи основе таких систем – волоконно-оптическим датчикам. Подобные датчики, обеспечивающие контактную или бесконтактную регистрацию изменений регистрируемых физических параметров и передачу сигналов по оптоволоконному каналу связи, благодаря своим высоким метрологическим характеристикам, стабильности и надежности, нечувствительности к электромагнитным полям получили в настоящее время самое широкое распространение в системах мониторинга и удаленного управления [1, 2].

Волоконно-оптические датчики находят все более широкое применение в современных интеллектуальных мониторинговых системах, предполагающих непосредственное встраивание датчиков в конструктивные элементы объектов, а также интеллектуальных распределенных многоточечных измерительных системах, входящих в структуры «Умный дом», «Умный город», «Умный регион».

В рамках выполненных в Белорусской государственной академии связи разработок предложен ряд методов оценки параметров различных видов физических воздействий с использованием регистрации эффектов, сопровождающих макро- и микроизгибы оптического волокна.

При этом перспективные оптические датчики на основе микро- и макроизгибов оптического волокна ориентированы на использование стандартных телекоммуникационных оптических волокон, применяемых в волоконно-оптических линиях связи. Разработаны конструкции целого ряда датчиков физических величин, в том числе волоконно-оптического датчика массы на основе микроизгиба оптического волокна, волоконно-оптического датчика обнаружения проникновения на объект на основе макроизгиба оптического волокна, волоконно-оптического теплового датчика с плавким замком, самовосстанавливающегося теплового датчика на основе макроизгиба оптического волокна, датчика искусственной освещенности на базе оптоволокна [1, 3, 4].

Используемые в ходе исследований опытные образцы датчиков, независимо от их назначения, изготавливаются путем 3D печати с использованием двух типов пластика – полилактидного пластика PLA, сополимера акрилонитрилбутадиенстирольного ABS и полиэтилентерефталатного пластика PET-G. Кроме этого, в отдельных случаях целесообразно применение пластика CARBEX CF, который представляет собой инженерный конструкционный материал на базе ABS пластика, наполненный углеродными волокнами. Благодаря содержанию углеродных волокон и нанотрубок этот пластик не боится ультрафиолета и прямых солнечных лучей, размеростабилен и достаточно устойчив к высоким температурам.

Разработанные 3D модели облегчают выбор параметров датчиков, прежде всего размеров изгибов и обеспечивают проверку соответствия размеров остальных деталей конструкции датчика.

На рис. 1 показана 3D модель базовой конструкции датчиков, использующих эффект формирования макроизгибов волокна. Основными конструктивными элементами этой конструкции являются опорная планка с выемкой и шток, формирующие макроизгиб оптического волокна с заданным радиусом.

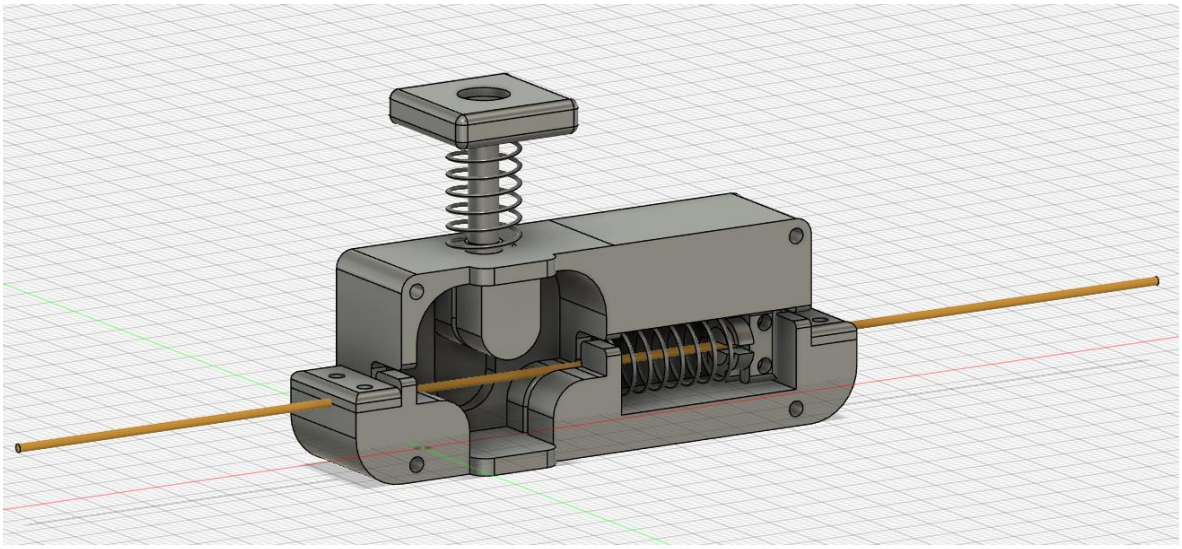


Рис. 1. 3D модель базовой конструкции датчиков, использующих эффект формирования макроизгиба оптического волокна

На рис. 2 показана 3D модель калибровочного датчика, основанного на базовой конструкции и использующего эффект формирования макроизгиба оптического волокна управляющим винтовым механизмом, а на рис. 3 −3D модель несколько более сложного оптоволоконного датчика на основе микроизгибов оптического волокна с внешним фотоприемником для съема покидающего волокно сигнала, установленным на перемещаемой платформе.

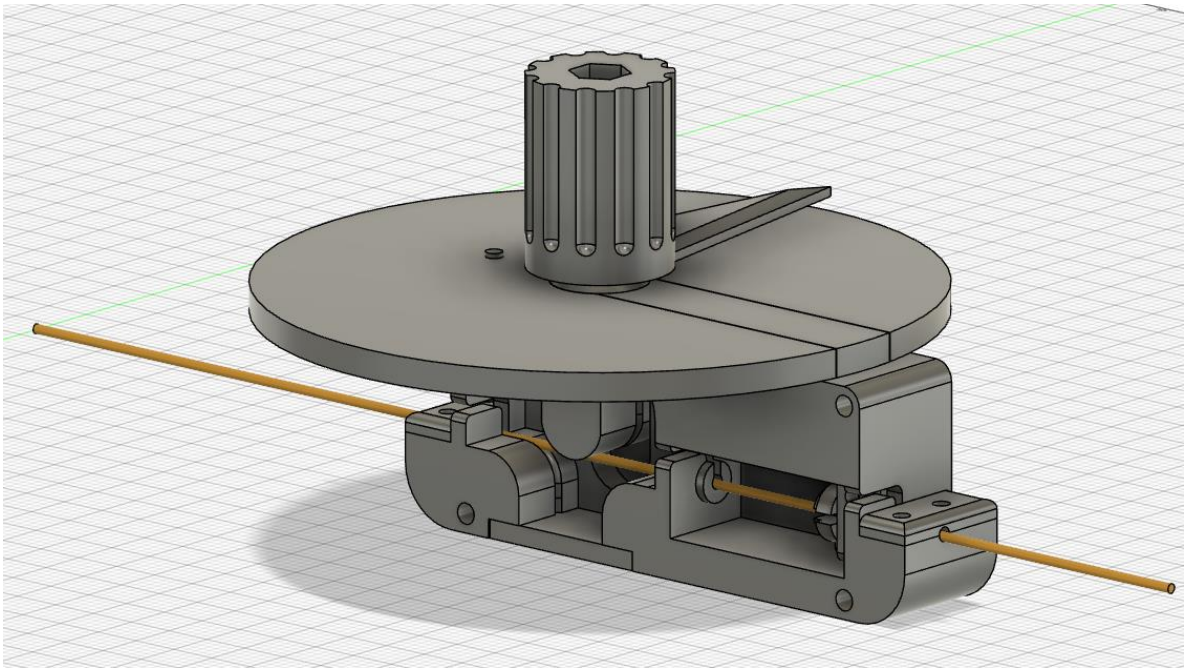


Рис. 2. 3D модель калибровочного датчика на базе макроизгиба оптоволокна с управляющим винтовым механизмом

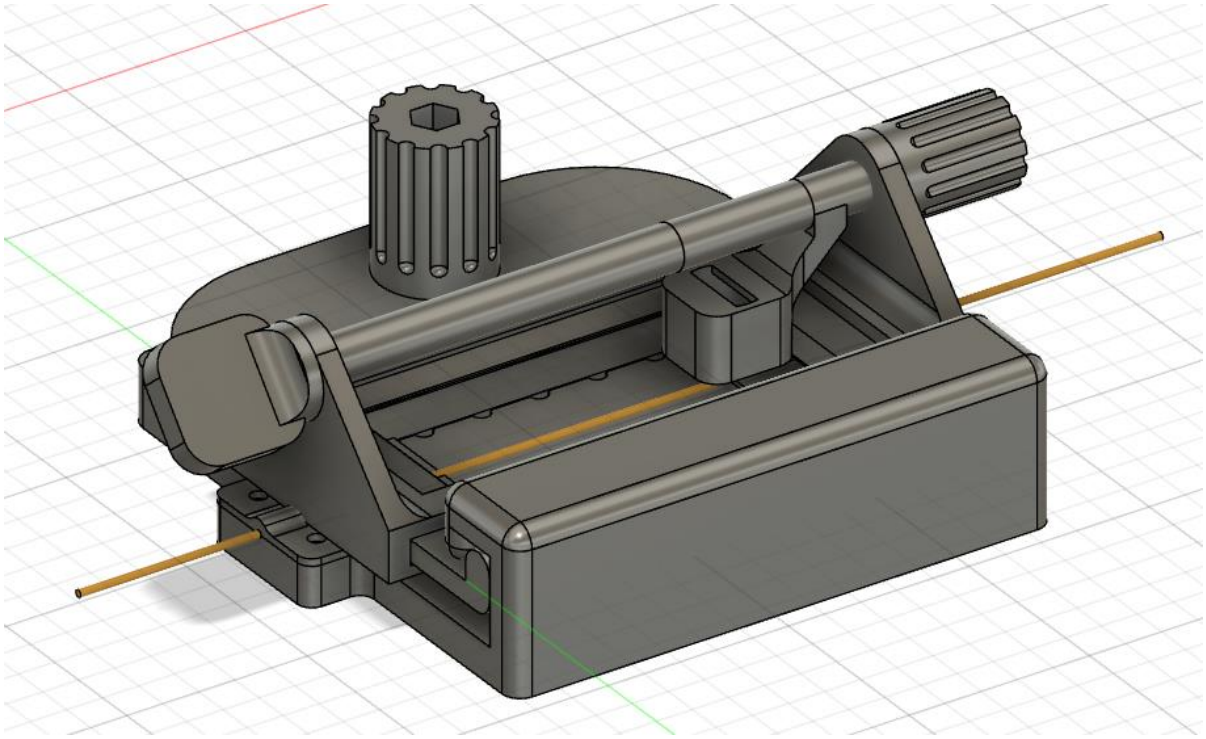


Рис. 3. 3D модель оптоволоконного датчика на основе микроизгиба оптического волокна с внешним фотоприемником для съема покидающего волокно сигнала

Представленная на рис. 2 3D модель позволяет проверить работу управляющего механизма, имеющего специальную шкалу отсчета, градуированную в градусах угла поворота, и оценить величину градуировочных коэффициентов «угол поворота – смещение штока – величина фотоотклика».

Датчик, 3D модель которого показана на рис. 3, реагирует на изменение механического давления, которое воздействует на чувствительные элементы датчика – микроизгибы волокна. При этом изменяется как мощность сигнала, передающегося по волокну за местом расположения микроизгиба, так и мощность сигнала, покидающего волокно, что фиксируется фотоприемником, устанавливаемым на перемещающейся платформе.

В качестве примера на рис. 4 показано визуализированное распределение мощности излучения, выводимого из оптического волокна в зоне микроизгиба, при неравномерном давлении вдоль оптического волокна. Оценка получена на установке, выполненной путем 3D печати на основе модели, показанной на рис. 3.

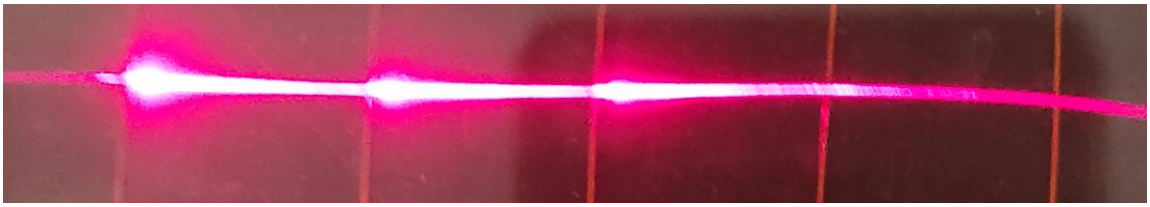


Рис. 4. Визуализация оценки распределения мощности, выводимой из оптического волокна в зоне микроизгиба, при увеличении величины воздействия справа налево

Улучшение параметров разрабатываемых датчиков на основе макро- и микроизгибов оптического волокна, а также совершенствование технологии их опытного производства, связаны с оптимизацией конструкции датчиков.

При этом такая оптимизация должна проводиться и с учетом возможности перевода предлагаемых датчиков из разряда экспериментальных лабораторных образцов в оптимизированные с точки зрения конструкции и технологии изготовления опытно-конструкторские разработки.

Список используемых источников

1. Гулаков И. Р., Зеневич А. О. Волоконно-оптические датчики физических величин: монография. Минск: Белорусская государственная академия связи, 2022. 367 с.

2. Гулаков И. Р., Зеневич А. О. Волоконно-оптические измерительные системы: учебное пособие. Минск: РИВШ, 2023. 372 с.

3. Зеневич А. О., Мансуров Т. М., Новиков Е. В., Лукашик Т. М., Матковская Т. А. Способ диагностики параметров излучения в оптическом волокне при помощи макроизгиба // Неразрушающий контроль и диагностика. 2023. № 3. С. 52–56.

4. Жданович С. В., Зеневич А. О., Коваленко Т. Г., Мансуров Т. М., Новиков Е. В. Оптическое волокно как основа для создания сигнализатора кипения жидкости // Изв. вузов. Приборостроение. 2024. Т. 67. № 7. С. 593–598

OPTIMIZATION OF THE DESIGN AND MANUFACTURING TECHNOLOGY OF SENSORS USING BENDS OF OPTICAL FIBER BASED ON 3D MODELING

Novikov E., Shvakov A.
Belarusian State Academy

The Belarusian State Academy has developed a number of methods for assessing the parameters of various types of physical effects based on recording the effects accompanying macro- and microbending of optical fiber, and the design of a number of physical quantity sensors using these methods. The use of 3D modeling in these works allows already at the design stage to check the functioning of the sensors, optimize the parameters of the developed sensors and the technology of their pilot production.

Key words: *fiber-optic sensor, bending of fiber, design, 3D model*

УДК 654.739
ГРНТИ 49.33.29

ДИПФЕЙКИ НА ИЗОБРАЖЕНИИ: ГЕНЕРАЦИЯ, ОБНАРУЖЕНИЕ И БОРЬБА

А. А. Павловская, М. В. Павловский, С. Л. Фёдоров

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

В статье рассматриваются современные методы генерации дипфейков, включая нейросетевые технологии, а также методы их обнаружения. Кроме того, обсуждаются меры борьбы с угрозой дипфейков, включая технологические решения и повышение осведомленности пользователей. Материал данной статьи демонстрирует, что, несмотря на растущую сложность подделок, комбинированный подход позволяет эффективно противодействовать их распространению.

дипфейки, генеративно-состязательные сети, автоэнкодеры, обнаружение дипфейков, сверточные нейронные сети, физиологические сигналы, биологические маркеры, фотоплетизмография, цифровая аутентификация, медиаграмотность, машинное обучение, искусственный интеллект

Современные технологии искусственного интеллекта, в частности методы глубокого обучения, открыли новые возможности для манипуляции визуальным контентом. Одним из наиболее тревожных проявлений этой тенденции стали дипфейки – реалистичные поддельные изображения и видео, созданные с использованием генеративных нейронных сетей. Проблема дипфейков приобрела особую актуальность в последние годы, поскольку их распространение через социальные сети может наносить ущерб репутации людей, влиять на политические процессы и подрывать доверие к цифровому контенту.

Современные методы генерации дипфейков в основном основаны на двух ключевых архитектурах глубокого обучения: генеративно-состязательных сетях (GAN) и автокодерах. Генеративно-состязательные сети, впервые предложенные Goodfellow и др. [1] в 2014 году, состоят из двух конкурирующих нейронных сетей – генератора, создающего поддельные изображения, и дискриминатора, пытающегося отличить их от реальных. В процессе обучения эти сети совершенствуются, что позволяет создавать высококачественные подделки.

Среди популярных инструментов для создания дипфейков следует отметить FakeApp, DeepFaceLab и Face Swap-GAN. FakeApp использует архитектуру автокодера, где одна и та же кодирующая сеть обучается на двух наборах изображений, а затем декодеры используются для замены лиц. DeepFaceLab предлагает более продвинутый фреймворк для замены лиц, включающий этап преобразования с кодером, декодером назначения и промежуточным слоем между ними. Для выделения лицевых ориентиров в этом инструменте используется алгоритм 2DFAN, а для сегментации лица – сеть TernausNet [2].

Face Swap-GAN представляет собой усовершенствованную версию дипфейков, использующую генеративно-состязательные сети с двумя типами функций потерь: состязательной и перцептивной. Этот подход позволяет создавать выходные изображения с разрешением до 256×256 пикселей с более естественными движениями глаз и меньшим количеством артефактов. Для повышения надежности обнаружения лиц в системе реализована многозадачная сверточная нейронная сеть FaceNet.

Большинство архитектур дипфейков используют ту или иную форму промежуточного представления, чтобы запечатлеть, а иногда и манипулировать структурой лица, позой и выражением лица. Один из способов – использовать систему кодирования действий на лице (FACS) и измерить каждую из таксономизированных единиц действия на лице (AU). Другой способ – использовать монокулярную реконструкцию для получения трехмерной изменяемой модели (3DMM) головы из 2D-изображения, где поза и выражение лица параметризуются набором векторов и матриц. Затем используется редактирование или 3D-рендеринг самой головы. Некоторые используют УФ-карту головы или тела, чтобы сеть могла лучше понять ориентацию фигуры. Другой подход заключается в использовании сегментации изображений, чтобы помочь сети разделить различные понятия (лицо, волосы и т.д.). При замене лиц используется линейная комбинация:

$$I_{result} = \alpha I_{source} + (1-\alpha) I_{target}, \quad (1)$$

где I_{source} – исходное лицо, I_{target} – целевое лицо, α – коэффициент смешивания (0,2-0,5), это позволяет плавно совмещать черты двух лиц при сохранении естественного вида.

Наиболее распространенным представлением являются ориентиры, которые описывают Li Y. и др. [3] (также известные как ключевые точки), ко-

торые представляют собой набор определенных положений на лице или теле, которые можно эффективно отслеживать с помощью библиотек CV с открытым исходным кодом.

Для создания $\boldsymbol{x_g}$, реконструкции и обмена лицами используются некоторые варианты этого процесса, проиллюстрированные на рис. 1.

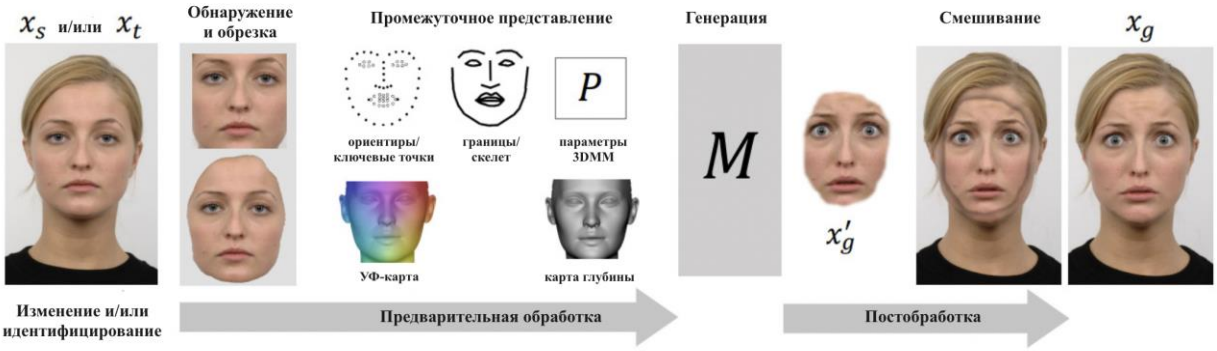


Рис. 1. Конвейер обработки для создания дипфейков с реконструкцией и заменой лиц

Пропускаем $\boldsymbol{x_g}$ через конвейер, который обнаруживает и обрезает лицо, извлекает промежуточные представления, генерирует новое лицо на основе некоторого управляющего сигнала (например, другого лица), а затем смешивает сгенерированное лицо обратно с целевым кадром.

В целом существует шесть подходов к управлению изображением:

– сеть работает непосредственно с изображением, и сама выполняет сопоставление;
– обучение сети ED отличать идентификатор от выражения, а затем изменение /смена местами кодировки целевого значения перед передачей его через декодер;
– добавление дополнительной кодировки (например, AU или встраивание) перед передачей ее в декодер;
– преобразование промежуточного представления лица/тела в желаемую идентичность/выражение перед;
– использование оптического поля из последующих кадров исходного видео для управления генератором;
– создание композиции исходного контента (волосы, сцена и т.д.) с использованием комбинации 3D-рендеринга, искаженного изображения или сгенерированного контента и передача композиции через другую сеть, чтобы повысить реалистичность.

Обнаружение дипфейков представляет собой сложную задачу, требующую комплексного подхода. Современные методы детектирования можно разделить на несколько категорий: анализ изображений, использование физиологических сигналов и исследование биологических маркеров.

Методы анализа изображений часто используют сверточные нейронные сети для выявления артефактов в поддельных изображениях. Например, исследование Wang и др. [4] продемонстрировало, что дилатированные остаточные сети (DRN) могут обнаруживать искажения лиц с точностью до 99,8 % для автоматически сгенерированных подделок и 97,4 % для ручных манипуляций. Другой подход, предложенный Dang и др. [5], использует механизм внимания для улучшения карт признаков в CNN, достигая AUC 100 % и EER менее 1,0 % на собственном наборе данных DFFD.

Физиологические сигналы, такие как паттерны моргания глаз и движения губ, также оказались эффективными для обнаружения дипфейков. Исследование, использующее долгосрочную рекуррентную сверточную нейронную сеть (LRCN) для анализа сигналов моргания глаз, достигло точности 99 %. Аналогично, метод DFT-MF, анализирующий движения рта с помощью CNN, показал точность 98,7 % для видео низкого качества и 73,1 % для высококачественного контента.

Биологические сигналы, такие как фотоплетизмография (PPG), предлагают еще один перспективный подход [6]. Система FakeCatcher анализирует пространственно-временные паттерны биологических сигналов, извлеченных из лицевых областей, демонстрируя точность 91,07 % на наборе данных Deep Fakes и 96 % на FaceForensics. Эти методы основаны на наблюдении, что синтетический контент плохо сохраняет биологические сигналы как в пространственном, так и во временном измерениях.

Несмотря на значительный прогресс в области обнаружения дипфейков, остается множество нерешенных проблем. Одной из основных трудностей является быстрая эволюция методов генерации, что требует постоянного обновления детектирующих алгоритмов. Кроме того, большинство современных методов обнаружения требуют значительных вычислительных ресурсов, что затрудняет их применение в реальном времени, особенно на мобильных устройствах.

Перспективным направлением исследований является разработка методов, сочетающих несколько подходов к обнаружению. Например, комбинация анализа изображений с исследованием физиологических и биологи-

ческих сигналов может повысить надежность детектирования. Также важное значение имеет создание стандартизированных наборов данных для сравнительного анализа различных методов, включая как существующие бенчмарки (FaceForensics++, Celeb-DF, DeepfakeTIMIT), так и новые коллекции, отражающие современные тенденции в генерации дипфейков.

Борьба с дипфейками требует комплексного подхода, включающего технологические, законодательные и образовательные меры. На технологическом уровне необходимо развивать методы цифрового водяного знака и аутентификации контента, которые могли бы обеспечить проверку подлинности изображений и видео. Законодательные инициативы должны быть направлены на регулирование использования технологий глубокой подделки и установление ответственности за их злонамеренное применение.

Особое внимание следует уделить образовательным программам, повышающим медиаграмотность населения. Исследования показывают, что люди без специальной подготовки способны обнаруживать дипфейки лишь с точностью около 53,5 %, что ненамного превышает случайное угадывание. Поэтому важно развивать системы обучения, которые позволят пользователям критически оценивать цифровой контент.

Проблема дипфейков представляет собой серьезный вызов для современного цифрового общества. В то время как технологии генерации продолжают совершенствоваться, создавая все более реалистичные подделки, методы обнаружения также развиваются, предлагая новые подходы к выявлению манипуляций. Успешное противодействие этой угрозе требует совместных усилий исследователей, законодателей и общества в целом. Будущие исследования должны быть направлены на разработку эффективных методов обнаружения, работающих в реальном времени, создание надежных систем аутентификации контента и развитие образовательных программ, повышающих осведомленность пользователей о цифровых угрозах.

Список используемых источников

1. Goodfellow I., Pouget-Abadie J., Mirza M. et al. Generative adversarial nets // Advances in neural information processing systems. 2014. Vol. 27. PP. 2672-2680.

2. Rossler A., Cozzolino D., Verdoliva L. et al. FaceForensics++: Learning to detect manipulated facial images // Proceedings of the IEEE/CVF International Conference on Computer Vision. 2019. PP. 1-11.

3. Li Y., Yang X., Sun P. et al. Celeb-DF: A large-scale challenging dataset for deepfake forensics // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020. PP. 3207-3216.

4. Wang S. Y., Wang O., Zhang R. et al. CNN-generated images are surprisingly easy to spot... for now // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020. P. 8695-8704.

5. Dang H., Liu F., Stehouwer J. et al. On the detection of digital face manipulation // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020. PP. 5781-5790.

6. Afchar D., Nozick V., Yamagishi J., Echizen I. MesoNet: a compact facial video forgery detection network // IEEE International Workshop on Information Forensics and Security (WIFS). 2018. PP. 1-7.

DIPFAKES IN IMAGES:GENERATION, DETECTION, AND COMBAT

Pavlovskaya A., Pavlovsky M., Fedorov S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses modern methods of generating deepfakes, including neural network technologies, as well as methods for detecting them. In addition, measures to combat the threat of deepfakes are discussed, including technological solutions and raising user awareness. The material in this article demonstrates that, despite the growing complexity of fakes, a combined approach can effectively counteract their spread.

Key words: *deepfakes, generative adversarial networks, autoencoders, deepfake detection, convolutional neural networks, physiological signals, biological markers, photoplethysmography, digital authentication, media literacy, machine learning, artificial intelligence*

УДК 654.739
ГРНТИ 49.33.29

УМЕНЬШЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ МОДЕЛЕЙ РАСПОЗНОВАНИЯ ДЕЙСТВИЙ ЧЕЛОВЕКА НА ИЗОБРАЖЕНИИ

А. А. Павловская, М. В. Павловский, С. Л. Фёдоров

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

В статье рассматривается метод снижения вычислительной сложности в задачах распознавания действий человека (HAR) за счет оптимального выбора ключевых кадров и адаптивного кадрирования видео. Метод сочетает детекцию краев, анализ межкадровых различий, пороговую обработку и усредняющие фильтры, что позволяет сократить объем обрабатываемых данных без потери информативности. Эксперименты показали повышение точности распознавания на 3 % по сравнению со случайным выбором кадров, а также ускорение обучения моделей. Подход особенно актуален для приложений реального времени, таких как видеонаблюдение и спортивная аналитика.

распознавание действий человека, ключевые кадры, адаптивное кадрирование

Рост объема видеоданных, генерируемых современными устройствами, создает значительные вычислительные проблемы для систем компьютерного зрения. Особенно это касается задач распознавания действий человека, где требуется обработка временных последовательностей с сохранением семантической согласованности. Традиционные подходы используют случайный выбор кадров или их равномерное прореживание, что приводит к потере важной информации и снижению точности моделей.

Основная сложность обработки видео заключается в избыточности данных – многие последовательные кадры содержат минимальные изменения, не несущие значимой информации о действии. Кроме того, вариативность разрешений исходных видео требует дополнительных операций масштабирования или кадрирования, которые могут негативно влиять на качество распознавания. Существующие решения либо требуют значительных вычислительных ресурсов (например, методы на основе оптического потока), либо не обеспечивают достаточной точности (случайное кадрирование).

В данной статье приводится метод предварительной обработки, который решает обе проблемы: сокращает объем обрабатываемых данных за счет выбора ключевых кадров и одновременно определяет оптимальные об-

ласти кадрирования на основе анализа движения. Метод не требует обучения и может быть интегрирован в существующие конвейеры обработки видео без модификации самих моделей распознавания. Экспериментальные результаты подтверждают эффективность подхода как с точки зрения точности распознавания, так и с точки зрения сокращения вычислительных затрат.

Существующие методы выбора ключевых кадров можно разделить на три основные категории: основанные на пространственно-временных признаках, использующие глубокое обучение и гибридные подходы. Методы первой категории, предложенные Zhenxing et al. [1] и Kyung и Yang [2], используют операторы Лапласа или разности кадров для выделения значимых изменений. Хотя эти методы обладают низкой вычислительной сложностью, они часто не учитывают семантику действий и могут пропускать важные фазы движения.

Подходы на основе глубокого обучения, включая работы Xu et al. [3] и Wu et al. [4], демонстрируют высокую точность, но требуют значительных вычислительных ресурсов для обучения и большого количества размеченных данных. В задачах распознавания действий часто отсутствуют достаточные объемы размеченных данных для эффективного обучения таких моделей. Гибридные методы, предложенные Fasogbon et al. [5], сочетают аппаратные датчики и алгоритмические подходы, но их применение ограничено специфическими сценариями.

Особого внимания заслуживает работа Xiang et al. [6], где ConvNet используется для одновременного анализа пространственных и временных признаков в задачах HAR. Однако этот подход требует значительных вычислительных ресурсов в режиме реального времени. В отличие от существующих решений, предлагаемый метод сочетает низкую вычислительную сложность с сохранением семантической согласованности действий, что делает его особенно подходящим для встраиваемых систем и приложений реального времени.

Архитектура описываемого метода состоит из двух основных этапов: сокращение длины видео за счет выбора ключевых кадров и адаптивное кадрирование выбранных кадров. Первый этап направлен на устранение избыточных кадров с минимальными изменениями, второй – на выделение областей с максимальной информацией о действии. Блок схема метода представлена на рисунке 1.

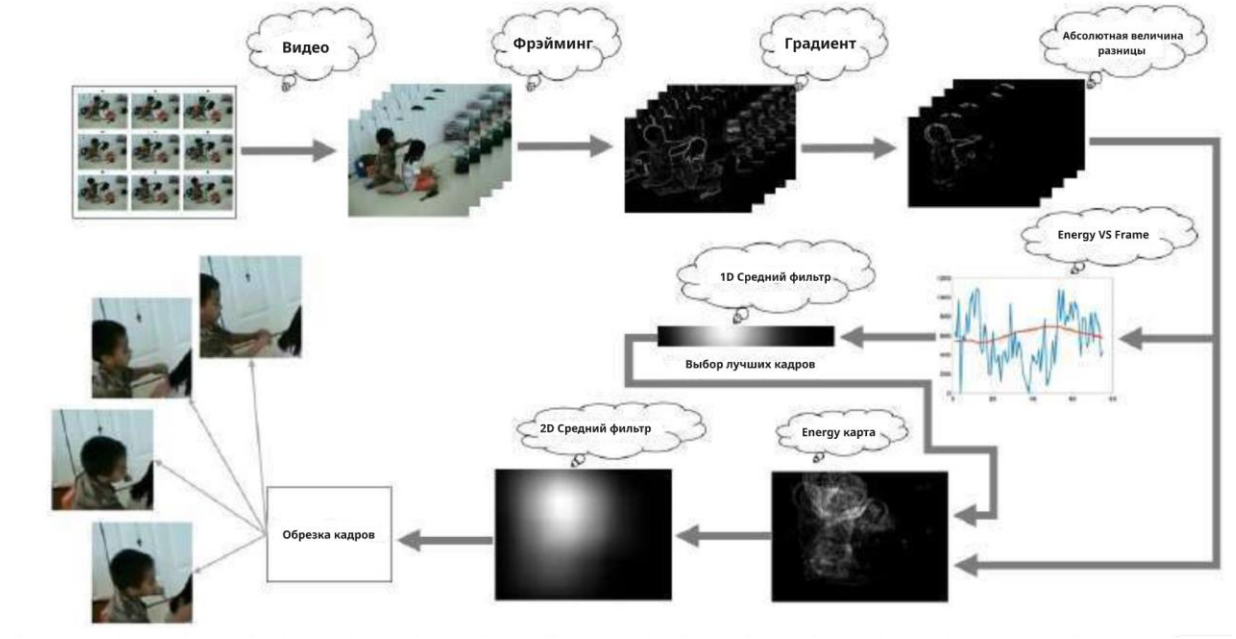
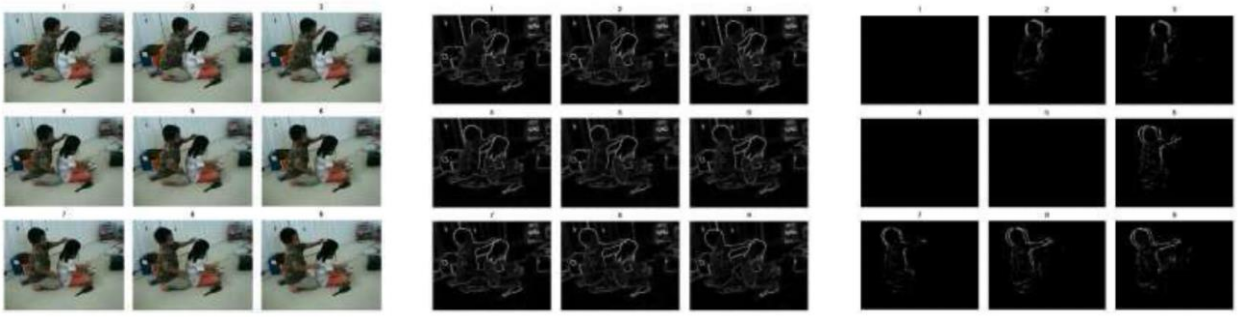


Рис. 1. Блок схема метода

Алгоритм выбора ключевых кадров начинается с разделения входного видео на отдельные кадры и применения оператора градиента для выделения границ. Сравнение различных операторов (Собеля, Прюитта, Робертса) показало, что оператор Собеля обеспечивает наилучший баланс между точностью и вычислительной эффективностью. После вычисления градиентов для каждого кадра определяется абсолютная разница между градиентами последовательных кадров, что позволяет оценить величину изменений. На рисунке 2 два показаны девять различных кадров входного видео, их градиент и абсолютное значение.



а) б) в)

Рис. 2. а): девять последовательных кадров видео; б): градиент каждого кадра; в): абсолютное значение разницы между градиентом каждого кадра и следующего кадра

Для устранения незначительных изменений применяется адаптивное пороговое значение P_tresh, оптимальное значение которого экспериментально установлено как 0.1. Пиксели с разницей градиентов ниже этого порога обнуляются. Затем вычисляется энергия каждого разностного кадра как сумма значений оставшихся пикселей. Кадры с энергией ниже порога E_M исключаются из дальнейшего анализа.

Заключительный шаг выбора ключевых кадров заключается в нахождении последовательности заданной длины N_frames с максимальной суммарной энергией с использованием скользящего окна. Эта последовательность содержит наиболее информативные кадры с точки зрения изменения границ, что коррелирует с фазами выполнения действия.

Этап адаптивного кадрирования начинается с построения карты энергии для выбранных ключевых кадров. Карта энергии создается путем суммирования разностных кадров, полученных на предыдущем этапе. Затем к карте энергии применяется усредняющий фильтр с размером окна, соответствующим требуемым размерам входных данных модели распознавания. Область кадрирования выбирается вокруг пикселя с максимальным значением на отфильтрованной карте энергии, что гарантирует включение наиболее информативных областей движения.

Для оценки эффективности метода были проведены эксперименты на стандартных наборах данных UCF101 (13,320 видео, 101 действие) и HMDB51 (6,766 видео, 51 действие). В качестве базовых моделей использовались современные архитектуры распознавания действий: Two-Stream I3D, Motion Guided Network, Spatiotemporal network и Correlation net. Все эксперименты проводились на системе с процессором Intel i7 9700, 16 ГБ оперативной памяти и видеокартой Nvidia RTX 2070 Super с использованием MATLAB 2020.

Сравнение различных операторов градиента показало, что оператор Собеля обеспечивает наилучшие результаты как на наборе UCF101 (увеличение точности до 2.7 % для Correlation net), так и на HMDB51 (улучшение на 5.1 % для Motion Guided Network). Анализ влияния порогового значения P_tresh подтвердил оптимальность значения 0.1, при котором достигается баланс между сохранением информативных кадров и отсеиванием избыточных данных.

Результаты применения метода предварительной обработки показали устойчивое улучшение точности всех тестируемых моделей. Наибольший

прирост точности на тестовых данных наблюдался для Motion Guided Network – 2.3 % на UCF101 и 2.3 % на HMDB51. Кроме того, было рассчитано относительное изменение времени обучения:

$$Relative_{Runtime} = \frac{HAR \text{ время обучения предложенного метода}}{HAR \text{ время обучения без предложенного метода}} \quad (1)$$

Важно отметить, что улучшение точности сопровождалось сокращением времени обучения в среднем на 6-8 % для большинства моделей, за исключением Correlation net на UCF101, где наблюдалось незначительное увеличение времени на 2 %.

Особый интерес представляют результаты на наборе HMDB51, который содержит более сложные и вариативные действия по сравнению с UCF101. Здесь метод продемонстрировал особенно значительное улучшение точности (до 7.05 % на обучающей выборке для Motion Guided Network), что свидетельствует о его эффективности в сложных сценариях с высокой степенью вариативности действий.

Данный метод демонстрирует несколько ключевых преимуществ по сравнению с существующими подходами. Во-первых, использование оператора градиента и разности кадров обеспечивает значительно меньшую вычислительную сложность по сравнению с методами, основанными на оптическом потоке или глубоком обучении. Во-вторых, иерархическая структура метода позволяет независимо оптимизировать параметры для конкретных задач и аппаратных платформ.

Важным аспектом является возможность генерации дополнительных обучающих данных без потери семантической согласованности. Выбирая различные временные интервалы вокруг оптимальной последовательности и варьируя области кадрирования вблизи максимума карты энергии, можно создать до 800 вариантов для каждого исходного видео, что особенно ценно при ограниченном объеме обучающих данных.

Ограничением метода является зависимость от четкости границ в исходном видео. В условиях низкого качества изображения или слабой контрастности эффективность метода может снижаться. Кроме того, метод ориентирован на действия, характеризующиеся явными движениями, и может быть менее эффективен для распознавания статических поз или мелких жестов.

Перспективным направлением развития метода является интеграция с семантической сегментацией человеческого тела, что позволит более точно

выделять релевантные области при наличии множества движущихся объектов в сцене. Также представляет интерес адаптация метода для работы с трехмерными данными, такими как видео с глубиной (RGB-D), где информация о глубине может существенно улучшить оценку значимости различных областей кадра.

В данной статье представлен эффективный метод предварительной обработки видео для систем распознавания действий человека, позволяющий сократить вычислительную сложность без потери точности. Метод основан на комбинации алгоритмов выделения границ, анализа разности кадров и адаптивного кадрирования, что обеспечивает его применимость в системах с ограниченными вычислительными ресурсами.

Экспериментальные результаты подтвердили, что метод позволяет увеличить точность распознавания на стандартных наборах данных при одновременном сокращении времени обучения моделей. Универсальность метода позволяет интегрировать его в существующие конвейеры обработки видео без модификации самих моделей распознавания.

Список используемых источников

1. Zhenxing Z., Li D., Wang L. Распознавание гонконгского языка жестов с использованием глубокого обучения и выбора ключевых кадров на основе оператора Лапласа [Hong Kong sign language recognition using deep learning with Laplacian operator-based keyframe selection] // Журнал визуальной коммуникации и представления изображений. 2020. Т. 71. С. 102731.

2. Kyung S., Yang H. Выбор ключевых кадров в системах отслеживания RGB-D видео с использованием комбинации разности кадров и признаков глубины [Keyframe selection in RGB-D video tracking systems using combined frame difference and depth features] // Труды IEEE по мультимедиа. 2019. Т. 21. № 5. С. 1234-1246.

3. Xu J., Wang H., Zhang Y. Извлечение ключевых кадров на основе автоэнкодера для создания миниатюр видео [Autoencoder-based keyframe extraction for video thumbnailing] // Доступ IEEE. 2020. Т. 8. С. 109869-109880.

4. Wu C., Zhang J., Saito K. Динамический выбор кадров для распознавания видео с использованием сетей LSTM [Dynamic frame selection for video recognition using LSTM networks] // Письма о распознавании образов. 2021. Т. 145. С. 1-7.

5. Fasogbon P., Lakaniemi A., Holm S. Выбор ключевых кадров с помощью IMU для генерации карт глубины на мобильных устройствах [IMU-assisted keyframe selection for depth map generation in mobile devices] // Датчики. 2021. Т. 21. № 3. С. 856.

6. Xiang T., Chen Z., Liu Y. Пространственно-временная сверточная сеть для распознавания действий человека с оптимизацией ключевых кадров [Spatio-temporal ConvNet for human action recognition with keyframe optimization] // Труды IEEE по схемам и системам для видеотехнологий. 2022. Т. 32. № 4. С. 2152-2165.

REDUCING THE COMPUTATIONAL COMPLEXITY OF MODELS FOR RECOGNIZING HUMAN ACTIONS IN IMAGES

Pavlovsky M., Pavlovskaya A., Fedorov S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article proposes a method for reducing computational complexity in human action recognition (HAR) tasks by optimally selecting key frames and adaptively cropping video. The method combines edge detection, interframe difference analysis, threshold processing, and averaging filters, which allows reducing the amount of processed data without losing information. Experiments showed a 3 % increase in recognition accuracy compared to random frame selection, as well as faster model training. The approach is particularly relevant for real-time applications such as video surveillance and sports analytics.

Key words: *Human action recognition, key frames, adaptive framing*

УДК 621.39
ГРНТИ 49.33.29

АНАЛИЗ ПРОБЛЕМ МАСШТАБИРУЕМОСТИ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ И СТРАТЕГИИ ИХ РЕШЕНИЯ

А. И. Парамонов, Ф. Н. Хоанг

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

Интернет вещей (ИВ) представляет собой стремительно развивающуюся парадигму, соединяющую миллиарды физических устройств через Интернет. Этот экспоненциальный рост порождает беспрецедентные проблемы масштабируемости, которые становятся критическим барьером для дальнейшего внедрения и надежной эксплуатации ИВ систем. Масштабируемость, как способность системы адаптироваться к изменяющимся нагрузкам и требованиям, является ключевой характеристикой, определяющей эффективность и жизнеспособность сетей Интернета вещей. В данной работе проводится систематический анализ основных проблем масштабируемости, охватывающих управление данными, сетевую инфраструктуру и безопасность. На основе анализа существующей литературы предлагаются и оцениваются стратегические подходы к их решению, включая децентрализованные вычисления, современные архитектурные паттерны и комплексные механизмы обеспечения безопасности. Цель статьи − предоставить структурированный обзор, который поможет исследователям и инженерам в разработке устойчивых и эффективно масштабируемых ИВ решений.

интернет вещей, масштабируемость, периферийные вычисления, сетевая перегрузка, большие данные, микросервисная архитектура, кибербезопасность.

Масштабируемость системы – это ее способность эффективно справляться с растущим объемом работы и адаптироваться к будущим изменениям без деградации производительности или необходимости полной перестройки архитектуры. Отсутствие должного внимания к этому аспекту может привести к отказам системы, увеличению задержек и неприемлемому потреблению ресурсов, что подрывает саму ценность ИВ приложений [1−3].

В контексте ИВ масштабируемость традиционно рассматривается в двух измерениях:

1. Вертикальное масштабирование (масштабирование вверх): Увеличение мощности существующих ресурсов путем добавления вычислительной мощности к одному узлу. Этот подход прост в реализации, но имеет ограничения по предельной мощности и более высокую стоимость.

2. Горизонтальное масштабирование (масштабирование вширь): Увеличение мощности путем добавления новых узлов (серверов) в систему, которые работают как единое целое для распределения нагрузки. Этот подход более гибок и предпочтителен для крупномасштабных распределенных систем.

В данной статье последовательно рассматриваются фундаментальные проблемы масштабируемости в ИВ, анализируются современные технологические стратегии для их решения и определяются ключевые направления для будущих исследований.

1. Основные проблемы масштабируемости в сетях ИВ

1.1. Управление огромными объемами данных

Триллионы подключенных устройств непрерывно генерируют данные, что создает фундаментальные проблемы для их сбора, хранения и обработки. Во-первых, централизованное хранение таких объемов данных становится экономически невыгодным и сложным в управлении. Во-вторых, передача всего потока необработанных данных в облако вызывает перегрузку сетевых каналов и приводит к значительным задержкам, что недопустимо для приложений реального времени (например, в промышленной автоматизации или автономном транспорте). В-третьих, обеспечение качества и согласованности данных в распределенной системе огромного размера становится нетривиальной задачей. Бизнес-логика, зависящая от этих данных, может давать сбои, если система не способна справиться с их объемом.

1.2. Перегрузка сетевой инфраструктуры и гетерогенность

Сетевая инфраструктура является «кровеносной системой» для ИВ, и ее ограничения напрямую влияют на масштабируемость. С увеличением плотности устройств в сети возрастает вероятность коллизий и взаимных помех, что снижает надежность связи. Пропускная способность сетей, особенно беспроводных (например, сотовых или Wi-Fi), является ограниченным ресурсом.

Ключевой проблемой является гетерогенность сетей и протоколов. В экосистеме ИВ одновременно существуют устройства, использующие различные технологии связи (например, Wi-Fi, Bluetooth, Zigbee, LoRaWAN) с разными операционными системами и стандартами. Обеспечение их бесшовного взаимодействия (интероперабельности) и централизованного управления в масштабе является сложнейшей инженерной задачей. Кроме

того, обеспечение безопасности на сетевом уровне требует внедрения новых криптографических протоколов, способных работать на устройствах с ограниченными ресурсами без ущерба для производительности.

1.3. Администрирование и жизненный цикл устройств

Управление жизненным циклом миллиардов устройств − от первоначальной настройки до вывода из эксплуатации − невозможно осуществлять вручную. Каждое устройство нуждается в уникальной идентификации, безопасной аутентификации и авторизации для доступа к ресурсам. Процессы первоначальной настройки, обновления программного обеспечения и конфигурации безопасности должны быть полностью автоматизированы. Устройства, которые были утеряны, украдены или скомпрометированы, должны быть немедленно изолированы от сети, чтобы предотвратить угрозы безопасности. Без автоматизированных механизмов управления администрирование крупномасштабной сети ИВ становится невыполнимой задачей.

2. Стратегические подходы к обеспечению масштабируемости

2.1. Децентрализация обработки: Периферийные вычисления

Вместо отправки всех данных в централизованное облако, концепция периферийных вычислений предлагает обрабатывать данные как можно ближе к их источнику − на самих устройствах или на локальных шлюзах. Этот подход напрямую решает проблему перегрузки сети и задержек. Данные фильтруются, агрегируются и анализируются локально, и в облако отправляется только значимая информация или результаты анализа. Такая архитектура позволяет создавать приложения реального времени, снижает затраты на передачу данных и повышает общую отказоустойчивость системы, так как локальные сегменты сети могут продолжать функционировать даже при потере связи с центральным сервером. Управление конвейером данных становится критически важным для эффективного распределения нагрузки между периферией и облаком.

2.2. Гибкая архитектура на основе микросервисов

Монолитные приложения, где вся логика тесно связана в одном модуле, плохо масштабируются. Современным подходом является микросервисная архитектура, при которой сложное приложение разбивается на набор небольших, независимых и слабосвязанных (микросервисов). Каждая служба отвечает за определенную бизнес-функцию (например, аутентифи-

кация, обработка данных с датчиков, управление пользователями) и может быть развернута, обновлена и масштабирована независимо от других.

Такой подход идеально соответствует требованиям горизонтального масштабирования. Если одна из служб (например, обработка видеопотока) испытывает высокую нагрузку, можно увеличить количество только ее экземпляров, не затрагивая остальную систему. Это также повышает отказоустойчивость: сбой в одном микросервисе не приводит к отказу всей системы, как это происходит в монолитной архитектуре. Кроме того, разные микросервисы могут использовать разные технологии хранения данных, наиболее подходящие для их конкретных задач, что повышает общую эффективность.

2.3. Автоматизация управления жизненным циклом устройств

Для решения проблемы администрирования гетерогенных устройств в большом масштабе необходимы платформы с высокой степенью автоматизации.

Автоматизированная начальная загрузка позволяет устройствам самостоятельно подключаться к сети, проходить аутентификацию и получать необходимую конфигурацию при первом включении без участия человека. Централизованные системы управления должны обеспечивать удаленное обновление программного обеспечения «по воздуху», мониторинг состояния устройств и применение политик безопасности в автоматическом режиме. Это не только снижает операционные расходы, но и позволяет оперативно устранять уязвимости в масштабах всей сети.

3. Обеспечение безопасности и надежности в масштабе

Масштабируемость не может рассматриваться в отрыве от требований безопасности и надежности. С увеличением числа устройств экспоненциально растет и поверхность атаки.

3.1. Комплексная безопасность и управление доступом

Безопасность в масштабируемых системах ИВ должна быть многоуровневой.

Управление идентификацией: каждое устройство и пользователь должны иметь уникальный цифровой идентификатор. Система должна обеспечивать строгую аутентификацию, чтобы только авторизованные субъекты могли получить доступ к данным и ресурсам. Попытки несанкционированного доступа должны немедленно блокироваться.

Конфиденциальность данных: сбор огромных массивов персональных или конфиденциальных данных требует внедрения надежных механизмов защиты. Сквозное шифрование от устройства до конечного приложения является обязательным требованием для предотвращения перехвата и компрометации данных.

Управление доступом: необходимо внедрять гибкие политики контроля доступа, которые определяют, какие действия разрешены для каждого пользователя или устройства. Например, администратор системы должен иметь более широкие права, чем обычный пользователь.

3.2. Отказоустойчивость и доверие

В крупномасштабной системе сбои отдельных компонентов (датчиков, шлюзов, серверов) являются не исключением, а штатной ситуацией. Архитектура системы должна быть спроектирована с учетом этого.

Отказоустойчивость достигается за счет избыточности критически важных компонентов и механизмов автоматического переключения на резервные узлы в случае сбоя. Децентрализованные архитектуры, такие как периферийные вычисления и ячеистые сети, по своей природе более устойчивы к сбоям, чем централизованные.

Доверие является фундаментальным аспектом для принятия технологии пользователями. Система должна быть предсказуемой и надежной. Для этого необходимы механизмы управления доверием, которые обеспечивают целостность данных и гарантируют, что взаимодействие между устройствами и службами происходит в соответствии с установленными правилами и политиками. Если пользователи не доверяют системе, они не будут ею пользоваться, что сведет на нет все технологические достижения.

Заключение

Проблема масштабируемости является главным комплексным вызовом для полномасштабного развертывания сетей Интернета вещей, затрагивая управление данными, сетевую инфраструктуру и безопасность. Эффективное решение требует перехода от централизованных монолитных систем к распределенным и гибким архитектурам.

Ключевыми стратегиями для достижения этой цели являются децентрализация обработки данных с помощью периферийных вычислений, применение микросервисной архитектуры для повышения гибкости и отказоустойчивости, а также полная автоматизация жизненного цикла устройств. Фундаментом для этих технологических решений должна

служить всеобъемлющая модель безопасности, обеспечивающая идентификацию, конфиденциальность и доверие в системе.

Успешная интеграция этих подходов позволит создавать надежные, безопасные и эффективные системы ИВ, способные обслуживать миллиарды устройств и поддерживать цифровую трансформацию экономики.

Список используемых источников

1. Кучерявый А. Е., Киричек Р. В., Маколкина М. А., Парамонов А. И., Дунайцев Р. А., Пирмагомедов Р. Я., Бородин А. С., Владыко А. Г., Мутханна А. С. А., Выборнова А. И., Владимиров С. С., Гришин И. В. Новые перспективы научных исследований в области сетей связи на 2021–2024 годы // Информационные технологии и телекоммуникации. 2020. Т. 8. № 3. С. 1–19.

2. Кучерявый А. Е. Триллионные сети // Телекоммуникации. 2013. № S7. С. 19–22. EDN:REKFXF

3. Кучерявый А. Е., Окунева Д. В., Парамонов А. И., Хоанг Ф. Н. Методы распределения трафика в гетерогенной сети Интернета вещей высокой плотности. Труды учебных заведений связи. 2024. Т. 10. № 2. С. 67-74. https://doi.org/10.31854/1813-324X-2024-10-2-67-74. EDN:RTNVEU

SCALABILITY CHALLENGES AND SOLUTIONS IN MASSIVE IOT NETWORKS

Paramonov A., Hoang F.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The rapid proliferation of Internet of Things (IoT) devices has led to unprecedented scalability challenges in managing massive IoT networks. As the number of connected devices continues to grow exponentially, ensuring seamless data transmission, maintaining network performance, and guaranteeing security have become critical concerns. This paper explores the primary scalability challenges associated with massive IoT networks, including data management, network congestion, and security vulnerabilities. By reviewing current literature and analyzing case studies, we identify and evaluate various solutions designed to address these challenges. Key approaches such as edge computing, advanced network protocols, and machine learning techniques are examined for their effectiveness in enhancing scalability and performance. Our findings suggest that a combination of these technologies, alongside robust security frameworks and adaptive resource management strategies, can significantly mitigate the scalability issues faced by massive IoT deployments. The paper concludes with recommendations for future research directions and practical implementations to ensure the sustainable growth of IoT networks.

Key words: *IoT scalability, edge computing, network congestion, data management, security vulnerabilities*

УДК 621.39
ГРНТИ 49.33.29

МОДЕЛЬ ГЕТЕРОГЕННОГО ИНТЕРНЕТА ВЕЩЕЙ: АРХИТЕКТУРА, КЛЮЧЕВЫЕ ТЕХНОЛОГИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

А. И. Парамонов, Ф. Н. Хоанг

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

Гетерогенный Интернет вещей объединяет разнообразные сети и каналы связи (беспроводные сенсоры, Wi-Fi, LPWAN, 4G/5G, оптика, акустика и др.), расширяя возможности приложений в умных домах, городах и промышленности. В статье предложена теоретическая четырехуровневая архитектура HetIoT (сенсорный, сетевой, облачный и прикладной уровни) и показана роль ключевых коммуникационных технологий. Обсуждаются главные проблемы – совместимость протоколов, маршрутизация, безопасность и энергоэффективность – а также перспективы: самоконфигурируемые сети, SDN, беспроводная передача энергии и интеллектуальная маршрутизация. Модель и обзор литературы позволяют оценить потенциал и ограничения HetIoT и наметить направления дальнейших исследований.

гетерогенные сети, Интернет вещей, канал связи, технологии IoT

Концепция гетерогенного Интернета вещей предполагает интеграцию множества сетей и устройств (WSN, Wi-Fi, 3G/4G/5G, mesh, автомобильные сети, RF, оптика, акустика и др.) для расширения функциональности систем передачи данных [1]. Уже сегодня гетерогенный Интернет вещей (HetIoT) применяется в умных домах, транспорте, экомониторинге, безопасности и промышленной автоматизации, а число подключенных устройств стремительно приближается к сотням миллиардов [2]. Одновременно многопротокольная среда усложняет маршрутизацию, взаимодействие и защиту данных [3]. В статье предложена четырехуровневая теоретическая архитектура HetIoT и проанализированы ключевые технологии и возникающие при этом проблемы.

Архитектура гетерогенных сетей Интернета вещей

Для описания гетерогенной IoT-системы используется четырехуровневая архитектура, объединяющая сенсоры, сеть, облачные вычисления и прикладные приложения (рис. 1). Такая архитектура позволяет разделить систему на функциональные слои и упростить взаимодействие между ними.

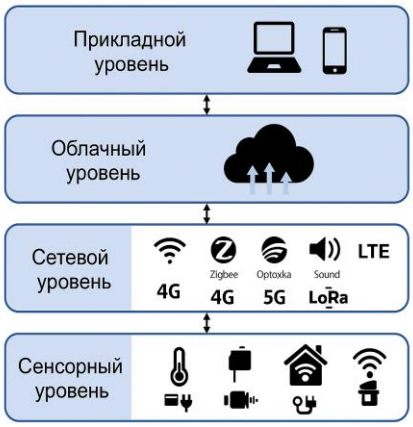


Рис. 1. Четырехуровневая архитектура гетерогенного Интернета вещей

1. Сенсорный слой

В сенсорном (датчиковом) слое располагаются многочисленные датчики различного типа, обеспечивающие сбор информации из физической среды. Это могут быть датчики температуры, влажности, давления, освещенности, движения, а также видеокамеры, микрофоны и др. Собранные сенсоры передают данные на вышележащие уровни для анализа и принятия решений. Нейроноподобная многопрыжковая сеть датчиков позволяет покрыть большие площади и обеспечить надежность: данные могут передаваться по нескольким путям до узлов-стоков (концентраторов), а оттуда – в сеть. В такой сети выделяют узлы-датчики, узлы-стоки и управляющие узлы, отвечающие за координацию и мониторинг сети.

Поскольку IoT-устройства часто работают от батарей и могут выходить из строя, для поддержки связности сети применяются методы энергоменеджмента и самоорганизации. Избыточные беспроводные связи удаляются, а роль магистральных узлов (бэконов) закрепляется за устройствами с наибольшим ресурсом энергии. Алгоритмы оптимизации топологии (например, гибридные эвристики DPSO, GRASP, WCM) повышают устойчивость сети к отказам и разряду. Таким образом, сенсорный слой отвечает за надежный сбор данных и обеспечивает резервирование связи на физическом уровне.

2. Сетевой слой

На сетевом уровне реализуются механизмы передачи данных между сенсорным слоем и облаком. Для этого HetIoT может использовать различные топологические модели: звездные, древовидные, масштабно-сетевые и гибридные схемы. Данные от сенсоров передаются через узлы-стоки, сверхузлы или ретрансляторы к облачному слою. В этой среде типичны сложности маршрутизации: совмещение протоколов разных стандартов мо-

жет привести к узким местам по пропускной способности, повышенному энергопотреблению узлов и новым уязвимостям.

Одним из ключевых требований к сетевому слою является приспособляемость к динамическому характеру IoT-сети. При отключении устройств или изменении радиоканалов сеть должна автоматически перестраиваться. Для этого используются самоорганизующиеся протоколы маршрутизации, которые динамически обновляют маршруты и поддерживают топологию при изменении сети. Также внедряются протоколы энергосбережения, позволяющие удлинить время работы батарей в «жестких» условиях эксплуатации. В целом, сетевой уровень отвечает за обеспечение транспортной емкости системы и гибкость маршрутизации в гетерогенной среде.

3. Облачный слой

Облачный слой служит вычислительным и аналитическим ядром HetIoT. Собранные данные передаются сюда для хранения, обработки и анализа. Благодаря высокой вычислительной мощности облака возможно применение масштабной аналитики: машинного обучения, интеллектуальной обработки сигналов и принятия решений на основе больших данных. Облачная инфраструктура аккумулирует результаты анализа, формирует команды управления устройствами и обеспечивает взаимодействие с прикладным слоем.

В HetIoT-архитектуре облако также выступает мостом для интеграции разнородных систем. Облачные сервисы абстрагируют различия протоколов и операционных систем нижележащих узлов, обеспечивая интероперабельность. По сравнению с традиционными middleware решение на базе облака менее чувствительно к проприетарным протоколам и существенно упрощает масштабирование системы. В критических сценариях (например, при авариях) облако способно быстро пересчитать пути и задать команды актуаторам.

4. Прикладной слой

Прикладной слой определяет конечные сервисы и приложения, предоставляемые пользователю. В этой модели он включает широкий спектр приложений: от мобильных коммуникаторов до специализированных IoT-сервисов. К примеру, в приложениях класса MCN (Mobile Communication Network) пользователи общаются через смартфоны и мессенджеры (WeChat, Skype и др.) в сетях 3G/4G/5G. Для интеллектуального транспорта используются автомобильные сети: «умные» автомобили и дорожная инфраструктура обмениваются данными о дорожной ситуации и прогнозах трафика. В умных домах и городах применяются Wi-Fi-сети – люди управляют бытовыми устройствами и датчиками через беспроводные роутеры. Беспроводные сенсорные сети мониторят окружающую среду: например, измеряют

температуру, влажность, концентрацию газа или дымовые уровни в лесных и промышленных районах.

В приложениях HetIoT пользователь получает данные и управляет системами через удобные интерфейсы, а облако удаленно координирует работу устройств на основе аналитики. Таким образом, прикладной слой демонстрирует реальное применение всего HetIoT-стека в повседневных и промышленных сценариях.

Ключевые технологии связи

HetIoT использует широкий спектр технологий передачи данных. Ниже приведены основные из них и их роль в гетерогенной IoT-среде:

1. Wi-Fi, ZigBee, Bluetooth LE. Эти технологии на основе IEEE 802.11/802.15.4 обеспечивают беспроводную связь на локальных расстояниях. Wi-Fi-сети (IEEE 802.11) дают высокую пропускную способность и применяются в умных домах, городских инфраструктурах и медицинских системах. Например, «умные» приборы подключаются к домашним маршрутизаторам, позволяя пользователям контролировать их через смартфоны. Технологии низкой мощности – ZigBee и Bluetooth Low Energy – подходят для сенсорных сетей, где требуется длительная работа от батарей и передаются небольшие пакеты данных. Они используются в системах домашней и промышленной автоматизации для сбора показаний с многочисленных датчиков.

2. LPWAN (LoRaWAN, Sigfox, NB-IoT, LTE-M и др.). LPWAN-технологии обеспечивают связь на большие расстояния (до нескольких километров) при минимальном энергопотреблении. Они рассчитаны на передачу небольших объемов данных от удаленных или распределенных устройств. Крупные сети LPWAN развертываются в городах и сельском хозяйстве: например, датчики освещенности, почвенной влажности или счетчики воды периодически отправляют короткие сообщения на сервер. LPWAN-протоколы специально разработаны для снижения энергопотребления устройств, чего удается достичь ценой низкой скорости передачи.

3. Сотовые сети (LTE/4G/5G). Сети сотовой связи предоставляют широкое покрытие и высокую скорость передачи, что важно для подвижных или мультимедийных приложений IoT. В HetIoT они используются для связи с автономными транспортными средствами, подключенными датчиками на удаленных площадках и другими IoT-устройствами, которым требуется большая пропускная способность или малая задержка. Современные 4G/5G-сети поддерживают огромный поток устройств и могут качественно обслуживать мобильные датчики в городах и на трассах.

4. Оптические и акустические каналы. Для некоторых задач применяются альтернативные среды передачи. Оптические технологии (Visible Light Communication, лазерная связь FSO, Li-Fi) позволяют достичь гигабитных скоростей, однако требуют прямой видимости и чувствительны к внешним условиям (например, туману или пыли). Они рассматриваются для локальных сетей в зданиях и интеркоммуникации устройств. Акустические каналы используются преимущественно в подводных IoT (IoUT). Под водой радиочастотная связь сильно затухает, поэтому данные передаются звуковыми волнами. В IoUT применяют акустические модемы, оптические импульсные системы и магнитную индукцию для связи между подводными устройствами и надводными станциями.

5. Каждая из перечисленных технологий дополняет другие: комбинация RF, LPWAN, оптических и акустических каналов позволяет достичь необходимого качества связи в гетерогенной сети IoT. Крупные системы HetIoT обычно гибко выбирают технологии для разных задач – от низкоскоростных сенсорных сообщений до высокоскоростной синхронизации и передачи мультимедиа.

Вызовы и проблемы

HetIoT сталкивается со множеством критических проблем, связанных с интеграцией разнородных компонентов. Основные из них:

1. Гетерогенность протоколов и стандартов. Разнородность сетевых технологий усложняет совместимость устройств: каждое семейство оборудования использует свои протоколы (модель TCP/IP, MQTT, CoAP, ZigBee, LoRaWAN и др.), что требует разработки шлюзов и адаптеров. Как отмечается в обзорах, такая сложность архитектуры и гетерогенность протоколов создают серьезные трудности при построении надежных HetIoT-приложений.

2. Маршрутизация и динамическая топология. В большой гетерогенной сети крайне сложна задача построения оптимальных маршрутов. Периодические отключения узлов или изменения каналов связи приводят к фрагментации сети. Из-за этого поддержка связности и балансировка нагрузки требуют разработки адаптивных протоколов. К тому же классические протоколы маршрутизации могут страдать от низкой эффективности в IoT (ограниченная полоса, энергопотребление, пропускная способность каналов). Необходима маршрутизация, учитывающая различные свойства каналов и устройства, что осложняет проектирование сети.

3. Энергопотребление. Большинство IoT-устройств питается от батарей или накопителей малого объема, поэтому энергосбережение – один из ключевых факторов. При гетерогенном подключении необходим компромисс между активностью устройств и сроком их службы. Экономичные протоколы (длительные периоды сна, редкая передача данных) уменьшают рас-

ход энергии, но ухудшают реакцию системы. В HetIoT требуется баланс между проницаемостью сети и энергоэффективностью устройств.

4. Безопасность и конфиденциальность. Масштабная IoT-сеть включает тысячи – миллионы сенсоров, часто расположенных в открытых или слабо контролируемых средах. Это делает сеть уязвимой к кибератакам и утечкам данных. Требуются сложные механизмы шифрования, аутентификации и защиты каналов в гетерогенной среде. Как отмечалось, обеспечение безопасности и конфиденциальности данных в HetIoT – одна из центральных проблем современных исследований.

5. Надежность и отказоустойчивость. Большой и разнообразный IoT-кластер подвержен частым изменениям: отказам узлов, помехам, отказу связи. Для надежного функционирования необходимо автоматическое восстановление топологии (самоорганизация), резервирование каналов и поддержка QoS. Исследования показывают, что способность сети к самоорганизации критически важна для устойчивости крупных HetIoT-инсталляций.

6. Объем данных. При увеличении числа датчиков растут объемы генерируемой информации. Поток данных из распределенных источников может достигать таких масштабов, что их предобработка, хранение и анализ становятся серьезной вычислительной задачей. Как указывалось в литературе, «огромное количество данных» от IoT-устройств создает сложности при управлении и мониторинге сети: нужны мощные архитектуры обработки и интеллектуальные алгоритмы фильтрации и сжатия данных.

Таким образом, главным вызовом HetIoT является сочетание инфраструктурной сложности с ограниченными ресурсами устройств. Решение этих задач требует комплексных подходов на всех уровнях архитектуры.

Перспективные направление развития

Для преодоления указанных проблем активно разрабатываются новые подходы. Среди перспективных направлений можно выделить:

1. Самоорганизующиеся сети и когнитивные алгоритмы. HetIoT-сеть должна уметь автоматически перенастраиваться при изменении условий. Алгоритмы самоорганизации на основе эвристик или методов машинного обучения позволяют динамически строить и поддерживать топологию без централизованного управления. В таких сетях узлы могут самостоятельно определять оптимальные маршруты и роли (например, выбирая магистральные узлы).

2. Программно-определяемые сети (SDN). SDN-архитектура выделяет отдельную управляющую плоскость и может гибко настраивать логику маршрутизации. При интеграции с IoT это позволяет реализовать централизованное управление сетью без переделки инфраструктуры. С помощью SDN-контроллеров

можно программно задавать политику маршрутизации и управления потоком данных, что упрощает адаптацию сети к разным приложениям без смены «железа».

3. Беспроводная передача энергии (WPT). Технологии WPT позволяют удаленно заряжать или питать IoT-устройства, что снижает зависимость от батарей. По мере миниатюризации датчиков внедряются магнитно-связанные и резонансные системы зарядки. Например, предполагается, что в будущем в помещениях появятся передатчики энергии, покрывающие несколько устройств одновременно. Использование WPT существенно продлит время автономной работы сенсоров и упростит техническое обслуживание HetIoT.

4. Интеллектуальная маршрутизация и анализ данных. С применением методов искусственного интеллекта и машинного обучения возможно прогнозировать нагрузки и оптимизировать маршруты в реальном времени. «Умные» алгоритмы маршрутизации смогут учитывать положение, энергоэффективность и загруженность узлов, а также предсказывать отказные ситуации. Кроме того, гибридные облачные/edge-архитектуры (с использованием fog-вычислений) позволят распределить обработку данных между облаком и краем сети, снизив задержку и нагрузку на центральные узлы.

Эти и другие инновационные подходы (например, внедрение сетей 6G, сетевого срезания) сформируют основу следующего поколения IoT-сетей. Они позволят повысить адаптивность, энергоэффективность и масштабируемость HetIoT, приблизив реализацию концепции «Интернета всего».

Заключение

В данной работе представлена концептуальная модель гетерогенного Интернета вещей, основанная на четырехуровневой архитектуре (сенсорный слой, сетевой слой, облако, прикладные сервисы). Рассмотрены ключевые технологии связи – от беспроводных сенсорных протоколов и LPWAN до 4G/5G, оптических и акустических каналов – и показано, как их комбинация может обеспечить взаимодействие разнообразных устройств. Выявлены основные проблемы HetIoT: межпротокольная совместимость, маршрутизация, безопасность, энергосбережение, надежность и обработка больших данных. Для решения этих проблем актуальны направления самоконфигурации сетей, SDN-подходы, беспроводная передача энергии и интеллектуальные алгоритмы управления. Использование предложенной архитектуры и передовых методов позволит гетерогенному IoT-сообщества эффективно масштабироваться и предоставлять новые удобные сервисы в будущем. Как отмечают авторы обзора, HetIoT способен «заполнить нашу жизнь» различными умными приложениями и сервисами, поэтому дальнейшее исследование этой области имеет высокую практическую значимость.

Список используемых источников

1. Кучерявый А. Е., Киричек Р. В., Маколкина М. А., Парамонов А. И., Дунайцев Р. А., Пирмагомедов Р. Я., Бородин А. С., Владыко А. Г., Мутханна А. С. А., Выборнова А. И., Владимиров С. С., Гришин И. В. Новые перспективы научных исследований в области сетей связи на 2021–2024 годы // Информационные технологии и телекоммуникации. 2020. Том 8. № 3. С. 1–19. DOI 10.31854/2307-1303-2020-8-3-1-19.
2. Кучерявый А. Е. Триллионные сети // Телекоммуникации. 2013. № S7. С. 19–22. EDN:REKFXF
3. Кучерявый А.Е., Окунева Д.В., Парамонов А.И., Хоанг Ф.Н. Методы распределения трафика в гетерогенной сети Интернета вещей высокой плотности. Труды учебных заведений связи. 2024. Т. 10. № 2. С. 67-74. https://doi.org/10.31854/1813-324X-2024-10-2-67-74. EDN:RTNVEU

MODEL OF THE HETEROGENEOUS INTERNET OF THINGS: ARCHITECTURE, KEY TECHNOLOGIES, AND FUTURE DIRECTIONS

Paramonov A., Hoang N.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The Heterogeneous Internet of Things (HetIoT) integrates a wide range of networks and communication media–including wireless sensor networks, Wi-Fi, LPWAN, 4G/5G cellular systems, optical links, and acoustic channels–to enhance the functionality of applications in smart homes, smart cities, and industrial environments. This paper introduces a theoretical four-layer HetIoT architecture, comprising the sensor, network, cloud, and application layers, and examines the role of key communication technologies within this framework. We analyze critical challenges such as protocol interoperability, routing strategies, security, and energy efficiency, and we outline promising future developments, including self-configuring network paradigms, software-defined networking (SDN) techniques, wireless power transfer mechanisms, and intelligent routing algorithms. The proposed model and accompanying literature survey provide a basis for assessing the capabilities and limitations of HetIoT systems and for guiding subsequent research efforts.

Key words: *heterogeneous networks, Internet of Things, communication channels, IoT technologies*

УДК 621.396.969
ГРНТИ 47.49.31

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ И КОНФИГУРАЦИЯ ПРОЕКТА OPENWIFI НА ПЛАТФОРМЕ LIBRESDR

К. Е. Рютин

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

Данная работа является продолжением исследования, посвященного имплементации и первичной экспериментальной апробации проекта с открытым исходным кодом OpenWiFi на платформе программно-конфигурируемого радио LibreSDR. Целью данной работы является оценка количественных и качественных характеристик точки доступа технологии Wi-Fi, реализованной проектом OpenWiFi на платформе LibreSDR. В результате исследования получена формализованная методика конфигурации параметров точки доступа и проведения измерений фактической скорости передачи данных между точкой доступа и подключенным к ней клиентским устройством. Результаты работы будут полезны как для последующей модернизации проекта OpenWiFi и проведения сопутствующих экспериментов, так и для организации образовательного процесса в рамках изучения технологий беспроводного доступа.

OpenWiFi, Wi-Fi, LibreSDR, SDR, скорость передачи данных.

Данная работа является продолжением исследования [1], посвященного имплементации и первичной экспериментальной апробации проекта с открытым исходным кодом OpenWiFi на платформе программно-конфигурируемого радио (ПКР, SDR – Software-Defined Radio) LibreSDR [2]. Целью данной работы является описание конфигурации параметров точки доступа (ТД, AP – Access Point), реализованной проектом OpenWiFi на платформе LibreSDR, и оценка фактической скорости передачи данных между ТД и подключенным к ней клиентским устройством.

Для конфигурации и запуска ТД необходимо подключиться с помощью хост-компьютера к удаленному терминалу LibreSDR по протоколу SSH (Secure SHell). Для конфигурации основных параметров ТД на пользовательском уровне, в проекте OpenWiFi предусмотрен соответствующий файл конфигурации hosapd-openwifi.conf. Команда открытия файла конфигурации ТД в консольном текстовом редакторе vi показана на рис. 1.

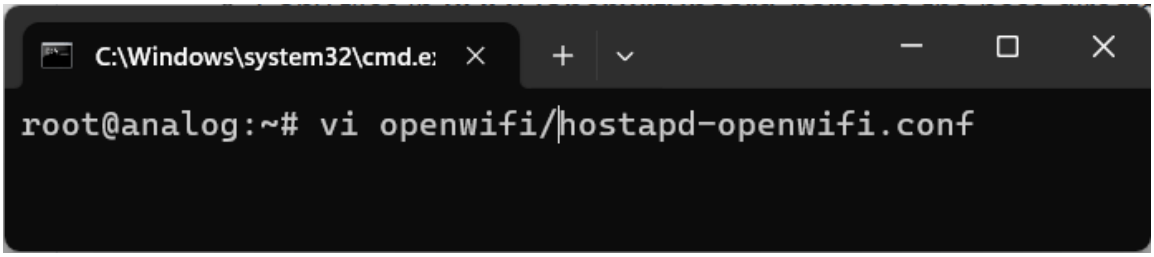


Рис. 1. Открытие файла конфигурации ТД в консольном текстовом редакторе

Содержание файла конфигурации ТД приведено на рис. 2. Среди параметров были изменены SSID и частотный канал. Идентификатор SSID был изменен с «openwifi» на «apino» и был выбран свободный частотный канал 48 (5,24 ГГц).

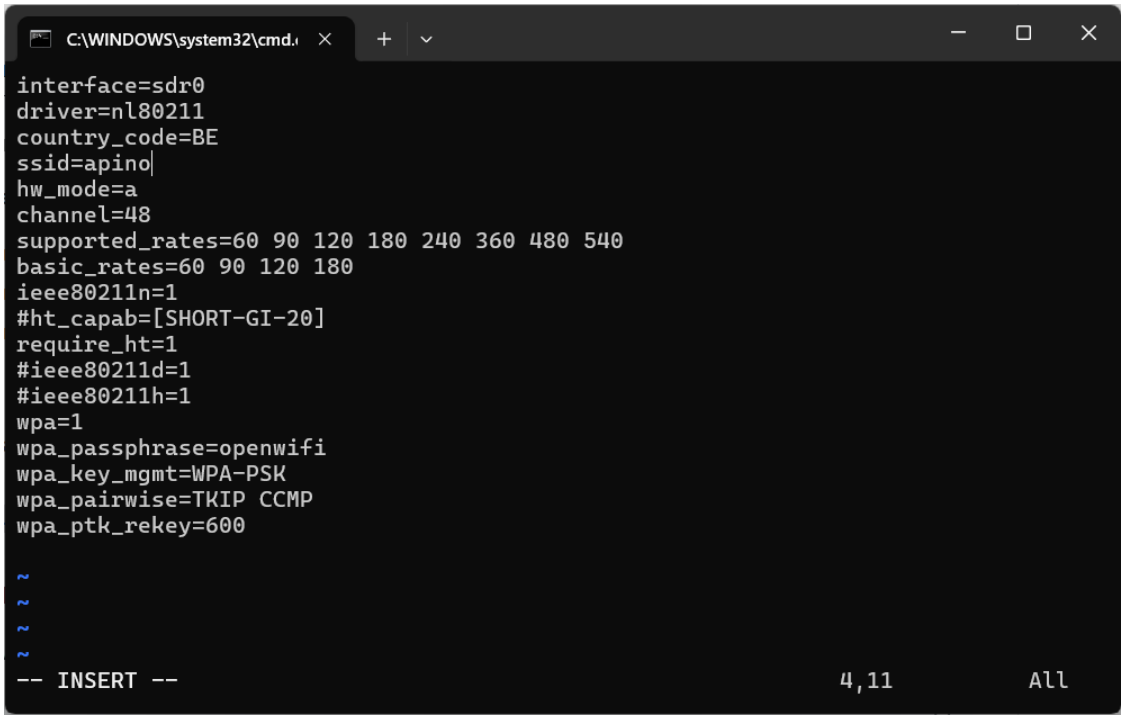


Рис. 2. Содержание файла конфигурации ТД

После запуска ТД исполнением соответствующих сценариев командной оболочки, клиентское устройство, представленное другим компьютером, было подключено к ТД. В дополнение к этому, ТД был предоставлен доступ к Интернету с хост-компьютера вводом следующих команд:

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -t nat -A POSTROUTING -o N -j MASQUERADE
sudo ip route add 192.168.13.0/24 via 192.168.10.122 dev E,
```

где N – имя сетевого порта ПК, подключенного к Интернету; E – имя сетевого порта ПК, подключенного к LibreSDR.

Далее были проведены эксперименты по измерению фактической скорости передачи данных между ТД и клиентским устройством. Для измерения скорости передачи данных была использована консольная утилита iperf [3]. Утилита iperf позволяет измерить реальную скорость соединения между двумя узлами сети, диагностирует сетевые задержки, определяет потери пакетов и тестирует стабильность соединения в целом. Запуск утилиты iperf на стороне ТД продемонстрирован на рис. 3.

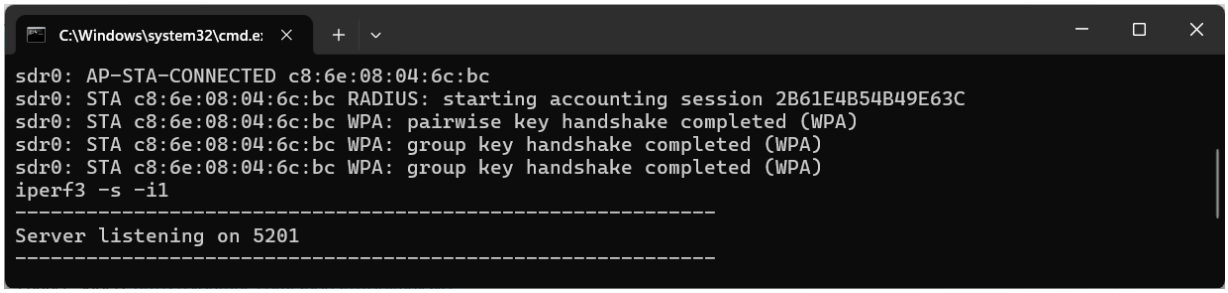


Рис. 3. Запуск утилиты iperf на стороне ТД

Запуск утилиты iperf на стороне клиентского устройства продемонстрирован на рис. 4. Для начала был выбран режим обмена UDP пакетами для измерения скорости.

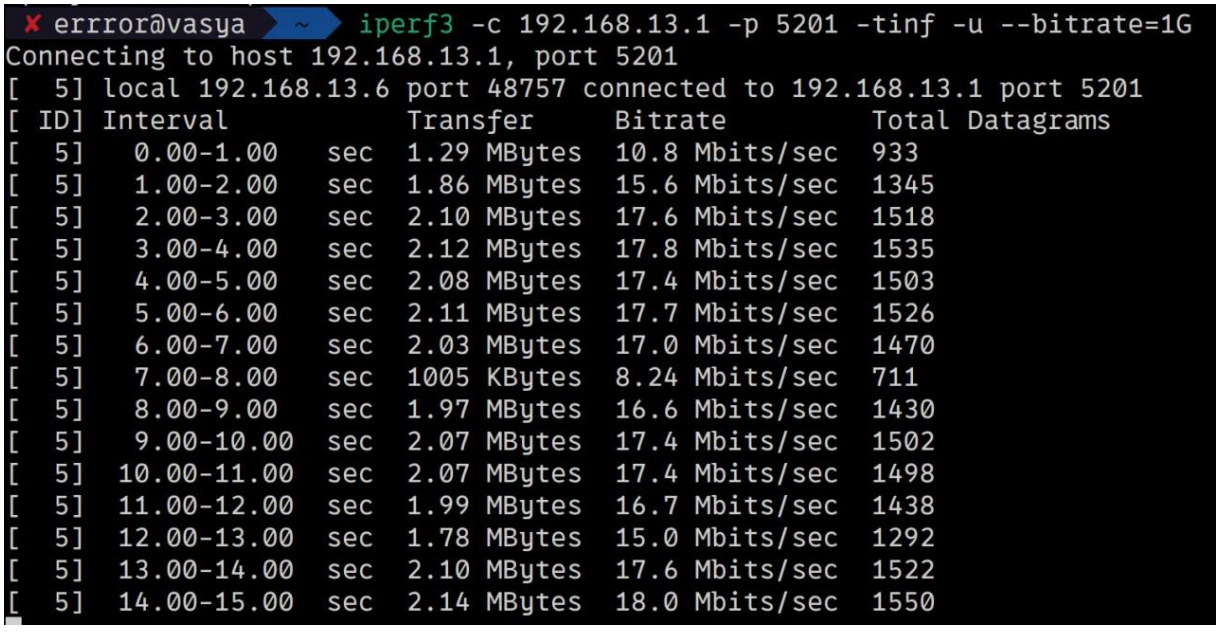


Рис. 4. Запуск утилиты iperf на стороне клиентского устройства

В первом эксперименте ТД и клиентское устройство располагались в непосредственной близости друг к другу. На рис. 5 показан экспериментальных стенд при размещении устройств вблизи.

Рис. 5. Экспериментальных стенд при размещении устройств вблизи

При обмене UDP пакетами в течении 5 минут, результирующая средняя скорость передачи данных составила 15,9 Мбит/с. Результат измерения скорости при размещении устройств вблизи показан на рис. 6.

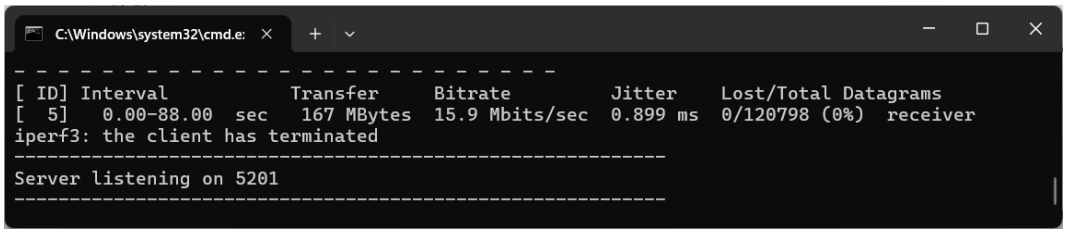


Рис. 1. Результат измерения скорости при размещении устройств вблизи

Во втором эксперименте ТД и клиентское устройство были территориально разнесены друг от друга на расстояние примерно 3 метра. На рис. 7 показан экспериментальный стенд при размещении устройств на расстоянии 3 м.

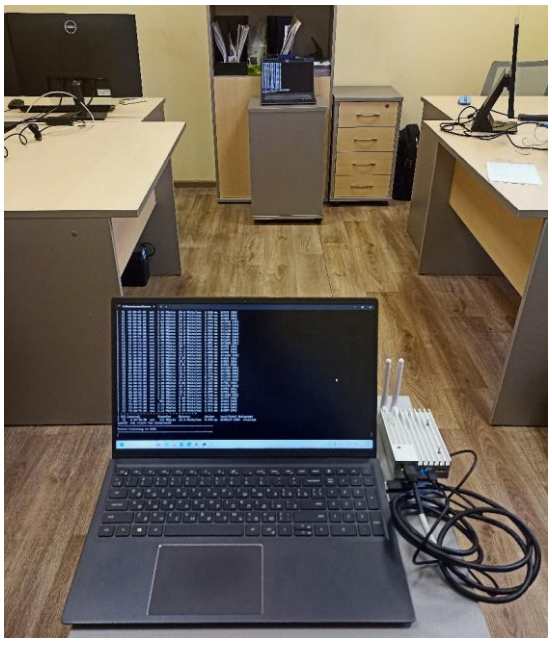


Рис. 7. Экспериментальный стенд при размещении устройств на расстоянии 3 м

При обмене UDP пакетами в течение 5 минут, результирующая средняя скорость передачи данных составила 5,44 Мбит/с. При этом доля потерянных датаграмм составила 15 %. Результат измерения скорости при размещении устройств на расстоянии 3 м показан на рис. 8.

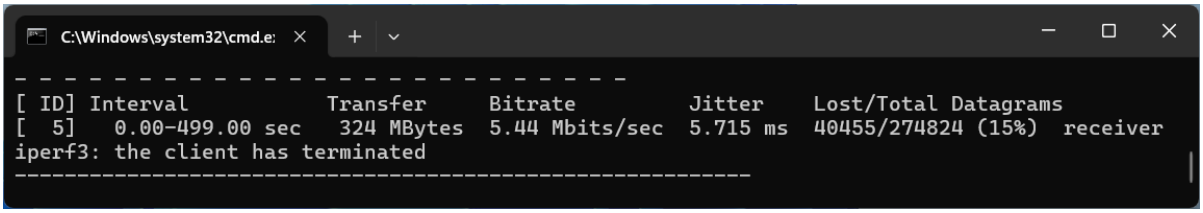


Рис. 2. Результат измерения скорости при размещении устройств на расстоянии 3 м

Далее были проведены повторные эксперименты с измерением скорости по TCP-трафику. В результате повторных экспериментов с использованием пакетов TCP, фактическая скорость передачи данных составила 17,1 Мбит/с при размещении устройств в непосредственной близости и 6,4 Мбит/с при размещении устройств на расстоянии трех метров.

Измеренная в проведенных экспериментах скорость передачи данных считается низкой, но минимально допустимой в задачах просмотра веб-страниц, просмотра видео в разрешении Full HD, стриминга видео в разрешении Full HD или для отправки данных телеметрии с беспилотных летательных аппаратов (БПЛА) [4]. Разработчики проекта OpenWiFi, в свою очередь, заявляют о достижении скорости передачи данных, равной 40-50 Мбит/с по TCP-трафику при работе ТД в диапазоне 5 ГГц в условиях отсутствия других Wi-Fi устройств, работающих на том же частотном канале и при расположении ТД и клиентского устройства в непосредственной близости [5]. Результаты работы будут полезны как для последующей модернизации проекта OpenWiFi и проведения сопутствующих экспериментов, так и для организации образовательного процесса в рамках изучения технологий беспроводного доступа.

Список используемых источников

1. Рютин К. Е., Фокин Г. А. LibreSDR: имплементация и экспериментальная апробация проекта OpenWiFi // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная Дню радио. 2025. № 1(80). С. 132-135. EDN:SKRHPE

2. Рютин К. Е., Фокин Г. А. LibreSDR: разработка и экспериментальная апробация встроенного программного обеспечения // Известия высших учебных заведений. Авиационная техника. 2025. № 1. С. 185-193.

3. iPerf – The ultimate speed test tool for TCP, UDP and SCTP URL: https://iperf.fr/ (дата обращения 20.06.2025).

4. Какая скорость интернета считается нормальной в 2025 году? URL: https://spb.rt.ru/events/p/speed-normal-2024 (дата обращения 20.06.2025).

5. iperf3 TCP between openwifi (Xilinx ZYNQ ADI AD9361) board and iPad: 50Mbps. URL: https://github.com/open-sdr/openwifi/discussions/272 (дата обращения 20.06.2025).

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Г. А. Фокиным.

PERFORMANCE ESTIMATION AND CONFIGURATION OF THE OPENWIFI PROJECT ON THE LIBRESDR PLATFORM

Ryutin K.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This study is a continuation of the research on the implementation and primary experimental validation of the open-source OpenWiFi project on the LibreSDR software-defined radio platform. The purpose of this work is to estimate the quantitative and qualitative characteristics of the Wi-Fi technology access point implemented by the OpenWiFi project on the LibreSDR platform. As a result of the research, a formalized methodology was obtained for configuring the access point parameters and measuring the real data rate between the access point and the client device connected to it. The results of the work will be useful both for the subsequent modernization of the OpenWiFi project and for conducting related experiments, as well as for organizing the educational process in the framework of studying wireless access technologies.

Key words: *OpenWiFi, Wi-Fi, LibreSDR, SDR, data rate*

УДК 621.396.677
ГРНТИ 47.45.29

ЭКСПЕРИМЕНТАЛЬНАЯ АПРОБАЦИЯ SDR ПЛАТФОРМЫ HACKRF ONE В СРЕДЕ GNU RADIO. ЧАСТЬ 1

Д. С. Рябиков

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

На сегодняшний день для прототипирования и экспериментальной апробации технических решений в области радиосвязи все чаще применяется программно-определяемое радио SDR (Software Defined Radio) в сочетании с открытым программным обеспечением, таким как GNU Radio. Одним из наиболее доступных и широко используемых SDR-устройств является HackRF One, сочетающее в себе широкий частотный диапазон, мобильность и поддержку открытого сообщества. В данной статье проведена экспериментальная проверка возможностей HackRF One при передаче и приеме сигнала с квадратурной фазовой манипуляцией QSPK (Quadrature Phase Shift Keying). Проведенное испытание показывает высокую эффективность платформы в задачах цифровой модуляции и демодуляции сигналов. Особое внимание уделено таким преимуществам HackRF One, как открытость исходного кода, экономическая доступность и простота интеграции в образовательные и научные лабораторные практики. Полученные результаты позволяют говорить о перспективах данной платформы для использования в академической и образовательной среде, особенно при подготовке студентов и молодых специалистов в области разработки и верификации систем радиосвязи на базе SDR-технологий.

GNU Radio, SDR, QPSK, HackRF One

Характеристики SDR HackRF One

HackRF One – это программно-определяемое периферийное устройство, способное передавать или принимать радиосигналы в диапазоне от 1 МГц до 6 ГГц. Разработанная для тестирования и разработки современных радиотехнологий и устройств следующего поколения, HackRF One [1] представляет собой аппаратную платформу с открытым исходным кодом, которую можно использовать в качестве периферийного устройства USB или запрограммировать для автономной работы. Основные характеристики и аппаратные компоненты платформы представлены в таблицах 1 и 2.

ТАБЛИЦА 1. Характеристики HackRF One

Название	Характеристика
Рабочая частота	от 1 МГц до 6 ГГц
Режим работы	полудуплексный
Максимальная частота дискретизации	20 МГц
Ширина квадратурных компонент	8 бит
Совместимое программное обеспечение	GNU Radio, SDR#, GQRX, QSpectrumAnalyzer, SDR Console
Программно настраиваемое усиление принимаемых и передаваемых сигналов	есть
Фильтр основной полосы частот	есть
Питание антенного порта с программным управлением	50 мА при 3,3 В
Тип разъема питания	USB 2.0
Тип антенного разъема	SMA
Тип разъемов тактовых входов и выходов для синхронизации	SMA
Дополнительные разъемы	внутренние штыревые разъемы для расширения
Программное обеспечение	свободно распространяемое

ТАБЛИЦА 2. Основные компоненты используемые в HackRF One

Название
Приемопередатчик MAX2837 от 2.3 до 2.7 ГГц
Приемопередатчик MAX2839 от 2.3 до 2.7 ГГц
АЦП/ЦАП MAX5864
Генератор тактовой частоты Si5351
Микросхема программируемой логики CPLD (Complex Programmable Logic Device) CoolRunner-II
Микроконтроллер LPC43xx ARM Cortex-M4
Микшер/синтезатор RFFC5072
8 битная Flash память W25Q80BV

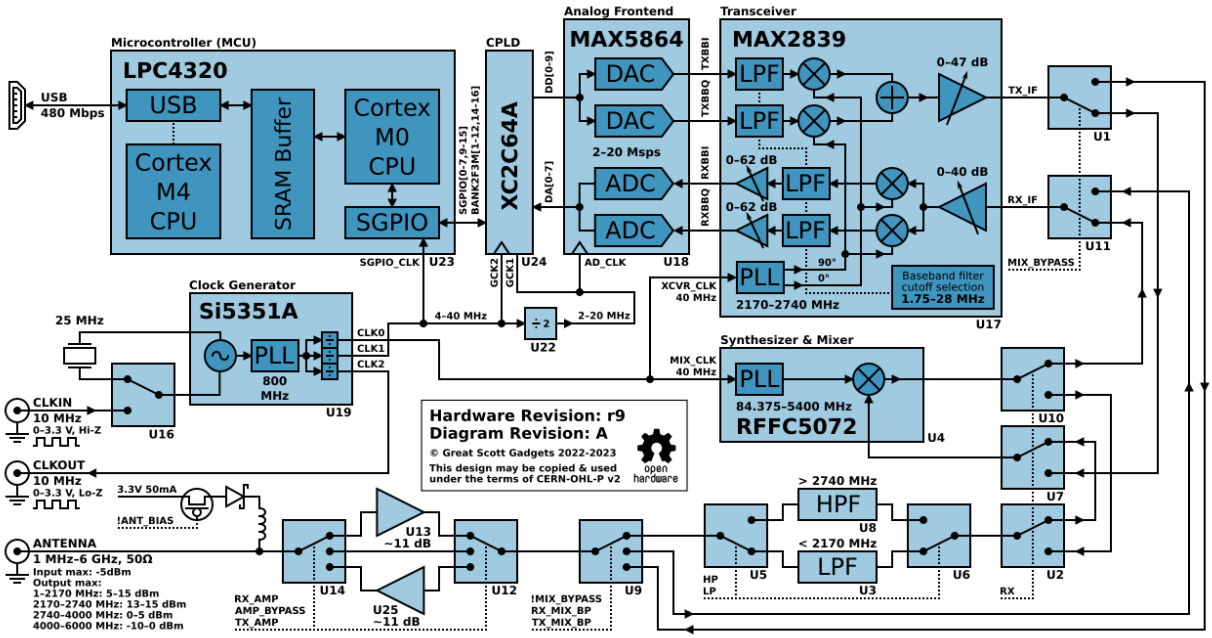


Рис. 1. Блок схема аппаратных компонентов HackRF One

Описание и возможности GNU Radio

GNU Radio [2] – это бесплатный инструментарий для разработки программного обеспечения с открытым исходным кодом, который предоставляет блоки обработки сигналов для реализации программных радиостанций. Его можно использовать с легкодоступным недорогим внешним радиочастотным оборудованием для создания программно-определяемых радиостанций или без оборудования в среде, подобной симулятору. Он широко используется в научных исследованиях, промышленности, академических кругах, правительстве и среди любителей для поддержки как исследований в области беспроводной связи, так и реальных радиосистем.

GNU Radio – это высокомодульная платформа, которая позволяет пользователям проектировать, моделировать и развертывать высокопроизводительные системы радиосвязи в реальном мире, ориентированная на блок-схемы, поставляется с обширной библиотекой блоков обработки, которые можно легко комбинировать для создания сложных приложений для обработки сигналов. GNU Radio используется в огромном количестве приложений [3] для радиосвязи в реальном мире, включая обработку звука, мобильную связь, спутники слежения, радарные системы, сети GSM, цифровое радио Mondiale и многое другое – все это в компьютерном программном обеспечении. Само по себе это не решение для взаимодействия с каким-либо конкретным оборудованием. Оно также не предоставляет готовых приложений для конкретных стандартов радиосвязи (например, 802.11, ZigBee, LTE

и т.д.), но может использоваться и использовался для разработки, реализаций практически любого стандарта связи с ограниченной полосой частот.

Для экспериментальной апробации [4] среды GNU Radio совместно с SDR HackRF One был реализован прием и передача сигнала методом квадратурной фазовой манипуляции QSPK (Quadrature Phase Shift Keying). QSPK – это метод модуляции, при котором два бита преобразуются в четыре символа. Каждый символ представляет сдвиг фазы в сигнале несущей. Данный метод для передачи и приема сигнала выбран в связи с его узнаваемостью и популярностью в области цифровой обработки сигналов [5].

Блок схемы для приемной и передающей частей, созданные в среде Gnu Radio, представлены на рисунках 2 и 3, а список используемых блоков в среде GNU Radio представлены в таблицах 3 и 4.

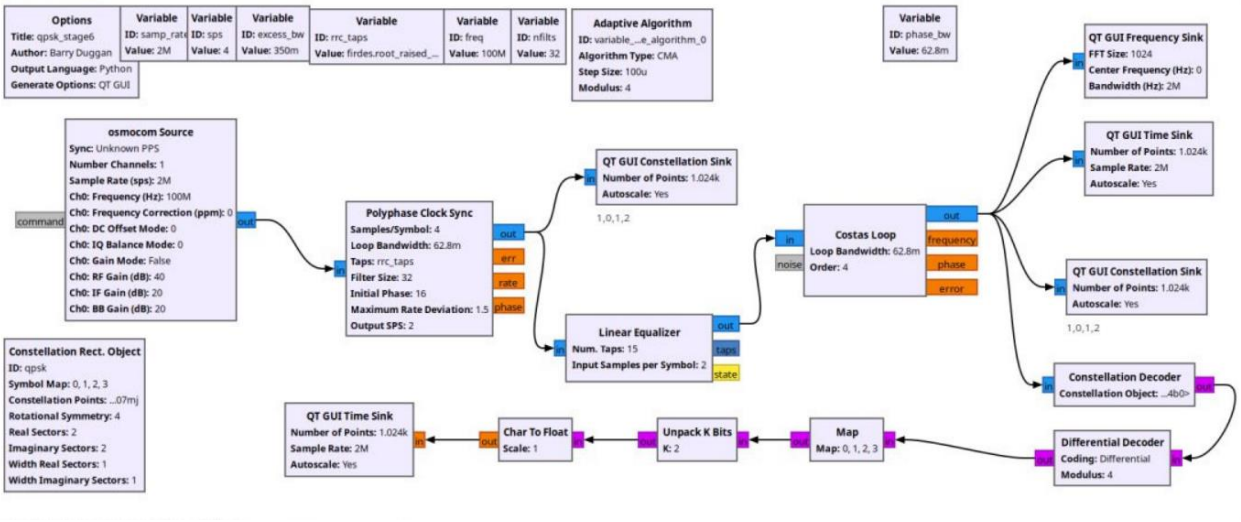


Рис. 2. GNU Radio блок схема приемной части

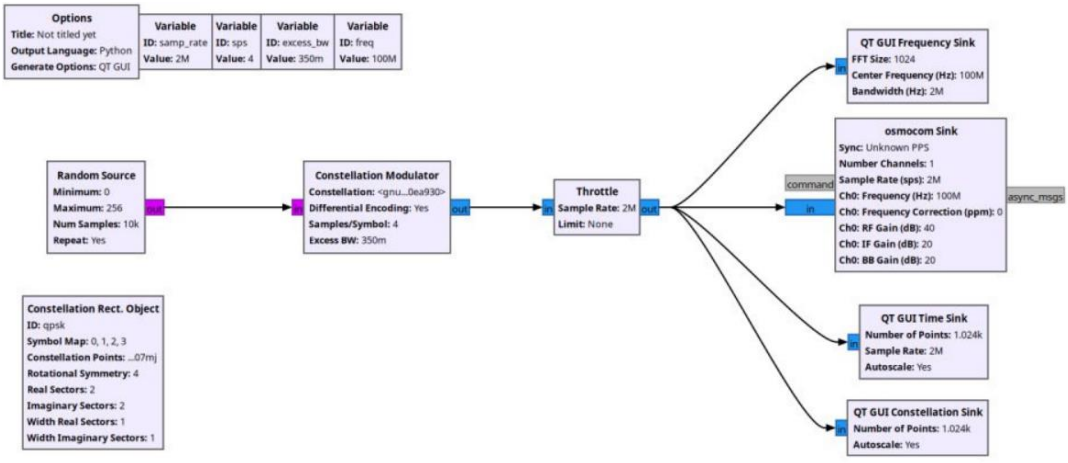


Рис. 3. GNU Radio блок схема передающей части

ТАБЛИЦА 3. GNU Radio блоки принимающей части

Название	Описание
Variable	Назначение переменной
osmocom Source	Принимает сигнал на SDR устройство
Constellation Rec. Object	Объект для создания прямоугольного созвездия
Polyphase Clock Sync	Синхронизатор времени с использованием многофазных блоков фильтров
Linear Equalizer	Выполняет линейное выравнивание потока сложных выборок
Costas Loop	Фиксирует центральную частоту сигнала и преобразует ее в основную полосу частот
Constellation Decoder	Декодируйте точки созвездия из сложного пространства в (распакованные) биты
Differential Decoder	Выполняет дифференциальное декодирование
Map	Сопоставляет входящий сигнал со значением на карте
Unpack K Bits	Преобразует байт с k соответствующими битами в k выходных байтов по 1 биту в каждом, расположенных в LSB
Char to Float	Преобразуйте поток символов в поток с плавающей точкой
QT GUI Frequency Sink	Графический приемник для отображения нескольких сигналов по частоте
QT GUI Time Sink	Графический приемник для отображения нескольких сигналов во времени
QT GUI Constellation Sink	Графический приемник для отображения совокупности квадратурных компонент из нескольких сигналов

ТАБЛИЦА 4. GNU Radio блоки передающей части

Название	Описание
Variable	Назначение переменной
Random Source	Генерирует несколько выборок случайных чисел
Constellation Modulator	Иерархический блок для дифференциальной общей модуляции с фильтром RRC
Constellation Rec. Object	Объект для создания прямоугольного созвездия
Throttle	Пропускает входные отсчеты с заданной средней скоростью
osmocom Sink	Передает сигнал на SDR устройство
QT GUI Frequency Sink	Графический приемник для отображения нескольких сигналов по частоте
QT GUI Time Sink	Графический приемник для отображения нескольких сигналов во времени
QT GUI Constellation Sink	Графический приемник для отображения совокупности квадратурных компонент из нескольких сигналов

Таким образом, SDR HackRF One в сочетании с открытым программным обеспечением GNU Radio представляет собой мощный и доступный инструмент для разработки, моделирования и экспериментального исследования систем радиосвязи. В рамках первой части работы были представлены основные технические характеристики HackRF One, а также функциональные возможности среды GNU Radio при построении цифровых трактов передачи сигналов. Были описаны ключевые блоки, необходимые для реализации модуляции и демодуляции сигнала с использованием метода QPSK. Полученные результаты легли в основу проведения дальнейших экспериментальных исследований, связанных с детальной настройкой параметров схемы и анализом качества принимаемого сигнала, что составляет предмет второй части данной работы.

Список используемых источников

1. HackRF’s documentations. URL: https://hackrf.readthedocs.io/en/latest/index.html (дата обращения 08.06.25).

2. GNU Radio Wiki. URL: https://wiki.gnuradio.org/index.php/Main_Page (дата обращения 08.06.25).

3. Marcelo B. P., Kenedy M., SDR-Based Spectrum Analyzer Based in Open-Source GNU Radio // Journal of Microwaves Optoelectronics and Electromagnetic Applications, 2021. PP. 542-555.

4. Фокин Г. А., Рютин К. Е., Экспериментальная апробация SDR-платформы LibreSDR // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная дню радио. 2024. №. 79. С. 174-177.

5. Feigin J., Practical Costas loop design: Designing a simple and inexpensive BPSK Costas loop carrier recovery circuit // RF signal processing, 2002. PP. 20-36.

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Г. А. Фокиным.

EXPERIMENTAL TESTING OF THE SDR PLATFORM HACKRF ONE IN THE GNU RADIO ENVIRONMENT. PART 1

Ryabikov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Today, software-defined radio SDR (Software Defined Radio) in combination with open-source software such as GNU Radio is increasingly being used for prototyping and experimental testing of technical solutions in the field of radio communications. One of the most affordable and widely used SDR devices is HackRF One, which combines a wide frequency range, mobility, and open community support. This article experimentally verifies the capabilities of HackRF One in transmitting and receiving a signal with Quadrature phase Shift Keying (QSPK). The conducted test shows the high efficiency of the platform in the tasks of digital signal modulation and demodulation. Special attention is paid to the advantages of HackRF One, such as open source, cost-effectiveness, and ease of integration into educational and scientific laboratory practices. The results obtained allow us to talk about the prospects of this platform for use in the academic and educational environment, especially in the training of students and young specialists in the development and verification of radio communication systems based on SDR technologies.

Key words: *GNU Radio, SDR, QPSK, HackRF One*

УДК 621.396.677
ГРНТИ 47.45.29

ЭКСПЕРИМЕНТАЛЬНАЯ АПРОБАЦИЯ SDR ПЛАТФОРМЫ HACKRF ONE В СРЕДЕ GNU RADIO. ЧАСТЬ 2

Д. С. Рябиков

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

Настоящая работа является продолжением серии публикаций, посвященных экспериментальному исследованию возможностей программно-определяемой радиоплатформы HackRF One совместно с программной средой GNU Radio. Во второй части подробно рассмотрена настройка и параметризация каждого функционального блока, используемого при передаче и приеме сигнала с квадратурной фазовой манипуляцией QPSK (Quadrature Phase Shift Keying). Приведено описание и назначение ключевых модулей схемы, даны рекомендации по выбору параметров для обеспечения устойчивого приема сигнала. Представлены результаты экспериментальной проверки, включая анализ качества принимаемого сигнала и устойчивости соединения в различных условиях. Полученные результаты позволяют говорить о перспективах данной платформы для использования в академической и образовательной среде, особенно при подготовке студентов и молодых специалистов в области разработки и верификации систем радиосвязи на базе SDR-технологий.

GNU Radio, SDR, QPSK, HackRF One

Настройки экспериментального стенда

Как было упомянуто в предыдущей работе, в качестве эксперимента был реализован прием и передача QPSK сигнала с одной SDR платформы HackRF One на другую. Внешний вид платформы представлен на рисунке 1, подробные настройки блоков, показанных в предыдущей статье, описаны в таблицах 1 и 2 соответственно. Экспериментальный стенд и принятый сигнал изображены на рисунках 3 и 4.

Каждый блок [1] в среде GNU Radio реализует определенную алгоритмическую операцию и может быть представлен как самостоятельный программный модуль, работающий в реальном времени.

Блоки можно условно разделить на следующие категории: источники, приемники, блоки обработки и блоки управления.

Каждый блок имеет входные и выходные порты, через которые организуется поток данных между элементами. Все блоки работают в рамках единого потокового механизма, обеспечивая параллельное выполнение операций с минимальной задержкой. Такая архитектура позволяет эффективно

моделировать сложные телекоммуникационные системы и прототипировать реальные радиоустройства [2] в условиях, близким к реальному времени.

Рис. 1. Внешний вид и печатная плата платформы HackRF One

Благодаря открытости исходного кода и расширяемой архитектуре, пользователь имеет возможность как использовать готовые блоки из стандартных библиотек, так и разрабатывать собственные модули на языках Python и C++, что делает GNU Radio мощным инструментом для научных исследований и образовательных задач в области радиосвязи и цифровой обработки сигналов.

ТАБЛИЦА 1. GNU Radio настройка блоков принимающей части

Блок	Значение
Random Source	Minimum: 0 Maximum: 256 Num Samples: 10000 Repeat: Yes
osmocom Source	
Constellation Rec. Object	Symbol Map: 0, 1, 2, 3 Constellation Points: [0.707+0.707j, -0.707+0.707j, -0.707-0.707j, 0.707-0.707j] Rotational Symmetry: 4 Real Sectors: 2 Imaginary Sectors: 2 Width Real Sectors: 1 Width Imaginary Sectors: 1

Блок	Значение
Polyphase Clock Sync	Samples/Symbol: 4 Loop Bandwidth: 0.0628 Filter Size: 32 Initial Phase: 16 Maximum Data Deviation: 1.5 Output SPS: 2
Linear Equalizer	Num. Taps: 15 Input Samples per Symbols: 2
Costas Loop	Loop Bandwidth: 0.0628 Order: 4
Constellation Decoder	Constellation Object: Constellation Rec. Object
Differential Decoder	Coding: Differential Modulus: 4
Map	Map: 0, 1, 2, 3
Unpack K Bits	K: 2
Char to Float	Scale: 1
QT GUI Frequency Sink	FFT Size: 1024 Central Frequency (Hz): 100000000 Bandwidth (Hz): 2000000
QT GUI Time Sink	Number of Points: 1024 Sample Rate (Hz): 2000000 Autoscale: Yes
QT GUI Constellation Sink	Number of Points: 1024 Autoscale: Yes

ТАБЛИЦА 2. GNU Radio настройка блоков передающей части

Блок	Значения
Random Source	Minimum: 0 Maximum: 256 Num Samples: 10000 Repeat: Yes
Constellation Rec. Object	Symbol Map: 0, 1, 2, 3 Constellation Points: [0.707+0.707j, -0.707+0.707j, -0.707-0.707j, 0.707-0.707j] Rotational Symmetry: 4 Real Sectors: 2 Imaginary Sectors: 2 Width Real Sectors: 1 Width Imaginary Sectors: 1

Блок	Значения
Constellation Modulator	Differential Encoding: Yes Samples/Symbol: 4 Excess BW: 0.35
Throttle	Sample Rate (Hz): 2000000 Limit: None
osmocom Sink	Number of Channels: 1 Sample Rate (Hz): 2000000 Ch0: Frequency (Hz): 100000000 Ch0: Frequency Correction (ppm): 0 Ch0: RF Gain (dB): 40 Ch0: TF Gain (dB): 20 Ch0: BB Gain (dB): 20
QT GUI Frequency Sink	FFT Size: 1024 Central Frequency (Hz): 100000000 Bandwidth (Hz): 2000000
QT GUI Time Sink	Number of Points: 1024 Sample Rate (Hz): 2000000 Autoscale: Yes
QT GUI Constellation Sink	Number of Points: 1024 Autoscale: Yes

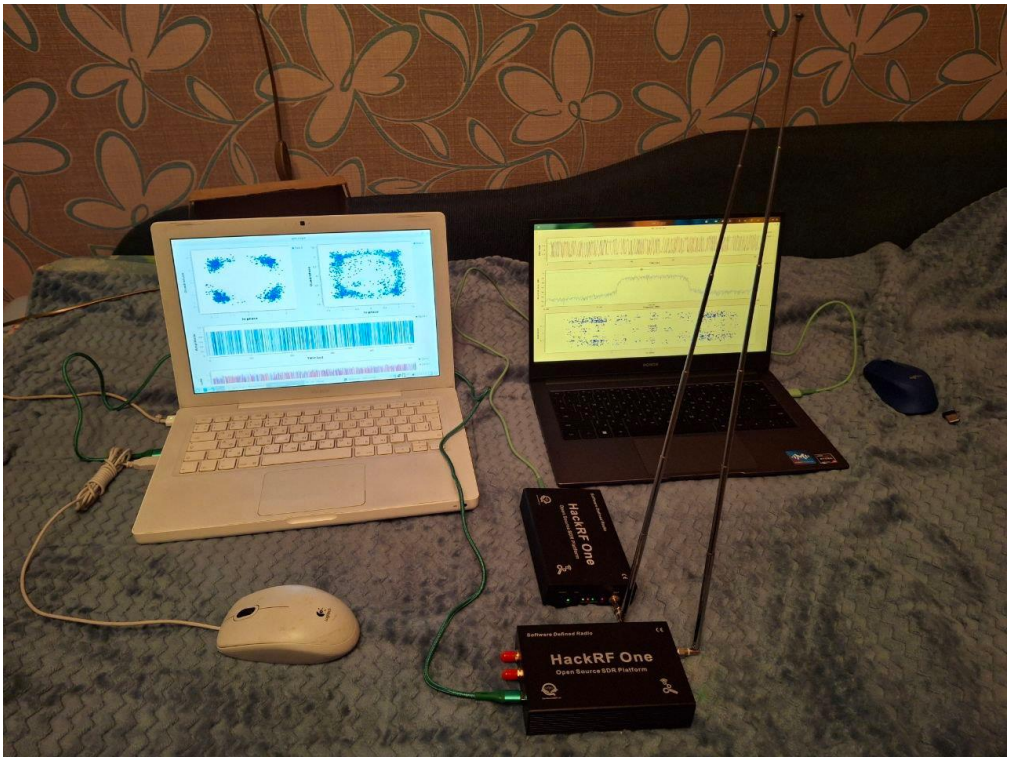


Рис. 2. Экспериментальный стенд

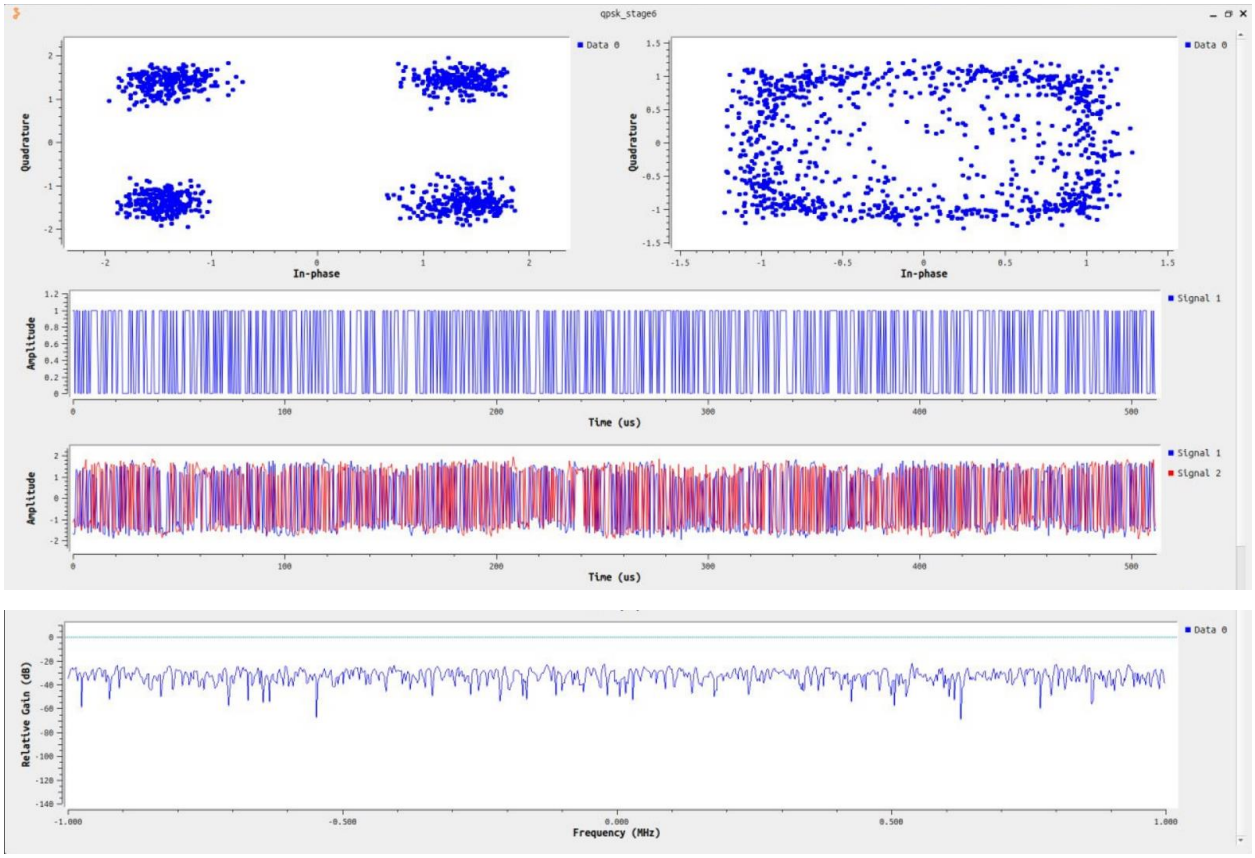


Рис. 3. Отображение принимаемого сигнала

Проведенная экспериментальная апробация программно-определяемой радиоплатформы HackRF One в составе программного комплекса GNU Radio [3] подтвердила ее работоспособность и эффективность при реализации базовых функций цифровой обработки сигналов, включая модуляцию и демодуляцию методом QPSK. Результаты эксперимента показали, что HackRF One обеспечивает достаточную точность и стабильность параметров сигнала для использования в учебных и исследовательских задачах. Таким образом, использование HackRF One совместно с GNU Radio открывает широкие возможности для обучения студентов, проведения научных исследований и разработки современных телекоммуникационных систем на основе технологии программно-определяемого радио.

Список используемых источников

1. GNU Radio – Category:Block_Docs URL: https://wiki.gnuradio.org/ index.php?title=Category:Block_Docs (дата обращения 19.06.25).

2. Фокин Г. А., Рютин К. Е., LibreSDR: Имплементация и экспериментальная апробация проекта OpenWIFI // Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная дню радио. 2025. № 80. С. 132-135.

3. Harris F., J., Malinda R., Multirate Digital Filters for Symbol Timing Synchronization in Software Defined Radios // IEEE Selected Areas in Communications. 2001. Vol. 19. №. 12. PP. 2346-2357.

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Г. А. Фокиным.

EXPERIMENTAL TESTING OF THE SDR PLATFORM HACKRF ONE IN THE GNU RADIO ENVIRONMENT. PART 2

Ryabikov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This work is a continuation of a series of publications devoted to the experimental study of the capabilities of the software-defined radio platform HackRF One in conjunction with the GNU Radio software environment. In the second part, the configuration and parameterization of each functional block used in the transmission and reception of a signal with quadrature phase Shift keying (QPSK) is considered in detail. The description and purpose of the key modules of the circuit are given, recommendations are given on the choice of parameters to ensure stable signal reception. The results of an experimental test are presented, including an analysis of the quality of the received signal and the stability of the connection under various conditions. The results obtained allow us to talk about the prospects of this platform for use in the academic and educational environment, especially in the training of students and young specialists in the field of development and verification of radio communication systems based on SDR technologies.

Key words: *GNU Radio, SDR, QPSK, HackRF One*

УДК 679.745.52
ГРНТИ 49.29.14

МЕТОД РАСЧЕТА ПРЕДЕЛЬНОЙ ПРОТЯЖЕННОСТИ КАБЕЛЬНОГО ТРАКТА С РЕПИТЕРАМИ PoE

А. Б. Семенов

Научно-исследовательский Московский государственный строительный университет

Рассмотрены предельные возможности репитеров PoE как средства наращивания протяженности тракта на основе кабелей из витых пар для подключения удаленных терминальных устройств к внутриобъектовой информационной системе. Обоснована необходимость применения таких репитеров при дальностях связи свыше 150 м, предложена модель соответствующей линии и получены аналитические соотношения, позволяющие выполнить ее инженерный расчет. Сделан вывод о возможности достижения предельной протяженности линии в 750 м при использовании для построения линии серийной элементной базы.

внутриобъектовые информационные системы, PoE-репитер, кабельный тракт, абонент

Современный объект недвижимости, на котором постоянно находятся люди, в соответствии с действующими строительными нормами оборудуется рядом инженерных систем. При этом классические водопровод, вентиляция, электроснабжение и аналогичные им коммуникации дополняются информационно-телекоммуникационной системой (ИТС), для обеспечения доступа к различным видам информационного сервиса и услугам электросвязи.

Характерной особенностью развития таких ИТС стало резкое расширение перечня входящих в нее систем: традиционные ЛВС и телефонная сеть дополняется системой видеонаблюдения, оповещения, контроля доступа и аналогичными им [1]. При этом для основной массы систем, вновь вводимых в состав ИТС, характерно следующее

– реализация физического и транспортного уровня происходит на той технике, которая применяется в классической ЛВС и телефонии;
– относительно умеренные скорости передачи (не свыше 100 Мбит/с);
– невысокие мощности потребления (единицы Ватт);
– явно выраженное тяготение к централизованной структуре.

Оценка распределения длин линий систем с централизованной структурой

Переход на централизованную модель построения ИТС сопровождается ростом протяженности линий для подключения к ИТС терминального

оборудования. При оценке их протяженности α можно исходить из того, что каждая из них линий представляет собой комбинацию из горизонтальной и магистральной составляющей, а ее стационарная часть выполняется единым пробросом. Тогда

$$\alpha = \beta + \gamma.$$

Здесь β и γ – протяженность «горизонтальной» и «магистральной» частей проброса, соответственно. Распределения β и γ известны из опыта построения классических СКС. Для β справедлив нормальный закон со средним значением s = 40 м и среднеквадратичным отклонением σ = 16 м, а γ распределена по показательному закону с параметром λ = 45 1/м [2].

При этом указанные статистики получены применительно к стационарным линиям, что делает излишним учет дополнительного увеличения длины проброса за счет неровности укладки.

Вычисление плотности суммы β и γ дает

$$\varphi_{\beta+\gamma}(x) = \frac{\lambda}{\sqrt{2\pi}\,\sigma} e^{\frac{-2\lambda(x-s)-(\lambda\sigma)^2}{2}} \int_0^{\infty} e^{-(\tau-(x-c-\sigma^2\lambda)^2/2\sigma^2} d\tau. \qquad (1)$$

Из (1) вытекает, что в 64 % случаев ожидаемая протяженность стационарной части составного тракта превышает 90 м.

Особенности электропитания терминального оборудования

Та часть физического уровня современных ИТС, которая обслуживает терминальное оборудование, строится на основе кабелей из витых пар. Это позволяет применить для питания терминальных устройств технологию PoE [3]. Обращение к ней не только делает эксплуатацию ИТС более удобной, но и в технически и экономически обоснованных случаях позволяет исключить прокладку отдельного кабеля питания.

Технология PoE стандартизирована группой спецификаций IEEE802.3af, IEEE802.3at и IEEE802.3bt и разрабатывалась применительно к 100-метровому модельному кабельному тракту при протяженности стационарной линии в 90 м, а ее работоспособность гарантировалась на технике категории 5e. Протяженность линии контролируется датчиком шлейфового сопротивления, который является штатным блоком источника. Эта особенность позволяет увеличить протяженность линии как отказом от канонической структуры в пользу построения тракта по схеме MPTL [4], которая обладает несколько меньшим значением шлейфового сопротивления, так и применением в линейной части кабелей с увеличенным диаметром ТПЖ. В

частности, при применении кабелей с увеличенным до максимально возможного значения диаметром ТПЖ в 0,64 мм получаем оценку

$$L_{max} = 100 \times (0{,}64/0{,}52)^2 = 151 \text{ м}.$$

Сопоставление полученного значения с оценкой по (1) свидетельствует о том, что 10 % кабельных трактов будет иметь протяженность, которая превышает 151 м. Это является весьма значимой величиной для практики реализации проектов и требует применения соответствующих технических средств или использования специальных проектных решений.

Возможно два основных варианта решения указанной проблемы. Первый из них заключается в применении в линейной части комбинированных кабелей с волоконными световодами для передачи сигналов и дополнительными медными жилами [5]. Дистанционное питание в этом случае осуществляется, например, с привлечением по технологии PoDL [6]. Второй вариант основан на обращении к репитерам, которые поддерживают технологию PoE. PoE-репитеры как продукт массового применения широко представлены в коммерческой продаже и перспективны для использования в проектах за счет того, что серийно выпускаются в обычном и уличном исполнении.

Расчетная модель

Структурно PoE-репитер включает в себя блоки регенератора уровня 1 и внутренний генератор, который

– вырабатывает стандартное напряжение PoE;
– использует часть мощности инжектора PoE для обеспечения функционирования своих внутренних схем.

С учетом необходимости питания схем репитера его выходное напряжение полностью соответствует спецификации IEEE 802.3af, но максимально допустимый ток уменьшается.

Схема линии и направление ее расчета представлены на рис. 1.

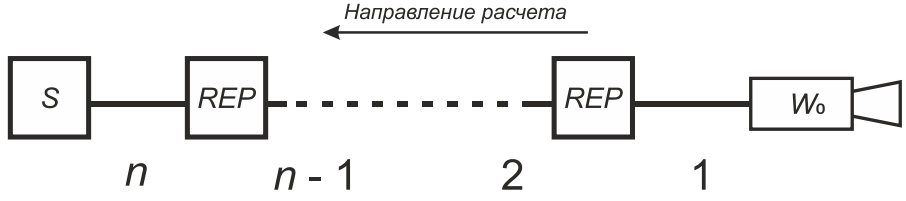


Рис. 1. Структурная схема линии с последовательно включенными PoE-репитерами и направление расчета линии

Эквивалентная схема отдельного сегмента структуры рис. 1 имеет вид, показанный на рис. 2.

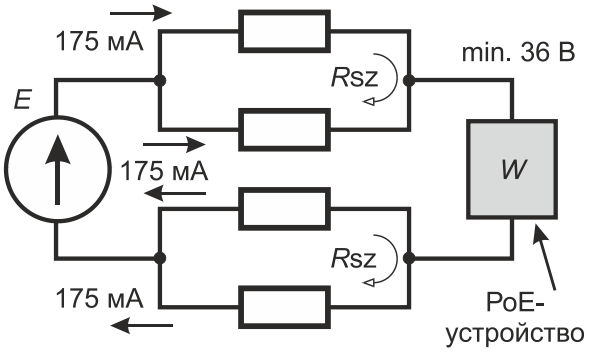


Рис. 2. Расчетная схема одного сегмента рассчитываемой линии

Генератор источника PoE для увеличения КПД построен по схеме импульсного преобразователя постоянного входного напряжения. Поэтому структура рис. 2 описывается нелинейным уравнением

$$E = Ri + W/i \quad ,$$

где $R = R_{sz}/2$, а R_{sz}.– половина шлейфового сопротивления витой пары, W – мощность терминального устройства как нагрузки.

С учетом ограничений спецификации IEEE802.3af дополнительно считается, что $E - Ri \geq 36$ В. Данное ограничение гарантированно выполняется на практике.

Анализ и результаты

Привлечение двухшаговой итерационной процедуры метода Ньютона при нулевом приближении $i_0 = W/E$ дает (максимальная ошибка для техники спецификации IEEE802.3af не превышает 5 %)

$$i \cong \frac{W}{E}\left(1 + \frac{R}{\frac{E^2}{W} - R}\right).$$

Отношение потерь в кабельном тракте к мощности потребления нагрузки составит

$$\frac{i^2 R}{W} = W\frac{R}{E^2}\left(1 + \frac{R}{\frac{E^2}{W} - R}\right)^2 \cong W\frac{R}{E^2}\left(1 + \frac{2R}{\frac{E^2}{W} - R}\right) \ll 1.$$

Эта особенность позволяет описать изменение мощности, потребляемой конкретным сегментом структуры рис. 1, в форме нелинейного дифференциального уравнения с разделяющимися переменными

$$dW = G(W + REP)^2 dn. \quad (2)$$

где REP – мощность потребления репитера, G = 0,11– эмпирический коэффициент пропорциональности.

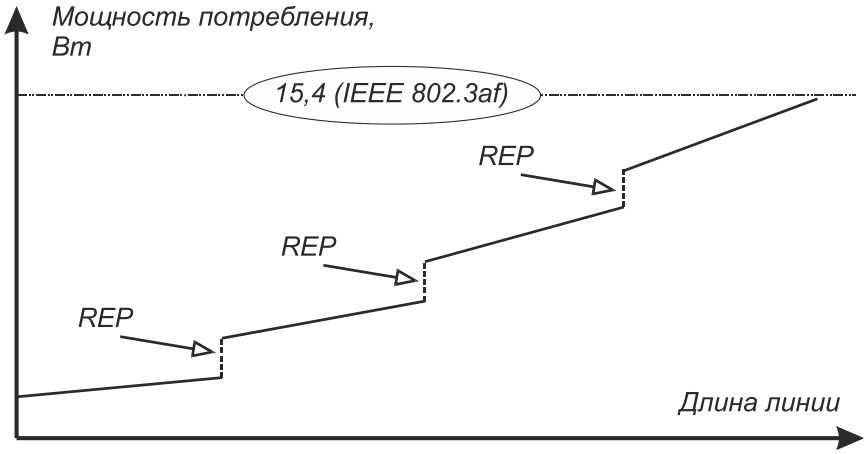


Рис. 3. Характер изменения потребляемой мощности по длине рассчитываемой линии

Решение данного уравнения затруднено из-за разрывного характера функции $W(n)$, что демонстрирует рис. 3. Тогда, переходя от (2) к сумме, получаем следующее окончательное выражение

$$W(n) = W_0 + nRep + G\sum_{j=1}^{j=n}(W_1 + jREP). \quad (3)$$

Здесь через W_0 обозначена мощность потребления терминального POE-устройства, W_1 – мощность потребления первого участка.

Дальнейшую качественную оценку выполним с привлечением (3). Для этого отметим, что $W_0 \approx G\sum_{j=1}^{j=n}(W_1 + jREP)$. В свою очередь, мощность потребления терминального устройства допустимо положить равной 3 Вт. Тогда предполагая мощность собственного потребления репитера равной $REP = 2$ Вт, получаем оценку максимального количества PoE-репитеров в линии

$$n = (15{,}4 - 2W_{0)})/REP = 4.$$

Максимальная длина составного тракта в случае применения PoE-репитеров составляет 150 м×(n + 1) = 750 м.

Заключение

Применение PoE-репитеров позволяет создавать линии подключения нагрузок класса 1 (мощность не более 4 Вт) длиной вплоть до 750 м.

Линии на основе кабелей из витых пар полностью с применением PoE-репитеров полностью закрывают нишу линий увеличенной протяженности, на которых применение волоконно-оптической техники не выгодно по экономическим причинам.

Основным источником потребления ресурсов мощности инжектора питания PoE на линиях большой длины со структурой рассматриваемой разновидности становится репитеры.

В качестве коммутаторов систем PoE с увеличенной дальностью действия должны использоваться High Power устройства с бюджетом мощности 15,4×*n* Вт, где *n* – количество портов, поддерживающих технологию PoE.

Список используемых источников

1. Семенов А. Б., Артюшенко В. М. Анализ современных технологических тенденций развития классических структурированных кабельных систем // Информационно-технологический вестник. 2023. № 2 (36). С. 27-39.

2. Артюшенко В. М., Семенов А. Б. Структурированные кабельные системы: проектирование и расчет. М.: Научный консультант, 2025. 580 С. ISBN 978-5-907933-36-1.

3. Семенов А. Б. Как технология PoE меняет подходы к построению и эксплуатации СКС // Вестник связи. 2021. № 8. С. 24-28

4. Семенов А. Б. Вилки полевого оконцевания для формирования линий MPTL // Вестник связи. 2024. № 5. С. 7-10.

5. Семенов А. Гибридные кабели для нижних уровней информационных систем // Первая миля. 2018. № 2 (71). С. 18-22.

6. Семенов А. Технология PoDL – система дистанционного питания для интернета вещей // Первая миля. 2022. № 8 (108). С. 58-63.

METHOD FOR CALCULATING THE MAXIMUM LENGTH OF A CABLE CHANNEL WITH ROE REPEATERS

Semenov A.
Research University Moscow State University of Civil Engineering

The limiting possibilities of RoE repeaters as a means of extending the length of a channel based on twisted pair cables for connecting remote terminal devices to an interbuilding information system are considered. The necessity of using such repeaters at communication ranges over 150 m is substantiated, a model of the corresponding line is proposed, and analytical ratios are obtained that make it possible to perform its engineering calculation. It is concluded that it is possible to achieve the maximum length of the channel at 750 m when using a serial element base to build the line.

Key words: *interbuilding information systems, PoE-repeater, cable channel, subscriber*

УДК 621.396.969
ГРНТИ 47.49.31

ИССЛЕДОВАНИЕ ТОЧНОСТИ ПЕРВИЧНЫХ ДАЛЬНОМЕРНЫХ ИЗМЕРЕНИЙ В СЕТЯХ LTE В УСЛОВИЯХ ОТСУТСТВИЯ ПРЯМОЙ ВИДИМОСТИ

Х. К. Хыа

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

Оценка точности первичных измерений или время прихода сигналов в условиях отсутствия прямой видимости является актуальным и важным вопросом при оценке точности позиционирования в сетях четвертого 4G и пятого 5G поколения. Существующие разные методы определения точности первичных измерений для уменьшения влияния многолучевого распространения. В настоящей работе формализована задача разработки моделирования оценки точности первичных измерений опорных сигналов позиционирования PRS пороговым методом в условиях отсутствия прямой видимости с помощью среды MATLAB.

4G LTE, MATLAB, PRS, корреляционный функции, время прихода сигналов, точность первичных измерений, NLOS, первый пик, пороговый метод.

Многолучевость является одной из основных проблем при выполнении оценки точных дальномерных измерений для позиционирования на основе временя прихода сигналов TOA (Time Of Arrival) или разность времени прихода сигналов TDoA (Time Difference Of Arrival) в городских условиях из-за большого количества отражений и перекрытий прямой видимости LOS (Line-Of-Sight) между базовой станцией и пользовательским оборудованием [1]. Следовательно, необходимы методы подавления многолучевости при определении точности первичных измерений TOA для уменьшения вносимой погрешности измерений в условиях отсутствия прямой видимости NLOS (Non-Line-Of-Sight) [2].

В данной работе рассматривается известный алгоритм оценки точности первичных измерений TOA опорных сигналов позиционирования PRS (Positioning Reference Signal), способный противодействовать или уменьшать влияние многолучевости при определенных условиях.

Широко применяемый дальномерный алгоритм основан на первом пике взаимной корреляции (между принятым и опорным сигналами) [2-5], превышающем заданный порог. Такой метод обычно называют «оценкой по первому пику» или «пороговым методом». Его ключевая особенность –

низкая вычислительная сложность, благодаря чему он широко используется сообществом 3GPP для оценки точности метода наблюдаемой разности времени прихода сигналов OTDoA (Observed Time Difference of Arrival) [2].

При условии точной частотной синхронизации принятый OFDM-сигнал в частотной области для *n*-й поднесущей записывается как [2]:

$$r(n) = H(n)b(n)e^{j\frac{2\pi\tau n}{N}} + w(n)$$

где *H(n)* – частотная характеристика канала, *b(n)* – опорный сигнал, *N* – общее число поднесущих в полосе, τ – временная задержка или точность первичных измерений, $w(n) \sim \mathcal{CN}(0, \sigma_w^2)$ – аддитивный белый гауссовский шум (АБГШ).

Пороговая оценка точности первичных измерений TOA определяется следующим образом [2-5]:

$$\hat{\tau} = \min_{\tau_{min} \le \tau \le \tau_{max}} \{\tau\} \text{ при условии } \Lambda(\tau) \ge \Lambda_{thr}$$

где τ_{min} и τ_{max} – минимальное и максимальное значение оценки точности первичных измерений TOA, Λ_{thr} – пороговое значение функции правдоподобия, а функция правдоподобия имеет вид [2]:

$$\Lambda(\tau) = \left| \sum_{n \in \mathcal{N}} r(n) b^*(n) e^{-j\frac{2\pi n\tau}{N}} \right|^2$$

где N – множество индексов поднесущих пилотного сигнала, $b^*(n)$ – копия опорного сигнала *b(n)*. Диапазон оценки должен быть адекватно определен в соответствии с точностью синхронизации сигнала.

Проблема определения первого пика в функции правдоподобия заключается в установлении порога, выше которого можно предположить, что обнаруженные пики соответствуют путям полезного сигнала. Установка слишком низкого порога вызывает обнаружение пика, который не представляет путь полезного сигнала. С другой стороны, установка слишком высокого порога приводит к тому, что детектор пиков пропускает первый путь, в худшем случае, становится оценки методом максимального правдоподобия. Порог Λ_{thr} может быть вычислен несколькими методами. Данное моделирование приводит оценку точности первичных измерений TOA пороговым методом как указано в [2]: $\Lambda_{thr} \simeq \Lambda_{max}/4$, где Λ_{max} – максимальное значение функции правдоподобия [2].

Моделирование оценки точности первичных измерений TOA для одного PRS OFDM-символа приводит в среде MATLAB [6] с использованием инструментария LTE Toolbox [7] и Communications Toolbox [8]. В начале задаются основные параметры системы и канала, а также определяют конфигурирование параметров базовой станции. Для формирования ресурсной сетки и генерации индексы и символы PRS использоваться функций `lteDLResourceGrid`, `ltePRSIndices`, `ltePRS` с помощью LTE Toolbox. Далее формируются OFDM-символа с PRS и преобразование во временную область с помощью обратного быстрого преобразования Фурье IFFT (Inverse Fast Fourier Transform).

Потом сформированный временной принятый сигнал PRS пропускается через две модели канала: канал с аддитивным белым гауссовским шумом АБГШ и многолучевой канал. При этом используется соответственно функций `awgn` и `comm.RayleighChannel` в Communications Toolbox. Вычисляются корреляционные функции между принятым и опорным сигналами с использованием функции `xcorr`. На рисунке 1 представлены примерные результаты вычисления корреляционных функции одного OFDM-символа для сигналов PRS используемых 100 ресурсных блоков через канал АБГШ и канал EPA (Extended Pedestrian A) с максимальным доплеровским сдвиг 5 Гц.

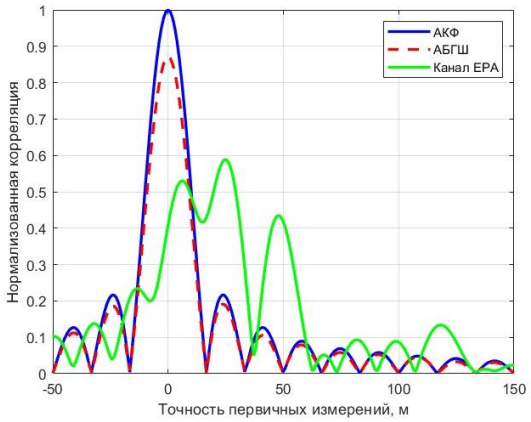


Рис. 1. Корреляционные функции одного PRS OFDM-символа

На основе вычисленных корреляционных функций рассчитывается функция правдоподобия $\Lambda(\tau)$. С помощью функции `findpeaks` находятся все пики в профиле $\Lambda(\tau)$. Определяется первый пик, амплитуда которого превышает порог Λ_{thr}. Временная задержка, соответствующая этому пику, принимается за оценку точности первичных измерений TOA. Пример оценки точности первичных измерений TOA пороговым методом показывает на рис. 2.

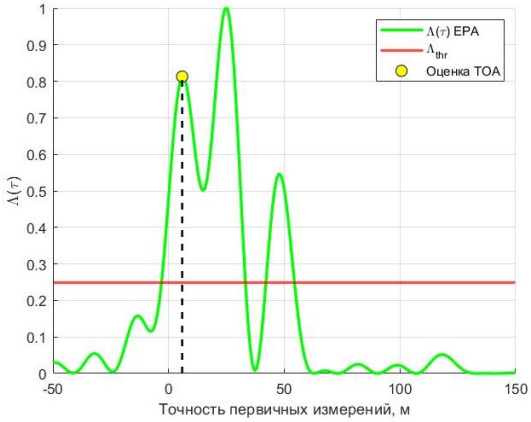


Рис. 2. Пример оценки точности первичных измерений TOA пороговым методом

На скрипт 1 представленные коды для моделирования оценки точности первичных измерений TOA пороговым методом для одного OFDM-символа сигналов LTE PRS с использованием LTE Toolbox и Communications Toolbox.

Скрипт 1: Моделирование АКФ сигнала LTE PRS с использованием LTE Toolbox

```
clear; clc; close all;
 % % Установка параметров
c = 3e8;
snr_db = 5;
 % % Конфигурация eNodeB
enb.NDLRB = 100; % Количество ресурсных блоков (NRB)
enb.NCellID = 0; % Идентификатор соты (Cell ID)
enb.CyclicPrefix = 'Normal'; % Циклический префикс
enb.DuplexMode = 'FDD'; % Режим дуплекса
enb.CellRefP = 1; % Количество антенных портов
enb.NPRSRB = enb.NDLRB; % Количество RB для PRS
enb.IPRS = 0; % Индекс конфигурации PRS
enb.PRSPeriod = 'On'; % Период PRS
enb.NSubframe = 1; % Период субкадра
 % % Генерация сетки ресурсов и сигнала PRS
sfGrid = lteDLResourceGrid(enb);
prs_indices = ltePRSIndices(enb);
prs_symbols = ltePRS(enb);
sfGrid(prs_indices) = prs_symbols;
 % % Извлечение одного PRS OFDM символа (например, символ 4)
symbol_index = 4;
ofdm_symbol = sfGrid(:, symbol_index);
 % % Переход в временную область (увеличенный IFFT для интерполяции)
info = lteOFDMInfo(enb); Fs = info.SamplingRate;
Nfft = info.Nfft * 10; time_domain_signal = ifft(ofdm_symbol, Nfft);
 % % Передача через каналы
rx_awgn = awgn(time_domain_signal, snr_db, 'measured');
path_delays = [0, 30, 70, 90, 110, 190, 410] * 1e-9;
avg_path_gains = [0.0, -1.0, -2.0, -3.0, -8.0, -17.2, -20.8];
epa_channel = comm.RayleighChannel( ...
 'SampleRate', Fs * 10, ...
 'PathDelays', path_delays, ...
```

```
 'AveragePathGains', avg_path_gains, ...
 'MaximumDopplerShift', 5, ...
 'Seed', 17, ...
 'PathGainsOutputPort', true);
[rx_epa_temp, ~] = epa_channel(time_domain_signal);
rx_epa = awgn(rx_epa_temp, snr_db, 'measured');
 % % Расчет корреляционных функций
[autocorr_tx, lags_tx] = xcorr(time_domain_signal, 'normalized');
[cc_awgn, lags_awgn] = xcorr(rx_awgn, time_domain_signal, 'normalized');
[cc_epa, lags_epa] = xcorr(rx_epa, time_domain_signal, 'normalized');
lags_m_tx = lags_tx / (Fs * 10) * c;
lags_m_awgn = lags_awgn / (Fs * 10) * c;
lags_m_epa = lags_epa / (Fs * 10) * c;
figure; plot_range = 300;
plot(lags_m_tx(abs(lags_m_tx) <= plot_range), abs(autocorr_tx(abs(lags_m_tx) <=
plot_range)), 'b', 'LineWidth', 2, 'DisplayName', 'АКФ');
hold on;
plot(lags_m_awgn(abs(lags_m_awgn) <= plot_range), abs(cc_awgn(abs(lags_m_awgn) <=
plot_range)), 'r--', 'LineWidth', 2, 'DisplayName', 'АБГШ');
plot(lags_m_epa(abs(lags_m_epa) <= plot_range), abs(cc_epa(abs(lags_m_epa) <=
plot_range)), 'g', 'LineWidth', 2, 'DisplayName', 'Канал EPA');
xlabel('Точность первичных измерений, м');
ylabel('Нормализованная корреляция');
xlim ([-50 150]); legend; grid on;
 % % Расчет функций правдоподобия
lambda_awgn = abs(cc_awgn).^2;
lambda_epa = abs(cc_epa).^2;
lambda_awgn = lambda_awgn / max(lambda_awgn); % Нормализация профиля
lambda_epa = lambda_epa / max(lambda_epa);
figure; hold on;
plot(lags_m_epa(abs(lags_m_epa)<=plot_range),
lambda_epa(abs(lags_m_epa)<=plot_range), 'g', 'LineWidth', 2, 'DisplayName',
'\Lambda(\tau) EPA');
xlabel('Точность первичных измерений, м'); ylabel('\Lambda(\tau)');
legend; grid on;
 % % Поиск первого пика, превышающего порог, с помощью findpeaks
lambda_thr = max(lambda_epa) / 4;
valid_idx = find(abs(lags_m_epa) <= plot_range); % Выбор области отображения
lags_plot = lags_m_epa(valid_idx);
lambda_plot = lambda_epa(valid_idx);
[peak_vals, peak_locs] = findpeaks(lambda_plot, lags_plot); % Поиск пиков
 % Поиск первого пика, превышающего порог
valid_peak_idx = find(peak_vals > lambda_thr, 1, 'first');
toa_m = peak_locs(valid_peak_idx);
toa_val = peak_vals(valid_peak_idx);
figure(gcf);
yline(lambda_thr, 'r', 'LineWidth', 2, 'DisplayName', '\Lambda_{thr}');
plot(toa_m, toa_val, 'ko', 'MarkerSize', 8, 'MarkerFaceColor', 'y', 'DisplayName',
'Оценка TOA');
line([toa_m toa_m], [0 toa_val], 'Color', 'k', 'LineStyle', '--', 'LineWidth',
1.5, 'HandleVisibility', 'off');
fprintf('TOA пороговым методом: %.2f м\n', toa_m); xlim ([-50 150]);
[max_lambda_value_global, idx_max_lambda_global] = max(lambda_epa);
toa_global_max_m = lags_m_epa(idx_max_lambda_global);
fprintf('TOA MLE: %.2f м\n', toa_global_max_m);
```

Список используемых источников

1. Фокин Г. А. Сетевое позиционирование 5G и вероятностные модели оценки его точности // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 12. С. 4–17. DOI: 10.36724/2072-8735-2020-14-12-4-17

2. del Peral-Rosado J. A., López-Salcedo J. A., Seco-Granados G. Impact of frequency-hopping NB-IoT positioning in 4G and future 5G networks // 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017. P. 815–820. DOI: 10.1109/ICCW.2017.7962759.

3. Хыа Х. К., Фокин Г. А., Рютин К. Е. Позиционирование устройств в сетях LTE. Часть 3. Исследование корреляционных функций опорных сигналов // Информационные технологии и телекоммуникации. 2024. Т. 12. № 4. С. 22–37. DOI: 10.31854/2307-1303-2024-12-4-22-37. EDN:TFCKCC

4. Del Peral-Rosado J. A. Evaluation of the LTE Positioning Capabilities in Realistic Navigation Channels. Universitat Autònoma de Barcelona, 2014. 164 p.

5. Huang M., Zhu C., Dammann A. Maximum likelihood TOA and OTDOA estimation with first arriving path detection for 3GPP LTE system // Transactions on Emerging Telecommunications Technologies. 2014. Vol. 27. DOI: 10.1002/ett.2871.

6. MATLAB. MathWorks. URL: https://www.mathworks.com/ (дата обращения 05.05.2025).

7. LTE Toolbox. MathWorks. URL: https://www.mathworks.com/products/lte.html (Дата обращения 05.05.2025).

8. Communications Toolbox. MathWorks. URL: https://www.mathworks.com/products/communications.html (дата обращения 05.05.2025).

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Фокиным Г. А.

STUDY OF ACCURACY IN PRIMARY DISTANCE MEASUREMENTS USING LTE NETWORKS UNDER NON-LINE-OF-SIGHT CONDITIONS

Hua H.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Estimating the primary measurement accuracy or the arrival time of signals in non-line-of-sight conditions is a relevant and important issue in positioning accuracy estimation in fourth 4G and fifth 5G generation networks. There are different existing methods to determine the accuracy of primary measurements to reduce the influence of multipath propagation. In this paper, we formalize the problem of developing a simulation of primary measurement accuracy estimation modeling of PRS positioning reference signals by threshold method in the non-line-of-sight conditions using MATLAB environment.

Key words: *4G LTE, MATLAB, PRS, correlation function, signal arrival time, primary measurement accuracy, NLOS, first peak, threshold method*

УДК 621.396.969
ГРНТИ 47.49.31

ИССЛЕДОВАНИЕ ТОЧНОСТИ ПЕРВИЧНЫХ ДАЛЬНОМЕРНЫХ ИЗМЕРЕНИЙ В СЕТЯХ LTE В УСЛОВИЯХ ПРЯМОЙ ВИДИМОСТИ

Х. К. Хыа

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

Оценка точности первичных измерений или время прихода сигналов становится более актуальным и важным вопросом для оценки точности позиционирования в сетях четвертого и пятого поколения. Одним из основных используемых методов является метод максимального правдоподобия, который основан на вычислении пика корреляции функции между переданным и принятым сигналами. В настоящей работе формализована задача разработки расчета моделирования автокорреляционной функции опорных сигналов позиционирования в среде MATLAB с использованием инструментария LTE Toolbox в условиях прямой видимости.

4G LTE, MATLAB, PRS, корреляционный функции, время прихода сигналов, точность первичных измерений, LOS.

Метод наблюдаемой разности времени прихода сигналов OTDoA (Observed Time Difference of Arrival) является одним из основных методов для определения местоположения в современных и перспективных сетях связи стандарта LTE (Long Term Evolution) [1]. Опорный сигнал позиционирования PRS (Positioning Reference Signal) используются для демодуляции и уточнения синхронизации, а также для отслеживания изменений временной задержки, что необходимо для позиционирования при движении UE [2].

Одним из широко используемых методов оценки точности времени прихода сигнала TOA (Time Of Arrival) в сетях LTE является метод максимального правдоподобия MLE (Maximum Likelihood Estimation) [3]. Этот метод основан на вычислении пика корреляции функции между переданным и принятым сигналами. В работе [3] нами были представлены математические преобразования, основанные опорными сигналах LTE, для построения и оценки влияния корреляционной функции. В данной работе мы представим разработку программы в среде MATLAB [4] с использованием инструментария LTE Toolbox [5] для более быстрого расчета автокорреляционной функции АКФ опорных сигналов PRS в условиях прямой видимо-

сти LOS (Line of Sight), что позволит оценить ее влияние на точность определения первичных измерений времени прихода сигналов TOA.

Моделирование проводит следующим образом. В начале установить основных параметров базовой станции eNB (Evolved Node B) и конфигурации сигналов PRS. Далее с помощью LTE Toolbox функций `lteDLResourceGrid`, `ltePRSIndices`, `ltePRS` формируются ресурсная сетка LTE, а затем генерируются индексы и символы PRS. Эти символы размещаются в соответствующем субкадре ресурсной сетки. На рисунке 1 представлено размещение PRS-символы в одном ресурсной блоке. PRS-символы представляют собой последовательность Задова-Чу.

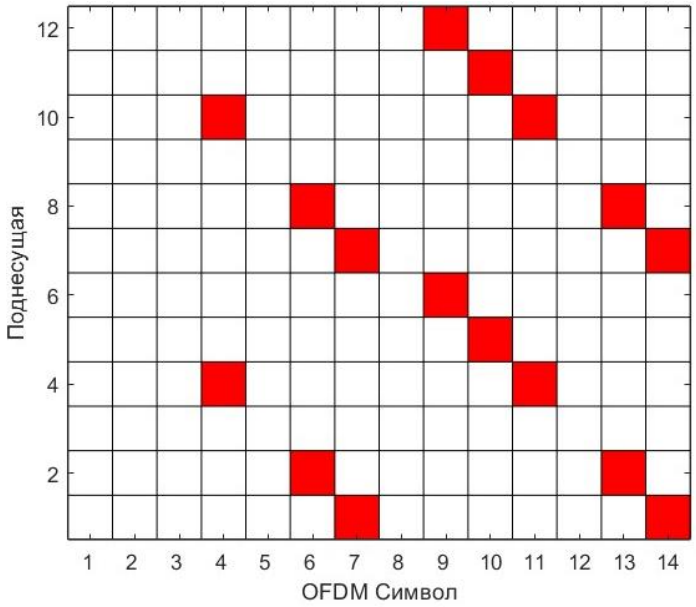


Рис. 1. Размещение PRS на ресурсной сетке (в одном ресурсной блоке РБ)

После формирования символов PRS в частотной области (в ресурсной сетке) выбирается один OFDM (Orthogonal Frequency-Division Multiplexing) символ. Как видно на рисунке 1, первые 3 символа OFDM не имеют сигнала PRS, поэтому в данном случае, указывает на извлечение четвертого символа `ofdm_symbol = grid(:, 4)`. Этот символ затем подвергается обратному быстрому преобразованию Фурье IFFT (Inverse Fast Fourier Transform) для получения сигнала во временной области. Используемое преобразование `ifft(ofdm_symbol, 10 * info.Nfft)` включает десятикратную передискретизацию, что может быть сделано для увеличения разрешения во временной области и потенциального улучшения точности оценки задержки.

Для полученного сигнала во временной области рассчитывается нормализованная автокорреляционная функция с помощью функции `xcorr` в

MATLAB. Нормализация важна для сравнения АКФ сигналов с разной мощностью. АКФ выдает значения задержек `lags` в отсчетах. Для привязки результатов к физическим единицам, значения задержек в отсчетах преобразуются в метры. Это делается с использованием частоты дискретизации сигнала $F_s = 30{,}72$ МГц, полученной из функции `lteOFDMInfo`, и скорости света с$= 3 \cdot 10^8$ м/с. Формула преобразования: $\tau_м = \tau \cdot F_s/c$, где $\tau_м$ – ошибка оценки TOA или точность первичных измерения в метр; τ – ошибка оценки TOA или точность первичных измерения в отсчеты. Присутствие `lags` деления на 10 согласуется с ранее примененной 10-кратной передискретизацией в IFFT, обеспечивая корректный пересчет расстояния.

На скрипт 1 представленные коды для моделирования АКФ сигнала LTE PRS с использованием LTE Toolbox.

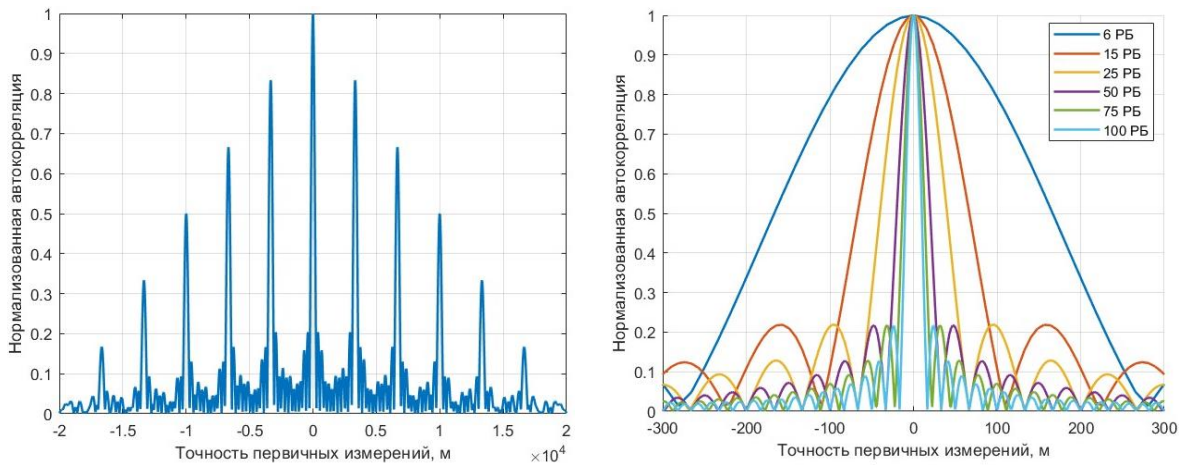
Скрипт 1: Моделирование АКФ сигнала LTE PRS с использованием LTE Toolbox

```
clear; clc; close all;
 % % Установка параметров
rb_values = [6, 15, 25, 50, 75, 100]; % Количество ресурсных блоков
cell_id = 0; % Идентификатор соты
c = 3e8; % Скорость света (метры/секунду)
 % Массивы для хранения данных автокорреляции для сводного графика
all_autocorr_data = cell(1, length(rb_values));
all_lags_meters = cell(1, length(rb_values));
colors = get(gca, 'colororder'); % Получение стандартных цветов MATLAB
 % % Цикл для различных значений RB
for idx = 1:length(rb_values)
 nrb = rb_values(idx);
 % % Конфигурация eNodeB
 enb.NDLRB = nrb; % Количество ресурсных блоков (NRB)
 enb.NCellID = cell_id; % Идентификатор соты (Cell ID)
 enb.CyclicPrefix = 'Normal'; % Циклический префикс
 enb.DuplexMode = 'FDD'; % Режим дуплекса
 enb.CellRefP = 1; % Количество антенных портов
 enb.NPRSRB = nrb; % Количество RB для PRS
 enb.IPRS = 0; % Индекс конфигурации PRS
 enb.PRSPeriod = 'On'; % Период PRS
 % % Генерация сигнала PRS для первого субкадра
 grid = [];
 for nsf = 1
 enb.NSubframe = mod(nsf, 10); % Субкадр 1
 sfGrid = lteDLResourceGrid(enb); % Создание сетки ресурсов
 % Создание индексов и символов PRS, размещение в сетке
 prs_indices = ltePRSIndices(enb);
 prs_symbols = ltePRS(enb);
 sfGrid(prs_indices) = prs_symbols;
 grid = [grid sfGrid];
 end
 % % Извлечение 1-го PRS OFDM символа (символ 4)
 ofdm_symbol = grid(:, 4); % Символ 4
```

```
% Проверка наличия данных в символе
non_zero_elements = sum(abs(ofdm_symbol) > 0);
fprintf('Количество используемых поднесущих в OFDM символе: %d\n', non_zero_ele-
ments);
if non_zero_elements == 0
fprintf('Предупреждение: OFDM символ полностью состоит из нулей для %d RB\n',
nrb);
% Попытка использовать другой символ
for sym_idx = 1:size(grid, 2)
test_symbol = grid(:, sym_idx);
if sum(abs(test_symbol) > 0) > 0
ofdm_symbol = test_symbol;
fprintf('Используется символ %d вместо\n', sym_idx);
break;
end
end
end
% % IFFT для перехода во временную область
info = lteOFDMInfo(enb);
Fs = info.SamplingRate; % Частота дискретизации в Гц
time_domain_signal = ifft(ofdm_symbol, 10 * info.Nfft);
% Использование Nfft из lteOFDMInfo, умноженное на 10
% % Расчет автокорреляционной функции
[autocorr, lags] = xcorr(time_domain_signal, 'normalized');
lags_time = lags / 10 / Fs; % Преобразование задержек из отсчетов в секунды
lags_meters = lags_time * c; % Преобразование времени в расстояние в метрах
% Сохранение данных для сводного графика
all_autocorr_data{idx} = autocorr;
all_lags_meters{idx} = lags_meters;
if nrb == 6
% % Построение графика 1: Размещение PRS на ресурсной сетке
prsGrid = zeros(size(grid));
prsGrid(prs_indices) = abs(prs_symbols);
customColormap = [1 1 1; 1 0 0]; % [белый; красный]
imagesc(abs(prsGrid)); % Отображение сетки
colormap(gca, customColormap);
caxis([0 max(abs(prsGrid(:)))]);
hold on;
[rows, cols] = size(prsGrid);
for i = 0.5:1:(cols+0.5) % Построение вертикальных линий
plot([i i], [0.5 rows+0.5], 'k-', 'LineWidth', 0.5);
end
for i = 0.5:1:(rows+0.5) % Построение горизонтальных линий
plot([0.5 cols+0.5], [i i], 'k-', 'LineWidth', 0.5);
end
hold off;
xlabel('OFDM Символ');
ylabel('Поднесущая');
axis equal;
axis tight;
set(gca, 'YDir', 'normal');
% Ограничение отображения только первыми 12 поднесущими
ylim([0.5 12.5]);
xlim([0.5 14.5]);
set(gca, 'XTick', 1:14, 'XTickLabel', 1:14);
% % Построение графика 2: Автокорреляционная функция сигнала 6 RB
figure;
```

```
 plot(lags_meters, abs(autocorr), 'LineWidth', 1.5, 'Color', colors(1,:));
 grid on;
 xlabel('Точность первичных измерений, м)'); % Ось X в секундах
 ylabel('Нормализованная автокорреляция');
 end
end
 % % Построение графика 3: Все 6 вариантов RB на одном графике
figure;
hold on;
for idx = 1:length(rb_values)
 plot(all_lags_meters{idx}, abs(all_autocorr_data{idx}), ...
 'LineWidth', 1.5, 'Color', colors(idx,:), ...
 'DisplayName', sprintf(' %d RB', rb_values(idx)));
end
hold off;
grid on;
xlabel('Точность первичных измерений, м');
ylabel('Нормализованная автокорреляция');
xlim([-300, 300]);
legend('Location', 'best');
```

Результаты моделирования представлены на рисунке 2.



а) б)

Рис. 2. АКФ сигналов PRS с использованием для а) 6 РБ б) разных количества РБ

Анализ рисунка 2 видно, что с увеличением полосы пропускания главный лепесток АКФ становится уже, что подтверждает повышение точности разрешения оценки расстояния, или, что то же самое, повышение точности первичных измерений времени прихода сигналов [3].

Проведенное исследование с использованием LTE Toolbox наглядно демонстрирует, как параметры сигнала LTE, в частности, количество ресурсных блоков, напрямую влияют на характеристики его автокорреляционной функции. Установлено, что увеличение полосы пропускания сигнала (увеличение количества РБ) приводит к сужению главного лепестка АКФ.

Это является критически важным фактором для повышения точности оценки задержки распространения сигнала и, как следствие, точности определения местоположения.

Список используемых источников

1. Фокин Г. А. Сетевое позиционирование 5G и вероятностные модели оценки его точности // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 12. С. 4–17. doi: 10.36724/2072-8735-2020-14-12-4-17

2. Сиверс М. А., Фокин Г. А., Духовницкий О. Г. Оценка возможностей метода разностно-дальномерного метода позиционирования абонентских станций в системах мобильной связи LTE средствами имитационного моделирования // Информационные технологии моделирования и управления. 2016. Т. 98. № 2. С. 149–160.

3. Хыа Х. К., Фокин Г. А., Рютин К. Е. Позиционирование устройств в сетях LTE. Часть 3. Исследование корреляционных функций опорных сигналов // Информационные технологии и телекоммуникации. 2024. Т. 12. № 4. С. 22–37. DOI: 10.31854/2307-1303-2024-12-4-22-37. EDN:TFCKCCMATLAB.

4. MathWorks. URL: https://www.mathworks.com/ (дата обращения 05.05.2025).

5. LTE Toolbox. MathWorks. URL: https://www.mathworks.com/products/lte.html (дата обращения 05.05.2025).

Статья представлена научным руководителем, профессором кафедры БТС СПбГУТ, доктором технических наук, доцентом Фокиным Г. А.

STUDY OF ACCURACY IN PRIMARY DISTANCE MEASUREMENTS USING LTE NETWORKS UNDER LINE-OF-SIGHT CONDITIONS

Hua H.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Estimating the accuracy of primary measurements or the arrival time of signals is becoming a more relevant and important issue for estimating the positioning accuracy in fourth and fifth generation networks. One of the main methods used is the maximum likelihood method, which is based on calculating the peak correlation function between the transmitted and received signals. This paper formalizes the problem of developing the calculation of modeling the autocorrelation function of positioning reference signals in MATLAB environment using LTE Toolbox in line-of-sight conditions.

Key words: *4G LTE, MATLAB, PRS, correlation function, signal arrival time, primary measurement accuracy, LOS*

РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ И РОБОТОТЕХНИКА

УДК 004.946
ГРНТИ 28.17.33

СЦЕНАРИЙ УСТАНОВЛЕНИЯ ОТНОШЕНИЙ МЕЖДУ АГЕНТАМИ В ДЕЦЕНТРАЛИЗОВАННОЙ КИБЕРФИЗИЧЕСКОЙ СРЕДЕ

С. В. Акимов, Г. В. Верхова

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

Представлены результаты исследований, выполненных авторами, в области формирования единой киберфизической среды, формируемой из локальных интероперабельных киберсред. Рассмотрен сценарий установления отношений между агентами, который является инвариантным к случаю размещения агентов в одной или нескольких киберсредах. Показано, что наиболее общий способ установления отношений между агентами основан на формировании окружения агента в виде прокси-агентов, с которыми агент имеет те или иные отношения.

единая киберфизическая среда, интеграция локальный интероперабельных киберсред, установление отношений между агентами, децентрализованная киберфизическая среда, friend-to-friend

Введение

Современные реалии требуют создание новых и развития существующих технологий, которые смогут удовлетворить потребности постиндустриального общества в формировании единой киберфизической среды, стирающей грань между физическим и виртуальным мирами. Учитывая эволюцию развития информационных технологий, в частности, Интернета и Всемирной паутины, можно предположить, что такая киберфизическая среда будет иметь децентрализованную архитектуру [1-4], что с одной стороны обеспечит ей высокую стабильность и адаптивность, а, с другой – позволить ограничить монополию владельцев цифровых площадок, предоставляющих в настоящий момент подавляющую часть цифровых сервисов. Од-

ной из основных функций единой киберсреды является обеспечение решения задач исследования, проектирования и управления, что может быть достигнуто за счет использования многоаспектных моделей [5]. Одной из важнейших задач создания единой киберфизической среды является сведение к минимуму рутинных операций.

Требования к архитектуре децентрализованной киберфизической среды

Децентрализованная киберфизическая среда должна обеспечить бесшовное киберпространство, формируемое из отдельных интероперабельных киберсред [6], что требует создания особой модели, положенной в ее основание, которая идеологически максимально приближена к friend-to-friend. Особенностью данной модели является автономное представление агента с формируемым окружением, заданным прокси-агентами, с которым агент устанавливает те или иные виды связей и осуществляет какое-либо информационное взаимодействие:

$$A \stackrel{\text{def}}{=} \langle Card_{Syber}, A_{Proxy} \rangle,$$

где $Card_{Syber}$ – цифровая визитка агента A, которая содержит необходимую информацию для идентификации агента и коммуникации с ним, включая информацию о конечных точках, которые обеспечивают доступ к функционалу, доступному прокси-агентам из его окружения A_{Proxy};

A_{Proxy} – прокси-агенты, входящие в окружение агента A; через прокси-агентов осуществляются все виды коммуникаций с ними. Прокси-агенты содержат всю необходимую информацию, необходимую для идентификации агента, представленного прокси-агентом, а также обеспечением всех видов коммуникаций с ним.

Агенты представляют принципалов, в роли которых могут выступать физические и юридические лица, объединения физических и юридических лиц, природные, техногенные и природно-техногенные объекты и системы. Агенты со своим окружением формируют коммуникационный слой единой децентрализованной киберфизической среды, и обеспечивают функции коммуникаций между агентами, включая установление отношений и управление правами доступом. Помимо коммуникационного слоя, киберфизическая среда содержит слой многоаспектных моделей, которые содержат всю необходимую информацию о принципалах, представленных в среде агентами, а также слой цифровых двойников, который создается путем реализации синхронизации моделей с состоянием принципалов.

Сценарий установления отношений между агентами

Одним из важнейших механизмов функционирования децентрализованной киберсреды является сценарий установления отношений между агентами, который должен осуществляться единообразным способом, вне зависимости от того, расположены агенты в рамках одной локальной киберсреды, или в различных киберсредах, которые могут быть никак не связаны между собой. В частном случае локальная киберсреда может быть сформирована на компьютере пользователя, с установленным специализированным программным обеспечением. Рассмотрим сценарий установления отношений между агентами.

Шаг 1. Пользователь, представленный агентом в своей киберсреде (Киберсреда А), копирует ссылку на конечную точку, обеспечивающую возврат цифровой визитки коагента, с которым предполагается установить связь. Цифровая визитка помимо краткой информации о коагенте, содержит коллекцию конечных точек, обеспечивающих основные действия с коагентом в рамках его киберсреды (Киберсреда В). Используя механизм своей киберсреды, агент запускает процесс установления отношений с коагентом.

Шаг 2. Киберсреда А посредством метода GET протокола HTTP получает цифровую визитку коагента, после чего создает прокси-агента, представляющего коагента, и связывает его с агентом, запустившим процесс установления связи.

Шаг 3. Используя информацию о конечных точках из цифровой визитки коагента, Киберсреда А, используя метод POST, отправляет запрос на установление связи в Киберсреду В, результатом выполнения которого является создание в ней прокси-агента агента, инициировавшего процесс установления связи, ассоциированной с коагентом. Коагенту отправляется запрос на подтверждения связи с заданным типом отношений.

Шаг 4. В случае подтверждения коагентом согласия на установление связи, в прокси-агенте агента, инициирующего запрос на установление связи, изменятся статус отношения на «Подтвержденный», после чего Киберсреда В отправляет с помощью метода POST в Киберсреду А информацию о подтверждении установления связи.

Шаг 5. Киберсреда А изменяет статус информации об отношении между агентом и коагентом подтвержденным, на чем данный сценарий завершается.

Заключение

Предложенный в статье сценарий установления отношений между агентами в децентрализованной киберфизической среде является одним из

важнейших механизмов формирования единого киберфизического пространства постиндустриального общества. В данный момент на кафедре систем автоматизации и робототехники продолжаются исследования в области формирования единой киберфизической среды, включая создание прототипа ядра, на котором отрабатывается представленный сценарий.

Список используемых источников

1. Haralambous Ya., Lenca Ph. Beyond the semantic Web: towards an implicit pragmatic Web and a Web of social representations // Future Internet. 2023. Т. 15. № 7. С. 239.

2. Alkhathami M. Cluster-Based Data Sharing for Web 3.0 in Intelligent Transportation Systems // Journal of Web Engineering. 2024. Vol. 23. № 7. PP. 1025-1040. DOI: 10.13052/jwe1540-9589.2375.

3. Rastogi A. Integrating Web 3.0 Technologies for Advanced Information Retrieval Systems in the Educational Sector // 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI), Greater Noida, India. 2023. PP. 200-204. DOI: 10.1109/ICCSAI59793.2023.10421149.

4. La Cava L., Greco S., Tagarelli A. Understanding the growth of the Fediverse through the lens of Mastodon // Applied Network Science. 2021. Т. 6. № 1. С. 64.

5. Акимов С. В., Меткин Н. П. Архитектура среды многоаспектного моделирования для автоматизации решения задач исследования, проектирования и управления // Вопросы радиоэлектроники. 2013. Т. 1. № 1. С. 32-40.

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

SCENARIO FOR ESTABLISHING RELATIONSHIPS BETWEEN AGENTS IN A DECENTRALIZED CYBER-PHYSICAL ENVIRONMENT

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

The results of the studies performed by the authors in the field of formation of a single cyber-physical environment formed from local interoperable cyber environments are presented. A scenario of establishing relations between agents is considered, which is invariant to the case of placing agents in one or several cyber environments. It is shown that the most general way of establishing relations between agents is based on the formation of the agent's environment in the form of proxy agents with which the agent has certain relations.

Key words: *unified cyber-physical environment, integration of local interoperable cyber environments, establishing relationships between agents, decentralized cyber-physical environment, friend-to-friend.*

УДК 004.946
ГРНТИ 28.17.33

МОДЕЛИРОВАНИЕ ЛОГИЧЕСКИХ И ТОПОЛОГИЧЕСКИХ ОТНОШЕНИЙ МЕЖДУ ПРИРОДНО-ТЕХНОГЕННЫМИ ГЕОСИСТЕМАМИ

С. В. Акимов, Г. В. Верхова

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

Приведены результаты исследований в области представления различных типов отношений в рамках децентрализованных многоаспектных геоинформационных моделей. Показано, что топологические и прочие отношения между геосистемами могут быть представлены с единых методологических позиций с помощью прокси-моделей, которые формируют окружение природно-техногенной геосистемы. Данный подход позволит формировать сложные модели и цифровые двойники геосистем, имеющих иерархическую структуру, а также задавать и обрабатывать любые виды отношений между геосистемами. Рассмотрен вопрос информационного наполнения моделей с помощью методов искусственного интеллекта, включая генерацию, дополненную поиском. Показаны преимущества децентрализованного геоинформационного моделирования для формирования единого геоинформационного пространства по сравнению с традиционными геоинформационными системами.

природно-техногенные геосистемы, геоинформационные модели, топологические отношения, логические отношения, многоаспектное моделирование, искусственный интеллект в геоинформационных технологиях, единая геоинформационная киберсреда

Геоинформационные системы (ГИС) находят все более широкое применение во всех сферах человеческой деятельности. В настоящий момент времени на рынке представлено большое разнообразие ГИС, обладающих мощными средствами геоинформационного моделирования. Тем не менее, существующие ГИС не в полном объеме поддерживают механизмы задания топологических и логических (семантических) отношений между пространственными объектами [1-2]. Другими важными проблемами являются развитие коллаборативных ГИС [3], методов многоаспектного геоинформационного моделирования [4] и создания цифровых двойников природно-техногенных геосистем [5-6].

Рассмотренные проблемы могут быть решены только на базе развития методов и технологий, изначально ориентированных на создание децентрализованных моделей природно-техногенных геосистем. В данной статье предложен метод моделирование логических и топологических отношений между природно-техногенными геосистемами, который может быть поло-

жен в основу создания единой геоинформационной киберсреды. Суть метода заключается в децентрализованном геоинформационном моделировании, в котором каждая природно-техногенная геосистема моделируется полностью независимо от других систем, а все виды отношений задаются с помощью прокси-моделей геосистем, входящих в ее окружение (рис. 1).

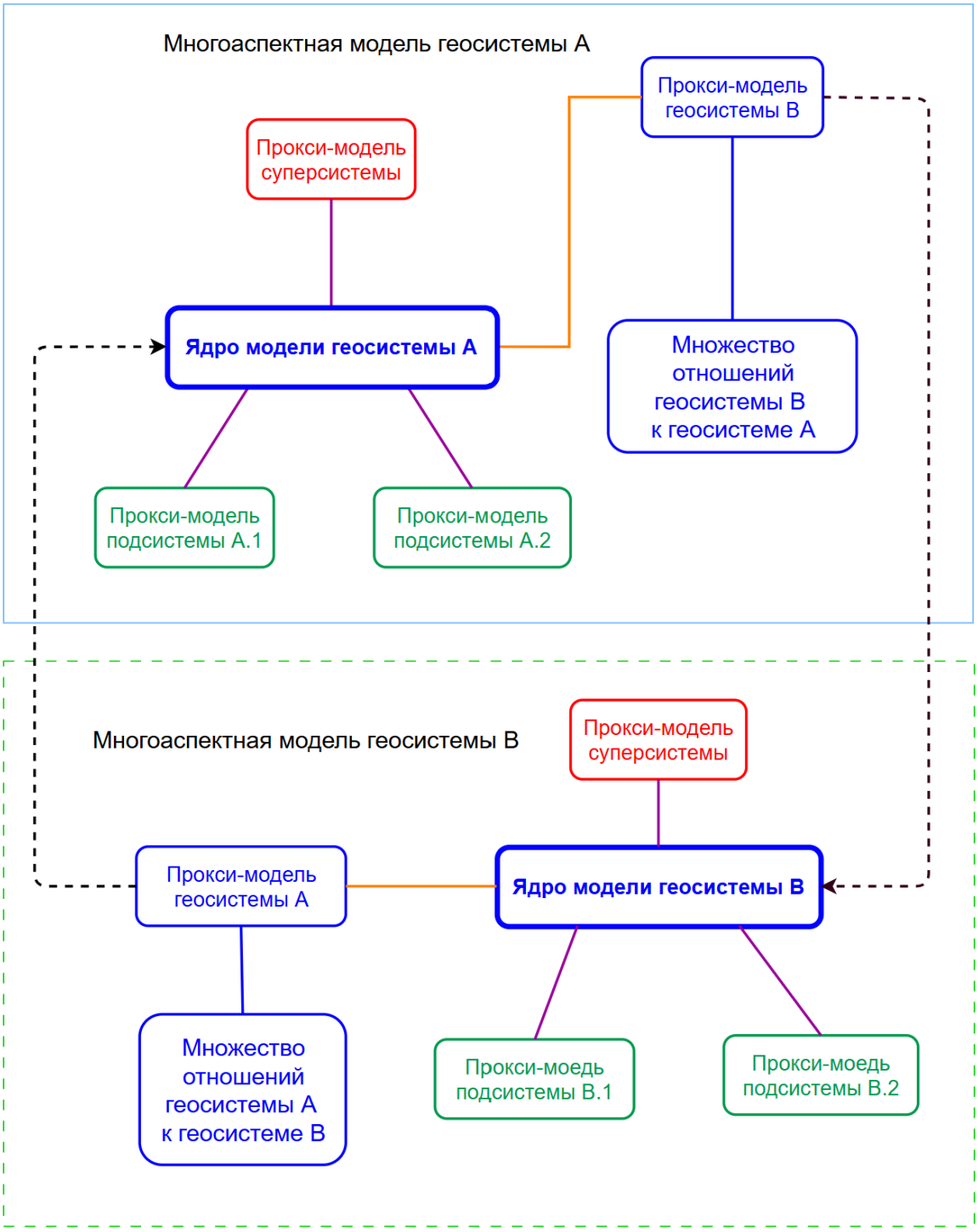


Рис. 1. Децентрализованное моделирование логических и топологических отношения между природно-техногенными геосистемами

Такой подход полностью соответствует концепции Web 3.0, обеспечивая любые виды коллабораций при создании геоинформационного киберпространства. Прокси-модели связаны с моделями геосистем, которые они представляет, что позволяет выполнять синхронизацию данных между геосистемами, а, при необходимости, и репликацию данных. Аналогичным образом может быть реализована синхронизация моделей с геосистемами, которых они представляют, тем самым превращая геоинформационные модели в цифровые двойники геосистем. Моделирование отношений между геосистемами позволяет сформировать связанное геоинформационное пространство, интегрируя информацию из различных источников с использованием методов искусственного интеллекта, включая RAG.

Предложенный метод моделирования логических и топологических отношений между природно-техногенными геосистемами обеспечит:

– представление любых видов отношений между природно-техногенными геосистемами с единых методологических позиций;
– единообразное представление логических и топологических отношений между природно-техногенными геосистемами вне зависимости от того, находятся они в рамках одной киберсреды или в разных киберсредах;
– коллаборативное многоаспектное геоинформационное моделирование;
– возможность формирования цифровых двойников природно-техногенных геосистем путем создания слоя кибернетических и физических пространств;
– возможность информационного наполнения моделей с помощью методов искусственного интеллекта, включая генерацию, дополненную поиском (RAG-системы).

Список используемых источников

1. Гордиенко Л. В. Формирование топологических правил для описания пространственных отношений объектов системы передачи электроэнергии в геоинформационной системе // Инженерный вестник Дона, 2020. № 12 (72). С. 442-449.

2. Андрианов Д. Е. Создание метода представления топологических отношений в трехмерном пространстве для задач городских ГИС // Геоинформатика. 2007. № 2. С. 1-3.

3. Аль Савафи М. Х., Перькова М. В. Оценка территории города по факторам с применением коллаборативных информационных технологий // Инновационная траектория развития современных наук о земле: становление, задачи, прогнозы: материалы междун. науч. конф., Белгород, БГТУ имени В. Г. Шухова, 2020. С. 3-7.

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

5. Нуриев Б. А., Атнабаев А. Ф. Разработка цифровых двойников для формирования экосистемы «Умный кампус УУНИТ» на базе ГИС-технологий // Информационные технологии. Проблемы и решения. 2024. № 3 (28). С. 100-105.

6. Сорокин А. Ю., Иванов Е. В., Безвесильная А. А., Климкин А. А. Подходе к повышению точности цифровых двойников рельефа местности на основе анализа цифровых пространственных геоданных // Научные и образовательные проблемы гражданской защиты. 2022. № 1 (52). С. 50-61.

MODELING LOGICAL AND TOPOLOGICAL RELATIONSHIPS BETWEEN NATURAL AND MAN-MADE GEOSYSTEMS

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

The article presents the results of studies in the field of representation of various types of relations within decentralized multi-aspect geoinformation models. It is shown that topological and other relations between geosystems can be represented from a single methodological position using proxy models that form the environment of a natural and man-made geosystem. This approach will allow forming complex models and digital twins of geosystems with a hierarchical structure, as well as setting and processing any types of relations between geosystems. The issue of information filling of models using artificial intelligence methods, including generation supplemented by search, is considered. The advantages of decentralized geoinformation modeling for the formation of a single geoinformation space are shown compared to traditional geoinformation systems.

Key words: *natural and man-made geosystems, geoinformation models, topological relations, logical relations, multi-aspect modeling, artificial intelligence in geoinformation technologies, unified geoinformation cyberenvironment*

УДК 621.396.962.23
ГРНТИ 47.49.29

АЛГОРИТМ META-ESPRIT ДЛЯ СОВМЕСТНОЙ ОЦЕНКИ СКОРОСТИ И УГЛА МЕСТА ЦЕЛЕЙ В ДОППЛЕРОВСКОЙ ЛОКАЦИИ

Р. А. Алли

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

Предложена модификация алгоритма ESPRIT для одновременного определения угла места и скорости вдоль оси визирования малоразмерных БПЛА в условиях ограниченного углового разрешения РЛС. Алгоритм основан на сингулярном разложении двумерного массива данных с раздельным анализом пространственных и временных компонент. Экспериментально показано ускорение обработки относительно классического алгоритма ESPRIT при погрешности оценки угла 0.5° и скорости 0.3 м/с, что приемлемо для задач ближней радиолокации (< 1 км). Алгоритм применим в охранных системах, автомобильных локаторах и интерфейсах радиолокационного распознавания жестов.

сверхразрешение, микродоплеровские признаки, ESPRIT, MUSIC, угловое разрешение, допплеровская локация, SVD-разложение

Распространение малоразмерных беспилотных летательных аппаратов (БПЛА) сделало задачи их обнаружения и классификации как никогда актуальными. Микроволновые допплеровские радиолокационные станции (РЛС) позволяют идентифицировать тип цели по характеристикам допплеровской модуляции, однако требуют высокого углового разрешения. Традиционные методы повышения разрешения ведут к уменьшению радиуса обзора или удорожанию аппаратуры.

Цель работы – разработка алгоритма совместной оценки угла места и скорости цели на основе модификации ESPRIT [1-3] с оптимизацией вычислительной сложности.

Алгоритмы сверхразрешения позволяют увеличить угловое разрешение в несколько раз без модификации оборудования. Многие алгоритмы сверхразрешения стали классикой радиолокации и уже давно активно применяются и совершенствуются. Наиболее востребованные алгоритмы – MUSIC [4, 5], ESPRIT [1-3] и их модификации. Поскольку решаемая задача предполагает работу в режиме реального времени в зашумленной среде с некоррелированными сигналами, наибольший интерес представляют алгоритмы MUSIC и ESPRIT, с которыми будет проводиться сравнение.

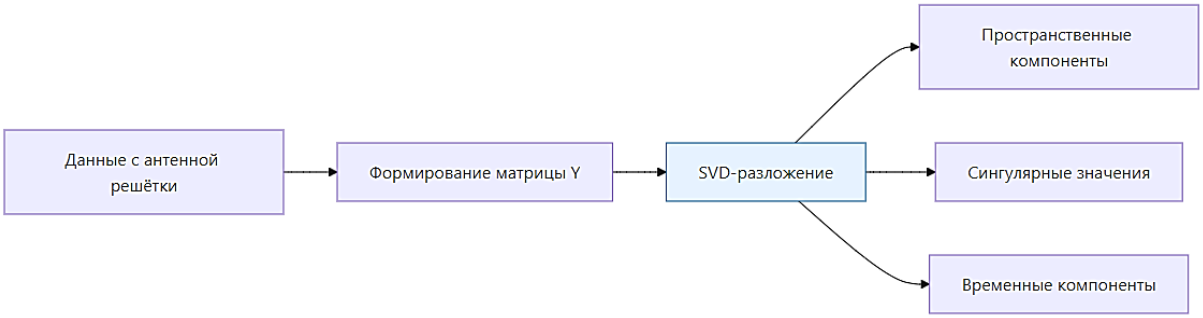


Рис. 1. Структурная схема математической модели

Исходные данные радиолокационного наблюдения формируют матрицу сигналов Y (рис.1):

$$\boldsymbol{Y} \in \mathbb{C}^{N_a \times N_p}, \quad (1)$$

где N_a – число антенных элементов, N_p – количество импульсов. SVD – сингулярное разложение матрицы [5]: $\mathbb{C}$ – пространство комплексных чисел.

Производится сингулярное разложение матрицы согласно уравнению:

$$\boldsymbol{Y} = \boldsymbol{U\Sigma V}^H, \quad (2)$$

где компоненты разложения обозначены как:

U – унитарная матрица пространственных компонент, где каждая компонента – антенна. Ее размерность $N_a \times N_a$.

$\sum$ – диагональная матрица сингулярных значений, размерностью $N_a \times N_p$.

$\mathbf{V}^{\mathrm{H}}$ – унитарная матрица временных компоненты (импульсов), размерность матрицы $N_p \times N_p$. Эрмитово сопряженная.

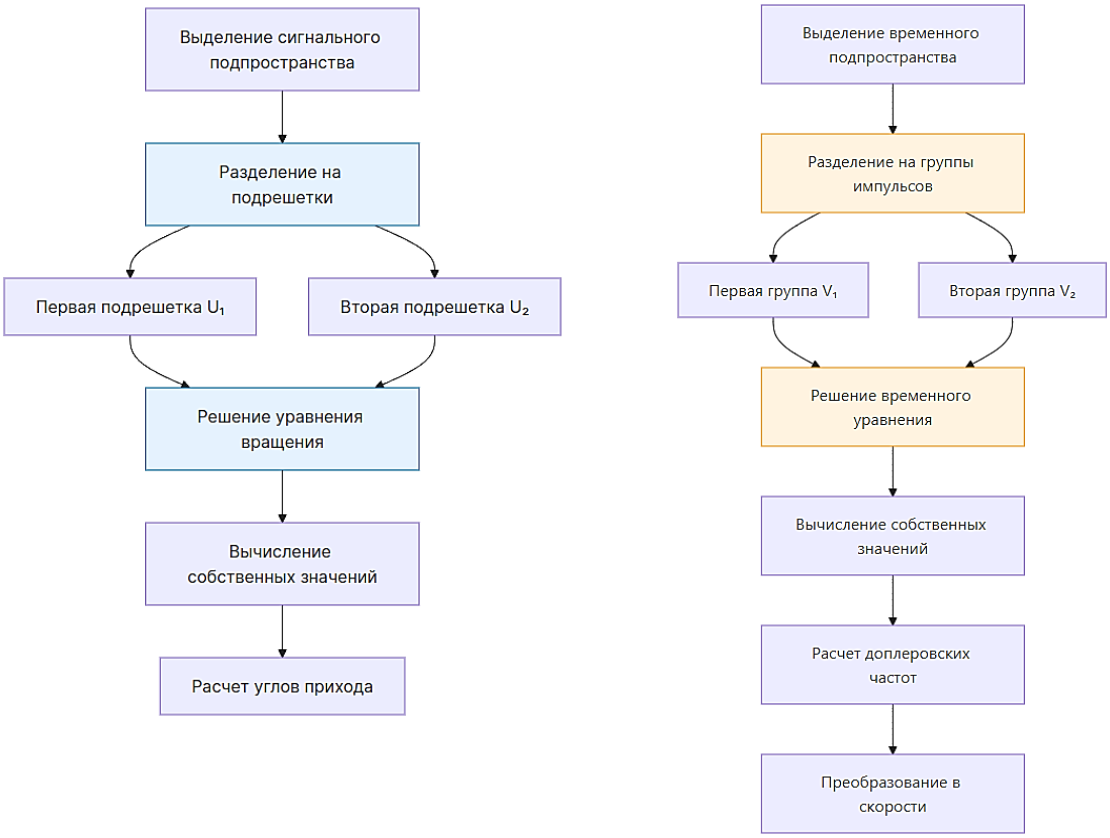
Сингулярные значения служат для определения количества источников. Диагональная матрица $\sum$ содержит их в порядке убывания:

$$\boldsymbol{\Sigma} = \begin{matrix} \sigma_1 & 0 & 0 \\ 0 & \sigma_2 & 0 \\ 0 & 0 & \sigma_3 \end{matrix}, \quad (3)$$

$$\text{где } \sigma_1 \geq \sigma_2 \geq \sigma_3 \geq 0 \quad (4)$$

В идеальном случае (без шума источники не коррелированы) положительными будет столько сигм, сколько источников (если источники не коррелированные). Однако шум приводит к тому, что все сигмы становятся больше нуля и тогда количество источников определяется по разности между сигмами. Если σ_3 и/или σ_2 значительно меньше сигмы σ_1, то они считаются шумом. Недостатком такого подхода является полная неустойчивость к нестационарным помехам, близким по амплитуде к сигналу источ-

ников. Его планируется исправить на следующих этапах обработки сигнала в рамках будущих работ.



а) б)

Рис. 2. а) Алгоритм расчета пространственных компонент. б) Алгоритм расчета временных компонент

На рисунке 2.а представлен набор операций, которые проводятся с пространственными компонентами. Вот как это выглядит по шагам:

1. Формирование сигнального пространства по d наибольшим сингулярным значениям:

$$U_s = U[:,1:d] \tag{5}$$

2. Разделение на перекрывающиеся подрешетки:

$$U_1 = U_s[1:,N_a-1,:] \tag{6}$$
$$U_2 = U_s[2:,N_a,:] \tag{7}$$

3. Решение уравнения сдвиговой инвариантности:

$$\Psi = (U_1^H U_1)^{-1} U_1^H U_2 \tag{8}$$

4. Расчет углов прихода через собственные значения λ_i матрицы Ψ:

$$\theta_i = arcsin\left(-\frac{arg(\lambda_i)\cdot\lambda}{2\pi\Delta}\right) \quad (9)$$

На рисунке 2.б представлен набор операций, которые выполняются с временными компонентами. Вот шаги алгоритма:

1. Формирование временного пространства по d наибольшим сингулярным значениям:

$$V_s = V[:,1:d] \quad (10)$$

2. Разделение на группы импульсов:

$$V_1 = V_s[1:,N_p-1,:] \quad (11)$$
$$V_2 = V_s[2:,N_p,:] \quad (12)$$

3. Решение уравнения сдвиговой инвариантности:

$$\Phi = (V_1^H V)^{-1} V_1^H V_2 \quad (13)$$

1. 4. Расчет допплеровских частот через собственные значения μ_i матрицы Ф:

$$f_{d,i} = \frac{arg(\mu_i)}{2\pi\Delta t} \quad (14)$$

5. Преобразование в скорости:

$$v_i = \frac{f_{d,i}\cdot c}{2f_c} \quad (15)$$

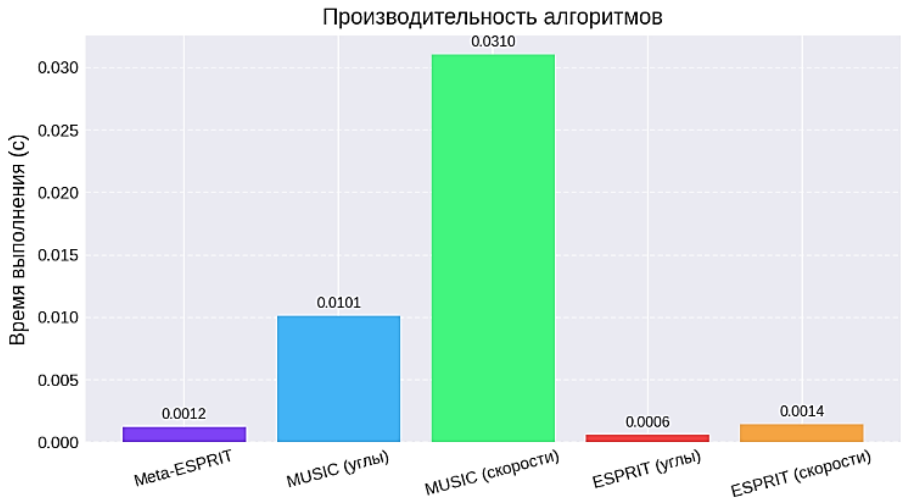


Рис. 3. Результат компьютерного моделирования работы алгоритмов. Оценка времени.

На рисунке 3 показан результат моделирования скорости работы алгоритмов [1-5] и их сравнение с предложенным. Предложенный алгоритм,

определяя скорость и угол места цели одновременно по скорости работы аналогичен ESPRIT который определяет только один параметр.

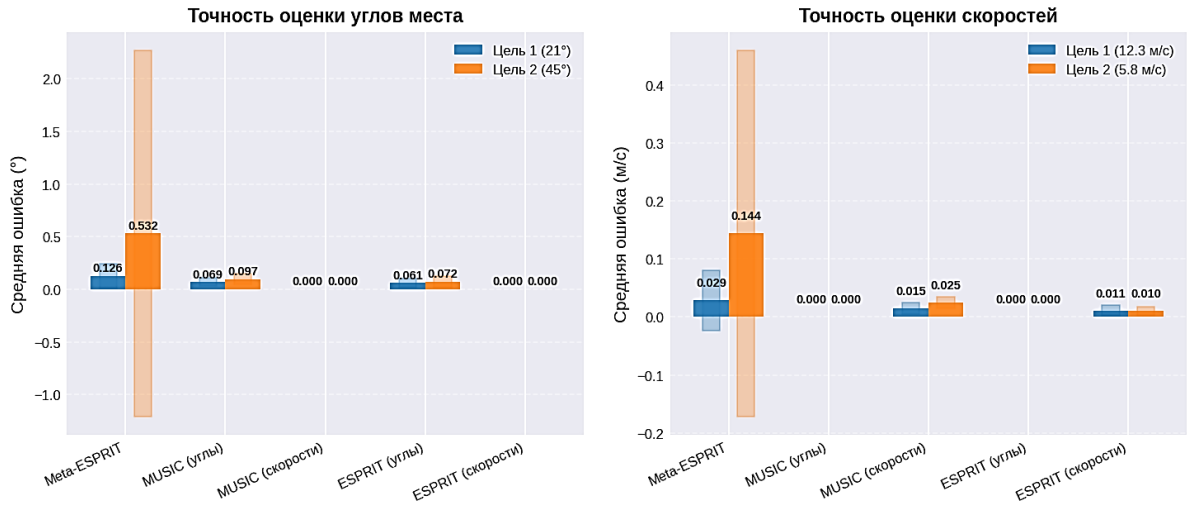


Рис. 4. Результат компьютерного моделирования работы алгоритмов. Оценка точности

Проведена оценка точности по углу места каждого из представленных на рисунке 4 алгоритмов [1-5] для сравнительного анализа. Алгоритмы с нулевой ошибкой с пространственной областью не работают. Хотя Meta-ESPRIT уступает в точности MUSIC (0.5° против 0.2°), погрешность приемлема для задач ближней локации (< 1 км). Для измерения скорости цели картина аналогична.

В ходе проведенного исследования разработан алгоритм совмещенной оценки скорости и угла места цели. Его удалось оптимизировать до уровня современных алгоритмов сверхразрешения по производительности, но он уступает им в точности. Алгоритм позволит уменьшить задержки при обработке радиолокационных целей увеличив оперативность обнаружения, распознавания и сопровождения летательных аппаратов.

Список используемых источников

1. Cao R., Zhang X. Joint angle and Doppler frequency estimation of coherent targets in monostatic MIMO radar // International Journal of Electronics. 2014. Т. 102, № 5. С. 792-814. DOI: 10.1080/00207217.2014.942804.

2. Roy R., Kailath T. ESPRIT – Estimation of signal parameters via rotational invariance techniques // IEEE Transactions on Acoustics, Speech, and Signal Processing. 1989. Vol. 37. № 7. PP. 984-995. DOI: 10.1109/29.32276.

3. Gong S., Xiong H., Peng M., Ding X., Tang H. Joint DOD and DOA estimation for bistatic multiple-input multiple-output radar target discrimination based on improved unitary ESPRIT method // IET Communications. 2018. Т. 12. № 12. С. 1397-1405. DOI: 10.1049/iet-com.2017.1086.

4. Schmidt R. Multiple emitter location and signal parameter estimation // IEEE Transactions on Antennas and Propagation. 1986. Vol. 34. № 3. PP. 276-280. DOI: 10.1109/TAP.1986.1143830.

5. Music Algorithm Explained via Frequency Time Analysis // arXiv. 2024. URL: https://arxiv.org/html/2502.17875v1 (дата обращения 11.07.2025). DOI: 10.48550/arXiv.2502.17875. – arXiv:2502.17875v1 [eess.SP].

Статья представлена научным руководителем, заведующим кафедры РТ СПбГУТ, кандидатом технических наук, доцентом К. О. Коровиным.

META-ESPRIT ALGORITHM FOR JOINT VELOCITY AND ELEVATION ANGLE ESTIMATION OF TARGETS IN DOPPLER LOCATION

Alli R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

A modification of the ESPRIT algorithm is proposed for simultaneous estimation of both elevation angle and radial velocity of small unmanned aerial vehicles (UAVs) under limited angular resolution conditions. Unlike classical ESPRIT, which estimates only one parameter, the proposed Meta-ESPRIT processes spatial and temporal signal components concurrently through singular value decomposition (SVD) of a 2D data array. Experimental results demonstrate that this dual-parameter estimation achieves comparable processing speed to single-parameter ESPRIT while maintaining angular accuracy of 0.5° and velocity accuracy of 0.3 m/s – critical for short-range radar applications (<1 km). The method is suitable for security systems, automotive radars, and radar-based gesture interfaces where real-time multi-parameter tracking is essential.

Key words: *super-resolution, micro-Doppler signatures, ESPRIT, MUSIC, angular resolution, Doppler location, SVD decomposition*

УДК 548.31
ГРНТИ 47.09.48

СОВРЕМЕННЫЕ БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ И ВИЗУАЛИЗАЦИИ СТРУКТУР КВАЗИКРИСТАЛЛОВ

А. И. Арсирий

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

Собраны данные о доступных наиболее распространенных применяемых базовых аппаратных (атомно-силовая, электронная микроскопия, рентгеновская дифракция, спектроскопия) и программных ресурсах (специальные программы и программные пакеты, такие как VESTA, Ovito, и CrystalMaker, а также LAMMPS, GROMACS), которые могут быть использованы при исследовании, изучении, построении и визуализации структур квазикристаллов. Приведены их области применения достоинства и недостатки.

квазикристаллы, методы исследования, визуализация структур

Квазикристаллы представляют собой уникальный класс материалов, обладающих дальним порядком, но не являются классической периодической структурой. Это открытие, совершенное в 1982 году, привело к революции в науке о материалах и к новым возможностям в области нанотехнологий и кристаллографии. Одним из ключевых аспектов изучения квазикристаллов является их визуализация, которая позволяет лучше понять их сложную структуру и свойства. В данной статье рассматриваются различные способы и ресурсы визуализации структур квазикристаллов, а также инструменты, используемые учеными для исследования этих материалов.

Прежде чем погружаться в способы визуализации, важно понимать, что представляет собой структура квазикристаллов. В отличие от обычных кристаллов, структура которых повторяется в трехмерном пространстве в виде периодического узора, квазикристаллы демонстрируют долгосрочные корреляции между атомами, но при этом не имеют строгой периодичности. Это открытие привело к развитию новых методов представления квазикристаллических структур, таких как использование теории квазипериодических решеток и моделей многомерных симметрий [1].

Аппаратные возможности исследования квазикристаллов

Существует несколько основных методов исследования структур квазикристаллов, которые позволяют, путем взаимодействия с исследуемыми образцами наглядно представить их сложные геометрические и симметрические свойства.

Микроскопия атомного силового микроскопа. Одним из наиболее популярных методов для изучения квазикристаллов является атомно-силовая микроскопия (AFM). Использование метода дает возможность рассмотреть поверхность большинства материалов с высоким разрешением, вплоть до атомарного масштаба. AFM дает картину топографической структуры внешнего слоя квазикристаллов, что интересно и важно для изучения их микроструктуры и особенностей строения поверхностных слоев. Преимущества AFM заключаются в его высокой чувствительности и возможности исследования образцов в различных условиях. Однако его ограничением является сравнительно небольшая область исследования, что может затруднять изучение более крупных образцов квазикристаллов.

Электронная микроскопия (SEM, TEM). Сканирующая электронная микроскопия (SEM) и трансмиссионная электронная микроскопия (TEM) – наиболее используемые аппаратные комплексы визуализации в изучения структуры квазикристаллов. SEM показывает состояние и структуру поверхности образцов с высоким разрешением, а TEM – исследует внутреннюю структуру с возможностью наблюдения атомного уровня. Для изучения квазикристаллических структур эти методы позволяют не только выявить атомарное расположение элементов, но и исследовать их ориентацию в трехмерном пространстве. Особенно полезна комбинация этих двух методов, так как они дополняют друг друга: SEM позволяет получить детализированные изображения поверхности, а TEM – изучить более глубокие слои материала.

Рентгеновская дифракция (XRD) – является одним из наиболее мощных методов исследования квазикристаллических структур. При этом методе анализируется поведение рентгеновских лучей, проходящих через образец. Образцом может быть порошок, монокристалл или тонкие пленки исследуемого материала. Для квазикристаллов характерны необычные дифракционные паттерны, которые могут быть использованы для определения симметрий, характерных для этих материалов. Рентгеновская дифракция позволяет выявить информацию о кратных симметриках и симметриях, присущих квазикристаллическим структурам. Однако она имеет свои огра-

ничения, так как квазикристаллы в большинстве имеют сложную симметрию, которую сложно раскрыть с помощью традиционной рентгеновской дифракции, предпочтительнее пользоваться более продвинутыми методами, например, нейтронной дифракцией.

Спектроскопия, в основном именно электронная спектроскопия, но, возможно, и спектроскопия рентгеновских лучей, также часто используются в изучении квазикристаллов. Эти методы дают информацию не только о химическом составе и электронной структуре, но и локальных состояниях атомов в материале. Использование спектроскопии выявляет точечные особенности взаимодействий атомов в квазикристаллических структурах.

Ресурсы, применяемые для моделирования и визуализации квазикристаллических структур

Молекулярное динамическое моделирование и моделирование с использованием методов плотностного функционала (DFT), удобный и широко применяемый инструмент для визуализации и анализа структур квазикристаллов. Экспериментальные исследования и математическое моделирование, объединенные с помощью этих комплектов, дают данные для составления прогнозов по составу материала, а созданные их виртуальные модели позволяют предсказывать их поведение в различных условиях.

Для лучшего восприятия и визуализации данных эксперимента и расчетов существуют специальные программы и программные пакеты, наиболее удобные и не требующие оплаты, это VESTA, Ovito, и CrystalMaker, которые позволяют получить трехмерные визуализации атомарных структур, в том числе и квазикристаллических, а уже с их помощью можно исследовать симметрические свойства и поведение атомов в сложных многомерных решетках.

Студенты и исследователи сейчас могут использовать как онлайн-ресурсы, так и офлайн продукты. Для работы с квазикристаллами предпочтительнее онлайн-ресурсы. Приведем несколько популярных и широко используемых платформ:

VESTA – это мощное программное обеспечение для визуализации атомных структур и расчета большинства основных структурных параметров. Это приложение активно используется для представления облика квазикристаллических решеток и построения трехмерных моделей. VESTA поддерживает большинство форматов данных и является удобным инструментом для работы с экспериментальными данными [2]. На рис. 1 приведен

пример визуализации кристаллической структуры с использованием пакета VESTA.

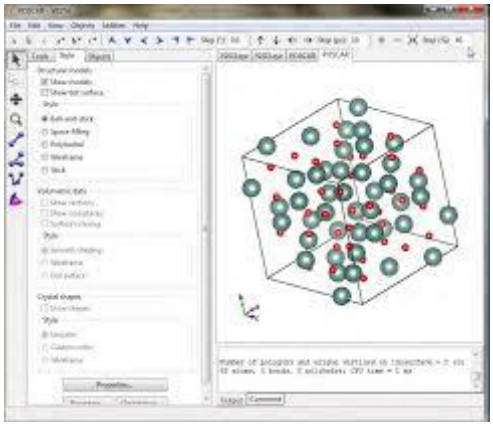


Рис. 1. Визуализация кристаллической структуры с помощью программного обеспечения VESTA

Ovito – это еще одно популярное программное обеспечение для анализа и визуализации данных молекулярных динамических симуляций. Оно позволяет исследовать квазикристаллические материалы и взаимодействия в них. Ovito удобен разнообразием своих инструментов для работы в нем, что делает его незаменимым для ученых, работающих с квазикристаллическими структурами [3]. На рис. 2 приведен пример визуализации кристаллической структуры с использованием пакета Ovito.

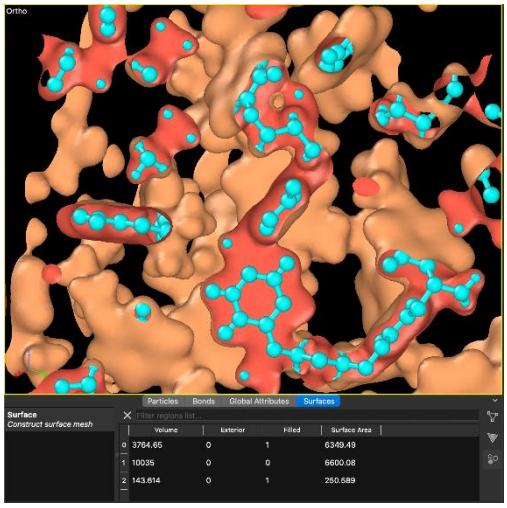


Рис. 2. Визуализация кристаллической структуры с помощью программного обеспечения Ovito

CrystalMaker – это программа, используемая для создания и визуализации в основном именно закономерных – кристаллических и квазикристаллических структур. Она позволяет анализировать данные дифракции различного генезиса, а также строить детализированные трехмерные модели,

что делает ее полезной для исследования квазикристаллических материалов [4]. На рис. 3 приведен пример визуализации кристаллической структуры с использованием пакета CrystalMaker.

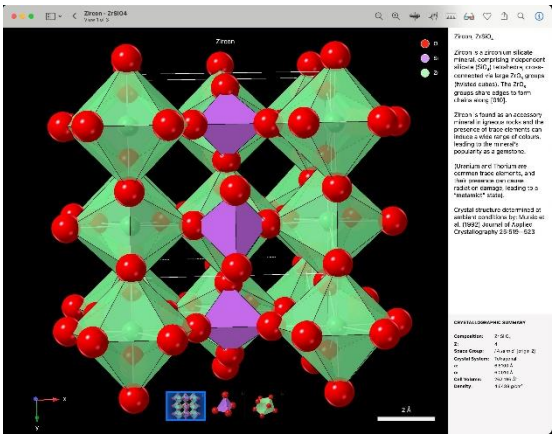


Рис. 3. Визуализация кристаллической структуры с помощью программного обеспечения CrystalMaker

Программные пакеты для молекулярного моделирования

Молекулярные симуляции, такие как программы LAMMPS [5], GROMACS [6] и других, могут быть использованы для создания и изучения моделей квазикристаллов. Эти программные пакеты предоставляют удобные инструменты для проведения симуляций на атомарном уровне для создания модели материалов с квазипериодическими структурами все они являются общедоступными в своей базовой версии.

Таким образом, решение весьма сложной задачи – построение структуры квазикристаллов, объединяющей экспериментальные (атомно-силовая микроскопия, электронная микроскопия, рентгеновская дифракция и спектроскопия) и математические методы анализа, строится на использовании различных методик и инструментов для их исследования и последующей визуализации, они позволяют изучить эти материалы с различных сторон, раскрывая их уникальные свойства. В числе наиболее применимых и доступных современных компьютерных программ и ресурсов – такие как VESTA, Ovito и CrystalMaker – позволяют ученым создавать трехмерные модели и проводить детальный анализ структур квазикристаллов, открывая новые горизонты для науки о материалах.

Список использованных источников

1. Мадисон А. Е. Симметрия квазикристаллов // Физика твердого тела. 2013. Т.55. № 4. С.784-796

2. Программное обеспечение для визуализации атомных структур и расчета различных структурных параметров VESTA. URL: https://jp-minerals.org/vesta/en/ (дата обращения 14.06.2025).

3. Программное обеспечение для анализа и визуализации данных молекулярных динамических симуляций Ovito. URL: https://www.ovito.org/ (дата обращения 14.06.2025).

4. Программа для создания и визуализации кристаллических и квазикристаллических структур CrystalMaker. URL: https://crystalmaker.com/ (дата обращения 14.06.2025).

5. Программный пакет для молекулярного моделирования https://www.lammps.org/ (дата обращения 14.06.2025).

6. Программный пакет для молекулярного моделирования. URL: https://www.gromacs.org/ (дата обращения 14.06.2025).

MODERN BASIC METHODS OF RESEARCH AND VISUALIZATION OF QUASI-CRYSTALS STRUCTURES

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

Data on the most widely used basic hardware (atomic force, electron microscopy, X-ray diffraction, spectroscopy) and software resources (special programs and software packages such as VESTA, Ovito, and CrystalMaker, as well as LAMMPS, GROMACS) that can be used in the study, investigation, construction and visualization of quasicrystal structures are collected. Their areas of application, advantages and disadvantages are given.

Key words: *quasicrystals, research methods, visualization of structures*

УДК 623.458
ГРНТИ 49.43.37

ОСОБЕННОСТИ АППАРАТНОЙ И ПРОГРАММНОЙ РЕАЛИЗАЦИИ SDR-МОДУЛЕЙ В БПЛА

П. А. Берестовский, П. В. Воробьев, В. И. Татаринов

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

В данной статье рассматривается возможность использования БПЛА не только как средства обнаружения, но и как инструмента для установления связи между человеком и наземным удаленным пунктом связи

программно-определяемое радио, SDR, беспилотный летательный аппарат, микрокомпьютер, отсутствие прямой видимости

Беспилотные летательные аппараты (БПЛА) популярны во многих областях применения благодаря своей гибкости и относительно низкой цене. БПЛА представляют собой недорогое решение для наблюдения и обнаружения людей после чрезвычайных ситуаций, нуждающимся в спасении, и спасательной командой. Предложенное решение должно обеспечивать визуальное обнаружение с использованием стандартных и тепловизионных камер, позволяя обнаруживать людей в условиях низкой видимости.

БПЛА стали очень популярными благодаря недавним достижениям в области систем управления, навигации и оборудования для получения изображений. Они используются в различных областях и предоставляют эффективное и недорогое решение для выполнения сложных задач, ранее требовавших более комплексных систем. БПЛА имеют множество возможных применений – от аэрофотосъемки, картографирования, наблюдения, поисково-спасательных операций до доставки грузов.

Некоторые исследования в области управления БПЛА в условиях отсутствия прямой видимости предполагают использование мобильных сетей для передачи управляющего сигнала при дистанционном управлении БПЛА [1] или для дистанционного зондирования местности [2]. Свойства мобильных сетей могут быть использованы также для различных задач обнаружения и локализации. Одним из возможных применений является обнаружение источника сигнала, исходящего от мобильного терминала. Местоположение мобильного терминала можно интерпретировать как место

нахождения человека, нуждающегося в спасении, или человека, с которым необходимо установить связь в случае отсутствия покрытия мобильной сети.

В последние годы было проведено множество исследований в области использования БПЛА, способных обнаруживать сигналы мобильных сетей [3,4].

В данной статье исследуется возможность использования программно-конфигурируемого радио (SDR), способного работать в роли базовой станции GSM, установленной на БПЛА, для связи с человеком в условиях отсутствия покрытия мобильной сети. Базовые станции GSM на БПЛА, построенные с использованием SDR, начали разрабатываться только в последние годы и все еще совершенствуются для применения в реальных условиях [5]. Помимо SDR и процессора, предложенная платформа БПЛА оснащена стандартной видеокамерой и тепловизионной камерой, способной работать в условиях низкой видимости.

Для такой платформы следует выбрать квадрокоптер или гексакоптер, поскольку их можно использовать в городских условиях, и на рынке существует множество готовых решений. Некоторые их представители способны переносить около 10 кг полезной нагрузки при общей взлетной массе более 20 кг. При использовании аккумулятора емкостью 22 А/ч можно обеспечить полет продолжительностью 18–20 минут.

БПЛА обычно оснащается модулем GPS, который тесно взаимодействует с контроллером полета. Такая система позволяет добиться точности полета порядка нескольких метров, поскольку однолучевой GPS может определять местоположение с точностью 2–5 м.

SDR-устройства стали очень популярными благодаря своей низкой цене и высокой способности имитировать дорогостоящее оборудование с помощью программных реализаций. Для моделирования поведения базовой станции GSM идеально подойдет платформа LimeSDR, способную работать в диапазоне 900 МГц.

Хотя мобильная связь уже достигла пятого поколения, и системы 4G широко доступны, GSM по-прежнему активно используется как наиболее устойчивая из технологий. Она ограничена в скорости передачи данных, но позволяет устанавливать связь даже при очень слабом уровне сигнала (-102 дБм). Благодаря этим свойствам и относительной простоте реализации, GSM лучше всего подходит в качестве основы для связи с использованием SDR, установленного на БПЛА.

Аппаратная часть базовой станции, установленной на БПЛА, состоит преимущественно из LimeSDR, одноплатного компьютера, антенн, источника питания, кабелей, разъемов, корпуса и крепежных элементов.

Схема прототипа базовой станции показан на рисунке 1. В будущих версиях будет реализован ряд улучшений, главным образом направленных на увеличение дальности обнаружения.

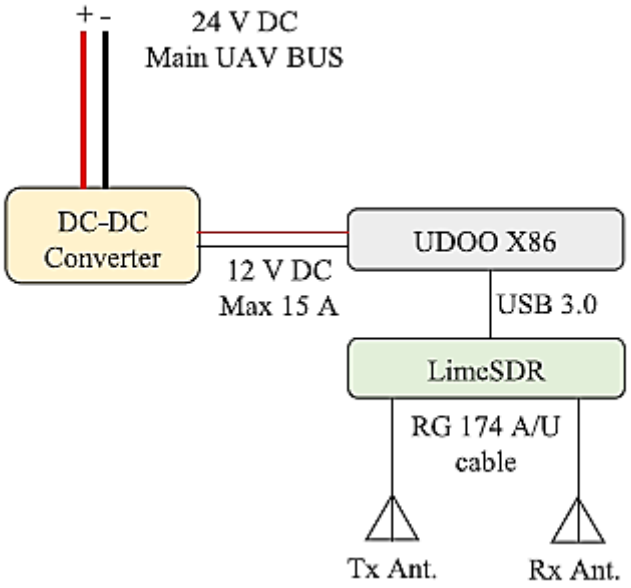


Рис. 1. Схема прототипа БС

Базовую станцию GSM целесообразно строить вокруг одноплатного компьютера, типа UDOO X86 Ultra. Его основными преимуществами является относительно высокая производительность и малые размер и вес (130 граммов). UDOO X86 Ultra оснащен четырехъядерным процессором Intel Pentium N3710, работающим до 2.56 ГГц, и 8 ГБ двухканальной оперативной памяти DDR3L. Также имеется интерфейс USB 3.0, важный для быстрой передачи данных с LimeSDR. Компьютер потребляет до 3 А тока при напряжении 12 В.

Устройство основано на LMS7002M – программируемом радиочастотном трансивере, который может принимать и передавать сигналы в диапазоне от 100 кГц до 3.8 ГГц. Основная функция ПЛИС LimeSDR – передача цифровых данных на компьютер через встроенный USB 3.0.

LimeSDR поставляется с программным обеспечением LimeSuite для программирования и настройки ПЛИС. Питание осуществляется либо через USB-порт (максимум 4.5 Вт, 0.9 А при 5 В для USB 3.0), либо через внешний

источник питания (6–12 В), в этом случае максимальное потребление составляет 25 Вт, хотя в нормальном режиме такая мощность никогда не требуется. По спецификациям максимальная выходная мощность составляет 10 дБм, однако это верно только для непрерывной волны на определенных частотах. На частоте 900 МГц выходная мощность составляет около 6 дБм.

На стороне программного обеспечения базовая станция работает под управлением Ubuntu 18.04 LTS. Основной набор программ, реализующих компоненты инфраструктуры мобильной сети, был разработан проектом Osmocom (open-source mobile communications). Этот проект направлен на создание свободного и открытого программного обеспечения для реализации стека протоколов GSM и сетевой архитектуры. Это особенно полезно для исследований, так как классические телекоммуникационные производители реализуют сетевые компоненты как проприетарное платное оборудование и ПО, без возможности их понять или модифицировать.

Весь софт Osmocom доступен в виде исходного кода и предкомпилированных двоичных файлов для множества архитектур и сценариев использования. Для наших целей мы собрали все из последних версий исходников.

Помимо стека Osmocom, целесообразно использовать – Asterisk. Asterisk – это программное обеспечение с открытым исходным кодом, реализующее частную АТС, которую авторы использовали для маршрутизации вызовов между мобильными телефонами. Оно предоставляет широкие возможности, которые будут полезны в дальнейших разработках.

Основная задача полевых испытаний – определить, будет ли созданная базовая станция работать в реальных условиях. Дополнительными задачами были проверка дальности обнаружения мобильной станции, измерение энергопотребления и, как следствие, повышение продолжительности полета БПЛА.

Список использованных источников

1. AbdElHamid A., Zong P. Development of UAV teleoperation virtual environment based-on GSM networks and real weather effects // International Journal of Aeronautical and Space Sciences. 2015. Vol. 16. PP. 463–474.

2. Daniel K. и Wietfeld C. Using public network infrastructures for UAV remote sensing in civilian security operations // Technical University of Dortmund, Germany, 2011.

3. Wolfe V., Frobe W., Shrinivasan V., Hsieh T.-Y. и Gates H. M. Feasibility study of utilizing 4G LTE signals in combination with unmanned aerial vehicles for the purpose of search and rescue of avalanche victims (Increment 1) // University of Colorado at Boulder, Research Report, 2014.

4. Стецко В. Ю. Аппаратно-программный комплекс обнаружения слабых сигналов квадрокоптера на базе SDR канала передачи данных на фоне непреднамеренных помех // Компьютерные системы и сети: сборник статей 59-й научной конференции аспирантов, магистрантов и студентов, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. Минск, 2023. С. 107–115.

5. Будкин Н. Д. Средства обнаружения беспилотных летательных аппаратов и перспективы их развития // Вестник науки. 2024. № 12 (81).

6. Семенюк А. В., Сычев И. В., Алферов Ю. В., Громов Ю. Ю., Шатских В. В., Губсков Ю. А. Обеспечение информационной безопасности через анализ радиоэлектронной обстановки беспилотного летательного аппарата с помощью программного обеспечения SDR-приемника // НиКа. 2020.

FEATURES OF HARDWARE AND SOFTWARE IMPLEMENTATION OF SDR MODULES IN UAVS

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

This paper discusses the possibility of using UAVs not only as a means of detection, but also as a tool for establishing communication between a person and a ground-based remote communication center.

Key words: *Software-defined radio, SDR, unmanned aerial vehicle, microcomputer, lack of line of sight*

УДК 623.458
ГРНТИ 49.43.37

ТЕХНИЧЕСКИЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ БПЛА И ДАЛЬНЕЙШИЕ ПЕРСПЕКТИВЫ ИХ РАЗВИТИЯ

П. А. Берестовский, П. В. Воробьев, Д. Ф. Ткачев

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

В статье рассматриваются решения по противодействию беспилотным летательным аппаратам, применяющие в своей работе технологии искусственного интеллекта. Приведены основные уязвимости протоколов связи БПЛА.

радиоэлектронная борьба, машинное зрение, искусственный интеллект, протокол связи, защита объектов

Основным способом противодействия БПЛА является огневое поражение, но если рассматривать поражение квадрокоптеров и FPV-дронов, то из-за высокой скорости и маневренности они являются сложной для обнаружения и поражения [1] (подавления) мишенью, поскольку из-за малых размеров радары комплексов ПВО их «не видят», а по причине наличия электродвигателей – ПЗРК не захватывают настолько слабоконтрастную тепловую цель.

То же самое можно сказать и о БПЛА самолетного типа. Использование композитных, радиопрозрачных материалов делают их невидимыми для радиолокационных комплексов, а использование электрических двигателей снижает шум и тепловую контрастность. В этих условиях ведущую роль в противодействии БПЛА играет радиоэлектронное подавление средствами радиоэлектронной борьбы (РЭБ).

Комплексы (средства) РЭБ с БПЛА осуществляют радиоподавление радиоэлектронных средств БПЛА путем воздействия на них преднамеренными радиопомехами [2]. При этом, помеховое воздействие формируется на все БПЛА, которые находятся в зоне подавления средств РЭБ.

В условиях стремительного развития технологий беспилотной авиации, особенно автономных БПЛА, оснащенных алгоритмами машинного обучения и адаптивными системами навигации, возникает необходимость в разработке и внедрении комплексных мер обеспечения безопасности критически важных объектов систем связи. Эти меры должны охватывать как фи-

зическую защиту инфраструктуры, так и киберпространственные аспекты, при этом активное использование технологий искусственного интеллекта позволяет значительно повысить эффективность систем противодействия.

Для повышения защищенности объектов связи от потенциального использования БПЛА в разведывательных или диверсионных целях применяются системы компьютерного зрения, основанные на глубоких нейронных сетях [3]. Примером может служить система DroneShield, которая использует комбинацию акустических сенсоров, камер и радиолокационных средств, обрабатываемых ИИ-алгоритмами в реальном времени. Такая система позволяет не только обнаруживать наличие БПЛА, но и прогнозировать траекторию его движения, а также оценивать потенциальную угрозу на основе анализа поведенческих паттернов. Интеграция с системами физической безопасности (например, перехватывающими дронами типа AUDS – Anti-UAV Defence System) позволяет реализовать многоуровневую стратегию противодействия.

Еще одним важным направлением является защита информационных систем, обеспечивающих функционирование объектов связи, от кибератак, осуществляемых через автономные БПЛА. Искусственный интеллект может быть использован в системах обнаружения вторжений (IDS/IPS), где методы машинного обучения, такие как ансамблевые алгоритмы (например, XGBoost, Random Forest) и рекуррентные нейросети (RNN), применяются для выявления аномалий в сетевом трафике, которые могут указывать на попытку взлома или передачу данных через скрытые каналы связи.

Еще одним примером является израильская система Skylock, которая применяется на стратегически важных объектах, включая телекоммуникационные узлы. Skylock использует ИИ для анализа поведенческих паттернов полетов БПЛА: если дрон демонстрирует поведение, характерное для разведывательных миссий (например, зависание над одной точкой или повторяющийся маршрут), система автоматически активирует средства противодействия – от радиоподавления до запуска перехватчика.

Автономные БПЛА часто используют следующие протоколы связи:

– Wi-Fi (IEEE 802.11) – используется для передачи видеопотока и управления дроном на ближних дистанциях.

– Bluetooth Low Energy (BLE) – для взаимодействия с мобильными устройствами или для инициализации старта полета.

– LoRaWAN/SigFox – применяются в промышленных и сельскохозяйственных дронах для передачи данных на дальние расстояния.

– GPS/GLONASS – для навигации и автономного маршрутизирования.

– 5G/LTE-M – в перспективных моделях для высокоскоростной передачи данных и удаленного управления.

Каждый из этих протоколов имеет свои уязвимости. Например, Wi-Fi уязвим к атакам типа deauthentication attack, которые могут быть реализованы с помощью программно-определяемых радиоплатформ (например, HackRF One). GPS может быть подвержен спуфингу, когда дрон получает ложные координаты. BLE уязвим к прослушиванию и воспроизведению (replay attack).

Для противодействия этим угрозам технологии ИИ применяются следующим образом:

Обнаружение аномалий в трафике: системы на основе рекуррентных нейросетей (RNN) и трансформеров (Transformer) анализируют временные последовательности сетевых данных, выявляя отклонения от нормального поведения. Например, проект Darktrace Industrial успешно применяется на объектах связи в Европе для обнаружения несанкционированного доступа через BLE-интерфейсы.

Генерация помех и имитация сигналов: ИИ-алгоритмы позволяют генерировать сложные помехи, адаптированные под конкретный протокол. Например, исследовательская группа MIT Lincoln Laboratory разработала систему, в которой нейросеть обучается эмулировать сигналы GPS для создания "ложных дорожек", направляющих БПЛА в безопасную зону.

Перспективным направлением развития является создание унифицированных платформ, объединяющих радиоэлектронные, видеоаналитические и киберзащитные компоненты под управлением единой ИИ-модели. Это позволит не только повысить оперативность реагирования, но и обеспечить адаптивность к быстро меняющимся угрозам, включая использование автономных БПЛА в качестве носителей киберугроз.

Таким образом, применение технологий искусственного интеллекта в сфере защиты объектов систем связи от автономных БПЛА открывает широкие возможности для повышения уровня безопасности. Конкретные примеры внедрения таких систем (DroneShield, Skylock, Стопдрон) показывают их эффективность в реальных условиях. Одновременно с этим, анализ используемых БПЛА протоколов связи (Wi-Fi, BLE, LoRa, GPS, 5G) позволяет целенаправленно разрабатывать ИИ-решения для противодействия наиболее уязвимым аспектам беспилотных систем.

Список использованных источников

1. Макаренко С. И., Тимошенко А. В. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 2. Огневое поражение и физический перехват // Системы управления, связи и безопасности. 2020. № 1.

2. Голубчиков С. В., Новиков В. К., Пономаренко А. В., Митрофанова С. В. Показатели и критерии оценки эффективности ведения радиоэлектронной борьбы в современных условиях // Воздушно-космические силы. Теория и практика. 2024. №3 1

3. Бондаренко В. А., Каплинский Г. Э., Павлова В. А., Тупиков В. А. Алгоритмическое обеспечение оптико-электронных систем комплекса защиты объектов от беспилотных летательных аппаратов // Известия ЮФУ. Технические науки. 2018. № 1 (195).

TECHNICAL MEANS OF COUNTERING UAVS AND FURTHER PROSPECTS FOR THEIR DEVELOPMENT

Berestovski P., Vorobyev P., Tkachev D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

This paper discusses solutions for countering unmanned aerial vehicles that use artificial intelligence technologies. The main vulnerabilities of UAV communication protocols are presented.

Key words: *electronic warfare, machine vision, artificial intelligence, communication protocol, object protection*

УДК 621.391.1
ГРНТИ 49.33.29

АНАЛИЗ ПОМЕХОУСТОЙЧИВОСТИ ПРИЕМА ДВОИЧНЫХ ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ Δ-СЛОЯ НЕРАЗЛИЧИМОСТИ В УСЛОВИЯХ ПРЕДНАМЕРЕННЫХ ПОМЕХ И ГАУССОВСКОГО ШУМА

В. Р. Бикбулатов, А. О. Негурица, А. М. Чуднов

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

Для приема фазоманипулированных псевдослучайных сигналов в условиях гауссовского шума вводится Δ-слой неразличимости (решающее правило приема). С учетом использования методов теории статических решений, динамического программирования и теории информации показано влияние решающего правила при приеме двоичных сигналов и аддитивных преднамеренной помехи и гауссовского шума.

система передачи информации, гауссовский шум, алгоритмы приема сигналов, рандомизированное решающее правило, гарантированная вероятность ошибки, база сигнала

В условиях современных вооруженных конфликтов, сопровождающихся активным применением средств радиоэлектронной борьбы, обеспечение устойчивой связи является критически важной задачей. Эффективность систем передачи информации (СПИ) напрямую зависит от их способности сохранять надежность обмена данными при воздействии внешних факторов, в частности – преднамеренных помех, создаваемых противником с целью деградации или полного подавления каналов связи.

Особенно остро эта проблема проявляется в военных и специальных системах, где противник может реализовать оптимальную стратегию постановки помех, опираясь на знания о параметрах защищаемой системы. Исходя из исследований [1-6], в таких условиях классические алгоритмы приема, включая широко используемый приемник Котельникова, не всегда обеспечивают достаточный уровень помехоустойчивости.

Одним из альтернативных подходов является использование рандомизированного решающего правила с Δ-слоем неразличимости [7, 8]. Этот метод предполагает наличие в пространстве сигналов области, внутри которой решение о переданном символе принимается случайным образом. Такой механизм затрудняет противнику выбор оптимальной стратегии подавления. Исследования [7, 8] показали, что:

– при $\Delta = 0$ приемник с Δ-слоем становится приемником Котельникова, принимающим решение в пользу ближайшего в евклидовой метрике эталонного сигнала;
– оптимальные значения Δ^* параметра Δ-слоя равны: $\Delta_1^* \approx 0{,}1716$ при $n = 1$ и $\Delta_2^* \approx 0{,}2584$ при $n = 2$;
– при оптимальном слое Δ^* приемник обеспечивает энергетический выигрыш в помехоустойчивости по отношению к приемнику Котельникова приблизительно на 1,38 дБ при $n = 1$ и 0,41 дБ при $n = 2$;
– для $n \geq 3$ приемник с Δ-слоем ($\Delta > 0$) оказывается неэффективным;
– приемник имеет простую реализацию.

Однако большинство существующих работ [1-8] ограничивалось рассмотрением только преднамеренных помех, без учета неизбежного в реальных радиоканалах гауссовского шума. Это снижает практическую применимость полученных выводов, поскольку в реальных условиях воздействие помех не бывает изолированным.

Разработка приемников, устойчивых к одновременному воздействию целенаправленных помех и гауссовского шума, является задачей первостепенной важности при создании перспективных систем радиосвязи. Эта проблема особенно значима в военных операциях и сценариях с высокой степенью неопределенности, когда параметры канала неизвестны, а источник помех может действовать активно и адаптивно.

Для настоящей работы предметом исследования является случай $n = 2$, представляющий теоретический и практический интерес, так как вариант для $n = 1$ рассматривался в [11].

В настоящей работе описана модель СПИ, а также поставлена задача на исследование, предложена методика оценки эффективности приемника с Δ-слоем с учетом воздействия как преднамеренных помех, так и случайных (гауссовских) шумов, подведены итоги.

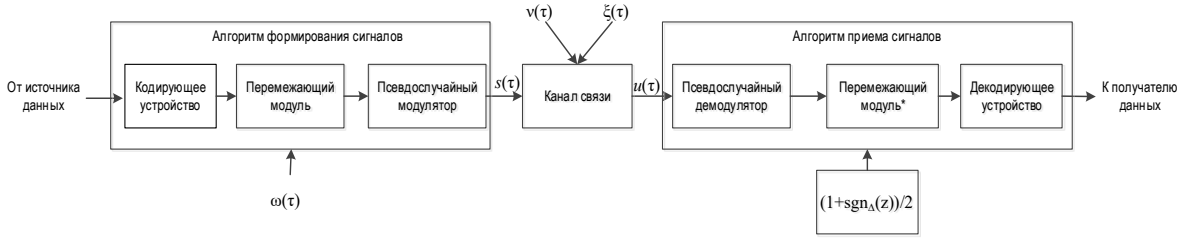


Рис. 1. Модель СПИ и постановка задачи

Вырабатываемые источником данных двоичные символы $x \in \{-1, 1\}$ представляются сигналами $s_1 \in S'(1)$, $s_x = x\, s_1$ которые передаются по каналу связи, подверженному воздействию аддитивной преднамеренной помехи

$\nu \in S\left(\sqrt{\delta}\right)$, где δ – отношение максимально допустимой энергии помехи к энергии сигнала.

Следует подчеркнуть, что алгоритм формирования сигналов и алгоритм их приема основаны на использовании заранее сформированной эталонной псевдослучайной последовательности ω (τ) с базой n. При этом приемник использует рандомизированное решающее правило с Δ – слоем неразличимости, которое представлено соотношением:

$$P_{\Delta}(u,\ s) = \frac{1}{2}(1 + sgn_{\Delta}(z)), \quad (1)$$

$$\text{где } \operatorname{sgn}_{\Delta}(z) = \begin{cases} -1, \text{ если } z < -1, \\ 0, \quad \text{если } |z \le \Delta|, \\ 1, \quad \text{если } z > 1. \end{cases} \quad (2)$$

На приемной стороне различие передаваемых символов осуществляется по принятому из канала сигналу $u = \omega \cdot s_x + \nu + \sigma\xi$ и известному в точке приема эталону псевдослучайной последовательности в соответствии с рандомизированным решающим правилом $d : R^n \times S'(1) \to \{-1, 1\}$, которое формирует решение о переданном символе $y = d(u_t, s_1)$ и выдает его получателю с учетом Δ – слоя неразличимости.

Вероятность ошибки бита сообщения при фиксированной мощности помехи $d = v^2$ в СПИ при $\sigma > 0$ определяется соотношением

$$P(d, \sigma^2, \Delta) = \frac{1}{2}(1 + \ + \frac{1}{2}[F_{\xi}(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) - F_{\xi}(\frac{1}{\sigma}(2 + \Delta + \sqrt{d})) - F_{\xi}(\frac{1}{\sigma}(2 - \Delta - \sqrt{d}))]),$$

которое было получено в [11].

Данное соотношение дополнительно к [7, 8] учитывает воздействие на переданный сигнал гауссовского шума.

По определению

$$P^{-}(\delta, \sigma^2, \Delta) = \max_{F_d \in \mathbb{F}(\delta)} \boldsymbol{E}_{F_d}[P(d, \sigma^2, \Delta)], \quad (3)$$

и поскольку максимум в (3) достигается при $\mathbf{E}[\mathcal{D}] = \delta$, корректным является определение наихудшего (оптимального) распределения помехи (т. е. наихудшей стратегии источника помехи) в виде

$$F_d^* = \operatorname*{argmax}_{F_d \in \mathbb{F}(\delta)} P(d, \sigma^2, \Delta). \quad (4)$$

На основе разработанной в [1] методики (см. теорему 2) устанавливается равенство

$$P^{-}(\delta, \sigma^2, \Delta) = P\hat{}(\delta, \sigma^2, \Delta), \quad (5)$$

где $P\hat{}(\cdot)$ – вогнутая (выпуклая вверх) оболочка функции $P(d, \sigma^2, \Delta)$ по первому аргументу [1, 2, 6, 7, 8, 11].

Следовательно, исследуемая в работе задача состоит в построении вогнутой оболочки функции $P(d, \sigma^2, \Delta)$ и проведении анализа на этой основе эффективности приемника с Δ-слоем в канале с преднамеренными помехами и случайным шумом для базы сигнала $n = 2$.

Полученные результаты

Для решения поставленной задачи был модифицирован и реализован вычислительный эксперимент [7, 8] для базы сигнала $n = 2$ с учетом гауссовского шума.

Моделирование производилось по следующим параметрам:

– 10^5 независимых испытаний;
– диапазон варьирования отношения помеха/сигнал для амплитудно-фазоманипулированных $(n = 2)$ $\delta \in [0,\ 4]$ с шагом 0,08;
– критические значения Δ - слоя $n = 2$: $\Delta\{0;\ 0{,}2584;\ 0{,}5\}$.

Результаты моделирования воздействия на систему передачи данных (рис. 2) оптимальной помехи и гауссовского шума показаны на рисунке 2 для σ = 0,1 и на рисунке 3 для σ = 0,2.

Из рисунка 2 видно, что при $n = 2$ максимальный энергетический выигрыш ≈ 0,41 (т. е. 9 %) сохраняется при σ = 0,1, как и в режиме без гауссовского шума [7, 8].

При увеличении мощности шума σ = 0,2 для $n = 2$ максимальный энергетический выигрыш составляет ≈ 0,3 дБ, т.е. на ≈ 5 % ниже, чем в [7, 8] при тех же условиях, но в отсутствие гауссовского шума.

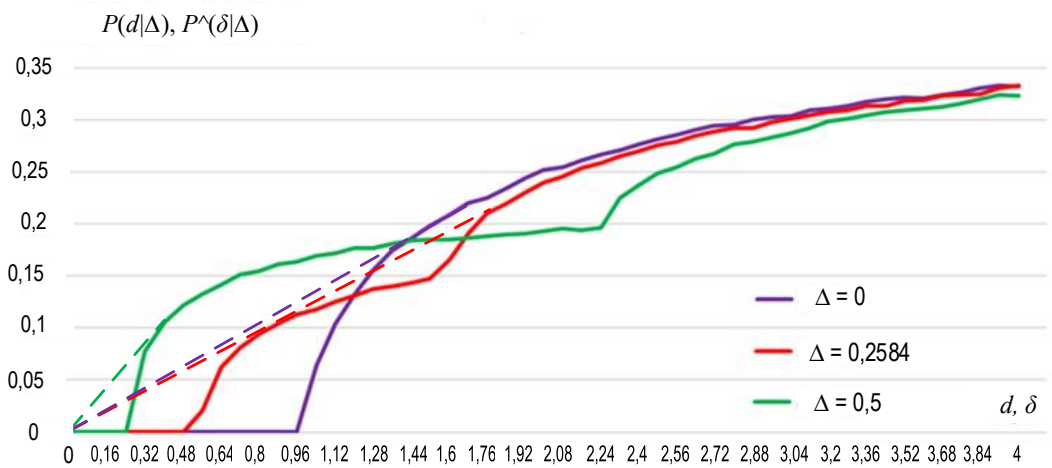


Рис. 2. Зависимость величин $P(d|\Delta), P\hat{}(d|\Delta)$
от значений d, δ текущей и средней мощности для различных при σ = 0,1

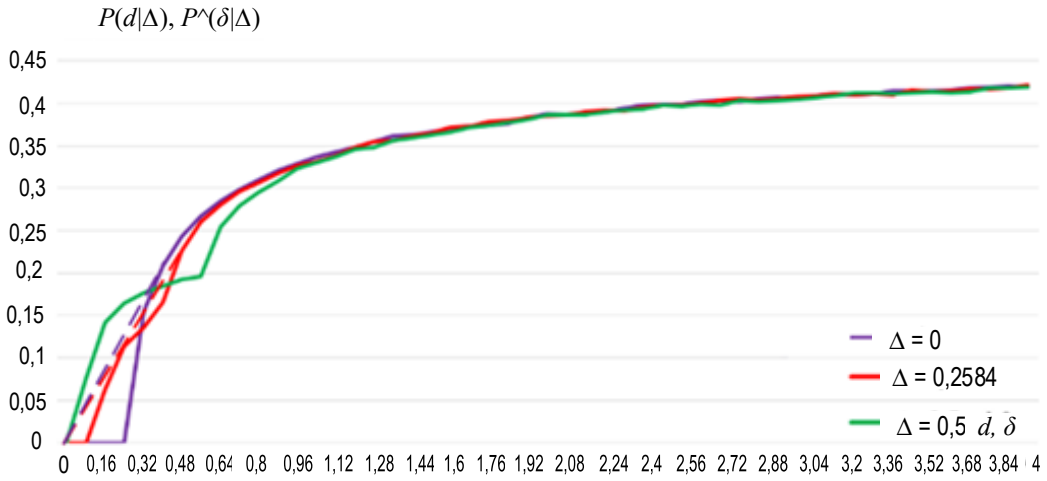


Рис. 3. Зависимость величин $P(d|\Delta), \hat{P}(d|\Delta)$
от значений d, δ текущей и средней мощности для различных при σ = 0,2

Результаты, полученные в ходе эксперимента (рис. 2 и рис. 3), позволяют оценить применимость Δ-слоя неразличимости в целях повышения помехоустойчивости приема двоичных псевдослучайных сигналов в условиях преднамеренных помех и гауссовского шума при $n = 2$. При этом следует отметить, что при учитывании гауссовского шума результаты неоднозначны, если при σ = 0,1 выигрыш не претерпевает значительных изменений, то при увеличении мощности шума до σ = 0,2 выигрыш уменьшается на 5 %.

Показанные выше результаты позволяют учесть постоянное наличие гауссовского шума при проектировании новых систем связи, а при использовании Δ-слоя неразличимости – оценить способность их функционирования в сложной радиоэлектронной обстановке. Демодуляция сигналов решающим правилом с Δ-слоем может использоваться для «мягкой» обработки в целом блоков данных на канальном уровне [9, 10], что может дать дополнительный выигрыш в помехозащищенности системы передачи информации.

Список используемых источников:

1. Чуднов А. М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации. 1991. Том 27. № 3. С. 57–65.

2. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем / А. М. Чуднов. СПб.: ВАС, 2021. 193 с.

3. Chudnov A. M., Kichko Ya. V., Sapunova L. P. Optimization of the guaranteed rate of information transmission by pseudo-random signals with a randomized base under conditions of deliberate interference // Radio engineering and electronics. 2023. V. 68. № 3. PP. 263–270.

4. Анализ помехоустойчивости локальных систем морской навигации в условиях воздействия оптимизированных помех / Е. И. Глушанков, Д. И. Кирик, З. К. Кондрашов [и др.] // Морской вестник. 2025. № 1(93). С. 89-91.

5. Одоевский С. М., Султанов Р. С., Ключников В. О. Оценка помехоустойчивости беспроводных линий связи с адаптивной модуляцией в условиях оптимизированных помех // Радиолокация, навигация, связь: Сборник трудов XXX Международной научно-технической конференции. В 5-ти томах, Воронеж, 16–18 апреля 2024 года. Воронеж: Издательский дом ВГУ, 2024. С. 238-247.

6. Чуднов А. М. Комментарии к статье Н. Н. Плотникова, А. В. Войнова и А. Н. Путилина «Выбор алгоритма адаптации по рабочей частоте в однополосной радиолинии тропосферной связи» // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2024. № 11-12(197-198). С. 20-30.

7. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the decisive rule for a receiver with a Δ-layer of indistinguishability of binary signals in a channel with intentional interference // Problems of Information Transmission. 2025. Vol. 61, № 1. P. 41-55.

8. Чуднов А. М., Сазонов В. В., Бикбулатов В. Р. Оптимизация области неразличимости приемником двоичных сигналов, передаваемых по каналу с преднамеренной помехой // Проблемы передачи информации. 2025. Т. 61. № 1. С. 47-59.

9. Гладких А. А. Основы теории мягкого декодирования избыточных кодов в стирающем канале связи / Ульяновск: УлГТУ, 2010. 379 с.

10. Савищенко Н. В. Помехоустойчивость когерентного приема многопозиционных сигналов КАМ и ФМ при неидеальной синхронизации // Информационно-управляющие системы. 2010. 1(44). С. 53-63.

11. Негурица А. О. Оценка эффективности использования δ-слоя неразличимости двоичных сигналов, принимаемых в условиях случайных и преднамеренных помех // Телекоммуникации и связь. 2025. № 4(07). С. 22-27.

ANALYSIS OF THE NOISE RESISTANCE OF THE RECEPTION OF DUAL PSEUDO-RANDOM SIGNALS USING Δ-LAYER OF INDISCRIMINABILITY IN CONDITIONS OF INTENTIONAL NOISE AND GAUSSIAN NOISE.

Bikbulatov V., Neguritsa A., Chudnov A.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

For the reception of phase-shifted pseudo-random signals in the presence of Gaussian noise, a Δ-layer of indistinguishability (the decision rule of reception) is introduced. Taking into account the use of methods of static decision theory, dynamic programming and information theory, the influence of the decision rule is shown when receiving binary signals and additive intentional interference and Gaussian noise.

Key words: *information transmission system, Gaussian noise, signal reception algorithms, randomized decision rule, guaranteed error probability, signal base*

УДК 621.396.67
ГРНТИ 49.43.29

МЕТОДЫ АДАПТИВНОЙ ОБРАБОТКИ СИГНАЛОВ В ГИБРИДНЫХ СЕТЯХ СВЯЗИ

И. А. Бойко, А. Г. Владыко, Е. И. Глушанков, И. А. Горобцов

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

Для повышения помехоустойчивости гибридных сетей связи в условиях воздействия различного рода взаимных помех важную роль играют методы адаптивной обработки сигналов, среди которых одними из наиболее эффективных являются методы пространственной обработки сигналов в приемных и передающих антенных системах.

адаптивные алгоритмы, пространственная обработка, помехоустойчивость

На приемной стороне главной задачей адаптивной обработки сигналов является формирование диаграммы направленности с главными лепестками в направлении источников полезных сигналов и глубокими нулями в направлении источников помех [1]. Для достижения этой задачи используются прямые методы пространственной обработки сигналов (ПОС), где в качестве опорного сигнала используются известные пилот-сигналы. Если же канал связи оказывает существенное искажение принимаемых сигналов в связи с замираниями и/или доплеровским сдвигом используют прямые методы пространственно-временной обработки сигналов (ПВОС) (рис. 1) [2].

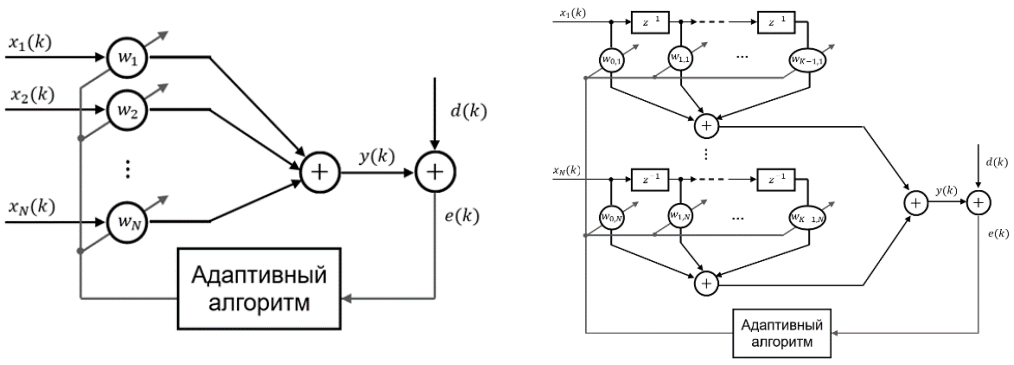


Рис. 1. Структурная схема алгоритма ПОС (слева) и ПВОС (справа)

Отсчеты дискретного сигнала, приходящие на N элементов ААР, можно рассматривать как сумму всех M полезных сигналов помехи и шума:

$$x(k) = A_1 d(k) + A_2 c(k) + n(k),$$

где $x(k)$ – вектор сигналов на элементах ААР длинной N, A_1 – управляющая матрица размерностью $N \times M$, определяющая фазовые сдвиги сигналов и зависящая от направления источников сигнала, $d(k)$ – вектор полезных сигналов длиной M, $c(k)$ – вектор помех длиной L, A_2 – управляющая матрица размерностью $N \times M$, определяющая фазовые сдвиги помех, $n(k)$ – вектор аддитивного белого гауссовского шума (АБГШ) длиной N.

Тогда сигнал на выходе ААР будет равен:

$$y(k) = W^H(k)x(k),$$

где $y(k)$ – вектор M выходных сигналов, $W(k)$ – матрица весовых коэффициентов размерностью $M \times N$, ^{H} – знак эрмитова сопряжения.

Алгоритмы класса RLS направлены на минимизацию суммы квадратов разности между желаемым сигналом и входным воздействием. Когда на каждой итерации поступают новые образцы входящих сигналов, решение задачи наименьших квадратов может быть вычислено в рекурсивной форме.

Матрица весовых коэффициентов алгоритма RLS:

$$W(k) = W(k-1) + k(k)e^H(k-1)$$

где $k(k)$ – вектор коэффициентов усиления, $P(k)$ – обратная корреляционная матрица, которые обновляются с каждой итерацией.

Алгоритм RLS показывает хорошие показатели, если образцовый $d(k)$ и/или входные сигналы $x(k)$ являются эргодическими процессами. Иначе вводят коэффициент забывания λ, $0 < \lambda \leq 1$, чтобы учитывать предшествующие отсчеты входного воздействия.

В этом случае рекуррентные формулы для вычисления вектора коэффициента усиления и обратной корреляционной матрицы примут вид:

$$k(k) = \frac{P(k-1)x(k-1)}{\lambda + x^H(k-1)P(k-1)x(k-1)},$$

$$P(k) = \frac{1}{\lambda}[P(k-1) - k(k)x^H(k-1)P(k-1)].$$

На рис. 2 представлена ДН ААР из 16×16 элементов, полученной в результате работы алгоритма RLS при углах источников полезных сигналов (-30°, -2°), (0°, -7°), (15°, 10°) и источников помех (-20°, -2°), (-10°, -7°).

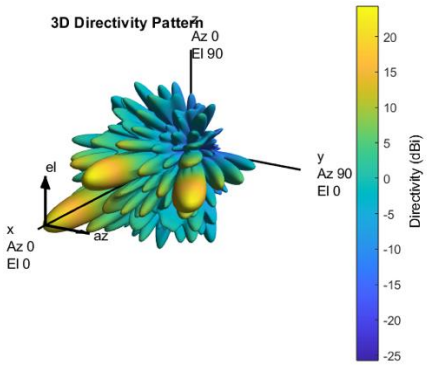


Рис. 2. ДН ААР, полученной в результате работы алгоритма RLS, ОСШ 20 дБ

На рис. 3 представлены зависимости ОСШ на выходе антенной решетки в результате работы различных алгоритмов ПОС от ОСШ в канале. На рис. 4 представлены результаты выигрыша в адаптации Δh в результате работы алгоритмов ПОС.

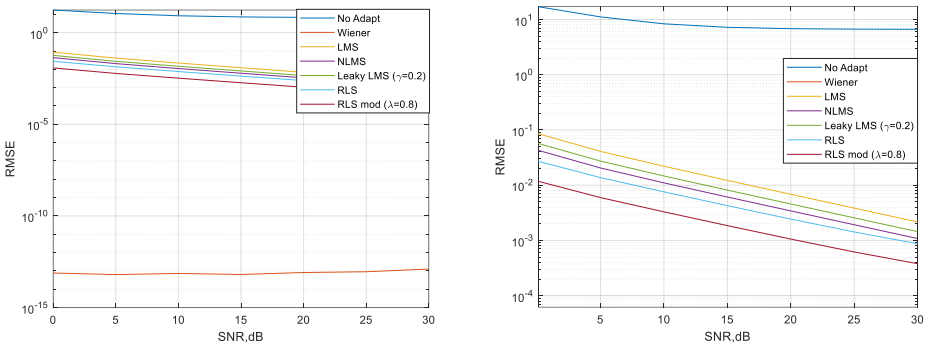


Рис. 3. Зависимости ОСШ на выходе ААР от ОСШ в канале

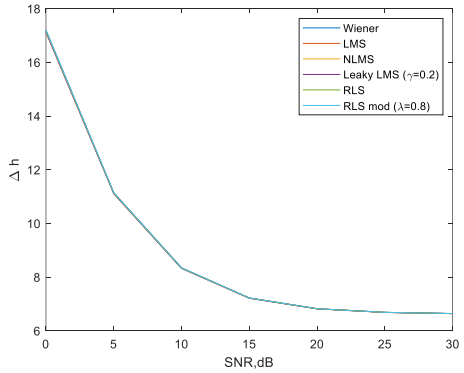


Рис. 4. Зависимости выигрыша от адаптации от ОСШ для различных алгоритмов

На передающей стороне главной задачей является передача сигнала с максимальным ОСШ. Поскольку канал связи вносит существенные искажения, на передающей стороне осуществляется прекодирование матрицей P размерностью $M \times N$ [3,4]:

$$y(k) = HPd(k) + n(k),$$

где H – канальная матрица размерностью $N \times M$.

Алгоритмом, обеспечивающим максимальную мощность передачи, является алгоритм MRT:

$$P = \sqrt{\beta} H^H.$$

На рис. 5 представлена ДН ААР из 16×16 элементов, полученной в результате работы алгоритма MRT при углах приемных станций (-30°, -2°), (0°, -7°), (15°, 10°).

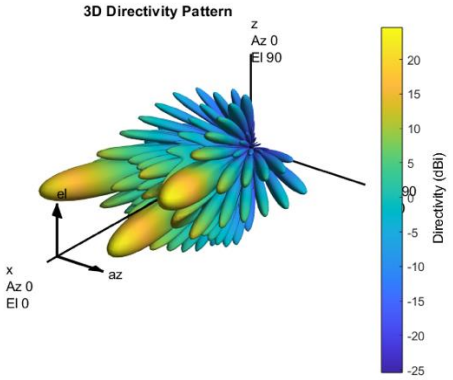


Рис. 5. ДН ААР из 16×16 элементов, полученной в результате работы алгоритма MRT, ОСШ 20 дБ

Оптимальным алгоритмом по МСКО будет являться алгоритм MMSE:

$$P = \sqrt{\beta} H^H (HH^H + \lambda I)^{-1},$$

где I – единичная матрица размерностью $N \times N$, λ – положительный фактор регуляризации, который зависит от дисперсии шума в канале и неточностью вычисления канальной матрицы.

Для алгоритма MMSE корреляционную канальную матрицу HH^{H} находят итерационным способом. Одним из способов обращения является модифицированный алгоритм Ньютона [5]. Повышение скорости сходимости обеспечивается за счет введения переменного шага λ_k:

$$\hat{G}^{-1} = X_k = X_{k-1}[(\lambda_k + 1)I - \lambda_k G X_{k-1}],$$
$$\lambda_k = \lambda_{k-1}(1 - \varepsilon),$$

где ε – константа, влияющая на уменьшение шага адаптации.

На рис. 6 приведено сравнение скорости сходимости алгоритмов Ньютона, Чебышева и модифицированного Ньютона. На рис. 7–8 показаны зависимости сходимости прекодирующей матрицы к оптимальным значениям от параметров λ_0 и ε.

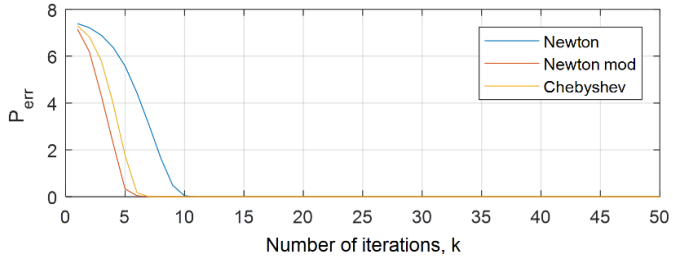


Рис. 6. Скорость сходимости прекодирующей матрицы к оптимальным значениям

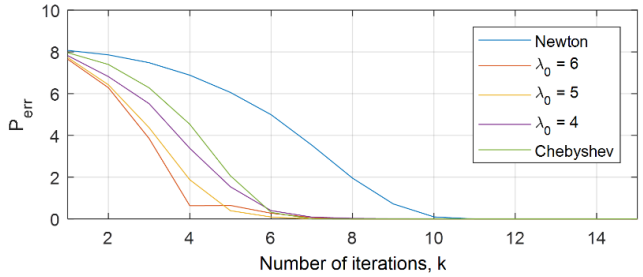


Рис. 7. Графики сходимости прекодирующей матрицы в зависимости от начального шага адаптации λ_0

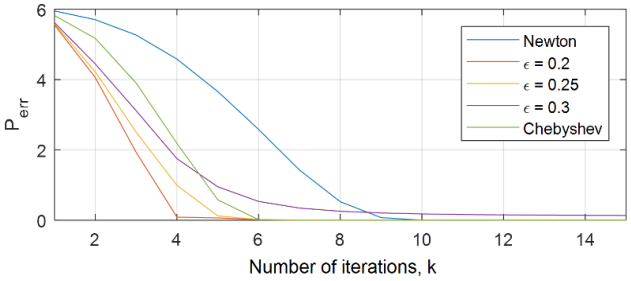


Рис. 8. Графики сходимости прекодирующей матрицы в зависимости от параметра ε

На рис. 9 представлены результаты выигрыша в адаптации Δh в результате работы алгоритмов прекодирования для ААР из 16×16 элементов для 3 приемных станций.

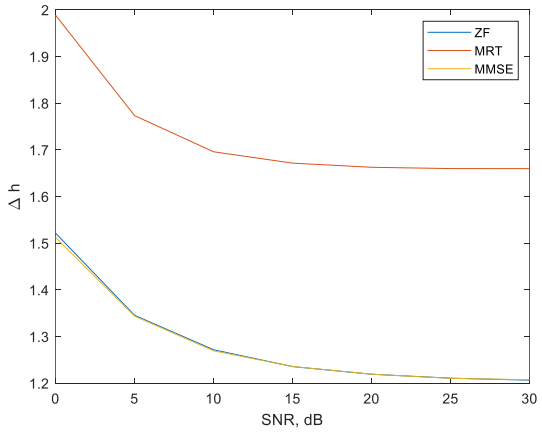


Рис. 9. Зависимости выигрыша от адаптации от ОСШ для различных алгоритмов прекодирования

В работе рассмотрены основные классы алгоритмов адаптивного обработки сигналов в гибридных сетях связи в режимах работы на прием и передачу, позволяющие увеличить энергетическую и спектральную эффективности за счет пространственного разнесения.

Для приемных антенных систем используются прямые методы адаптивного диаграммообразования. Компромиссом между скоростью сходимости и вычислительной сложностью будет являться класс алгоритмов RLS.

Для передающих антенных систем используются методы предварительного кодирования. Для малого количества приемных станций эффективнее будет алгоритм MRT. При большом количестве – алгоритм MMSE. Использование модифицированного алгоритма Ньютона позволяет увеличить скорость сходимости алгоритма.

Список используемых источников

1. Глушанков Е.И., Коровин К.О., Бойко, И.А. Реализация алгоритма адаптивного диаграммообразования с обращением корреляционной матрицы на ПЛИС // Электросвязь. 2024. № 12–2. С. 70–75. EDN:UENNBQ

2. Джиган В. И. Адаптивная антенная решетка для приема сигналов в условиях помех и многолучевости //Цифровая обработка сигналов. 2019. № 4. С. 20–27. EDN DQYLGI.

3. Глушанков Е.И., Коровин К.О., Бойко, И.А, Борисов М.Г. Современное состояние и перспективы развития адаптивных антенных комплексов в радиотехнических системах // Вестник СПбГУТ. 2024. Т. 2. №1, 14 с. EDN:AKVWWB

4. Albreem M. A., Al Habbash A. H., Abu-Hudrouss A.M., Ikki S.S. Overview of precoding techniques for massive MIMO // IEEE Access. 2021. № 9, PP. 60764-60801. DOI:10.1109/ACCESS.2021.3073325.

5. Glushankov E. I., Boyko I. A., Kirik D. I., Korovin K. O. Development of a Modified Newton Iteration Algorithm for massive MIMO systems with precoding and its study in MATLAB environment // Journal of Physics: Conference Series. 2022. Vol. 2291. P. 012011. DOI: 10.1088/1742-6596/2291/1/012011.

Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2025-005, «Прикладные научные исследования в области разработки методов мониторинга и идентификация типов трафика для эффективного использования сетевого ресурса в гибридных сетях связи» (регистрационный номер ПТНИ: 1024062100008-4).

SIGNAL PROCESSING METHODS IN HYBRID COMMUNICATION NETWORKS

Boiko I., Vladyko A., Glushankov E., Gorobtsov I. *Adaptive*
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Adaptive signal processing methods play an important role in order to increase the noise immunity of hybrid communication networks under the influence of various types of mutual interference, among which spatial signal processing methods in receiving and transmitting antenna systems are among the most effective.

Key words: *adaptive algorithms, spatial processing, noise immunity.*

УДК 654.739
ГРНТИ 49.33.29

К СОДЕРЖАТЕЛЬНОМУ НАПОЛНЕНИЮ ОБУЧЕНИЯ 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

Обосновывается необходимость приведения содержания учебных дисциплин по физическим основам электроники в соответствие с современным состоянием науки и технологий. Определяются ориентиры обновления содержания обучения, к основным из которых относятся его полнота, системность и целостность, широта в охвате динамики и передовых достижений научно-технологического прогресса, методологическая основательность, развивающий характер. Приводится содержание проблематики, рекомендуемое к интеграции в учебные программы, и показываются возможности ее реализации в практике обучения.

физические основы электроники, обновление содержания обучения, перспективные направления развития, физико-технологическое решение задач, проблемы в практике обучения и подходы к их разрешению

Важнейшее требование, которому должно удовлетворять содержание обучения при подготовке специалистов, состоит в его основательности для профессиональной деятельности. Происходящие в последней коренные изменения диктуют необходимость систематического обращения к анализу содержания реализуемых в образовательном процессе учебных программ в целях приведения его в соответствие с возникающими реалиями. В существующих реалиях фактором первого порядка, предопределяющим потребность в модернизации учебных программ, является стремительный технологический прогресс, осуществляемый на базе продуктивного применения достижений науки.

В этой связи особого внимания заслуживает содержание дисциплин, посвященных научным основам ключевых современных технологий. К таким дисциплинам, несомненно, относятся отражающие научные основы и методы создания элементов электронной базы инфокоммуникационных систем и предназначенных для них материалов физические основы электро-

ники, развитию содержания обучения которым посвящена настоящая работа.

Руководствуясь запросами со стороны профессионального образования [1-3], следует констатировать, что содержание действующих программ по физическим основам электроники нуждается в гармонизации с потребностью в специалистах, способных к получению и применению научных знаний в целях решения актуальных практических задач, во многих отношениях, к основным из которых относятся следующие.

Первое – полнота содержания обучения, которое нуждается в более широком охвате существующих элементов электронной базы и обогащении информацией, необходимой для сущностного понимания проблематики перспективных направлений научно-технологического развития и конструктивного участия в решении его задач.

В плане объектного охвата в пространстве существующего – это, по крайней мере, включение в содержание обучения физике не утративших своей востребованности и проявляющих тенденцию к развитию резистивных и емкостных элементов.

В плане обеспечения задела на будущее настоятельно необходима актуализация в содержании обучения фундаментальных основ целого ряда интенсивно развивающихся и определяющих облик электроники в ближайшей перспективе направлений. К их числу относятся полупроводниковая электроника сверхвысокочастотного и оптического диапазонов, фотовольтаика, спинтроника, плазмоника, квантовые технологии связи и вычислений, электроника нейроморфных систем. Соответственно, должен быть существенно расширен и круг изучаемых в дисциплинах объектов и явлений, охватывая в части объектов полупроводниковые структуры с квантоворазмерными функциональными элементами, бистабильные материалы, оптические композиты, а в части явлений – нелинейные эффекты с внешним электрическим и оптическим управляющими сигналами, фазовый переход «полупроводник-металл», эффекты, обусловленные спин-поляризованным током, плазмонный резонанс.

Второе – системность и целостность содержания обучения, которые должны стать неотъемлемыми атрибутами в отражении:

– физических эффектов, лежащих в основе принципа действия подлежащих изучению элементов электронной базы;
– ориентировочной роли физической концепции создания элементов с необходимыми свойствами в проектировании функциональных материалов и технологий;

– функциональных возможностей изучаемых элементов, находящих практическое применение.

Так, при изучении физических основ гетероструктурной полупроводниковой электроники в части инжекционных гетеролазеров должна быть представлена вся совокупность базовых физических эффектов – односторонняя инжекция, сверхинжекция, электронное ограничение, оптическое ограничение, эффект широкозонного окна; выработанные на физическом уровне подходы к выбору и созданию функциональных материалов (согласованность параметров кристаллической решетки компонентов структуры, применение многокомпонентных твердых растворов) и, наконец, наиболее важные применения гетероструктур в электронике в качестве рабочих структур транзисторов, лазеров, светодиодов, фотодетекторов [4].

Целостность и системность должны быть присущи содержанию не только лекционного курса, но и практикума по дисциплине. Целесообразным здесь является построение практикума из циклов заданий, тематически охватывающих физику определенных классов элементов электронной базы [5].

Еще один существенный здесь аспект – целостность и системность в отражении подлежащих физико-технологическому решению основных типов задач [6]. К таковым относятся задачи анализа строения и электронных свойств функциональных структур, решение которых дает системообразующие результаты, задачи практической, в том числе прогностической, диагностики и задачи управления свойствами в целях достижения требуемых характеристик.

Третье – необходимость предметного прослеживания динамики прогресса и передовых достижений науки и технологий.

В тематике гетероструктурной полупроводниковой электроники - это следующее за классическими гетероструктурами рассмотрение физики гетероструктур с функциональными элементами нанометровых размеров с присущим им квантованием энергии и обусловленных этим резонансного туннелирования и сопряженного с ним вынужденного излучения, востребованности и состояния субмикронных технологий, связанного с отсутствием необходимости согласования параметров кристаллических решеток расширения круга представляющих интерес материалов, наиболее перспективных гетероструктур с квантовыми точками, в ряду способов получения массивов которых видное место занимает самоорганизация.

Четвертое – потребность в усилении внимания к процессуальной стороне приведшего к значимым достижениям физико-технологического решения проблемных задач: его логике, структуре и средствам.

Содержание обучения физическим основам электроники должно раскрывать не только подлежащие освоению научные знания в их логически завершенном виде, но и накопленный опыт получения и применения этих знаний. Принципиально важными здесь представляются следующие моменты.

Во-первых, предметное отражение проявляемой в физико-технологическом решении целого ряда проблемных задач, нелинейность методологии, прежде всего, первоочередность теоретических исследований, ведущих к выработке предопределяющих достижений результатов модельных представлений.

Показательный пример тому – история создания полупроводниковых лазеров, регулятивом разработки которых послужила сформулированная на теоретическом уровне концепция двойных гетероструктур [4].

Во-вторых, максимально возможное отражение в содержании обучения возможностей, открываемых применением в принятии и реализации технических решений методов научной инженерии.

Продолжая конкретизацию выдвигаемых положений на примере изучения физики полупроводниковых гетеролазеров, отметим возможности демонстрации ведущей роли в их разработке инженерии зонных диаграмм и волновых функций.

В-третьих, акцентирование внимания в содержании обучения физическим основам электроники на необходимости использования для получения требуемой информации комплекса взаимодополняющих методов и обращенность к этим методам, как к предмету изучения.

Понимание востребованности такой комплексности дает изучение, например, проблем диагностики приборных структур с функциональными элементами нанометровых размеров. Круг задействованных здесь методов включает в себя количественную просвечивающую и растровую электронную микроскопию, высокоразрешающую рентгенодифрактометрию, электронную спектроскопию для химического анализа, рентгеноспектральный микроанализ, широкодиапазонную спектроскопию полной проводимости и емкостную спектроскопию, необходимые для интерпретации получаемых результатов методы численного моделирования [7].

Пятое – активизация развивающего ресурса обучения физическим основам электроники.

Особого внимания здесь заслуживает обеспечение основательности содержания заданий, выполняемых обучающимися самостоятельно, в плане раскрытия, развития и реализации интеллектуальных и творческих способностей. Целесообразными здесь являются задания по изучению проблем, к решению которых имеются множественные физические подходы. Таковыми являются, например, задания по изучению физических основ создания элементов энергонезависимой памяти [8], устройств для управления лазерным излучением [9, 10], элементной базы систем, предназначенных для квантовой связи и квантовых вычислений [11].

Содержание самостоятельной работы должно включать в себя и задания в пространстве открытых, еще не нашедших своего решения проблем, что может способствовать вовлечению наиболее подготовленных обучающихся в их решение и стать для них профессиональной пробой специализации.

Принципиально важное значение в плане достижения целей личностного развития обучающихся имеет использование в организации образовательного процесса активных технологий [12], выбор которых должен осуществляться с учетом уровня подготовленности обучающихся.

Для определенной части контингента можно ограничиться применением технологии активного восприятия информации, для более продвинутых обучающихся – применять технологию проблемных ситуаций и, наконец, для наиболее способных – исследовательский и проектный (проектно-исследовательский) методы обучения.

Разрешению с очевидностью существующих проблем в реализации нового содержания обучения в образовательном процессе – ограниченности отводимого на обучение времени, дефицита учебно-информационного и кадрового обеспечения могут способствовать представленные в [13, 14] разработанные методические подходы и приемы.

Список используемых источников

1. Новиков А. М. Профессиональное образование в России. М.: ИЦПНПО, 1997. 253с.

2. Новиков А. М. Российское образование в новой эпохе. Парадоксы наследия, векторы развития. М.: Эгвес, 2000. 96с.

3. Бюллетень Научно-методического совета по физике. СПб.: Изд-во Политехн. ун-та, 2012. № 4.

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

5. 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.

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. 127с.

7. Алферов Ж. И., Копаев П. С., Сурис Р. А., Осеев А. А., Гапонов С. В., Попов В. И., Полторацкий Э. А., Сибельдин Н. Н. Наноматериалы и нанотехнологии // Нано- и микросистемная техника. От исследований к разработкам. Под ред. д.т.н., проф. П. П. Мальцева. М.: Техносфера, 2005. С. 19-34.

8. Красников Г. Я. Энергонезависимая твердотельная память в современной микроэлектронике. 3.1. Под ред. чл.-корр. РАН Ю. Л. Чаплыгина. М.: Техносфера, 2016. С. 464-479.

9. Розеншер Э., Винтер Б. Оптоэлектроника. М.: Техносфера. 2004. 592 с.

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

11. Валиев К. А. Квантовая информатика: квантовые компьютеры, связи и криптография // Базовые лекции по электронике. Под общ. ред. В. М. Пролейко. М.: Техносфера, 2009. Том II. Твердотельная электроника. С. 595-607.

12. Селевко Г. К. Энциклопедия образовательных технологий. В 2 Т. М.: НИИ школьных технологий, 2019. 1635 с.

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

14. Костарев С. В., Жуков В. А., Остроумова Ю. С., Ханин С. Д. Предпосылки и ориентиры обновления учебно-методического обеспечения обучения физике при подготовке инженерных кадров // Физическое образование: от прошлого к будущему. Материалы Всероссийской научно-методической конференции с международным участием. СПб.: Изд-во Политехн. ун-та, 2017. С. 63-67.

TOWARDS THE MEANINGFUL CONTENT OF THE TRAINING THE PHYSICAL BASICS OF ELECTRONICS

Borisov S.[1], Landa A.[1], Ostroumova Yu.[2], Khanin S.[1], Shumakov P.[1]
[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications
[2]Military Medical Academy of S. M. Kirov

The necessity of bringing the content of academic disciplines on the physical foundations of electronics in line with the current state of science and technology is substantiated. The guidelines for updating the content of education are determined, the main ones of which include its completeness, consistency and integrity, breadth in the coverage of dynamics and advanced achievements of scientific and technological progress, methodological thoroughness, and developmental nature. The content of the issues recommended for integration into educational programs is given, and the possibilities of its implementation in teaching practice are shown.

Key words: *the physical foundations of electronics, updating the teaching content, promising areas of development, physical and technological problem solving, problems in teaching practice and approaches to their resolution*

УДК 654.739
ГРНТИ 49.33.29

ПРОБЛЕМНО-ДЕЯТЕЛЬНОСТНЫЙ ПОДХОД К ОБУЧЕНИЮ ФИЗИЧЕСКИМ ОСНОВАМ ЭЛЕКТРОНИКИ: ПРЕДПОСЫЛКИ ИСПОЛЬЗОВАНИЯ И МЕТОДИКО-ТЕХНОЛОГИЧЕСКАЯ РАЗРАБОТКА

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

Обосновывается целесообразность и раскрываются возможности организации обучения физическим основам электроники на основе применения проблемно-деятельностного подхода. Приводятся выполненные в логике этого подхода, могущие быть использованными в практике обучения методические разработки. Развивается идея дифференцированного, предписывающего учет уровня подготовленности и потенциала обучающихся, педагогико-технологического обеспечения образовательного процесса. Определяются предпочтительные в плане реализации проблемно-деятельностного подхода технологии обучения.

организация обучения, ресурсность проблемно-деятельностного подхода, содержание проблематики обучения, задачно-деятельностная форма представления содержания, педагогико-технологическое обеспечение образовательного процесса

Будучи направленным на подготовку к будущей деятельности в условиях интенсивного технологического прогресса, профессиональное образование в качестве своего стратегического ориентира должно иметь сформированность у обучающихся умений и опыта получения и применения научных знаний в целях решения актуальных практических задач. Для достижения этой цели необходимы соответствующие подходы к организации образовательного процесса. Одним из таковых представляется подход, предписывающий организацию обучения через проблемно-детерминированную деятельность (далее, проблемно-деятельностный подход).

Реализация этого подхода в практике обучения с определенностью способствует становлению у будущих специалистов требуемых компетенций, в силу придания приобретаемым знаниям смысла предмета и средства деятельности, и развитию личности, в силу ресурсности проблемно-детерминированной деятельности в формировании интеллектуальных и творческих

качеств, стремления к конструктивному применению способностей к получению прогрессивных решений.

Проблемно-деятельностный подход был и остается предметом обширных исследований в области дидактики высшей школы [1-4] и на протяжении длительного времени результативно используется в практике обучения ведущими образовательными учреждениями. Однако в полной мере этот подход к организации образовательного процесса используется, как правило, только начиная с третьего курса обучения, когда обучающиеся погружаются в решение проблемных профессиональных задач. В преподавании же предшествующих этому общих дисциплин доминирующим остается сообщающее обучение, что не позволяет в полной мере реализовать имеющийся у этих дисциплин образовательный потенциал. К таковым относятся дисциплины, отражающие физические основы электроники. В настоящей работе с дидактических и методологических позиций обосновывается целесообразность обучения этим дисциплинам в логике реализации проблемно-деятельностного подхода и развивается его методико-технологическое обеспечение.

Основанием для реализации проблемно-деятельностного подхода к обучению физическим основам электроники является следующее. Во-первых, соответствие содержания предмета обучения – физических процессов, ответственных за формирование функциональных свойств элементов электронной базы инфокоммуникационных систем и материалов для их создания – выделяемым в педагогике как основные стимулам познавательного интереса [5, 6]: актуальности, новизне, жизненной значимости. В дополнение к тому отметим профессиональную значимость содержания предметного материала для обучающихся, специализирующихся в области электроники и инфокоммуникационных систем, а также рельефное отражение в содержании обучения инженерного потенциала теоретических знаний.

Во-вторых, сопряженная с объектной ориентацией содержания обучения его проблемность и, соответственно, ресурсность в плане формирования у обучающихся таких важных для специалиста качеств как целеустремленность, ясность и основательность мысли и действий, открытость по отношению к новому, продуктивная самостоятельность в выдвижении и реализации новых идей.

В-третьих, присущая решению на физическом уровне широкого круга проблемных задач электроники множественность подходов, открывает воз-

можности развития в обучении способностей к критическому анализу, аргументации предлагаемого решения, его адекватной оценке.

В-четвертых, наличие в содержании обучения целого ряда открытых проблем, что создает условия для выработки у обучающихся индивидуального стиля мышления и действий, раскрытия, развития и реализации остро востребованных в научно-технологической деятельности творческих способностей.

Наконец, методологический ресурс обучения физическим основам электроники, предопределяемый возможностью целостного отражения на физическом уровне процесса решения проблемных задач, что создает условия для предметного изучения его логико-операциональной структуры, методов и средств электронной инженерии. Особо отметим открываемые изучением физических основ электроники в логике проблемно-деятельностного подхода возможности формирования физического понимания на всех его основных уровнях [7] – объяснения, описания наблюдаемых и прогнозирования новых, могущих найти практическое применение, явлений и овладения являющимся основой этого понимания, ключевым в научно-технологическом решении проблемных задач методом моделирования.

Следуя проблемно-деятельностному подходу к организации обучения, развертка предметного материала физических основ электроники в учебном процессе должна быть динамической, осуществляемой в логике, приведшей к достижению подлежащих изучению результатов деятельности, начиная с ее системообразующего, представляющего в освоении наибольшую сложность компонента – постановки проблемы.

В качестве основных при изучении физических основ электроники могут рассматриваться следующие два типа проблем: первый – определение принципов, могущих являться базовыми для создания функциональных элементов и материалов с необходимыми свойствами; второй – определение и обоснование направлений практического применения свойств отдельных изучаемых классов объектов. В первом случае основанием для постановки проблемы должны являться результаты анализа существовавшего до ее решения состояния дел в изучаемой области; во втором – анализ свойств рассматриваемых объектов на предмет их практического применения. Принципиально важной при этом является максимально возможная вовлеченность в постановку проблемы самих обучающихся.

Так, при освоении физических принципов создания полупроводниковых лазеров, способных работать в непрерывном режиме при обычных тем-

пературах, на этапе постановки проблемы обучающимся может быть поручено выявить на основе имеющихся знаний присущие гомоструктурам в рассматриваемом аспекте ограничения, каковые связаны с высокой пороговой плотностью тока вследствие необходимости использования вырожденного полупроводника и трудности пространственного совмещения электронного и светового потоков. Обоснованному определению направлений применения в электронике квантовых точек может предшествовать осуществляемый обучающимися обзор свойств этого класса объектов, охватывающий характерные размеры, распределение электронных состояний по энергиям, оптические свойства.

Деятельностной должна быть позиция обучающихся и при освоении концепции решения изучаемой проблемы, что может выражаться в совместном с преподавателем выявлении и обосновании целесообразности практического использования базовых физических эффектов. Таковыми в части полупроводниковых гетеропереходов являются эффекты широкозонного окна, односторонней инжекции, сверхинжекции, а при переходе к двойным гетероструктурам, в дополнение к этому – эффекты электронного и оптического ограничения [8]; в части квантовых точек – влияние на их энергетический спектр геометрических размеров и электрического поля [9].

Предпочтительной формой представления содержания занятий, направленных на изучение проблем, к решению которых существуют различные, конкурирующие между собой физические подходы, является задачно-деятельностная форма, а проведения таких занятий – семинары, на которых осуществляется сравнительный анализ защищаемых обучающимся решений. Конкретизации этого могут служить методические разработки по изучению проблем создания высокоомных и термостабильных резистивных материалов и модуляторов (ограничителей) интенсивного излучения.

Сказанное относительно постановки задачи и определения физического подхода к ее решению применимо не только к теоретической составляющей дисциплины, но и к практикуму по ней, что было показано в [4, 10] на примерах выполнения циклов заданий по экспериментальному решению задач по выбору материалов и приборных структур для создания чувствительных элементов датчиков оптического излучения в ультрафиолетовом диапазоне и датчиков температуры.

В плане педагогико-технологического обеспечения организация обучения в логике проблемно-деятельностного подхода предпочтение должно отдаваться активным технологиям [11]. При этом в выборе технологии сле-

дует учитывать уровень когнитивных способностей контингента обучающихся и осуществлять в соответствии с этим дифференцированный подход.

В организации обучения определенной части контингента можно ограничиться технологией активного восприятия информации, предлагая обучающимся задания по сущностному освоению содержания проблематики перспективных направлений научно-технологического развития, каковой, например, является проблематика нанофотоники и наноплазмоники [12].

Для более подготовленной части контингента обучающихся наряду с указанной технологией к организации процесса обучения может быть привлечена технология проблемных ситуаций, предписывающая обучающемуся активную позицию в выявлении, постановке и выборе путей решения проблемы.

Наконец, в организации обучения наиболее подготовленных, обладающих соответствующим потенциалом обучающихся могут быть полномасштабно использованы исследовательский и проектно-исследовательский методы, что предполагает максимально самостоятельное получение недостающей для решения проблемы информации с использованием для этого всего необходимого комплекса методов и средств [13]. Реализация указанных методов с необходимостью требует интеграции учебной, научной и инженерной работы. Результат – приобретение реализованного опыта аутентичной к профессиональной деятельности, осуществления всего спектра востребованных в ней видов, что отвечает сформулированному основоположником проектного метода Дж. Дьюи пониманию образования [14] как постоянной реорганизации и перестройке опыта, ведущих к приобретению умений применять способности к новым целям.

Список используемых источников

1. Новиков А. М. Профессиональное образование в России. М.: ИЦПНПО, 1997. 253 с.

2. Попков В. А., Коржуев А. В. Дидактика высшей школы. М.: Издательский центр «Академия», 2008. 224 с.

3. Гуляев В. Н. Развитие теории и практики проблемно-деятельностного обучения в высшей военной школе. Дис...докт.пед.наук. М., 2003. 302 с.

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

5. Щукина Г. И. Проблема познавательного интереса в педагогике. М.: Педагогика, 1971. 352 с.

6. Ланина И. Я. Формирование познавательных интересов учащихся на уроках физики. М.: Просвещение, 1985. 126 с.

7. Кондратьев А. С. Физическое понимание и его уровни // Вестник Северо-Западного отделения РАО, 1998. Вып. 3. С. 137-144.

8. 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.

9. Kushagra Agarwel, Himanshu Rai, Sandip Mondal Quantum dots: an overview of synthesis, properties and applications // Materials Research Express, 2023. Vol. 10. PP. 1-26.

10. 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.

11. Селевко Г. К. Энциклопедия образовательных технологий. В 2 Т. М.: НИИ школьных технологий, 2019. 1635 с.

12. 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.

13. 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.

14. Дьюи Дж. Демократия и образование. М.: Педагогика-Пресс, 2000. 384 с.

PROBLEM-BASED APPROACH TO LEARNING THE PHYSICAL BASICS OF ELECTRONICS: PREREQUISITES FOR USE AND METHODOLOGICAL AND TECHNOLOGICAL DEVELOPMENT

Borisov S.[1], Landa A.[1], Ostroumova Yu.[2], Khanin S.[1], Shumakov P.[1]
[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications
[2]Military Medical Academy of S. M. Kirov

The expediency is substantiated and the possibilities of organizing training in the physical basics of electronics based on the application of a problem-based approach are revealed. The methodological developments carried out in the logic of this approach, which can be used in the practice of teaching, are presented. The idea of a differentiated approach prescribing consideration of the level of preparedness and potential of students, pedagogical and technological support of the educational process is being developed. The preferred learning technologies in terms of the implementation of the problem-based approach are determined.

Key words: *the organization of training, the resourcefulness of the problem-activity approach, the content of the problems of learning, the task-activity form of presentation of the content, pedagogical and technological support of the educational process*

УДК 004.38
ГРНТИ 55.30.03

РАЗРАБОТКА РОБОТОТЕХНИЧЕСКОЙ ОМНИПЛАТФОРМЫ ДЛЯ МАНЕВРЕННОГО ПЕРЕМЕЩЕНИЯ В ОГРАНИЧЕННОМ ПРОСТРАНСТВЕ

А. Э. Брагина, Н. В. Чикалов

Научно-исследовательский институт «Рубин»

В статье представлена разработка мобильной омниколесной платформы, предназначенной для тестирования алгоритмов автономной навигации и позиционирования в условиях ограниченного пространства. Описана конструкция платформы, базирующаяся на трех омниколесах, представлена детализация аппаратной реализации.

омниколесная платформа, ROS Nav2, автономная навигация, мобильная робототехника

В настоящее время наблюдается стремительное развитие и внедрение мобильных робототехнических систем в такие области, как промышленная автоматизация, внутренняя логистика, медицинское обслуживание и интеллектуальные транспортные системы [1]. Особенно актуальной становится задача повышения маневренности и компактности роботизированных платформ, работающих в ограниченных пространствах – например, в складских помещениях, лабораториях и узких коридорах производственных цехов.

Классические мобильные платформы с дифференциальным приводом или управляемыми осями обладают ограниченными возможностями перемещения, требующими разворота корпуса для изменения направления движения. Это приводит к потере времени, усложнению навигации и повышенному риску столкновений с объектами в тесных зонах. В связи с этим особый интерес представляют омниколесные платформы, способные перемещаться в любом направлении без изменения ориентации корпуса [2]. Такие платформы обеспечивают: произвольное движение в плоскости (вперед, назад, вбок, по диагонали), повышенную точность позиционирования, сокращение времени маневров, возможность работы в условиях плотной застройки и динамической среды.

В статье рассматривается модель мобильной омниплатформы с тремя колесами, обеспечивающими движение в любом направлении без поворота корпуса. Платформа предназначена для тестирования алгоритмов автономного позиционирования и навигации.

Платформа состоит из следующих основных компонентов:

1. Микроконтроллер Arduino Mega 2560 выполняет низкоуровневое управление моторами, обработку сигналов с энкодеров и реализацию регулятора скорости;

2. Микро-ПК ZX01 PLUS (на базе Intel *N*100) осуществляет расчет желаемых скоростей платформы, используя Nav2 ROS, построение траектории и отправку управляющих сигналов;

3. Омниколеса обеспечивают возможность движения в любом направлении;

4. Двигатель постоянного тока с диском для измерения скорости энкодера JGA25-370;

5. Драйверы для моторов: Pololu Dual VNH5019 и Motor Shield L298P;

6. Лидар используется для построения карты окружающего пространства и обеспечения навигации;

7. Камера предназначена для распознавания объектов, маркировки, *QR*-кодов и других визуальных элементов, используемых для последующей интерпретации и принятия решений;

8. Источники питания:

– Li-Ion аккумулятор – основное питание моторов;

– PowerBank – питание Arduino и микрокомпьютера.

Схема подключения представлена на рисунке 1.

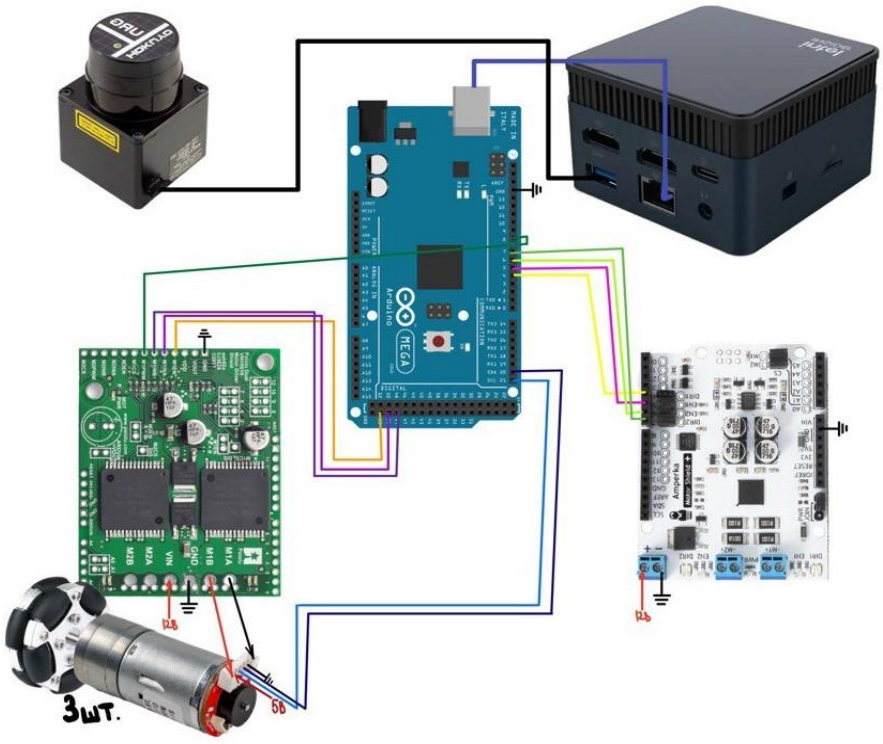


Рис. 1. Схема соединения компонентов платформы

Платформа построена на базе трех омниколес, установленных симметрично относительно центра масс на одинаковом расстоянии 0,1 м и под углами $\theta_1 = 0°$, $\theta_2 = 120°$, $\theta_3 = 240°$ от оси, направленной вперед.

Каждое колесо воспринимает комбинацию линейного и вращательного движения. Скорость вращения i-го колеса ω_i определяется из кинематического уравнения:

$$\omega_i = \frac{1}{R}(-sin(\theta_i) * v_x + cos(\theta_i) * v_y + L * \omega)$$

где R – радиус колеса, v_x и v_y – линейные скорости платформы в плоскости, ω – угловая скорость платформы вокруг вертикальной оси.

Подставляя углы колес и упрощая, получаем:

$$v_1 = v_y + L * \omega$$
$$v_2 = \frac{\sqrt{3}}{2} * v_x - \frac{1}{2} * v_y + L * \omega$$
$$v_3 = -\frac{\sqrt{3}}{2} * v_x - \frac{1}{2} * v_y + L * \omega$$

Управление платформой построено по следующему принципу: генерация траектории осуществляется на микро-ПК. Для каждого шага вычисляется желаемая скорость движения платформы в виде вектора (v_x, v_y, ω). Затем эти скорости передаются на Arduino и там выполняется пересчет скоростей платформы в скорости отдельных колес (v_1, v_2, v_3) по приведенной выше кинематической модели. Значения скоростей колес используются для формирования ШИМ-сигналов управления моторами. С каждого мотора считываются текущие значения тиков с энкодеров. На их основе оцениваются реальные скорости колес. Для коррекции управляющих воздействий реализован ПИД-регулятор, обеспечивающий стабилизацию скоростей. Обратно на микро-ПК отправляется рассчитанная текущая скорость платформы, полученная через обратное преобразование значений скоростей от энкодеров.

Общий вид собранной платформы и ее 3D-модель показаны на рисунке 2.

Представленная в работе омниплатформа демонстрирует практическую реализацию компактной и маневренной мобильной робототехнической системы, способной перемещаться в любом направлении без поворота корпуса. Такая конструкция особенно эффективна в условиях ограничен-

ного пространства, где требуется высокая точность позиционирования и оперативное выполнение маневров.

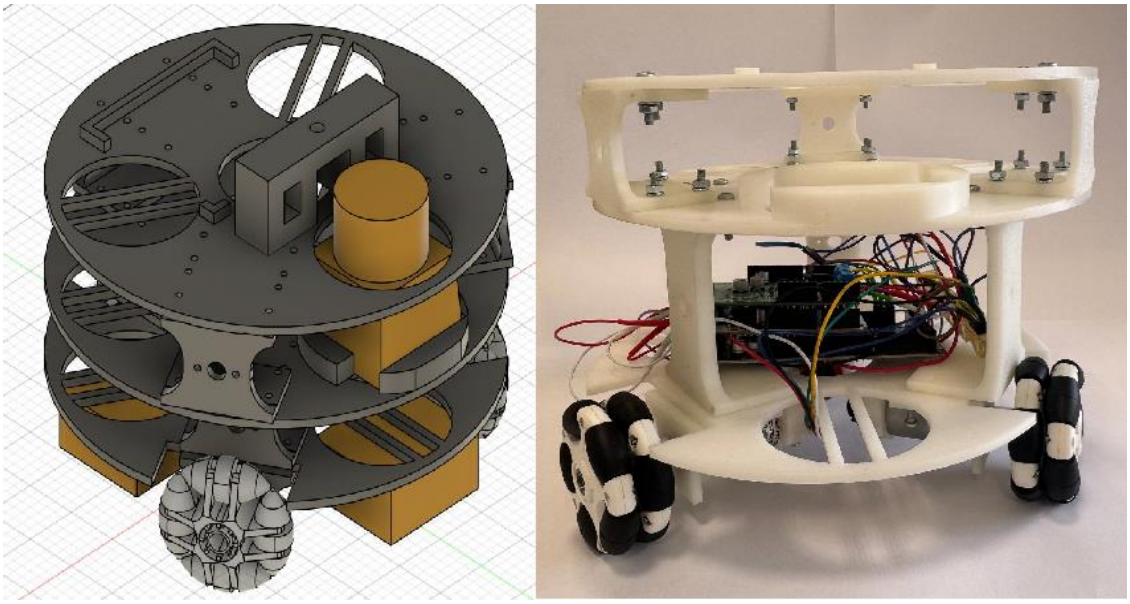


Рис. 2. Макет и реализация платформы

Разделение вычислительных задач между микроконтроллером и внешним микрокомпьютером позволяет гибко масштабировать систему: от простого управления по заданным скоростям до построения полной карты окружающей среды и распознавания объектов с помощью лидара и камеры. Применение обратной связи от энкодеров и ПИД-регулирование вращения колес обеспечивают стабильное движение по заданной траектории с возможностью динамической коррекции.

Разработка может быть использована в качестве базовой платформы для отладки алгоритмов навигации, построения карт местности с использованием технологии SLAM, тестирования систем компьютерного зрения, а также как учебный или исследовательский стенд для изучения методов управления мобильными роботам.

Список используемых источников

1. Ядровская М. В., Гурин И. В. Исследование актуальности робототехнических технологий // Advanced Engineering Research. 2022. Т. 22. № 4. С. 353-364.

2. Караваев Ю. Л. Теоретические и экспериментальные исследования динамики и управления некоторых систем с качением: дис. ... канд. физ.-мат. наук: 01.02.01 / Караваев Юрий Леонидович. Ижевск, 2015. 106 с.

Статья представлена ученым секретарем диссертационного совета АО "НИИ "РУБИН", кандидатом технических наук, доцентом Ю. В. Саниным.

DEVELOPMENT OF A ROBOTIC OMNIPLATFORM FOR MANEUVERABLE MOVEMENT IN CONFINED SPACES

Bragina A., Chikalov N.
Research Institute "Rubin"

This article presents the development of a mobile omni-wheeled platform designed for testing autonomous navigation and positioning algorithms in confined spaces. The platform's design, based on three omni wheels, is described, and a detailed hardware implementation is presented.

Key words: *omni-wheeled platform, ROS Nav2, autonomous navigation, mobile robotics*

УДК 004.38
ГРНТИ 47.59.49

РАЗРАБОТКА ОСНОВНЫХ ЭЛЕКТРОННЫХ УЗЛОВ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА

А. Э. Брагина, Н. В. Чикалов

Научно-исследовательский институт «Рубин»

В статье рассматривается разработка пульта управления для беспилотного летательного аппарата на отечественных компонентах. Описывается функционал устройства, позволяющий оператору контролировать полет и получать телеметрические данные. Также представлены макеты изделия. Подчеркивается важность развития отечественных технологий в области управления беспилотными аппаратами.

импортозамещение, разработка БПЛА, микроконтроллер, передача данных по радиоканалу

В современном мире беспилотные летательные аппараты (БПЛА) активно внедряются в различные отрасли: сельское хозяйство, логистику, мониторинг, безопасность [1]. Они обладают большим рядом преимуществ: вертикальный взлет, простая конструкция [2]. Однако, зависимость от импортных компонентов (микроконтроллеры, навигация, датчики, радиосвязь) создает трудности в производстве и использовании. Практически все российские БПЛА создаются на основе китайских контроллеров. Отсутствие отечественной базы обуславливает угрозу независимости, ограничивает импортозамещение, повышает уязвимость, влияет на стоимость и сроки. Формирование отечественной компонентной базы для БПЛА, включая исследования, разработку технологий и поддержку производителей, критически важно, а также соответствует указу Президента № 309 от 07.05.2024 о достижении технологического лидерства [3].

В статье описывается модель БПЛА и система управления на российской компонентной базе, включающая дрон и пульт. Подробно описаны обе части системы.

Для управления БПЛА рассматриваются радиоканалы (868 МГц, 915 МГц, 2.4ГГц; MAVLINK, ELRS) и оптические каналы. В данной работе для реализации радиоуправления выбран приемопередатчик E220-900T22D (900 МГц) по следующим причинам:

– низкое энергопотребление;

– большая дальность передачи (5 км);
– высокая проникающая способность;
– высокая масштабируемость сети.

Плата «Vostok UNO-VN035» была выбрана в качестве аппаратной платформы для этой разработки, поскольку она соответствует основному требованию – использование отечественных компонентов. Схема сборки пульта управления приведена на рис. 1.

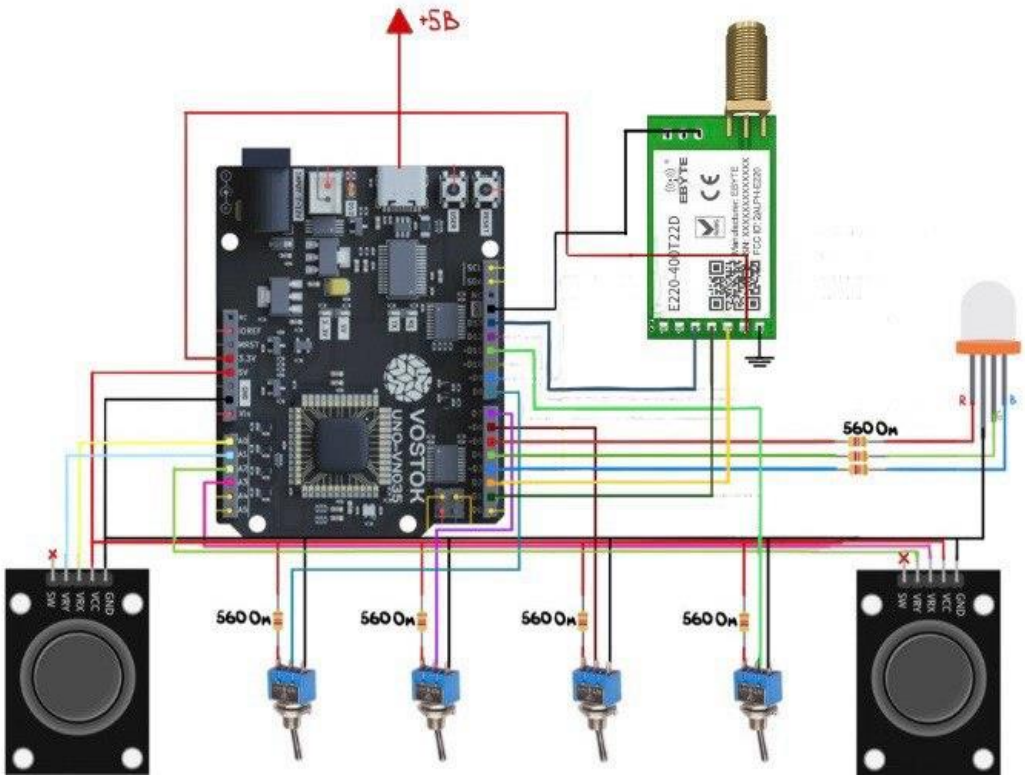


Рис. 1. Схема пульта управления летательного аппарата

1. Vostok UNO-VN035: Центральный микроконтроллер, реализующий логику управления БПЛА. Он выполняет АЦП аналоговых сигналов с джойстиков HW-504, преобразует их в цифровые команды и передает данные управления через интерфейс UART на радиопередатчик E220-900T22D.

2. Джойстик HW-504 (для Arduino): Потенциометрический датчик, генерирующий аналоговый сигнал напряжения, пропорциональный отклонению джойстика. Сигнал передается на вход АЦП Vostok UNO-VN035.

3. E220-900T22D: Радиочастотный передатчик, принимающий данные по UART от Vostok UNO-VN035 и модулирующий их для беспроводной передачи на БПЛА.

Напечатанная на 3D-принтере модель пульта (рис. 2) демонстрирует возможность локализации производства оборудования. Такой подход обес-

печивает контроль над процессом, позволяя быстро адаптировать конструкцию и дизайн под конкретные потребности.

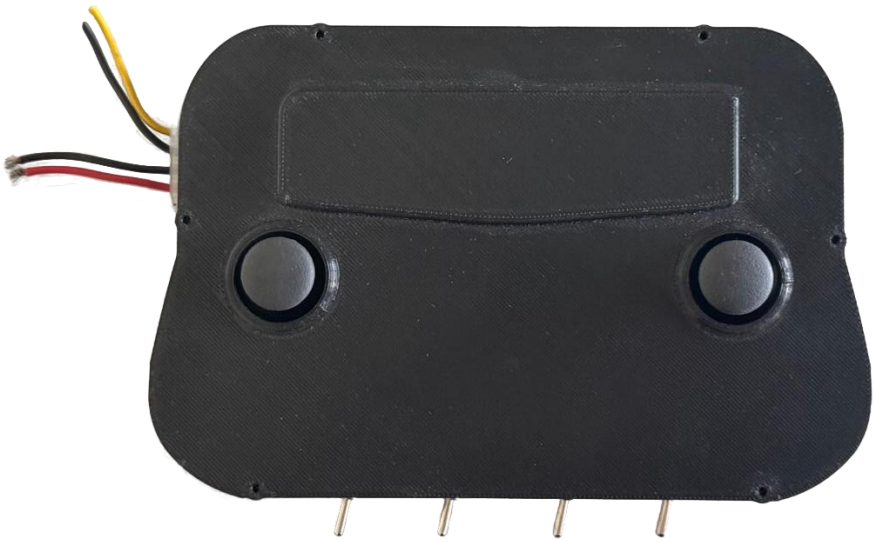


Рис. 2. Макет пульта управления летательным аппаратом

БПЛА принимает управляющие команды по радиоканалу и выполняет их благодаря следующим ключевым элементам:

1. Приемник E220-900T22D: получает и декодирует управляющие сигналы, передавая их на управляющее устройство.

2. Полетный контроллер "Vostok UNO-VN035": обрабатывает полученные данные и формирует управляющие сигналы для двигателей.

3. Датчик ИМ-10НС: в конструкции модуля используются акселерометры с температурной калибровкой, гироскопы и магнитометр, данные которых передаются в вычислитель, где происходит интегрирование с использованием адаптивного сигма-точечного фильтра Калмана, что позволяет обеспечивать точность и стабильность навигационных параметров.

4. Бесколлекторные моторы Diatone Mamba TOKA 2808.

5. Регуляторы скорости ESC: контролируют мощность двигателей, обеспечивая необходимое ускорение и маневренность, а также питают бортовую электронику.

Возможный макет БПЛА, созданный при помощи 3D-принтера, изображен на рисунке 3.

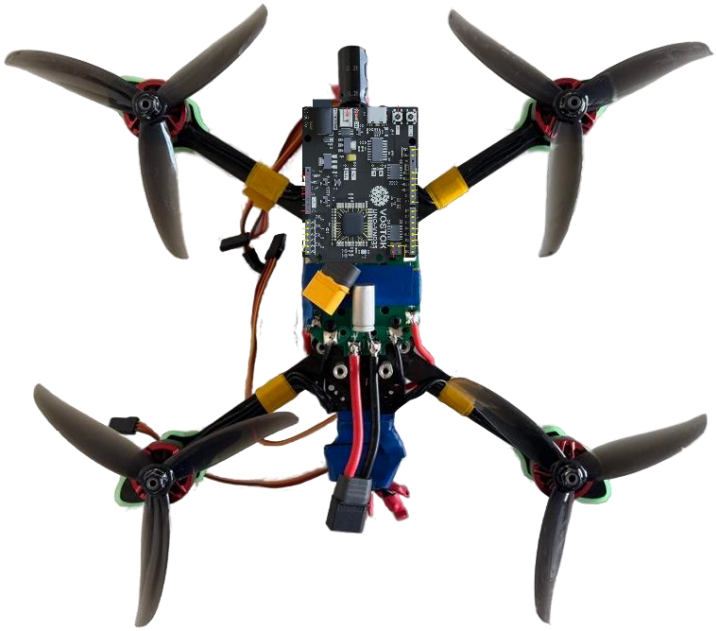


Рис. 3. Макет квадрокоптера

Проект по созданию российской компонентной базы (полетные контроллеры, электроника для пультов управления, esc и т.д.) для БПЛА имеет значительный экономический потенциал. Импортозамещение снизит зависимость от зарубежных поставщиков, а разработка доверенного отечественного ПО повысит безопасность. Полный контроль над производственным циклом позволит быстро адаптировать продукцию к требованиям рынка и конкурировать на международной арене. Кроме того, будет создана основа для интеграции БПЛА в более масштабные системы, например, беспилотные транспортные системы.

Список используемых источников

1. Исследование российского гражданского рынка беспилотных авиационных систем (БАС): аналитический отчет. Москва: Ассоциация «Аэронекст», 2023. С. 6-7.

2. Москаева, Е. В. Качество беспилотного летательного аппарата мультироторного типа / Е. В. Москаева, А. Я. Дмитриев // Известия Тульского государственного университета. Технические науки. 2020. № 12. С. 598-602. URL: https:// cyberleninka.ru/article/n/kachestvo-bespilotnogo-letatelnogo-apparata-multirotornogo-tipa/viewer (дата обращения 30.01.2025).

3. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: Указ Президента Российской Федерации от 07.05.2024 № 309. URL: http://publication.pravo.gov.ru/Document/View/0001202405070015 (дата обращения 07.05.2024).

Статья представлена ученым секретарем диссертационного совета АО "НИИ "РУБИН", кандидатом технических наук, доцентом Ю. В. Саниным.

DEVELOPMENT OF KEY ELECTRONIC COMPONENTS FOR AN UNMANNED AERIAL VEHICLE

Bragina A., Chikalov N.
Research Institute "Rubin"

This article discusses the development of a control panel for an unmanned aerial vehicle (UAV) based on domestic components. The functionality of the device, which allows the operator to control the flight and receive telemetry data, is described. Prototypes of the product are also presented. The importance of developing domestic technologies in the field of unmanned aerial vehicle control is emphasized.

Key words: *import substitution, UAV development, microcontroller, radio channel data transmission*

УДК 621.396.96
ГРНТИ 27.23.29

МЕТОДЫ МОДЕЛИРОВАНИЯ НЕПРЕРЫВНЫХ КАНАЛОВ СВЯЗИ В ГИБРИДНЫХ СЕТЯХ СВЯЗИ

А. Г. Владыко, Е. И. Глушанков, И. А. Горобцов, А. Ж. Лялина

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

В работе представлены методы математического моделирования непрерывных каналов связи в гибридных сетях, ориентированных на современные технологии беспроводной передачи. Предложены модели, основанные на стохастических дифференциальных уравнениях, отражающие физические свойства распространения сигнала в различных радиосредах. Разработанные схемы охватывают ключевые технологии, включая многолучевое распространение, интеллектуальное управление отражением и кодовые конструкции. Проведен сравнительный анализ устойчивости передачи данных в зависимости от условий среды. Результаты моделирования подтверждают эффективность предложенных решений для повышения надежности связи.

непрерывные каналы связи, гибридные сети, стохастические дифференциальные уравнения, модель распространения сигнала, интеллектуальные поверхности, пространственно-временное кодирование, помехоустойчивость

Одним из важнейших этапов исследования каналов связи является разработка математических моделей сигналов в непрерывных каналах связи является, так как проведение натурных испытаний, как правило, является сложным и не всегда возможным процессом и предполагает существенные временные затраты. Поэтому создание моделей является необходимым этапом изучения характеристик каналов связи и разработки алгоритмов первичной обработки сигналов в них. Одним из основных требований, предъявляемых к таким моделям, является их адекватность реальным процессам, происходящим в канале, которую можно оценить путем сравнения по критериям согласия результатов моделирование случайных процессов с теоретическими плотностями распределения вероятностей. Одним из наиболее конструктивных подходов к моделированию является использование метода переменных состояния и построение моделей в форме стохастических дифференциальных уравнений. При этом моделирование сигналов в непрерывных каналах связи в форме стохастических дифференциальных уравне-

ний предполагает решение задачи синтеза таких уравнений. Использование подобных моделей позволяет создать программные и аппаратные имитаторы каналов, с использованием которых возможно исследование алгоритмов обработки сигналов.

Система моделирования непрерывных каналов связи в гибридных системах связи

Для исследования физических процессов в гибридных системах связи (ГСС) были разработаны комплексные модели на платформе Simulink, охватывающие как блоки цифровой обработки сигналов, так и модули имитации радиосреды на основе стохастических дифференциальных уравнений (СДУ). Эти модели позволяют оценивать устойчивость систем к замираниям, многолучевому распространению и шумам, возникающим в условиях 5G/6G, RIS, NOMA и спутниковых каналов связи [1-9].

Модель представлена на рис. 1.

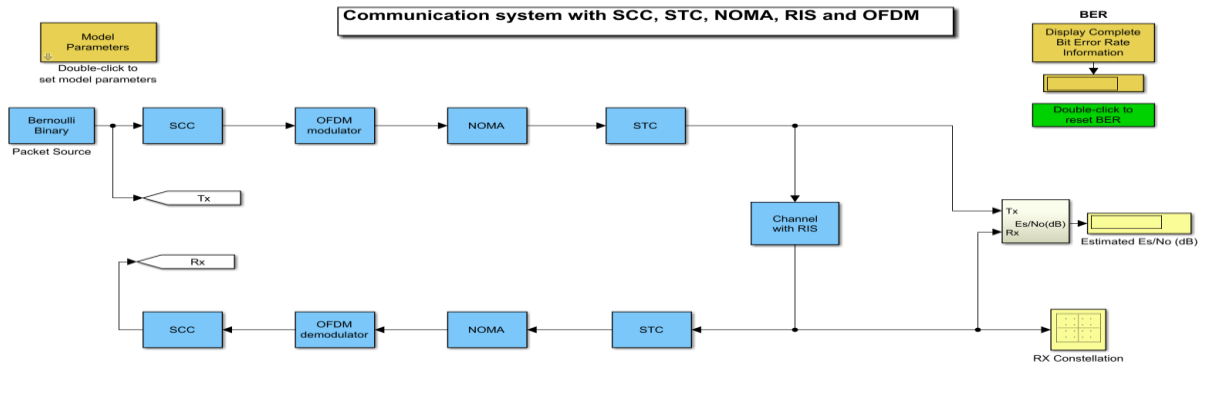


Рис. 1. Структура модели в среде Simulink

Модели непрерывных каналов связи на основе стохастических дифференциальных уравнений

Для описания непрерывных каналов связи использованы стохастические дифференциальные уравнения, отражающие как диффузные, так и линейные искажения в канале. Выведены модели с различными законами распределения, представленные в таблице 1 [10-13].

ТАБЛИЦА 1. Модели непрерывных каналов связи на основе стохастических дифференциальных уравнений

	ПРВ	СДУ	Описание
Распределение Райса	$p(\gamma)=\begin{cases}\frac{\gamma}{\sigma_0^2}e^{-\frac{\gamma^2-A^2}{2\sigma_0^2}}I_0\left(\frac{\gamma A}{\sigma_0^2}\right)\\ \text{для } \gamma\geq 0,\ A\geq 0\\ 0\end{cases}$	$A(t)=A(t_0)-\int_{t_0}^{t}\alpha A(\tau)d\tau+\int_{t_0}^{t}\frac{\beta}{A(\tau)}d\tau+\vartheta_A(t),$	моделирование мобильных каналов без прямой видимости, городская застройка, NLOS-сценарии
Распределение Рэлея	$p(\gamma)=\begin{cases}\frac{\gamma}{\sigma_0^2}e^{-\frac{\gamma^2}{2\sigma_0^2}}\text{ для }\gamma\geq 0\\ 0\end{cases}$	$A(t)=A(t_0)-\int_{t_0}^{t}\frac{4\sigma^2}{N_0}A(\tau)d\tau+\int_{t_0}^{t}\frac{N_0}{4A(\tau)}d\tau+\vartheta_A(t)$	динамика каналов с прямой видимостью, дроны, спутники, V2X
Распределение Накагами	$p(\gamma)=\frac{2m^m\gamma^{2m-1}}{\Gamma(m)a^{2m}}e^{-\frac{m}{a^2}\gamma^2}$ для $\gamma\geq 0$	$A(t)=A(t_0)+\int_{t_0}^{t}K\left(\frac{2m-1}{A(\tau)}-\frac{mA(\tau)}{a^2}\right)d\tau+\sqrt{K}\vartheta_A(t)$	универсальное приближение реальных fading-сценариев, включая как Рэлея, так и Райса
Логнормальное распределение	$p(\gamma)=\frac{1}{\gamma\sqrt{2\pi\sigma_M^2}}e^{-\frac{(\ln\gamma-m_M)}{2\sigma_M^2}}$ для $\gamma\geq 0$	$A(t)=A(t_0)-\int_{t_0}^{t}\frac{K}{A\sigma^2}\ln\left(\frac{A}{\mu}+\sigma\right)d\tau+\sqrt{K}\vartheta_A(t)$	моделирование медленных замираний (shadowing), агрегация рассеянных процессов
Гамма распределение	$f(x)=\beta x\left(\frac{\alpha}{x}-\frac{1}{\beta}\right), g(x)=\frac{\beta}{2}+\sqrt{2\beta x}$	$A(t)=A(t_0)-\int_{t_0}^{t}\frac{K}{A\sigma^2}\ln\left(\frac{A}{\mu}+\sigma\right)d\tau+\frac{\beta}{2}+\sqrt{2\beta A}\vartheta_A(t)$	моделирование теневого замирания в лесистой, горной, городской среде
Ка распределение	$p(\gamma)=\frac{\nu L\sqrt{2\pi}}{z_0\Gamma(\nu)\Gamma(L)}\frac{e^{f(x,z_0)}}{\sqrt{\lvert f''(x,z_0)\rvert}}$	$A(t)=A(t_0)-\int_{t_0}^{t}K\frac{f'(A,z_0)}{2}d\tau+\sqrt{K}\vartheta_A(t)$	сложные радиосреды с одновременным рассеянием и теневым замиранием, военные и морские каналы
	$f=-\frac{x}{z}-\nu z+(\nu-1)\ln\nu z$ $z_0=\frac{\nu-1}{2\nu}\left(1\pm\sqrt{1+\frac{4\nu x}{(\nu-1)^2}}\right)$		

Каждая модель построена в форме СДУ вида:

$$\frac{dA(t)}{dt}=f_A[A(t)]+g_A[A(t)]\vartheta_A(t), \quad (1)$$

где $f_A[A(t)]$, $g_A[A(t)]$ – неизвестные коэффициенты СДУ; $\vartheta_A(t)$ – белый шум единичной интенсивности. Коэффициенты СДУ синтезированы на основе представления соответствующих плотностей уравнением Фоккера-Планка-Колмогорова, определения коэффициентов сноса и диффузии и получения на их основе неизвестных коэффициентов СДУ.

Результаты моделирования

В ходе исследования были разработаны и протестированы модели ключевых компонентов гибридных систем связи (ГСС), включая блоки физического уровня с сигнально-кодовыми конструкциями (СКК), пространственно-временным кодированием (ПВК), модуляцией OFDM, схемами множественного доступа (NOMA), интеллектуальными переотражающими поверхностями (RIS), а также стохастическими моделями непрерывных каналов связи (НКС). Все модели реализованы в среде Simulink и позволяют проводить численные эксперименты по оценке качества связи в различных сценариях. Результаты моделирования для рэлеевского канала представлены на рис. 2.

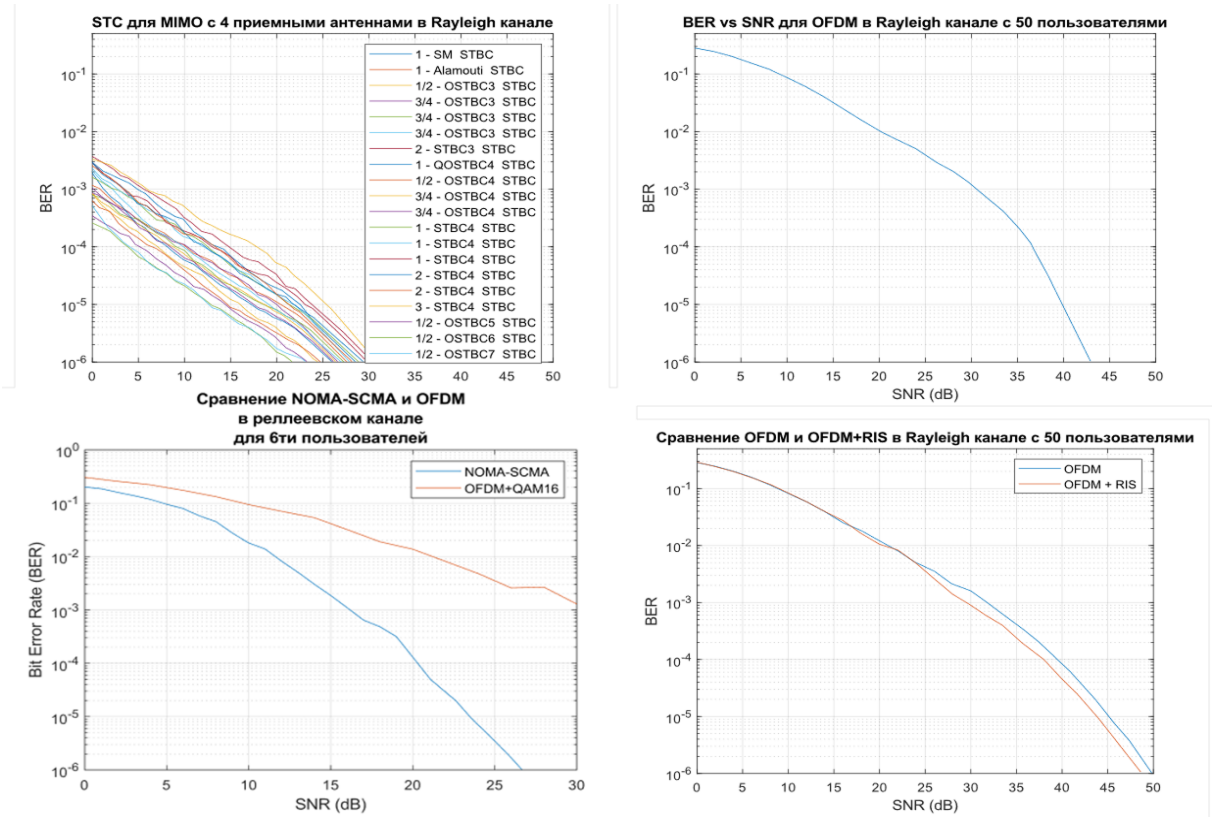


Рис. 2. Результаты работы разработанной модели

Таким образом, модели на основе СДУ позволяют реалистично воссоздать различные среды распространения сигнала. STTC обеспечивает значительный выигрыш в устойчивости для всех рассмотренных каналов, особенно в условиях многолучевого распространения. Наибольший эффект достигается в сложных каналах типа Релея и логнормального, где простые схемы связи теряют надежность.

Список используемых источников

1. Proakis J.G., Salehi M. Digital Communications. McGraw-Hill, 5th ed., 2008.

2. Tse D., Viswanath P. Fundamentals of Wireless Communication. Cambridge University Press, 2005.

3. Liang Y.-C., Chen R., Li G.Y., et al. Cognitive Wireless Mesh Networks with STC and MIMO // IEEE Signal Processing Magazine. 2008. Vol. 25. № 6. PP. 71–81. 2008.

4. Goldsmith A. Wireless Communications. Cambridge University Press, 2005.

5. Ding Z., Liu Y., Choi J., Elkashlan M., et al. Application of Non-Orthogonal Multiple Access in LTE and 5G Networks // IEEE Communications Magazine. 2017. Vol. 55. № 2. PP. 185–191.

6. Lu Y., Zhu J., et al. Simultaneous Wireless Information and Power Transfer With NOMA for 5G Systems // IEEE Transactions on Vehicular Technology. 2018. Vol. 67. № 6. PP. 5761–5773.

7. Björnson E., Sanguinetti L. Intelligent Reflecting Surfaces for Wireless Communications. Now Publishers, 2021.

8. Zhang S., Zhang Q., Di B., Song L. Reconfigurable Intelligent Surfaces for 6G: Principles, Applications, and Research Directions // IEEE Communications Magazine. 2020. Vol. 58. № 6. PP. 50–56.

9. Tang W., Chen M.Z., et al. Wireless Communications With Reconfigurable Intelligent Surface: Path Loss Modeling and Experimental Measurement // IEEE Transactions on Wireless Communications. 2021. Vol. 20. № 1. PP. 421–439.

10. Kontorovich V. M. Probability Theory Methods in Radiophysics and Communication Theory, Moscow: Radio i Svyaz, 2003.

11. Glushankov E., Kirik D., Tsvetkov D. Development of a Software Package for the Study of MIMO Systems With Spectral-Code Constructions and Space-Time Coding. AIP Conference Proceedings, 2023.

12. 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.

13. Rappaport T. S. Wireless Communications: Principles and Practice. Prentice Hall, 2nd ed., 2002.

Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2025-005, "Прикладные научные исследования в области разработки методов мониторинга и идентификация типов трафика для эффективного использования сетевого ресурса в гибридных сетях связи" (регистрационный номер ПТНИ: 1024062100008-4).

MODELING METHODS FOR CONTINUOUS COMMUNICATION CHANNELS IN HYBRID COMMUNICATION NETWORKS

Vladyko A., Glushankov E., Gorobtsov I., Lyalina A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Currently, hybrid communication networks that integrate multiple radio technologies require accurate modeling of signal propagation to ensure reliable data transmission. This report presents mathematical modeling methods for continuous communication channels based on stochastic differential equations, which reflect the physical characteristics of signal propagation in various radio environments. The developed models incorporate key wireless technologies, including multipath propagation, intelligent reflection control, and signal-code constructions. A comparative analysis of transmission robustness under different environmental conditions is carried out. Simulation results confirm the effectiveness of the proposed solutions in enhancing the reliability of hybrid wireless systems.

Key words: *continuous communication channels, hybrid networks, stochastic differential equations, signal propagation model, intelligent surfaces, space-time coding, interference resilience*

УДК 681.5:681.586
ГРНТИ 55.30.31

МОДЕРНИЗАЦИЯ МОБИЛЬНОГО РОБОТА ROBO-PICA ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

П. А. Волынкин

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

Робототехнический комплекс ROBO-PICA используется в СПбГУТ в рамках учебных курсов "Программирование мобильных робототехнических комплексов" и "Программирование беспилотных транспортных средств". Основой этого робота является контроллер RBX-877 V2.0 на базе микроконтроллера PIC16F887. Данный комплекс является роботом 2-го поколения с адаптивным управлением. Сильно ограниченный объем памяти для программы не позволяет в данном роботе реализовать функции искусственного интеллекта. В работе рассматриваются как аппаратные, так и программные решения расширения возможностей робототехнического комплекса ROBO-PICA до уровня роботов 3-го поколения. На начальном этапе исследуются и реализуются варианты внедрения для данного комплекса возможностей технического зрения.

робототехнический комплекс, искусственный интеллект, техническое зрение

Робототехническая мобильная платформа ROBO-PICA (рис. 1), используемый в учебном процессе в рамках учебных курсов «Программирование мобильных робототехнических комплексов» и «Программирование беспилотных транспортных средств» представляет собой мобильный робот 2-го поколения, что не дает возможности в полной мере реализовать в учебном процессе элементы искусственного интеллекта.

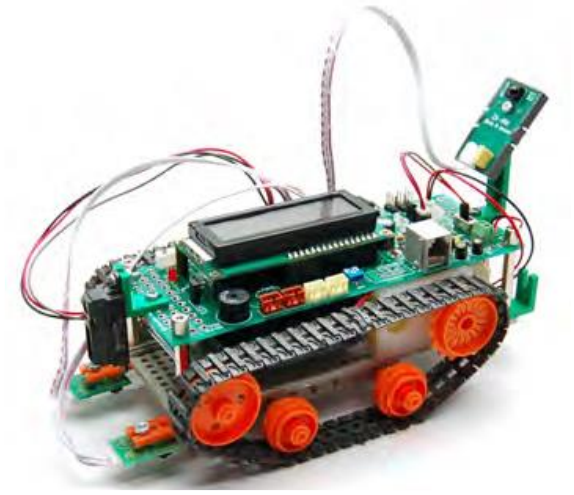


Рис. 1. Робототехническая мобильная платформа ROBO-PICA

В связи в этим ставится задача по разработке аппаратно-программные решения для перевода робота в разряд роботов 3-го поколения (начиная с машинного зрения).

В качестве контроллера в мобильном робототехническом комплексе ROBO-PICA) используется плата управления RBX-877 V2.0, где центральное место которого занимает микроконтроллер PIC16F887, построенный по гарвардской архитектуре RISC с 35 простыми инструкциями [1]. Для программирования этого микроконтроллера имеется в наличии специальная версия языка С для микроконтроллеров – microC компании microElektronika.

Рис. 2. Контроллер RBX-877 V2.0

Кроме контроллера в состав комплекса входит набор датчиков (расстояния, отражатели для движения по трассе, пульт дистанционного управления и приемником). Однако, ввиду крайне малого размера оперативной памяти как данных (256 байт), так и инструкций (8 КСлов), получать и обрабатывать видеоизображения нет возможности, то есть такой комплекс можно отнести к роботам 2-го поколения с адаптивным управлением. 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.

К аппаратным решениям можно отнести следующее варианты:

– расширение объемов памяти инструкций и данных для микроконтроллера PIC16F887. Но для этого варианта придется полностью разрабатывать и заменять контроллер;
– функции управления движущими элементами комплекса, а также прием сигналов от датчиков расстояния и отражателей могут быть возложены на контроллер RBX-877 V2.0. А получение видеосигнала, его обработкой и управлением контроллером будет заниматься микрокомпьютер с достаточным объемом памяти и интерфейсами для связи с контроллером;

Второй вариант реалистичнее. В этом случает потребуется просто подобрать соответствующий требуемым параметрам микрокомпьютер.

Для взаимодействия с контроллером робота такой микрокомпьютер должен поддерживать интерфейсы, присутствующие у микроконтроллера PIC16F887, а именно:
– программируемые одноразрядные порты ввода-вывода;
– UART;
– I^2C.

С точки зрения памяти для инструкций и данных требования могут быть следующими:
– память RAM > = 256 Mb;
– память Flash > = 8 Gb.

Кроме этого, микрокомпьютер должен обладать интерфейсом для подключения видеокамеры достаточного разрешения для реализации машинного зрения.

Для связи с компьютером потребуется интерфейсы USB и HDMI, а для хранения исходного кода и размещения операционной системы – интерфейс microSD.

Сравнивая наиболее популярные одноплатные микрокомпьютеры, к которым относятся: Onion Omega2S, Orange Pi Zero, FriendlyElec NanoPi NEO3, Arduino mega 2560 r3, Raspberry Pi 4 B, ASUS Tinker Board S, Odroid-XU4, NVIDIA Jetson Nano Developer Kit, Khadas VIM2, Udoo x86, предъявленным требованиям удовлетворяет в наилучшей степени Raspberry Pi 4 B.

Данный микрокомпьютер построен на гарвардской RISC архитектуре ARM11, имеет 4 ядра процессора разрядность 64 бита. Тактовая частота процессора составляет 1.5 ГГц [2].

Для связи с контроллером робота у выбранного микрокомпьютера имеются интерфейсы: HDMI (для связи с монитором персонального компьютера в ходе разработки программного обеспечения), USB 2.0 (3.0). Для по-

лучения видеосигнала видеокамера Raspberry Camera подключается к микрокомпьютеру посредством интерфейса 15-pin MIPI. Операционная система и программное обеспечение размещается на карте MicroSD размером от 16 до 32 Гб. Интерфейсы низкого уровня (одноразрядные порты ввода-вывода, UART, I²C) дают возможность передавать информацию для управления контроллером робота RBX-877 V2.0 с микрокомпьютера. Учитывая, что в будущем к микрокомпьютеру может быть подключен не один контроллер, а еще и другие устройства, для связи микрокомпьютера с контроллером выбирается интерфейс I2C, так как UART менее стабильно работает и позволяет связывать между собой только одну пару устройств.

В результате была предложена и реализована следующая структурная схема усовершенствованного робота, показанная на рис. 3.

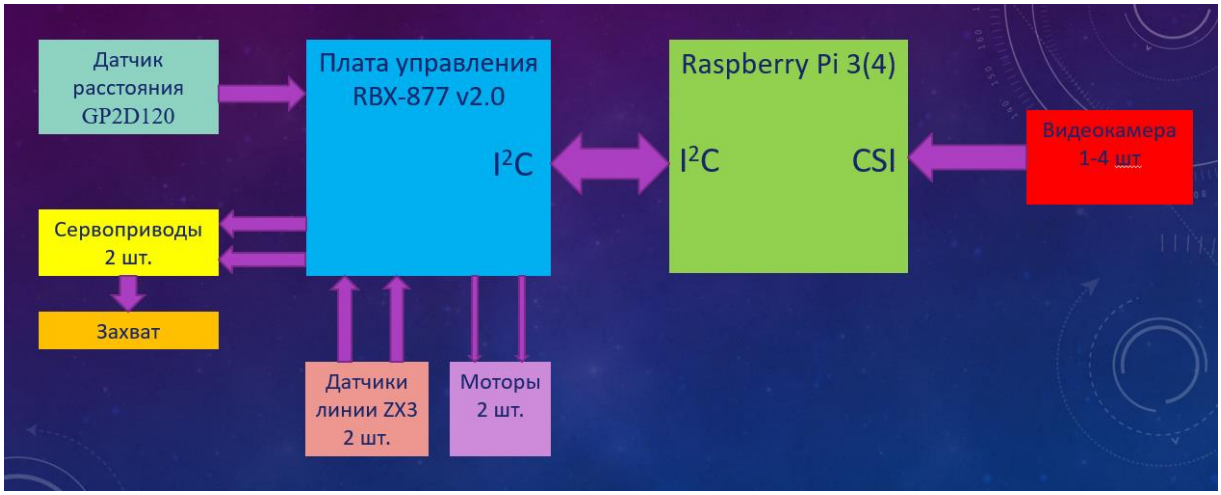


Рис. 3. Архитектура усовершенствованного робота с машинным зрением

Микрокомпьютер имеет возможность работать под управлением операционной системы Debian Linux Raspberry Pi OS, которая устанавливается на microSD карту. В составе этой ОС предлагается штатное средство разработки на языке Python.

Было разработано программное обеспечение, позволяющее получать от видеокамеры сигнал, обрабатываемый алгоритмами технического зрения. Данное ПО позволяет роботу обнаруживать и идентифицировать объекты, попадающие в поле его зрения. В результате, микрокомпьютер вырабатывает управляющие сигналы, которые поступают по интерфейсу I^2C на контроллер мобильного робота, который в свою очередь посылает сигналы двигательной системе робота. На контроллер робота возложены исключительно функции управления двигательной системой. На рис.4 показан результат полученного и отфильтрованного видеосигналов.

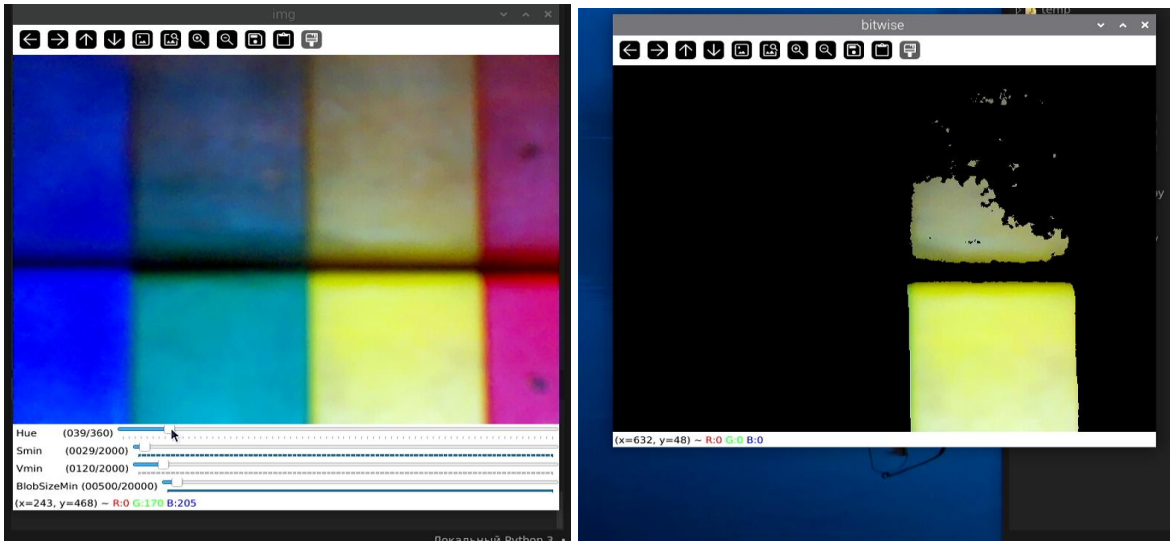


Рис. 4. Исходный (слева) и отфильтрованный (справа) видеосигналы для поиска объектов заданного (в данном случае – желтого) цвета.

Усовершенствованный робот показан на рис 5.

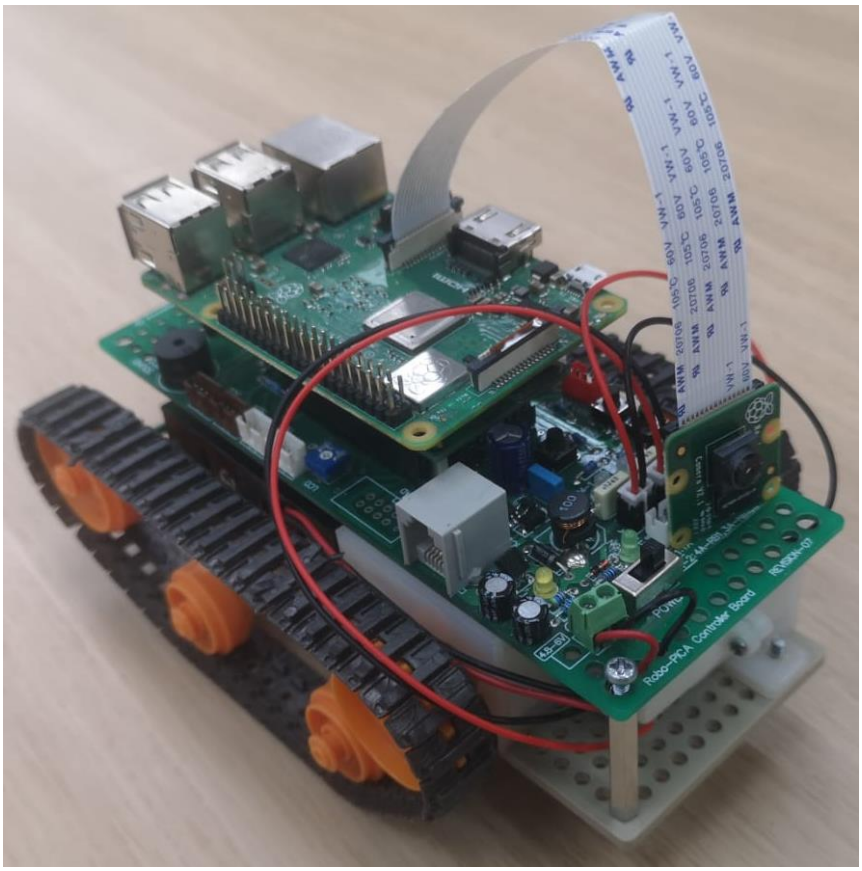


Рис. 5. Усовершенствованный мобильный робот ROBO-PICA с блоком компьютерного зрения на микрокомпьютере Raspberry Pi.

В дальнейшем планируется разместить на робототехнической платформе манипулятор типа «схват» и разработать программное обеспечение,

позволяющее роботу искать требуемые объекты, захватывать их и перемещать на заданные площадки.

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

IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE ELEMENTS IN THR ROBO-PICA RBX-877 MOBILE ROBOTICS COMPLEX

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

The ROBO-PICA robotics complex is used in St. Petersburg State University as part of the training courses "Programming of mobile robotic complexes" and "Programming of unmanned vehicles". The basis of this robot is the RBX-877 V2.0 controller based on the PIC16F887 microcontroller. This complex is a 2nd generation robot with adaptive control. The very limited amount of memory for the program does not allow this robot to implement artificial intelligence functions. The paper considers both hardware and software solutions for expanding the capabilities of the ROBO-PICA robotics complex to the level of 3rd generation robots. At the initial stage, implementation options for this set of technical vision capabilities are being explored and implemented.

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

УДК 621.396
ГРНТИ 47.49.02

ОЦЕНКА ТОЧНОСТИ ФИЛЬТРАЦИИ РАДИОНАВИГАЦИОННЫХ ПАРАМЕТРОВ

Е. И. Глушанков, А. В. Суденкова

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

В качестве показателя точности фильтрации навигационных параметров, как правило, используется дисперсия ошибки оценивания, которая, хотя и является самодостаточной «внутренней» метрикой ошибки и позволяет сравнивать алгоритмы между собой, не предоставляет информацию о потенциальной точности фильтрации. С другой стороны, целью фильтрации является отделение полезного сигнала от шума, что на практике означает необходимость определения выигрыша в отношении сигнал-шум – «внешней» метрики ошибки. В работе представлен обзор различных способов оценки точности радионавигационных параметров на примере работы фильтров Калмана 1-го и 2-го порядков и фильтра по критерию максимума апостериорной вероятности при воздействии на сигнал белого и цветного шума.

радионавигационный сигнал, отношение сигнал-шум, граница Крамера-Рао, фильтр Калмана, плотность вероятности.

Рассмотрим следующую модель наблюдаемого радионавигационного сигнала:

$$s(t) = A \times sin(\,(\omega - \omega_d(t)) \cdot (t - \tau_з(t)) + \phi(t)) + v(t). \qquad (1)$$

где A – постоянная амплитуда сигнала, $\omega_d(t) = 2\pi f_d$ – допплеровский сдвиг частоты, $\tau_з(t)$ – временной сдвиг, $\varphi(t)$ – фазовый сдвиг, $v(t)$ – измерительный шум.

Случайными параметрами, подлежащими оценке, являются ω_d, $\tau_з$ и φ. Вектор состояния, описывающий динамику изменения случайных параметров сигнала с учетом их плотностей распределения вероятности (ПРВ):

$$dX(t)/dt = \left[d\tau_з(t)/dt \quad d\omega_d(t)/dt \quad d\phi(t)/dt \right]$$

Можно выделить две подхода к оценке точности фильтрации:

1. «Внутренняя» характеристика точности – дисперсия ошибки оценивания.

2. «Внешняя» характеристика точности – выигрыш в отношении сигнал-шум (ОСШ) после применения фильтрации.

«Внутренняя» характеристика точности – дисперсия ошибки оценивания (среднеквадратическая ошибка).

Ковариационная матрица ошибок оценивания

При моделировании алгоритмов Калмана или других методов, основанных на итеративном принципе получения оценки исследуемого параметра, вычисляется ковариационная матрица ошибок, которая позволяет судить о расхождении сигнала состояния с его оценкой в реальном времени. Для линейных фильтров ковариационная матрица характеризует потенциальную точность оценивания наряду с предельными границами.

На рисунках 1–2 представлены полученные в ходе фильтрации графики значений элементов ковариационной матрицы $V_x(t)$ для частоты ($V_\varphi(t)$) и фазы ($V_{fd}(t)$) при белом гауссовском шуме (БГШ) измерений для фильтров Калмана 1-го порядка точности, 2-го порядка и фильтра по критерию максимума апостериорной вероятности (МАВ). Верхние индексы над символами φ и f_d обозначают соответствующие им ПРВ (индекс «*MT*» – параметр имеет распределение фон Мизеса-Тихонова, индекс «*N*» – параметр имеет нормальное распределение).

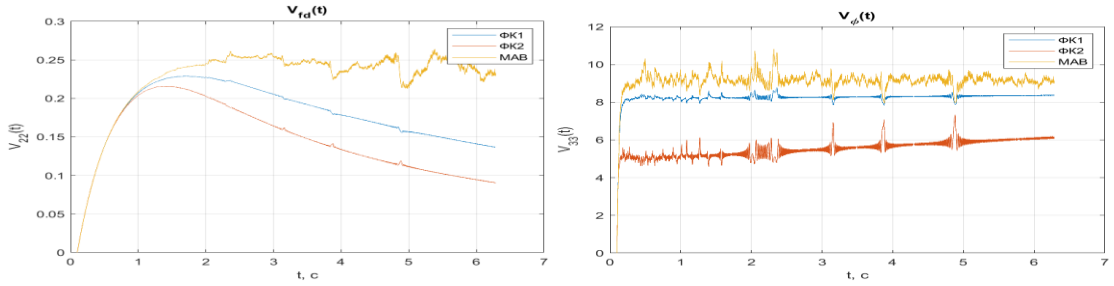


Рис. 1. Элементы ковариационной матрицы при БГШ (φ^{MT}, f_d^N) при ОСШ 20 дБ

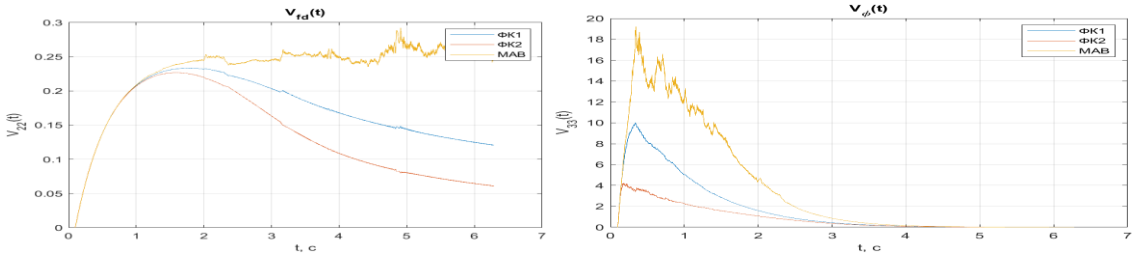


Рис. 2. Элементы ковариационной матрицы при БГШ (φ^N, f_d^N) при ОСШ 20 дБ

Потенциальная точность фильтрации, предельные границы

Для определения потенциальной точности оценок случайных параметров навигационных сигналов применяются алгоритмы, основанные на вы-

числении различного вида предельных границ. Одной из самых распространенных является граница Крамера-Рао (ГКР), позволяющая оценить минимально достижимую дисперсию ошибки оценивания.

Пусть оценки фазы, доплеровского сдвига и задержки являются несмещенными. Если в качестве характеристики точности принять квадрат ошибки, то эффективной оценкой является такая оценка, которая имеет наименьшую дисперсию относительно исследуемого параметра. Известно [1], что дисперсия оценок максимального правдоподобия совпадает с ГКР, из чего вытекает неравенство Крамера-Рао:

$$D_X \geq -\left(E\left[\frac{\partial^2 ln\, p(X|s)}{\partial X^2}\right]\right)^{-1}, \quad (2)$$

где $p(X|s)$ – апостериорная ПРВ, D_X – дисперсия ошибки оценивания параметра X за интервал наблюдения T.

Приведем выражения для ГКР задержки, фазы и доплеровского сдвига при условии, что они были выведены для неизменных на интервале наблюдения параметров с равномерными априорными ПРВ [2]. Синтезированные алгоритмы фильтрации не удовлетворяют этому требованию, следовательно, действительная потенциальная точность оценок не обязана равняться вычисленным ГКР, однако по величине несовпадения ГКР и настоящих оценок все еще можно делать выводы относительно точности алгоритмов фильтрации в первом приближении.

ГКР для фазы сигнала (здесь и далее представлены выражения D, справедливые для гауссовского белого или цветного [3] шума измерений):

$$D_{\phi} = \frac{1}{4q^2},$$

где q – ОСШ.

ГКР для частоты Доплера:

$$D_{fd} = \frac{1}{4(2\pi \cdot q \cdot T)^2}, \text{ при } q << 1 \text{ или } D_{fd} = \frac{1}{2q(2\pi \cdot T)^2}, \text{ при } q >> 1$$

ГКР для задержки:

$$D_{\tau} = \frac{1}{4(q \cdot \beta)^2},\ \beta = \sqrt{\int_{-\Delta f/2}^{\Delta f/2} (2\pi f)^2 S_h(f) df},$$

где β – ширина спектра огибающей радиосигнала, Δf – ширина спектра импульса, $S_h(f)$ – спектральная плотность мощности корреляционной функции прямоугольного символа кодовой последовательности:

$$S_h(f) = \tau_c \left(sin(\pi f \tau_c) \Big/ \pi f \tau_c \right)^2,$$

где $\tau_c = 1/\Delta f$.

Вычисление среднеквадратической ошибки *MSE* (Mean Square Error) после накопления оценок за интервал наблюдения эквивалентно нахождению дисперсии, что позволяет сравнивать *MSE* с ГКР без дополнительных преобразований:

$$MSE = \sum_{i=1}^{N} (X_i - \hat{X}_i)^2 / N,$$

где X_i – i-й случайный параметр, $\hat{X}_i$ – оценка параметра X_i, N – количество итераций за время наблюдения.

Примем $\tau_c = T$, тогда при отношении сигнал-шум, равном 19 дБ и 20 дБ, результаты сравнения ГКР и *MSE* представлены соответственно в таблицах 1 и 2.

ТАБЛИЦА 1. Сравнение среднеквадратической ошибки и границы Крамера-Рао для задержки, частоты Доплера и фазы сигнала при ОСШ = 19 дБ

		τ, с	f_d, Гц	φ, рад
MSE (БГШ) φ^N, f_d^N	ФК1	0.000855	0.000393	0.00177
	ФК2	0.000855	0.000337	0.00059
	МАВ	0.000855	0.000350	0.00454
MSE (цветной шум) φ^N, f_d^N	ФК1	0.0013	0.00034	0.0034
	ФК2	0.0013	0.00022	0.00045
	МАВ	0.0013	0.00026	0.0044
MSE (БГШ) φ^{MT}, f_d^N	ФК1	0.000834	0.000826	0.01178
	ФК2	0.000834	0.000297	0.00455
	МАВ	0.000834	0.000682	0.00512
MSE (цветной шум) φ^{MT}, f_d^N	ФК1	0.0053	0.000388	0.01095
	ФК2	0.0053	0.000211	0.00491
	МАВ	0.0053	0.000253	0.00528
Граница Крамера-Рао		0.000782	0.0000121	0.0000396

ТАБЛИЦА 2. Сравнение среднеквадратической ошибки и границы Крамера-Рао для задержки, частоты Допплера и фазы сигнала при ОСШ = 20 дБ

		τ, с	f_d, Гц	φ, рад
MSE (БГШ) φ^{MT}, f_d^N	ФК1	0.000322	0.000435	0.01368
	ФК2	0.000322	0.000267	0.00716
	МАВ	0.000322	0.000330	0.00778
MSE (БГШ) φ^{N}, f_d^N	ФК1	0.0005	0.00042	0.01129
	ФК2	0.0005	0.00021	0.00021
	МАВ	0.0005	0.00033	0.01698
Граница Крамера-Рао		0.0000493	0.0000096	0.000025

Из таблиц можно сделать вывод, что с учетом принятых допущений, отличия в точности оценивания параметров для фильтров Калмана и фильтра МАВ с нижней границей дисперсии лежат в пределах 1–2 порядков. При этом разница на порядок для цветного и белого шума наблюдается только в отношении задержек.

Для расчета ГКР разработаны также рекуррентные способы [4, 5], целью которых является снижение вычислительной сложности при большом количестве измерений; они применяются в нелинейных системах оценивания, для которых трудно получить аналитическое представление апостериорной ПРВ. ГКР относительно проста в вычислении, но не является самой точной характеристикой потенциальной точности, и, кроме того, не учитывает пороговый эффект [6]. Самая высокая (и, следовательно, самая точная, при том учитывающая пороговый эффект) граница – граница Баранкина, не имеет аналитического решения, и даже численное ее определение затруднено, поэтому на практике в качестве компромисса между требуемой точностью и вычислительной сложностью применяются границы Чепмена-Роббинса, Бхатачария и др.

Принцип получения ГКР для шума с неизвестной ПРВ следующий:

1. Задание ПРВ:

Если шум представлен в виде стохастического дифференциального уравнения (СДУ), по его коэффициентам с помощью уравнения Фоккера-Планка-Колмогорова (УФПК) определяются коэффициенты сноса и диффузии, затем по ним находится плотность вероятности.

Например, для процесса $\gamma(t)$: $d\gamma(t)/dt = -a\gamma(t) + n(t)$, где $n(t)$ – белый гауссовский шум, a – константа.

Коэффициент сноса: -aγ(t) , коэффициент диффузии: $N_0/2$.

УФПК для ПРВ p: $dp(\gamma)/dt = a\,\partial\gamma(t)\cdot p(\gamma,t)/\partial y + N_0/2\cdot \partial^2 p(\gamma,t)/\partial y^2$.

2. Подстановка ПРВ в выражение (2) или какой-либо другой алгоритм вычисления предельных границ.

«Внешняя» характеристика точности – выигрыш в ОСШ

Отдельный интерес на практике представляет измерение выигрыша в ОСШ, вычисляемого как отношение ОСШ после фильтрации (SNR_{out}) и до (SNR_{in}):

$$K = SNR_{out}[dB] - SNR_{in}[dB],$$

где SNR_{in} [раз] = P_s/P_v, P_s – мощность сигнала, которую можно определить численно как дисперсию сигнала D($s(t)$) (1); P_v – мощность шума наблюдений, заданная величина;

SNR_{out} [раз] = $P_{\hat{s}}/P_{\hat{v}}$, где $P_{\hat{s}}$ можно вычислить как дисперсию оценки вектора наблюдения (например, при подстановке оценок случайных параметров в уравнение (1)); $P_{\hat{v}}$ – оценочная мощность шума наблюдений, которую можно рассчитывать как $D(z_{ideal}(t) - \hat{z}(t)) = D([z(t) - v(t)] - \hat{z}(t))$.

Список используемых источников

1. Cramér H. Mathematical methods of statistics. Princeton university press, 1999. Т. 9.

2. Перов А. И. и др. ГЛОНАСС. Принципы построения и функционирования // Радиотехника. 2010. 800 с.

3. Белокришнан А. Теория фильтрации Калмана: Пер. с англ. М.: Мир, 1988. 168 с.

4. Simandl M. Lecture notes on state estimation of nonlinear non-Gaussian stochastic systems // University of West Bohemia, Pilsen. 2006. 155 p.

5. Арсеньев Д. Г., Берковский Н. А. Рекуррентное вычисление нижних границ РАО-Крамера в байесовских задачах с нелинейными измерениями при постоянном векторе состояния // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Физико-математические науки. 2012. №. 4 (158). С. 57–64.

6. Гвоздарев А. С., Артемова Т. К., Артемов К. С. Анализ поведения пороговой величины отношения сигнал/шум в задачах оценки параметров объектов в радиоголографии эталонным фазовым методом // Журнал радиоэлектроники. 2015. №. 10. С. 8–18.

ASSESSMENT OF THE ACCURACY OF FILTERING RADIO NAVIGATION PARAMETERS

Glushankov E., Sudenkova A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

As a measure of navigation parameter filtering accuracy, the estimation error variance is typically used. Although this is a self-sufficient 'internal' error metric and allows for algorithm comparison, it does not provide information about the potential filtering accuracy. On the other hand, the goal of filtering is to separate the useful signal from noise, which in practice means determining the signal-to-noise ratio improvement—an 'external' error metric. This paper reviews various methods for assessing the accuracy of radio navigation parameters, using the example of 1st- and 2nd-order Kalman filters and a maximum a posteriori probability filter under the influence of white and colored noise on the signal.

Key words: *radio navigation signal, signal to noise ratio, Cramer-Rao bound, Kalman filter, probability density function*

УДК 621.396.2
ГРНТИ 49.03.05

ВЫБОР ОПТИМАЛЬНОГО СВЕРТОЧНОГО КОДЕРА ДЛЯ РЕШЕТЧАТОЙ КОДОВОЙ МОДУЛЯЦИИ

Н. К. Елисеев

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

В работе представлены результаты экспериментального исследования помехоустойчивости сигнально-кодовых конструкций на основе 8-позиционной фазовой манипуляции с применением решетчатой кодовой модуляции в радиоканалах с аддитивным белым гауссовским шумом, замираниями Райса и Рэлея. Произведена оценка влияния длины кодового ограничения (от 3 до 9) оптимизированных сверточных кодеров со степенью кодирования 1/2 на энергетическую эффективность передачи с помощью анализа зависимости вероятности битовой ошибки от отношения сигнал/шум. Оценки помехоустойчивости получены с помощью программного моделирования системы передачи информации. Установлено, что использование решетчатого кодера с длиной ограничения 9 обеспечивает выигрыш в среднем 7 дБ по сравнению с некодированной передачей и превосходство на 2,5 дБ относительно базового кодера с длиной ограничения 3 при фиксированной вероятности битовой ошибки 10^{-5}. Результаты исследования подтверждают потенциал сложных сверточных кодов для повышения помехоустойчивости современных систем связи.

сигнально-кодовые конструкции, СКК, решетчатая кодовая модуляция, РКМ, TCM, сверточные коды, помехоустойчивость, свободное расстояние, энергетическая эффективность, имитационное моделирование, вероятность битовой ошибки, BER

Повышение помехоустойчивости передачи цифровых сигналов по радиоканалам связи, подверженным замираниям, остается актуальной задачей [1]. В современных системах связи классический подход к модуляции «в целом» уступает место более эффективным сигнально-кодовым конструкциям (СКК), объединяющим стадии кодирования и модуляции сигнала [1, 2]. Сигнально-кодовые конструкции осуществляют отображение информационных бит на сигнальное созвездие не независимо, а на основе состояний конечного автомата (кодера), что позволяет вводить избыточность и структурировать пространство сигналов для повышения расстояния между разрешенными последовательностями [1, 2]. Основу многих практических СКК составляют решетчатые СКК, использующие решетчато-кодовую модуляцию (РКМ, Trellis-Coded Modulation, TCM), ключевым элементом которых является решетчатый кодер, базирующийся на принципах сверточ-

ного кодирования [1, 3]. На рисунке 1 представлен пример обобщенной схемы решетчатой кодовой модуляции для сигнала ФМ-8: входной поток бит обрабатывается сверточным (решетчатым) кодером со скоростью кодирования $R = 2/3$, после чего кодированные тройки бит отображаются на сигнальное созвездие.

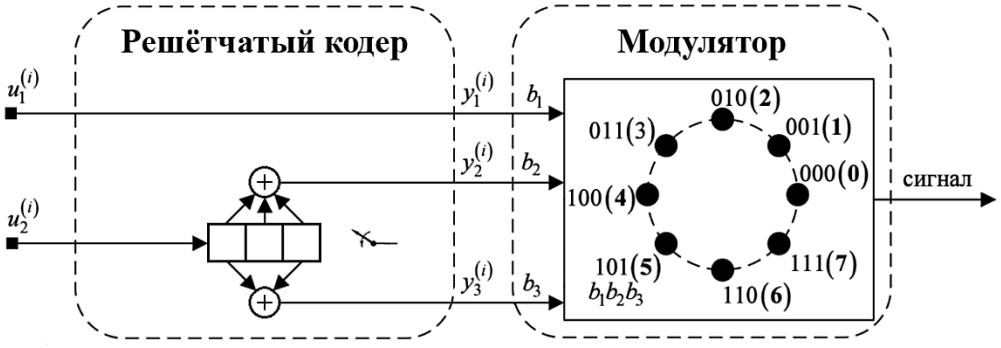


Рис. 1. Обобщенная схема РКМ для сигнала ФМ-8

Эффективность решетчатой СКК напрямую зависит от характеристик используемого сверточного кодера. Сверточный кодер представляет собой устройство с памятью, преобразующее за такт k входных информационных бит в n выходных (кодированных) символов с избыточностью по определенному алгоритму, задаваемому генераторными полиномами [3, 4]. Отношение $R = k/n$ называют относительной скоростью кода или степенью кодирования. Выходные символы, создаваемые кодером на данном такте, зависят от m информационных символов, поступивших на этом и предыдущем тактах. Таким образом, выходные символы сверточного кодера однозначно определяются его входным сигналом и состоянием, зависящим от $m - k$ предыдущих информационных символов [3, стр. 14]. Основными элементами сверточного кодера являются: регистр сдвига, сумматоры по модулю 2 и коммутатор. Регистр сдвига является динамическим запоминающим устройством, число ячеек K называется длиной кодового ограничения. Выбор связей между сумматорами и разрядами регистра влияет на характеристики сверточного кода [1, стр. 408]. На рисунке 1 изображен сверточный кодер с $K = 3$, $R = 1/2$ и векторами кода: $g_1 = 111$, $g_2 = 101$.

Критически важным параметром, определяющим помехоустойчивость сверточного кода и, следовательно, всей СКК, является свободное расстояние решетки кода d_f (просвет) – минимальное расстояние Хэмминга (или Евклида, в случае СКК) между всеми возможными парами различных кодовых последовательностей [3, 4, 5]. Повышение помехоустойчивости решетчатых СКК может быть достигнуто, в частности, за счет применения свер-

точных кодеров с максимально возможным свободным расстоянием для заданных R и K, поскольку оно связано с возможностями коррекции ошибок кода [1, стр. 432]. Задача выбора связей, дающих оптимальные дистанционные свойства, сложна и в общем случае не решается [1, стр. 408]. В таблице 1 представлены известные оптимальные сверточные коды по Оденуальдеру для $R = 1/2$ и K от 3 до 9, обеспечивающих максимальный просвет [1, стр. 441].

ТАБЛИЦА 1: Оптимальные сверточные коды ($R = 1/2$)

Длина кодового ограничения K	Просвет d_f	Векторы кода g_1; g_2
3	5	111; 101
4	6	1111; 1011
5	7	10111; 11001
6	8	101111; 110101
7	10	1001111; 1101101
8	10	10011111; 11100101
9	12	110101111; 100011101

Целью настоящей работы являлось экспериментальное исследование и количественная оценка выигрыша в помехоустойчивости решетчатых СКК на основе сигналов ФМ-8 при использовании оптимальных сверточных кодеров с длиной кодового ограничения K от 3 до 9 в каналах с аддитивным белым гауссовским шумом (АБГШ), плоскими замираниями Райса и Рэлея. Исследование выполнено методом имитационного моделирования на программной модели системы связи [6], позволившей получить оценку вероятности битовой ошибки (BER) сигнала для отношения сигнал-шум в диапазоне от −10 до 30 дБ с шагом 0,5 дБ при скорости битового потока 600 Мбит/с. Энергетический выигрыш оценивался на уровне $\mathrm{BER} = 10^{-5}$. Для проведения сравнительного исследования в программную модель был добавлен блок модуляции СКК с оптимальными сверточными кодерами для K от 3 до 9 (таблица 1), блок демодуляции СКК с «мягкой» схемой принятия решений и декодер Витерби [5] с оптимальным значением глубины отслеживания символов (4 длины кодового ограничения K [1, стр. 440]).

Полученные зависимости вероятности битовой ошибки (BER) от отношения сигнал/шум (E_b/N_0) для сигнала с модуляцией «в целом» и решетчатых СКК с K от 3 до 9 в канале с АБГШ представлены на рисунке 2.

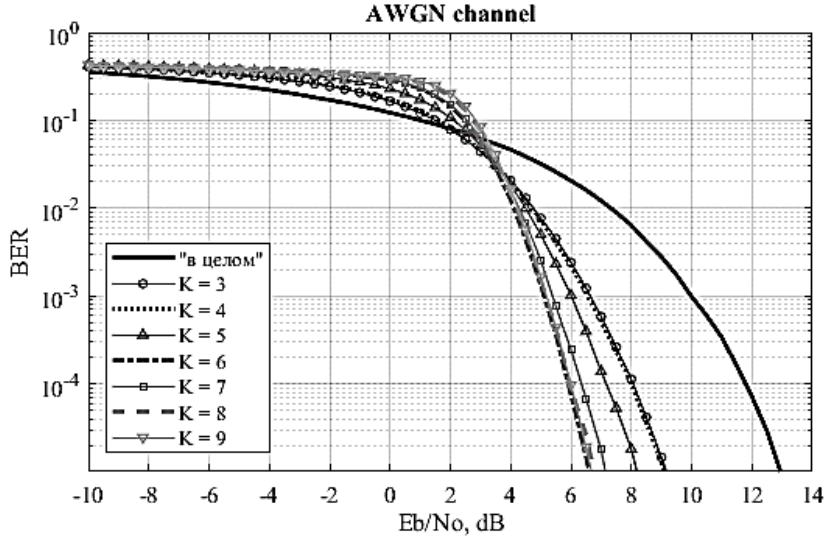


Рис. 2. ПУ решетчатых СКК в канале с АБГШ

Из графиков на рисунке 2 видно, что использование решетчатой СКК с простым в реализации сверточным кодером ($K = 3$) позволяет получить выигрыш в помехоустойчивости (ПУ) в 4 дБ относительно модуляции «в целом». Усложнение структуры кодера позволяет добиться дальнейшего повышения ПУ на 2,5 дБ при $K = 9$, что суммарно позволяет повысить энергетическую эффективность сигнала на 50 % относительно модуляции «в целом».

Практический интерес представляет оценка BER решетчатых СКК для реальных радиоканалов, подверженных замираниям. На рисунках 3 и 4 представлены графики оценок вероятности битовой ошибки для сигналов РКМ и модуляции «в целом», прошедших через каналы с замираниями Райса и Релея соответственно.

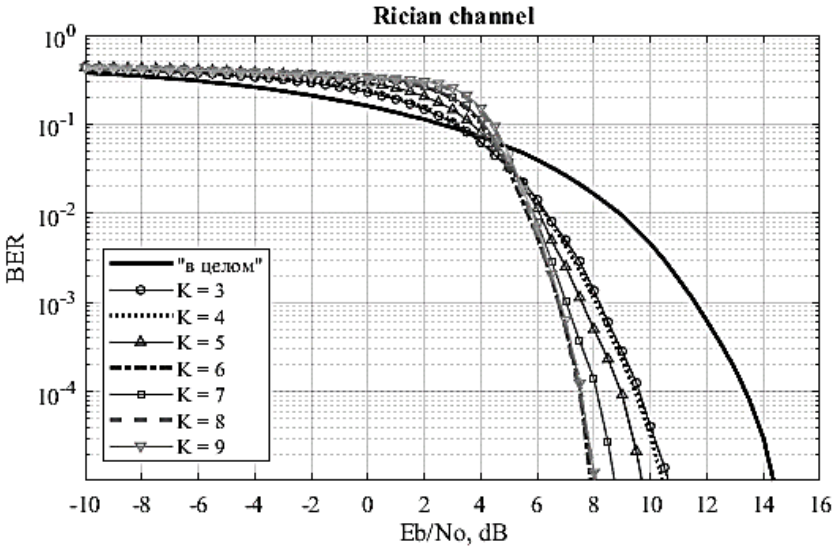


Рис. 3. ПУ решетчатых СКК в канале с замираниями Райса

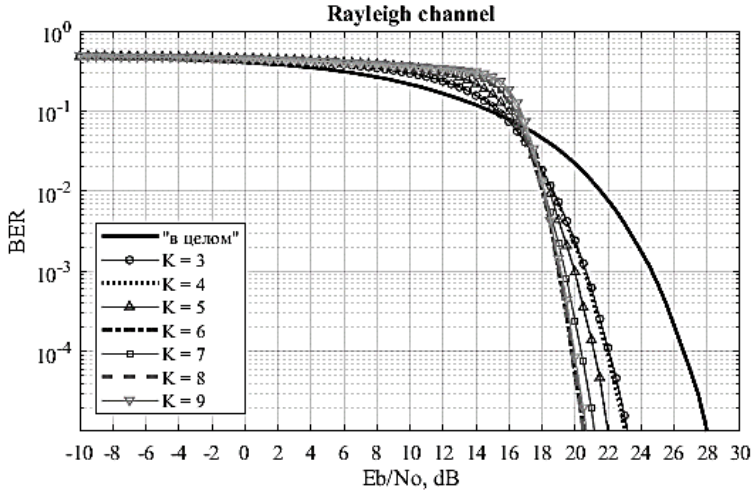


Рис. 4. ПУ решетчатых СКК в канале с замираниями Рэлея

Как видно из графиков, наличие замираний в канале понижает средний уровень ПУ: для замираний Райса в среднем на 1,5 дБ, Рэлея – на 14 дБ в сравнении с каналом с АБГШ. Относительное положение кривых оценок помехоустойчивости для K от 3 до 9 соответствует оценкам для канала с АБГШ. По результатам сравнительного исследования можно сделать вывод, что оптимальной решетчатой СКК по критерию помехоустойчивости для сигналов ФМ-8, подверженных замираниям, является решетчатая СКК с $K = 9$: энергетический выигрыш для канала с замираниями Райса составил 6,5 дБ (+44,8 %), для канала Релея – 7,5 дБ (+26,8 %) относительно BER для сигналов с модуляцией «в целом».

Проведенное методом имитационного моделирования исследование фазоманипулированных сигналов, подверженных искажениям в канале связи позволило количественно оценить влияние длины кодового ограничения K и структуры сверточного кодера на помехоустойчивость решетчатой СКК. Анализ полученных зависимостей BER от отношения сигнал/шум для кодов с K от 3 до 9 демонстрирует значительный выигрыш от применения сверточных кодеров с большей длиной кодового ограничения и максимально возможным свободным расстоянием вне зависимости от искажений в радиоканале. Наиболее существенное улучшение ПУ наблюдается при переходе от стандартного кодера с малым K ($K = 3$) к кодам с $K = 9$.

Полученные результаты подтверждают теоретические предпосылки о прямой зависимости помехоустойчивости СКК от свободного расстояния решетки сверточного кода d_f [3, 4, 5] и важности использования кодов с большой длиной ограничения K для достижения высокой энергетической эффективности [1]. Хотя реализация декодеров Витерби [5] для кодов с большим K (особенно $K = 9$) требует повышенной вычислительной сложности, достигнутый выигрыш в 2,5 дБ по сравнению с $K = 3$ делает приме-

нение таких СКК оправданным в системах связи, критичных к энергетической эффективности и работающих в условиях ограниченного отношения сигнал/шум. Дальнейшие исследования могут быть направлены в сторону повышения ПУ решетчатых СКК за счет увеличения сложности сверточного кодера и поиска путей снижения сложности декодирования.

Список используемых источников

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. М.: Издательский дом «Вильямс», 2003. 1104 с.

2. Варгаузин В. А., Цикин И. А. Методы повышения энергетической и спектральной эффективности цифровой радиосвязи: учеб. пособие. СПб.: БХВ-Петербург, 2013. 352 с.

3. Никитин Г. И. Сверточные коды. Учебное пособие. СПб.: СПбГЭТУ "ЛЭТИ", 2010. 112 с.

4. Золоторев В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник. М.: Горячая линия-Телеком, 2004. 272 с.

5. Viterbi A. J., Omura J. K. Principles of Digital Communication and Coding. New York: McGraw-Hill. 1979. 584 p.

6. Елисеев Н. К. Сравнительный анализ моделей канала связи с замираниями // 79-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная Дню радио: сб. докладов. СПб.: СПбГЭТУ «ЛЭТИ», 2024. С. 82–85.

Статья представлена научным руководителем, профессором кафедры РТ СПбГУТ, доктором технических наук, профессором Глушанковым Е. И.

SELECTION OF AN OPTIMAL CONVOLUTIONAL ENCODER FOR TRELLIS-CODED MODULATION

Eliseev N.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper presents the results of an experimental study on the noise immunity of signal-code structures based on 8-ary Phase Shift Keying (8-PSK) employing Trellis Coded Modulation (TCM) in radio channels characterized by Additive White Gaussian Noise (AWGN), Rician fading, and Rayleigh fading. The impact of the constraint length (ranging from 3 to 9) of optimized rate-1/2 convolutional encoders on the power efficiency of transmission was evaluated by analyzing the Bit Error Rate (BER) dependence on the Signal-to-Noise Ratio (SNR). Noise immunity estimates were obtained through software simulation of the information transmission system. It was established that employing a trellis encoder with a constraint length of 9 provides an average gain of 7 dB compared to uncoded transmission and outperforms a baseline encoder with a constraint length of 3 by 2.5 dB at a fixed BER of 1e-5. The research results confirm the potential of complicated convolutional codes for enhancing the noise immunity of modern communication systems.

Key words: *coded modulation schemes, trellis-coded modulation, TCM, convolutional codes, noise immunity, free distance, power efficiency, computer simulation, bit error rate, BER*

УДК.681.51
ГРНТИ 47.05.05

РАЗРАБОТКА И СОЗДАНИЕ ВИРТУАЛЬНОГО ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ИССЛЕДОВАНИЮ ВЛИЯНИЯ ПОТЕРЬ НА ХАРАКТЕРИСТИКИ РЕАКТИВНЫХ ФИЛЬТРОВ

З. В. Зайцева

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

Рассматриваются вопросы разработки и создания виртуального лабораторного практикума по исследованию влияния потерь на характеристики реактивных фильтров на основе использования интегрированной программной среды Mathcad и Fastmean. Разработана методика оценки влияния потерь на характеристики реактивных фильтров с использование компьютерных технологий, позволяющих проводить моделирование при выполнении лабораторных работ

лабораторный практикум, реактивные фильтры, потери энергии, интегрированная программная среда, моделирование процессов

Электрические фильтры являются важными компонентами в электронных системах, используемыми для выделения или подавления определенных частотных составляющих сигнала. Идеальные фильтры предполагают отсутствие потерь энергии, однако в реальных условиях потери неизбежны [1, 2]. При практической реализации реактивных *LC*-фильтров конденсаторы и катушки индуктивности могут иметь существенные активные потери энергии [3-5]. Эквивалентная схема конденсатора с потерями, используемая в большинстве случаев, представляется в виде параллельного соединения емкости C_i и резистивной проводимости G_i. Схема реальной катушки индуктивности представляют в виде последовательного соединения элемента индуктивности L_k и резистивного сопротивления R_k (рис. 1).

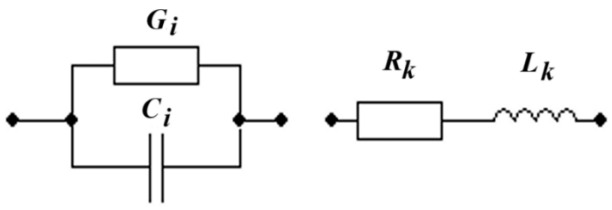


Рис. 1. Элементы *LC*-фильтра с учетом потерь

Потери в элементах фильтрующей цепи влияют не только на ее частотные функции, но и на массогабаритные показатели. Оценка потерь в элементах производится по их добротностям (Q) или по коэффициентам (d) потерь:

$$d_i = \frac{G_i}{\omega_0 C_i} = \frac{1}{Q_C};$$
$$d_k = \frac{R_k}{\omega_0 L_k} = \frac{1}{Q_L},$$

где $G_i = \frac{1}{R_i}$ – проводимость потерь конденсатора C_i;

R_k – сопротивление потерь катушки L_k;

ω_0 – граничная частота полосы пропускания ФНЧ.

В большинстве случаев рассматривают полуоднородные потери, когда для всех емкостей $d_i = d_C$ и для всех индуктивностей $d_k = d_L$. Это обусловлено с тем, что фильтрующие цепи, как правило, реализуются на однотипных элементах. Таким образом, с учетом потерь в элементах их комплексные сопротивления и проводимости получают некоторые малые приращения

Таким образом, с учетом потерь в элементах их комплексные сопротивления и проводимости получают некоторые малые приращения:

$$Z_k = j\omega L_k + R_k = L_k\left(j\omega + \frac{R_k}{L_k}\cdot\frac{\omega_0}{\omega_0}\right) = L_k(j\omega + d_L\cdot\omega_0) = j\omega L_k + L_k d_L\omega_0;$$
$$Y_i = j\omega C_i + G_i = C_i\left(j\omega + \frac{G_i}{C_i}\cdot\frac{\omega_0}{\omega_0}\right) = C_i(j\omega + d_C\cdot\omega_0) = j\omega C_i + C_i d_C\omega_0.$$

Таким образом,

$$R_k = L_k d_L\omega_0, \quad (1)$$
$$G_i = C_i d_C\omega_0. \quad (2)$$

Мощность потерь в элементах фильтрующей цепи может быть найдена следующим образом:

$$P_{\text{п}} = \sum_{i=1}^{N_C} U_i^2 G_i + \sum_{k=1}^{N_L} I_k^2 R_k = (d_C W_C + d_L W_L)\omega_0.$$

С учетом приведенных выражений коэффициент полезного действия (КПД) фильтрующей цепи:

$$\eta = \frac{P_{\text{Н}}}{P_{\text{вх}}} = \frac{P_{\text{Н}}}{P_{\text{Н}} + P_{\text{П}}} = \frac{P_{\text{Н}}}{P_{\text{Н}} + (d_C W_C + d_L W_L)\omega_0} = \frac{1}{1 + d_C\widehat{W}_C + d_L\widehat{W}_L}, \quad (3)$$

где $\widehat{W}_C = \frac{W_C \omega_0}{P_\text{Н}}$ – относительная суммарная энергия, запасенная в конденсаторах;

$\widehat{W}_L = \frac{W_L \omega_0}{P_\text{Н}}$ – относительная суммарная энергия, запасенная в катушках индуктивности.

Исследование влияния потерь на характеристики реактивных фильтров было предложено провести на основе использования интегрированной программной среды Mathcad и Fastmean. Известно, что компьютерные технологии обучения позволяют использовать более оптимальные возможности человеко-машинного взаимодействия в формате студент-персональный компьютер (ПК) [6-8].

В лабораторном практикуме студентам были предложены для анализа фильтры нижних частот с характеристиками Чебышева и Золотарева-Кауэра. Была поставлена задача получить характеристики ослабления данных фильтров без учета потерь, затем рассчитать сопротивления потерь для каждого конденсатора и катушки индуктивности фильтров и проанализировать, как меняются характеристики ослабления фильтров с учетом потерь в реактивных элементах.

Поставленная задача решалась следующим образом. Был проведен анализ фильтров с использованием программы Fastmean, в результате которого были построены схемы фильтра Чебышева и фильтра Золотарева-Кауэра (рис. 1) и получены графики ослабления фильтров (рис. 2). Оба фильтра имеют одинаковое ослабление Δa на граничной частоте полосы пропускания f_0.

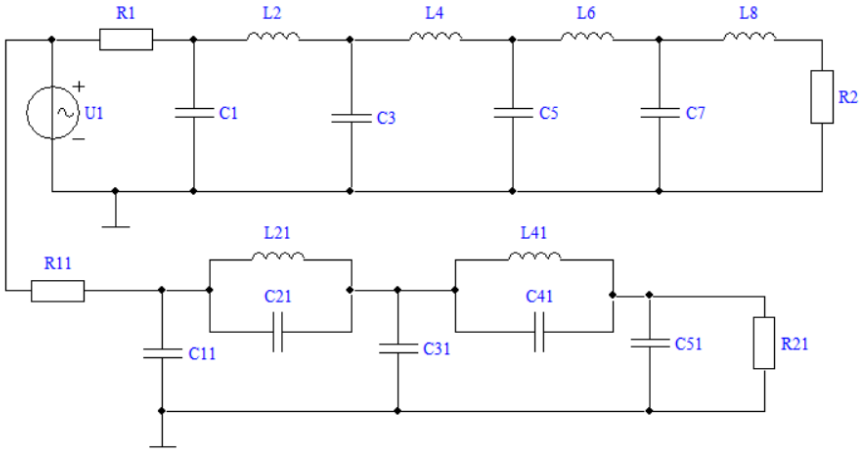


Рис. 1. Схемы фильтра Чебышева и фильтра Золотарева-Кауэра

Следующим этапом было исследование энергетических характеристик фильтров. В программе Fastmean был построены суммарные энергетические функции по емкостям и индуктивностям для обоих видов фильтра в полосе пропускания (рис. 3).

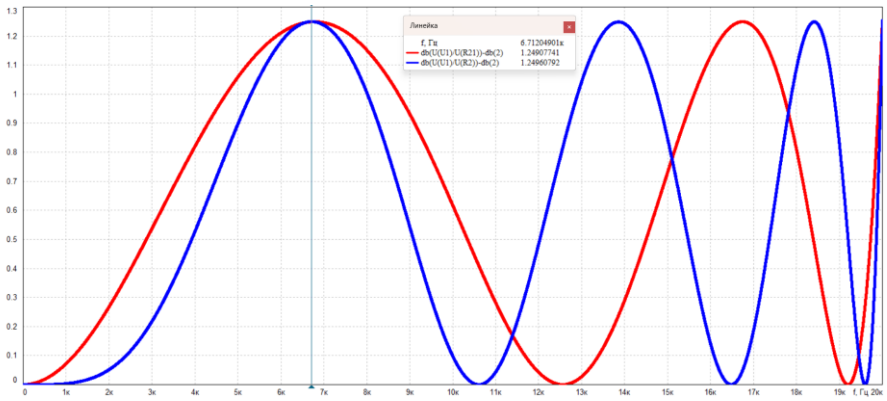
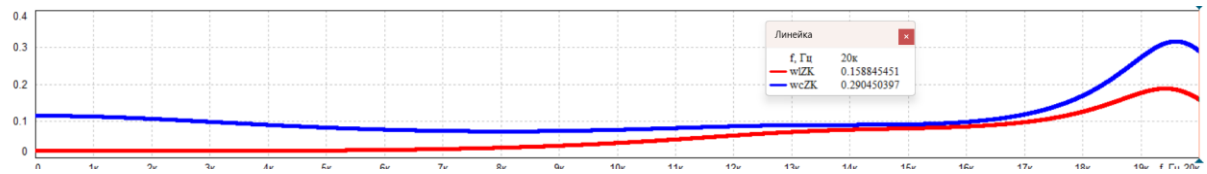
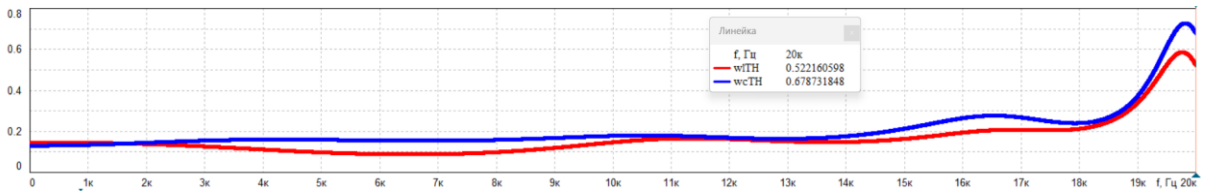


Рис. 2. Графики ослабления фильтров Чебышева (синий) и Золотарева-Кауэра (красный)



а)



б)

Рис. 3. Суммарные энергетические функции по емкостям (синий график) и индуктивностям (красный график) для фильтра: а) Золотарева-Кауэра; б) Чебышева

Далее в Mathcad были рассчитаны сопротивления потерь для каждой катушки индуктивности и проводимости потерь для каждого конденсатора по формулам (1) и (2) для фильтров Чебышева и Золотарева-Кауэра. Полученные сопротивления потерь были добавлены в схемы фильтров (рис. 4). Были построены характеристики ослабления фильтров в полосе пропускания.

На рис. 5 приведены полученные графики ослабления фильтров Чебышева (синий) и Золотарева-Кауэра (красный) с учетом потерь на реактивных элементах.

В процессе выполнения лабораторной работы перед студентами была поставлена задача проанализировать влияние потерь на характеристику ослабления фильтров. Номинальные (без учета потерь) характеристики ослабления (рис. 2) имеют равноволновый характер, при этом минимальное значение затухания $a_{\min} = 0$, а максимальное – $a_{\max} = \Delta a_{\text{ном}}$. При введении потерь происходит увеличение затухания в рабочей области, при этом $a_{\min} > 0$ и неравномерность затухания $\Delta a = a_{\max} - a_{\min}$ также увеличивается. Наибольшее приращение затухания в полосе пропускания, обусловленное потерями в элементах, имеет место на граничной частоте. Это приращение можно подсчитать по формуле $a_{\text{П max}} = a_{\max} - \Delta a_{\text{ном}}$.

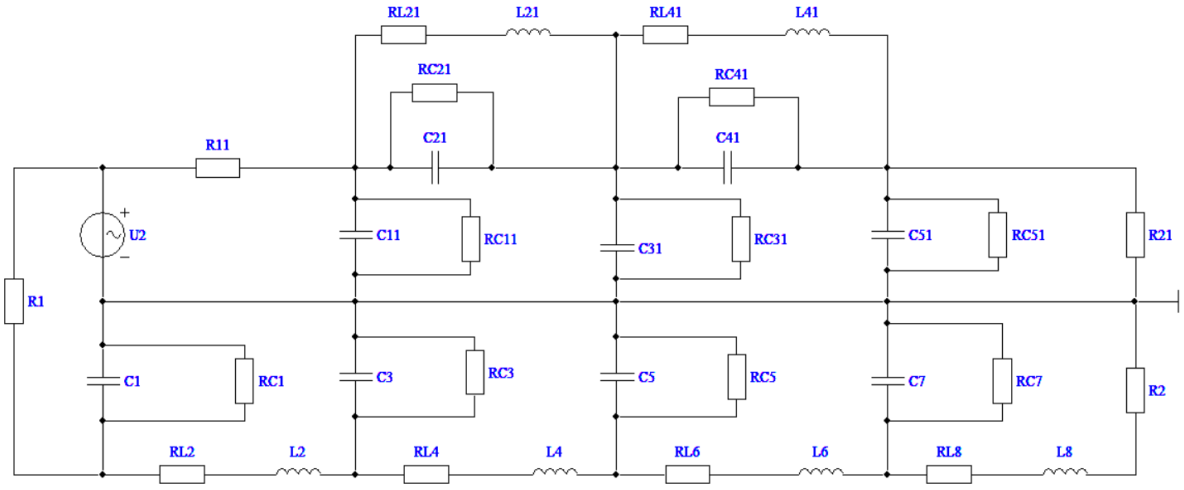


Рис. 4. Схемы фильтра Чебышева и фильтра Золотарева-Кауэра с учетом потерь на реактивных элементах

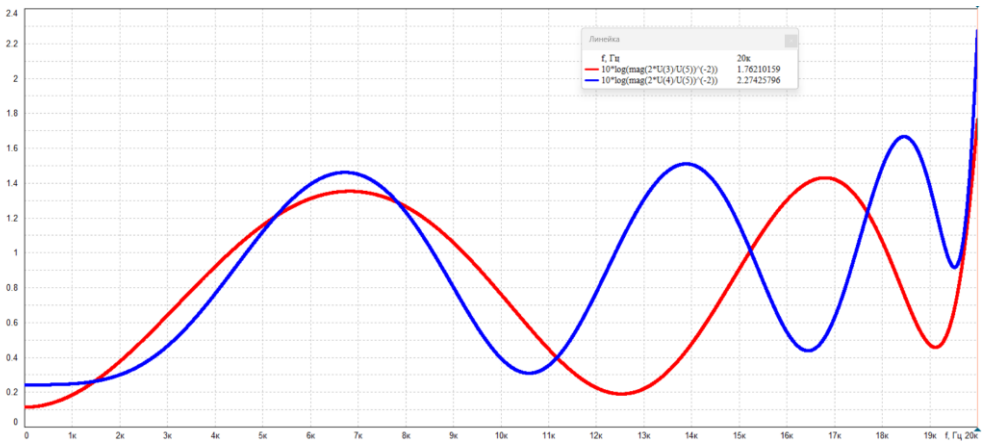


Рис. 5. Графики ослабления фильтров Чебышева (синий) и Золотарева-Кауэра (красный) с учетом потерь на реактивных элементах

Потери в элементах приводят к увеличению $a_{\max}$, $a_{\min}$ и неравномерности затухания Δa (рис. 5). Причем у ФНЧ Золотарева указанные величины существенно меньше, чем ФНЧ Чебышева при одинаковых добротностях элементов.

Суммарные энергетические характеристики (рис. 3) позволяют рассчитать коэффициент полезного действия (КПД) фильтров, используя формулу (3) и провести сравнительный анализ фильтров.

Таким образом, виртуальная лабораторная работа по исследованию влияния потерь на характеристики реактивных фильтров, выполненная в интегрированной программной среде Mathcad и Fastmean, позволяет наглядно оценить, как изменяются частотные и энергетические характеристики фильтров с учетом потерь, какие фильтры предпочтительнее для использования. Студенты применяют на практике теоретические знания, развивают навыки моделирования и работы с программами, получают опыт анализа и проектирования электронных систем.

Список используемых источников:

1. Дмитриков В. Ф., Сергеев В. В., Самылин И. Н. Повышение эффективности преобразовательных и радиотехнических устройств. М.: Радио и связь, Горячая линия-Телеком, 2005.

2. Сергеев В. В., Станкеев М. Е., Расчет LC-фильтров с минимальными массогабаритными показателями для преобразовательных и радиотехнических устройств, работающих в ключевом режиме. Электропитание. 2012. № 2. С. 51-54.

3. Теория электрических цепей. Расчет LC-фильтров с учетом эксплуатационных показателей: [Электронный ресурс]: учеб. пособие для вузов / В. В. Сергеев. - 2-е изд., стер. СПб.: Лань, 2022. 116 с. - URL: https://e.lanbook.com/book/238811. ISBN 978-5-507-44727-5

4. Сергеев В. В. Оценка влияния потерь в элементах *LC*-фильтра на характеристику затухания. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей: в 4х томах. Санкт-Петербург, 2021. С. 563-567.

5. Сергеев В. В., Зайцева З. В. Электронные цепи и методы их расчета. Расчет LC-фильтров и сравнительный анализ их показателей активности / Санкт-Петербург, СПбГУТ, 2016.

6. Зайцева З. В., Логвинова Н. К. Компьютерный расчет линейных и нелинейных цепей при постановке виртуальных лабораторных работ // Актуальные проблемы инфотелекоммуникаций в науке и образовании; сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 томах. 2019. С. 401-406.

7. Зайцева З. В., Логвинова Н. К. Виртуальный лабораторный практикум для технических дисциплин при дистанционном обучении // Актуальные проблемы инфотелекоммуникаций в науке и образовании; сборник научных статей X Международной научно-технической и научно-методической конференции: в 4 томах. Санкт-Петербург, 2021. С. 218-223.

8. Зайцева З. В., Логвинова Н. К. Возможности человеко-машинного взаимодействия в обучающей среде технического вуза // Актуальные проблемы инфотелекомму-

никаций в науке и образовании. Материалы XIII Международной научно-технической и научно-методической конференции. В 4-х томах. Санкт-Петербург, 2024. С. 558-563.

DEVELOPMENT AND CREATION OF A VIRTUAL LABORATORY WORKSHOP FOR STUDYING THE IMPACT OF LOSSES ON THE CHARACTERISTICS OF REACTIVE FILTERS

Zaitseva Z.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The issues of development and creation of a virtual laboratory workshop for studying the impact of losses on the characteristics of reactive filters using Mathcad and Fastmean integrated software environment are discussed. A technique has been developed to assess the impact of losses on the characteristics of reactive filters using computer technologies that allow simulation during laboratory work.

Key words: *laboratory workshop, reactive filters, energy losses, integrated software environment, process simulation*

УДК 004.942
ГРНТИ 28.17.19

СИНТЕЗ ВХОДНОГО ВОЗДЕЙСТВИЯ ПО ТРЕБУЕМОМУ ТОРМОЗНОМУ УСИЛИЮ ДЛЯ МОДЕЛИРОВАНИЯ ЭЛЕКТРОГИДРАВЛИЧЕСКОГО ТОРМОЗНОГО МЕХАНИЗМА

В. В. Зеленцов, А. О. Калибабчук

Московский государственный технический университет имени Н. Э. Баумана

Для проведения математического моделирования индивидуального электрогидравлического тормозного механизма необходимо сформировать набор входных воздействий. Входом системы является требуемый тормозной момент, выходом – давление в тормозной магистрали. Входное воздействие должно охватывать как классические для теории автоматического управления гармоническое и ступенчатое воздействия, так и моделировать процесс работы антиблокировочной системы, а также отражать реальные эксплуатационные сценарии использования тормоза.

электрогидравлический тормозной механизм, входное воздействие

Входом системы является требуемое тормозное усилие, которое принято задавать в качестве тормозного момента [1], прикладываемого к колесу транспортного средства. Примем, что на вход системы подается требуемое (иначе желаемое) тормозное усилие в виде тормозного момента, измеряемого в системе СИ, а именно в ньютонах на метр.

Требования к тормозным системам, а также замедлению транспортных средств при торможении определяются международным регламентом, диктующим требования как по эксплуатационным характеристикам тормозных система, так и по их конструктивному исполнению. Согласно Техническому регламенту Таможенного союза, легковые автомобили при торможении по сухой асфальтированной дороге должны достигать ускорения замедления не менее 5,3 м/с^2, а грузовые автомобили должны замедляться с ускорением не менее 4,6 м/с^2 [2].

В рамках исследовательской задачи рассматривается легковой автомобиль снаряженной массой в 1400 кг. Транспортное средство оснащено колесами с шинами размерностью 195/75R15. При этом согласно [3], в таблице 1 приведено соответствие теоретического ускорения торможения транспортного средства на сухой асфальтированной дороге к необходимому для обеспечения этого торможения тормозному усилию.

Согласно ГОСТ Р 51709-2001, время срабатывания тормозной системы транспортного средства, допущенного до передвижения по дорогам общего пользования, должно быть не более 0,6 с [4]. Под этим временем подразумевается время от момента нажатия на педаль тормоза, до момента, когда транспортное средство начинает развивать требуемое тормозное усилие.

ТАБЛИЦА 1. Соответствие ускорения торможения транспортного средства к развиваемому тормозному моменту

Тормозное ускорение, м/с^2	Тормозной момент, Н м
1	148,55
2	362,02
3	527,40
4	783,69
5	991,91
6	1164,13
7	1452,78
8	1805,34
9	2073,28
10	2455,64

Исходя из требований ГОСТ Р 51709-2001, требований по развиваемому тормозному ускорению и данным, приведенным в таблице 1, можно сделать вывод, что в качестве первого набора входных воздействий, которые будут применяться для моделирования поведения электрогидравлического тормозного механизма, следует выбрать набор ступенчатых воздействий, различающихся по амплитуде. Причем максимальный требуемый тормозной момент примем равным 2500 Нм (максимальная амплитуда), а минимальный примем равным 250 Нм. Будет применено 10 различных уровней ступенчатого воздействия с равным шагом по амплитуде. График входного ступенчатого воздействия показан на рисунке 1.

Современные автомобили оснащаются различными системами безопасности. Рассматривая тормозную систему, автомобили должны оснащаться антиблокировочной системой (АБС). Применение такой системы подразумевает необходимость модулирования тормозного усилия с частотой от 5 до 25 Гц, в некоторых случаях и при большей частоте [5].

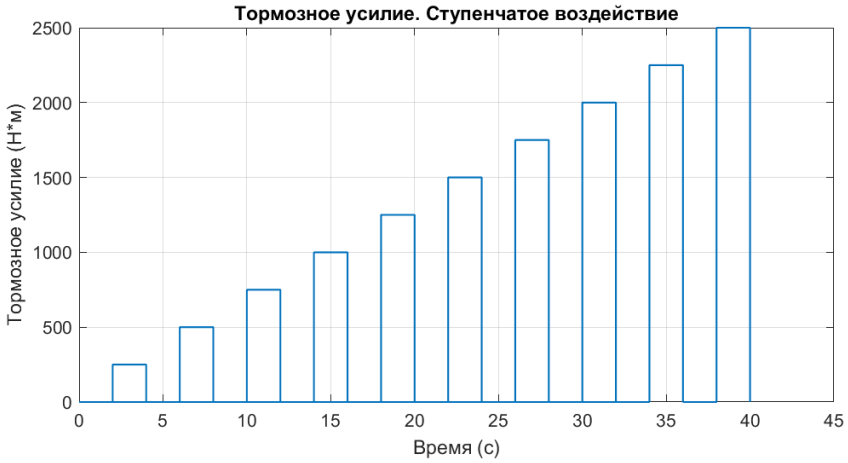


Рис. 1. Ступенчатое входное воздействие

Сцепление колес с дорогой зависит от множества факторов дорожной обстановки. Основная задача системы АБС – это поддержание тормозного усилия на таком уровне, чтобы не допустить блокировку колеса. Алгоритм работы системы АБС показан на рисунке 2 [5].

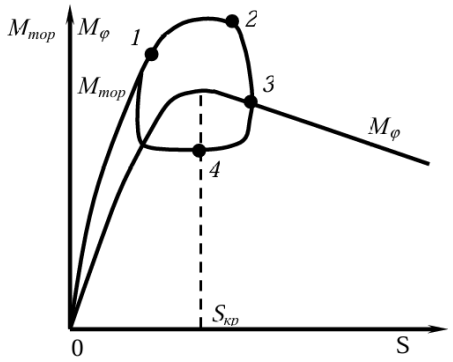


Рис. 2. Зависимость тормозного момента от проскальзывания колеса

В процессе работы система АБС ограничивает максимальное тормозное усилие на определенном расчетном уровне и поддерживает наиболее эффективное среднее тормозное усилие путем повторяющихся циклов уменьшения и увеличения давления в тормозной магистрали.

Для моделирования работы системы АБС будем использовать гармоническое входное воздействие с частотой в 10 Гц и амплитудой в 250 Нм. Средний уровень тормозного усилия, поддерживаемый гармоническим воздействием, зададим несколькими значениями: 500, 1000, 1500, 2000 Нм. Переключение между различными уровнями среднего может происходить в процессе торможения, так как транспортное средство может проезжать участки с различным сцеплением. Оценка среднего уровня требуемого тормозного усилия производится контроллером верхнего уровня, реализующего алгоритм работы АБС. Входной сигнал такого вида показан на рисунке 3.

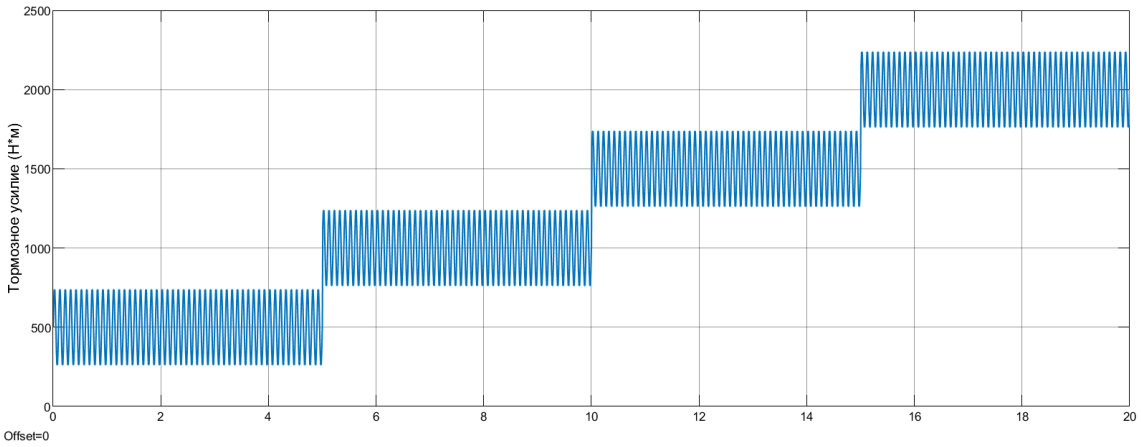


Рис. 3. Гармоническое входное воздействие

Наиболее качественное представление о поведении системы в ходе реальной эксплуатации может дать моделирование системы на наборе входных данных, собранных в процессе реальной эксплуатации. Такой параметр, как тормозное усилие на колесе, достаточно трудно измерить на реальном транспортном средстве. Поэтому в качестве альтернативы для сбора данных о требуемом тормозном моменте в ходе реальной эксплуатации была использована универсальная платформа для симуляции поведения транспортного средства, физических процессов и работы различных алгоритмов и систем BeamNG.tech [6]. Данная среда соответствует международным стандартам и используется многими автопроизводителями для моделирования различных процессов.

В процессе моделирования производилось управление транспортным средством с указанными ранее характеристиками в различных городских сценариях передвижения автомобиля. При помощи MATLAB Bridge [7] осуществлялось считывание информации о тормозном моменте на переднем левом колесе автомобиля и запись данных на диск. Далее данные о тормозном усилии во времени были очищены от промежутков времени, когда тормозная система не активна (например, при передвижении между светофорами). Запись данных производилось с частотой 50 Гц.

Модель транспортного средства была оснащена системой АБС, поведение которого имитирует работу систем АБС на реальных транспортных средствах. Поэтому можно полагать, что полученные данные о тормозном усилии близки поведению реального транспортного средства. На рисунке 4 показаны собирательные 70 секунд из массива записанных данных, которые демонстрируют тормозные моменты при торможении на сухом асфальте с различным усилием и в различных сценариях.

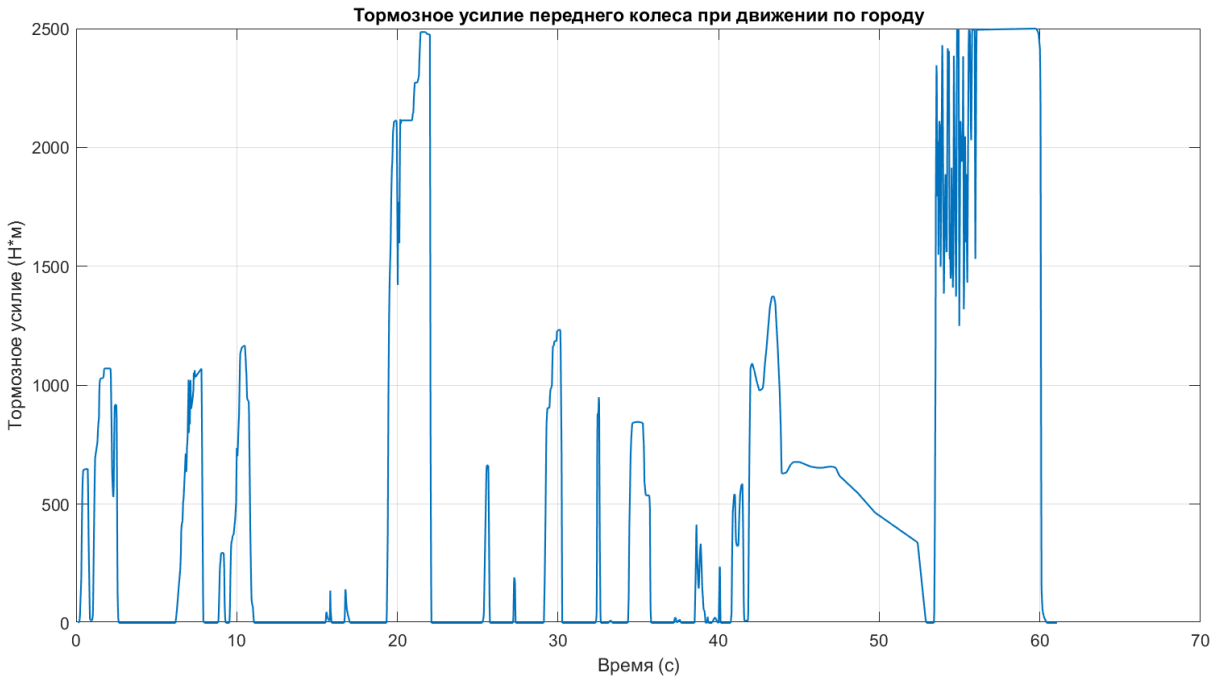


Рис. 4. Входное воздействие возникающее при реальной эксплуатации

В ходе работы были определены основные параметры и характеристики входных воздействий для моделирования электрогидравлического тормозного механизма легкового автомобиля. Установлено, что для адекватного моделирования необходимо использовать комбинацию ступенчатых воздействий с амплитудой от 250 до 2500 Нм и гармонических сигналов с частотой 10 Гц и амплитудой 250 Нм, имитирующих работу системы АБС при различных уровнях среднего тормозного усилия (500, 1000, 1500, 2000 Нм). Разработанный подход к формированию входных воздействий, основанный на данных, полученных в процессе виртуального моделирования в среде BeamNG.tech, позволяет наиболее точно воспроизвести реальные условия эксплуатации тормозной системы и соответствует требованиям международных стандартов по характеристикам тормозных систем транспортных средств.

Список используемых источников

1. Скутнев В. М. Тормозные системы легковых автомобилей: учеб. пособие / В. М. Скутнев. М.: КуАИ, 1983. 63 с.

2. ТР ТС 018/2011. О безопасности колесных транспортных средств. М.: Изд-во ЦЕНТРМАГ, 2025. 428 с.

3. Лукин П. П. Конструирование и расчет автомобиля: учеб. для втузов по спец. «Автомобили и тракторы» / П. П. Лукин, Г. А. Гаспарянц, В. Ф. Родионов. М.: Машиностроение, 1984. 376 с.

4. ГОСТ Р 51709-2001. Автотранспортные средства. Требования безопасности к техническому состоянию и методы проверки. М.: Изд-во стандартов, 2006. 62 с.: ил.

5. Петров А. П., Хоменко С. Е. Антиблокировочная и противобуксовочная системы тормозов: Учебное пособие. Курган: Изд-во Курганского гос. ун-та, 2003. 103 с.

6. BeamNG.tech documentation // BeamNG GmbH URL: https://documentation.beamng.com/beamng_tech/ (дата обращения 26.05.2025).

7. BeamNG.tech Support for MATLAB and Simulink // The MathWorks, Inc. URL: https://www.mathworks.com/matlabcentral/fileexchange/166246-beamng-tech-support-for-matlab-and-simulink (дата обращения 26.05.2025).

SYNTHESIS OF THE INPUT EFFECT BASED ON THE REQUIRED BRAKING FORCE FOR MODELING AN ELECTROHYDRAULIC BRAKING MECHANISM

Zelentsov V., Kalibabchuk A.
The Bauman Moscow State Technical University

To carry out mathematical modeling of an individual electrohydraulic braking mechanism, it is necessary to form a set of input effects. The input of the system is the required braking torque, the output is the pressure in the brake line. The input effect should cover both classical harmonic and step effects for the theory of automatic control, as well as simulate the operation of the anti-lock braking system, as well as reflect real-world operational scenarios for using the brake.

Key words: *electrohydraulic braking mechanism, input signal*

УДК 621.396.67
ГРНТИ 47.45.29

АНАЛИЗ ВЛИЯНИЯ КОЛИЧЕСТВА НАПРАВЛЕННЫХ ИЗЛУЧАТЕЛЕЙ В КОЛЬЦЕВОЙ АНТЕННОЙ СИСТЕМЕ НА ОГИБАЮЩУЮ ДИАГРАММЫ НАПРАВЛЕННОСТИ

К. О. Коровин, П. А. Межевов

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

Бортовые антенные системы БПЛА могут быть выполнены в виде ненаправленных излучателей, антенных решеток различной конфигурации, а также в виде других типов антенн. В данной работе рассматривается кольцевая антенна система с переключением излучающего элемента, оценивается влияние отдельного элемента и количества элементов на диаграмму направленности, в частности на ее огибающую. В качестве примера рассмотрен микрополосковый излучатель и построенные на его основе системы из 4, 6, 8 и 16 элементов.

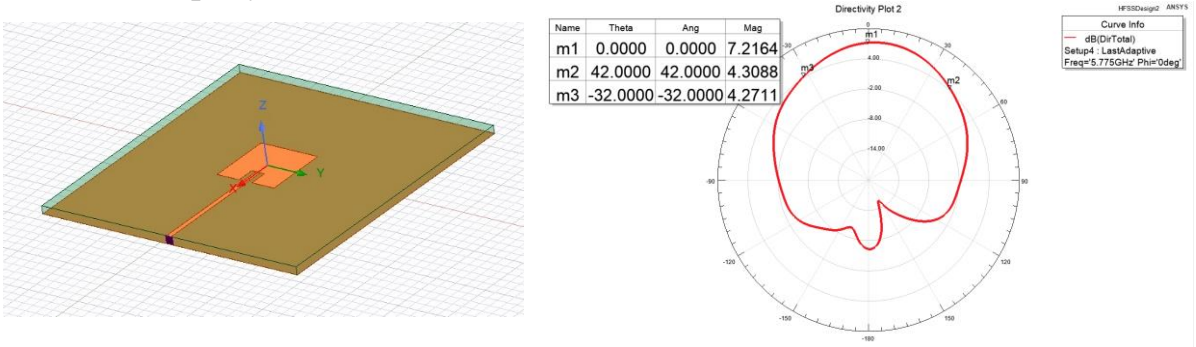
кольцевая антенная решетка, переключаемая антенная решетка, БПЛА

В качестве бортовых антенных решеток БПЛА чаще всего используются ненаправленные излучатели [1], однако возможен вариант использования антенных решеток [2], в частности переключаемых антенных систем.

Использование антенных решеток позволяет добиться большего коэффициента направленного действия (КНД), однако усложняет конструкцию антенной системы.

В данной работе рассматриваются кольцевые антенные системы из 4, 6, 8 и 16 антенных элементов. В качестве элемента выбран микрополосковый излучатель, в связи с его малыми массогабаритными параметрами и частым использованием в антенных системах БПЛА [3].

Одиночный излучатель и его диаграмма направленности (ДН) представлены на рисунке 1, а и б соответственно.



а) б)

Рис. 1. Микрополосковый излучатель (а) и его ДН (б)

Ширина ДН для такого излучателя составляет 72°, а КНД 7,2 дБ.

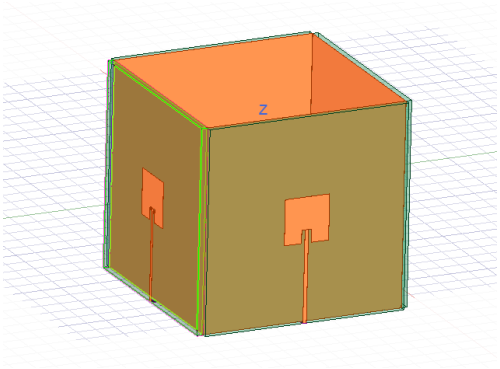
Для определения минимальной ширины ДН используется формула 1

$$N = \frac{360}{2\theta_{0.5}}; \quad (1)$$

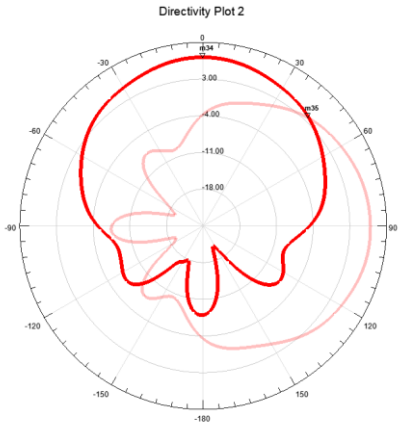
где N – количество излучателей, $2\theta_{0.5}$ – ширина ДН.

Таким образом, разработанный излучатель удовлетворяет требованиям при $N > 4$.

При 4 элементах (рисунок 2) можно наблюдать снижение КНД с 7,2 дБ в максимуме до 3,9 дБ в точке переключения.



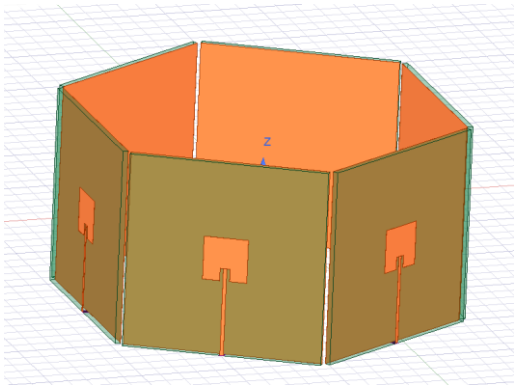
Name	Phi	Ang	Mag
m34	0.0000	0.0000	7.1576
m35	44.0000	44.0000	3.8925

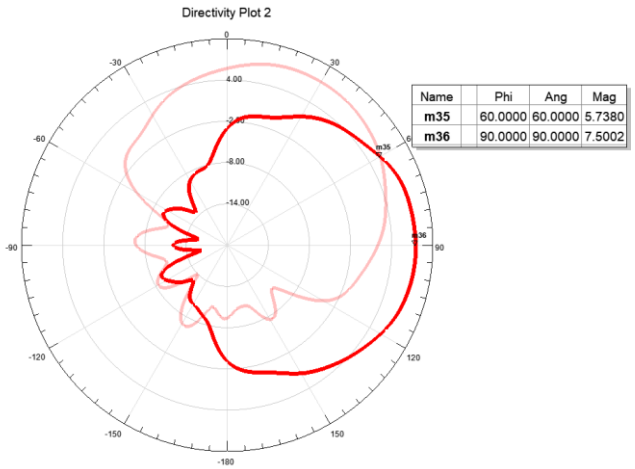


а) б)

Рис. 2. Переключаемая антенная система из 4 элементов (а), ДН при переключении на соседний элемент (б).

На рисунках 3, 4 и 5 представлены антенные системы из 6, 8 и 16 элементов соответственно с их ДН в режиме переключения.

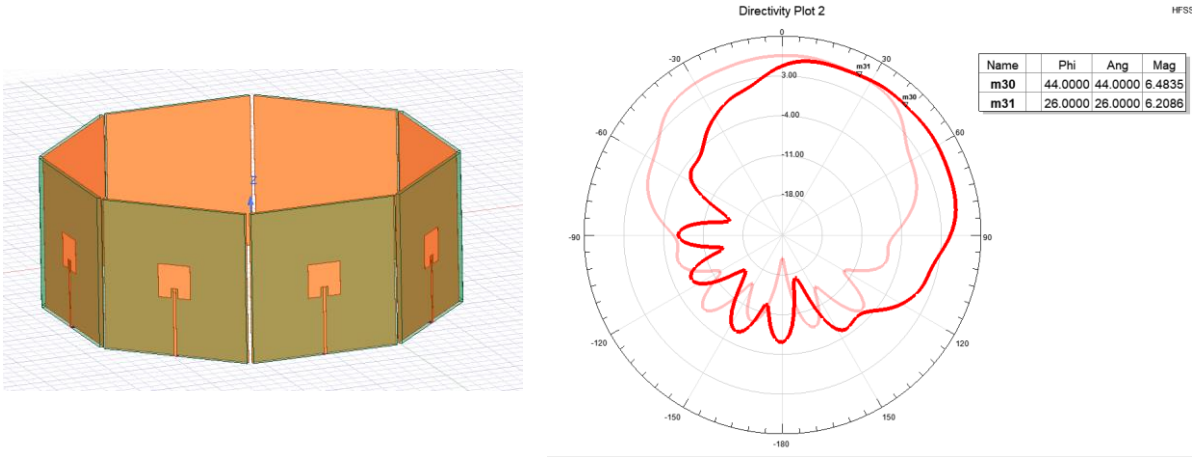




Name	Phi	Ang	Mag
m35	60.0000	60.0000	5.7380
m36	90.0000	90.0000	7.5002

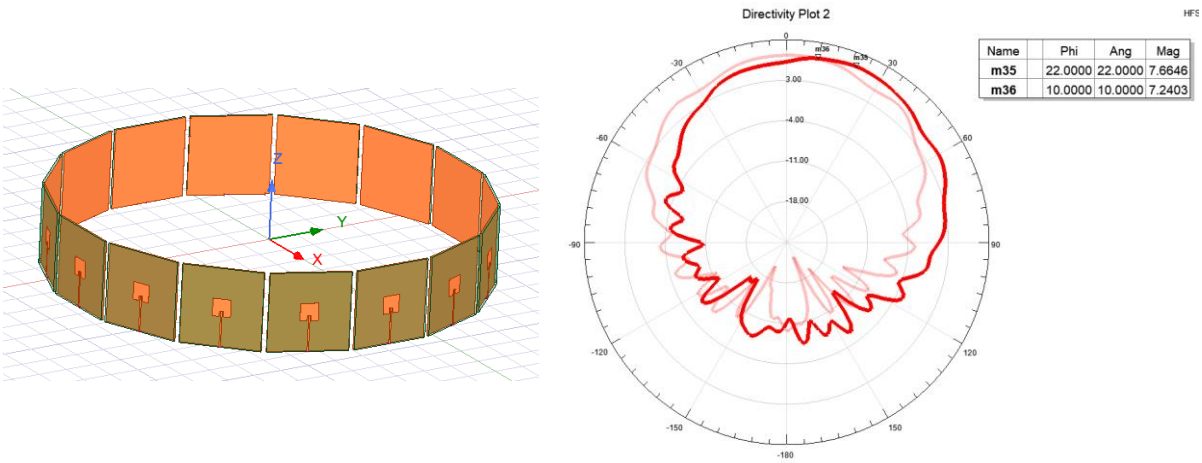
а) б)

Рис. 3. Переключаемая антенная система из 6 элементов (а), ДН при переключении на соседний элемент (б).



а б

Рис. 4. Переключаемая антенная система из 8 элементов (а), ДН при переключении на соседний элемент (б).



а б

Рис. 5. Переключаемая антенная система из 16 элементов (а), ДН при переключении на соседний элемент (б).

Результаты моделирования сведены в таблицу 1.

ТАБЛИЦА 1. Результаты моделирования переключаемых антенных систем

	4 элемента	6 элементов	8 элементов	16 элементов
КНД, дБ	7,2	7,5	6,5	7,6
КНД в точке переключения, дБ	3,9	5,7	6,2	7,2
Размеры системы, мм	52x52x52	94x94x52	128x128x52	277x277x52

Анализ таблицы 1 показывает, что большее количество элементов при одинаковом излучателе дает более округлую форму огибающей ДН. Однако также значительно увеличиваются массогабаритные параметры такой системы.

Также следует заметить, что использование более узконаправленных излучателей при большом количестве элементов позволяет добиться значительного увеличения КНД с допустимыми колебаниями огибающей до -3дБ от максимума.

Список используемых источников

1. Андрющенко М. С. и др. Антенные системы беспилотных летательных аппаратов // Известия Тульского государственного университета. Технические науки. 2024. № 5. С. 230-236.

2. Межевов П. А., Коровин К. О., Ликонцев А. Н. Создание кольцевой антенной решетки на основе излучателей Вивальди для широкополосного канала связи с ретрансляцией // Известия высших учебных заведений России. Радиоэлектроника. 2023. Т. 26. № 3. С. 58-66.

3. Панченко Б. А., Нефёдов Е. И. Микрополосковые антенны. М: Радио и связь, 1986. 144 с.

ANALYSIS OF THE INFLUENCE OF THE NUMBER OF DIRECTIONAL RADIATORS IN A RING ANTENNA SYSTEM ON THE RADIATION PATTERN ENVELOPE

Korovin K., Mezhevov P.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

On-board antenna systems of UAVs can be implemented in the form of non-directional emitters, antenna arrays of various configurations, and also in the form of other types of antennas. In this paper, a ring antenna system with switching of the radiating element is considered, the influence of a separate element and the number of elements on the radiation pattern, in particular on its envelope, is estimated. As an example, a microstrip emitter and systems based on it of 4, 6, 8 and 16 elements are considered.

Key words: *Ring antenna array, switchable antenna array, UAV*

УДК 004.046
ГРНТИ 20.51.19

К ВОПРОСУ ПРИМЕНЕНИЯ ПРОЦЕССНОГО ПОДХОДА К УПРАВЛЕНИЮ РАСПРЕДЕЛЕННЫМИ ПРОИЗВОДСТВАМИ

А. Г. Любимов

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

В работе рассматривается процессный подход к моделированию и управлению сложными распределенными производствами. В рамках единого проекта производственные процессы описываются в виде модели сквозного процесса, включающего типовые процессы производства изделий, процессы сборочных операций узлов и процессы распределения готовых изделий и узлов в центральных автоматизированных накопителях и складах. Для визуализации содержания типовых процессов и разработки структуры управляющих программ в динамике исполнения операций предлагается использовать аппарат временных раскрашенных сетей Петри.

распределенное производство, процессный подход, сквозные процессы, раскрашенные сети Петри

Распределенное производство предполагает выполнение различных производственных и технологических процессов создания изделий (деталей, сборочных единиц) на специализированных, как правило, территориально разнесенных предприятиях. Понятие «производство» принято рассматривать с двух основных позиций [1]:

– как обособленные структурные подразделения предприятия (цех, производственная линия, участок и т.п.);

– как производственный процесс изготовления конкретного продукта (изделия).

Различие в подходах к рассмотрению производства обусловливает основные концепции организации и управления:

– концепция на основе функциональной модели;

– концепция на основе процессного подхода.

При организации производства в пространстве и во времени в рамках обособленных структурных подразделений, как правило, используется функциональная модель управления. В основе концепции функционального подхода к управлению делегирование полномочий и ответственности осуществляется через выполняемые функции, т.е. заключается в объединении сотрудников в отдельные структурные единицы (отделы, департаменты и прочее) по принципу однообразия выполняемой деятельности с жесткой вертикальной иерархией.

Вместе с тем производственный процесс в целом представляет собой совокупность взаимосвязанных технологических процессов и операций по изготовлению конкретного изделия (продукта). Сущность процессного подхода к управлению производством заключается в следующем [2]: «последовательные и прогнозируемые результаты достигаются более эффективно и результативно, когда деятельность осознается и управляется как взаимосвязанные процессы, которые функционируют как согласованная система». Основой данной методологии является понятие «процесса».

Процесс – устойчивая, целенаправленная совокупность взаимосвязанных видов деятельности, которая по определенной технологии преобразует входы в выходы, представляющие ценность для получателя (потребителя) [3]. На рисунке 1 в общем виде приведено схематичное представление любого процесса.

Рис. 1. Обобщенная схема процесса

Применение процессного подхода для организации автоматизированных производств, при сложившейся практике использования функциональной модели управления, остается в настоящее время актуальной задачей. Планирование и управление распределенным производством сложных изделий (комплексов), как правило, предлагается организовывать в рамках специального проекта на основе процессного подхода. *Проект* – уникальный процесс, состоящий из совокупности скоординированных и управляемых видов деятельности [2].

Для применения процессного подхода к управлению распределенными производствами в рамках специального проекта предлагается рассматривать сквозные процессы как периодически повторяемую деятельность, результатом которой является некоторый ресурс, имеющий ценность для конкретного получателя (рис. 2).

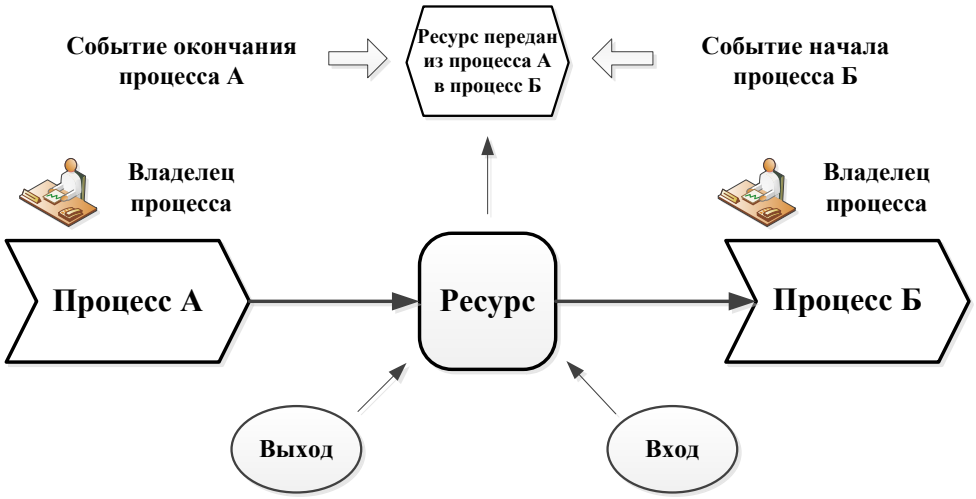


Рис. 2. Схема сквозного процесса

С позиций руководителя проекта представление деятельности обособленных подразделений и отдельных предприятий кооперации в виде сквозного процесса предлагается считать необходимым, но не достаточным условием по управлению распределенным производством. Широко используемые инструменты сетевого планирования и управления сложными проектами (например, диаграммы Ганта) не дают полной информации о ходе выполнения конкретных задач (процессов) структурных подразделений и предприятий на обособленных производствах, организуемых в рамках функциональной модели управления. Декомпозиция сквозного процесса до уровня элементарных процессов (технологических операций) позволит руководителю проекта получать полную информацию для оперативного принятия адекватных управленческих решений.

Декомпозицию сквозного процесса можно представить в виде совокупности типовых моделей, отражающих характерные особенности конкретного вида производства. В таблице 1 в качестве примера приведены типовые модели процессов сборочного производства.

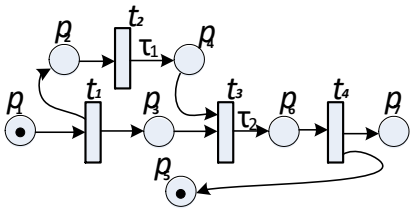
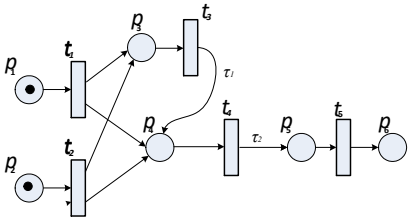
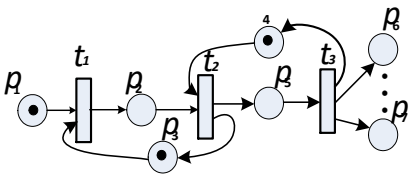
Сквозной процесс сборочного производства сложного изделия, в общем виде, включает следующие взаимосвязанные типовые процессы: изготовление (обработка) изделия на технологическом оборудовании, сборочные операции из компонентов (деталей), обработка и распределение изделий на автоматизированных накопителях и складах.

ТАБЛИЦА 1. Типовые модели сборочного производства

Содержание процесса	Модель процесса
Операция изготовления (обработки) изделия на технологическом оборудовании	
Операция изготовления сборочной единицы (узла) из компонентов (деталей) согласно спецификации	
Операция обработки и распределения готовых изделий (деталей, сборочных единиц, узлов) в автоматизированных накопителях и складах	

Для отображения содержания типового процесса, отражающего динамику выполняемых технологических операций, предлагается использовать аппарат раскрашенных временных сетей Петри (таблица 2).

ТАБЛИЦА 2. Пример описания действий типовых процессов сетями Петри

Модель процесса	Содержание действий
	
	
	

Применение процессного подхода в системе управления распределенным производством позволяет:

– понимать и постоянно контролировать выполнение требований к качеству конечного продукта;

– рассматривать сквозные процессы с точки зрения добавления ими ценности;

– достигать результативного функционирования процессов;

– обеспечить переход к комплексной автоматизации сквозных производственных процессов и управлению гибкими производственными системами.

Список используемых источников

1. Шишмарев В. Ю. Автоматизация технологических процессов: Учеб. пособие для студ. сред. проф. образования / Владимир Юрьевич Шишмарев. М.: Издательский центр «Академия», 2005. 352 с. ISBN 5-7695-2054-X

2. ГОСТ Р ИСО 9000-2015. Системы менеджмента качества. Основные положения и словарь. М: Стандартинформ, 2015. 49 с.

3. Репин В В., Елиферов В. Г. Процессный подход к управлению. Моделирование бизнес- процессов / Владимир Репин, Виталий Елиферов. М.: Манн, Иванов и Фербер. 2013. 544 с. ISBN 978-5-91657-554-5

ON THE APPLICATION OF THE PROCESS APPROACH TO MANAGING DISTRIBUTED PRODUCTION

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

The paper considers a process-based approach to modeling and managing complex distributed production processes. Within a single project, production processes are described as an end-to-end process model that includes typical product manufacturing processes, assembly operations for components, and distribution of finished products and components in central automated storage facilities and warehouses. To visualize the content of typical processes and develop the structure of control programs in the dynamics of operation execution, it is proposed to use the concept of timed colored Petri nets.

Key words: *distributed production, process approach, end-to-end processes, colored Petri nets*

УДК 621.391.1
ГРНТИ 49.33.29

СИНТЕЗ РЕШАЮЩЕГО ПРАВИЛА ПРИЕМНИКА С Δ-СЛОЕМ НЕРАЗЛИЧИМОСТИ ПСЕВДОСЛУЧАЙНЫХ СИГНАЛОВ ПРИ НЕКОГЕРЕНТНОМ ВОЗДЕЙСТВИИ ПРЕДНАМЕРЕННЫХ ПОМЕХ

А. О. Негурица, В. В. Сазонов,

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

Для приема псевдослучайных сигналов в условиях некогерентного воздействия преднамеренной помехи вводится рандомизированное решающее правило с Δ-слоем неразличимости сигналов. На основе методов теории статистических решений, теории информации и динамического программирования показана квазиоптимальность предлагаемого решающего правила приемника по минимаксному критерию, при приеме аддитивной смеси некогерентной преднамеренной помехи и псевдослучайных фазамонипулированных сигналов.

преднамеренная помеха, класс помех с ограниченной средней мощностью, база сигнала, отношение шум/сигнал, энергетический выигрыш, система передачи данных, рандомизированный алгоритм приема сигналов, приемник Котельникова.

Известно [1-6], что исследования в области приема псевдослучайных сигналов при воздействии помех на решение задач анализа и оптимизации параметров и режимов обработки имеют ряд сложностей. Данные сложности заключаются в противодействии преднамеренным помехам, структура которых может быть специально подобранной противником для нанесения максимального ущерба алгоритмам работы системы передачи данных: ее срыва или деградации характеристик.

При заранее заданном алгоритме формирования равновероятных сигналов $\{\pm 1\}$ задача обеспечения помехоустойчивости системы связи сводится к поиску оптимального рандомизированного алгоритма приема сигналов. Элемент рандомизации в алгоритме приема сигналов характеризуется наличием Δ-слоя неразличимости – области сигнального пространства, в котором решение $\{\pm 1\}$ принимается случайно. Для помехи, ограниченной средней мощностью, алгоритм приема сигналов с оптимизированным Δ-слоем эффективен при базе сигнала ($n = 1$ и $n = 2$) и гарантирует помехоустойчивость выше (от 0,41 до 1,38 дБ) приемника Котельникова [7, 8]. Общая постановка и пути решения проблемы передачи данных по каналам с

неполно заданными характеристиками рассматривались в [7, 8]. Однако, в [7, 8] вопросах помехоустойчивости приема двоичных псевдослучайных сигналов с использованием Δ-слоя неразличимости в условиях некогерентности преднамеренных помех не рассмотрено.

Дальнейшее изложение построено следующим образом. На основе задачи анализа помехоустойчивости приема двоичных псевдослучайных сигналов с использованием Δ-слоя неразличимости в условиях некогерентности преднамеренных помех, делаются выводы по применению полученных результатов.

Структурная схема однонаправленной системы передачи данных, функционирующей в условиях преднамеренных помех показана на рис. 1, где$x(t)$ и $y(t)$ обозначены передаваемые источником и выдаваемые получателю данные, $s(t)$ и $u(t)$ – передаваемые, принимаемые сигналы, умноженные (X) на эталонные псевдослучайные последовательности; $\nu(t)$ – преднамеренная помеха (некогерентно воздействующая на принимаемые сигналы).

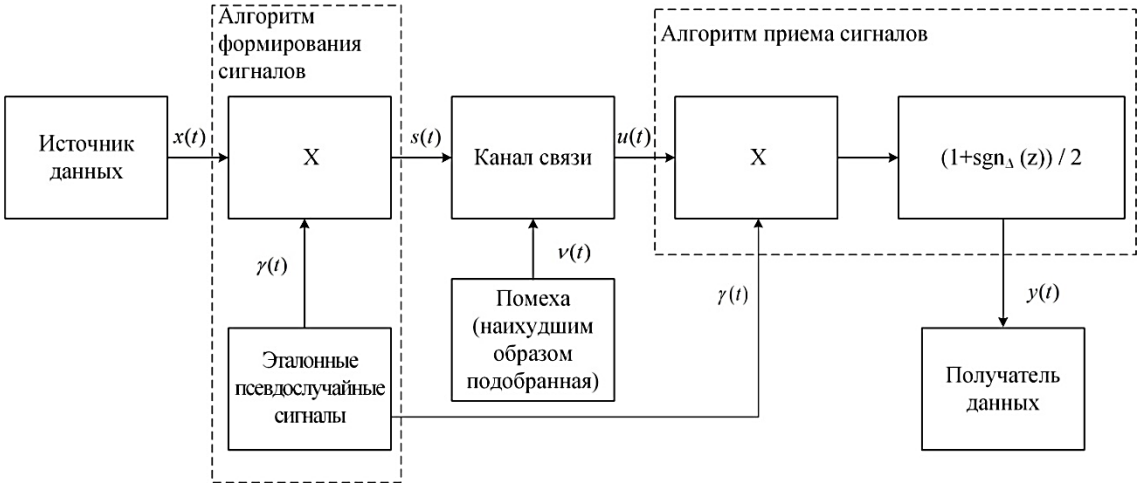


Рис. 1. Структурная схема взаимодействия элементов в однонаправленной системе передачи данных с источником преднамеренных помех

Двоичные символы $x \in \{\pm 1\}$ источника данных представляются сигналами $s_1 \in S'(1)$, $s_x = xs_1$, которые передаются по каналу связи, подверженному воздействию аддитивной преднамеренной помехи $\nu \in S(\sqrt{\delta})$, где δ – отношение средней энергии помехи к энергии сигнала, $S'(r), S(r)$ – соответственно сфера и шар в $\mathbb{R}^n$ радиуса r.

Алгоритм формирования сигналов и алгоритм их приема основаны на использовании заранее сформированной эталонной псевдослучайной последовательности $\gamma(t)$ с базой n с учетом некогерентного воздействия помехи

на сигнал (по причине практической нереализуемости помехи, накладываемой на сигнал с заданной разностью фаз несущих колебаний). При этом приемник использует рандомизированное решающее правило, которое в общем случае задается вероятностью $P(u,s)$ выдачи получателю символа 1 при получении из физического канала сигнала $u = s_x + v$ и имеющемся на приеме эталонном сигнале s с Δ-слоем неразличимости в области принятия решений. Для алгоритма приема с Δ-слоем функция $P_\Delta(u,\ s)$ представляется соотношением:

$$P_\Delta(u,\ s) = \frac{1}{2}(1 + sgn_\Delta(u,\ s)), \tag{1}$$

где $sgn_\Delta(z) = \begin{cases} -1, & if \quad z \le -\Delta, \\ 0. & if \quad -\Delta < z < \Delta, \\ 1, & if \quad z \ge \Delta. \end{cases}$

При Δ = 0 алгоритм приема сигналов вырождается в нерандомизированный алгоритм и совпадает с приемником Котельникова.

Задача оптимизации помехоустойчивости системы передачи данных в условиях преднамеренного (некогерентого) воздействия помехи состоит в минимизации гарантированной вероятности ошибки

$$P^-(\delta, n, \Delta) = \max_{F_v \in \mathbb{F}(\delta)} \boldsymbol{E}[P(\delta, n, \Delta)] = \max_{F_v \in \mathbb{F}(\delta)} \boldsymbol{E}[P(\delta, n, \Delta | F_v)],$$

определенной как максимальное ее значение при наихудшем для системы распределении помехи F_v при ограничении ее средней мощности (т. е. в классе $\mathbb{F}(\delta)$). Эта задача направляется на оптимизацию величины Δ и формулируется в минимаксной постановке в виде

$$P^-(\delta,\ n,\ \Delta) \to \min_{\Delta}. \tag{2}$$

Основу задачи (2) составляет определение зависимостей: распределения $F_v^*(\delta) = \text{argmax}_{F_v}\mathbf{E}[P(\delta, n, \Delta)]$ и функции $P^-(\delta, n, \Delta)$, принцип нахождения которых определен в [2] (с. 61, теорема 2), соотношением

$$P^-(\delta, n, \Delta) = P^\wedge(\delta, n, \Delta),$$

где $P^\wedge(\delta, n, \Delta)$ – выпуклая оболочка зависимости $P(\delta, n, \Delta)$ по аргументу δ. При этом, как показано, наихудшая стратегия помехи определяется двухатомным распределением $F_v^*(\delta) \in \mathbb{F}(\delta)$.

Для решения задачи (2) с построением выпуклых оболочек $P^\wedge(\delta, n, \Delta)$ был проведен вычислительный эксперимент с учетом в модели [7, 8] влияния некогерентного воздействия помехи (фаза помехи равномерно распре-

делена от 0 до 2 π). Параметры моделирования: 10^5 независимых испытаний; диапазон варьирования отношения помеха/сигнал для фазоманипулированных сигналов $(n = 1)\delta \in [0,\ 2]$ с шагом 0,04, для амплитудно-фазоманипулированных $(n = 2)\delta \in [0,\ 4]$ с шагом 0,08; критические значения Δ-слоя для $n = 1$: $\Delta\{0;\ 0{,}1716;\ 0{,}3\}$, $n = 2$: $\Delta\{0;\ 0{,}2584;\ 0{,}5\}$. Результаты моделирования оценки помехоустойчивости системы передачи данных с преднамеренным когерентным (для сравнения) и некогерентым воздействием помех показаны на рис. 2.

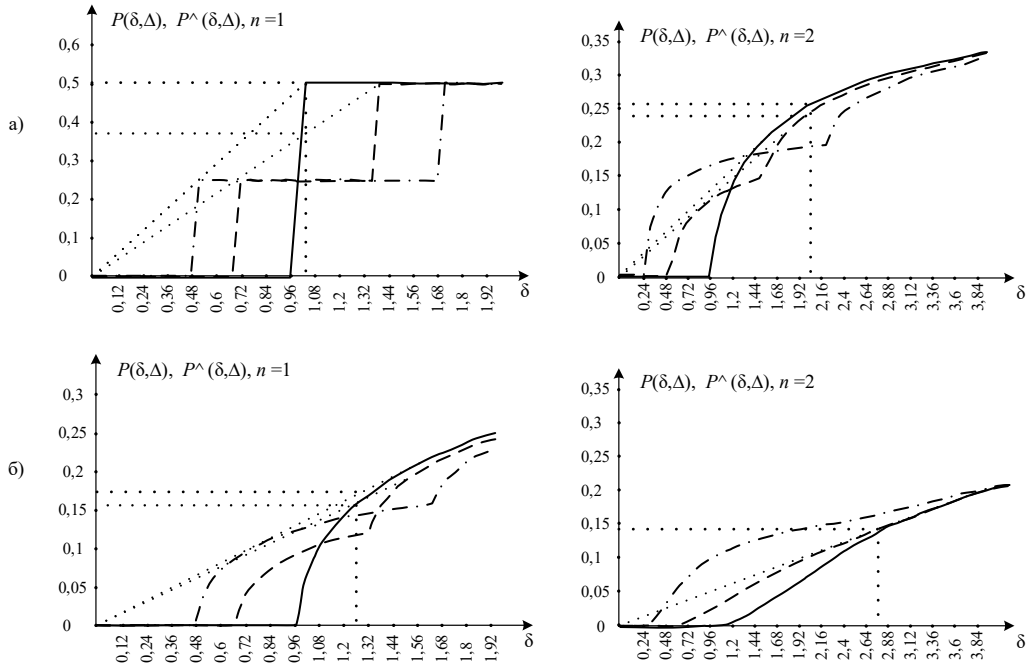


Рис. 2 Графики зависимостей$P(\delta,\ \Delta)$ и их выпуклых оболочек $P^{\wedge}(\delta,\ \Delta)$
(а – в условиях оптимальных (когерентных) преднамеренных помех;
б- в условиях некогерентности преднамеренных помех)

Из рисунка 2а видно, что для $n = 1$ максимальный энергетический выигрыш 1,38 дБ, а для $n = 2$ максимальный энергетический выигрыш 0,41 дБ, что соответствует ранее полученным результатам [7, 8].

Из рисунка 2б видно, что для $n = 1$ максимальный энергетический выигрыш 1,3 дБ, а для $n = 2$ энергетический выигрыш пренебрежимо мал. При этом, следует отметить, что наличие некогерентной составляющей в преднамеренной помехе приводит к снижению выигрыша (при $n = 1$ с 28 % до 7 %, а при $n = 2$ до 8 %), при использовании в алгоритме приема Δ-слоя неразличимости.

Данные результаты показывают, что предложенное в [7, 8] рандомизированное решающее правило с Δ-слоем неразличимости (1) является эффек-

тивным в условиях некогерентного воздействия преднамеренной помехи. В данных условиях имеет место энергетический выигрыш, для фазоманипулированных сигналов, до 1,3 дБ по сравнению с классическим приемником Котельникова ($\Delta = 0$). Этот выигрыш меньше, чем при когерентном воздействии (оптимальной) преднамеренной помехи (1,38 дБ), но остается значительным.

Полученные результаты показывают возможность повышения помехоустойчивости систем передачи данных (посредством введения в алгоритм обработки принимаемого сигнала правила с Δ-слоем неразличимости в области принятия решений (1)), работающих в сложной радиоэлектронной обстановке с преднамеренными некогерентными помехами.

Список используемых источников:

1. Чуднов А. М. Математические основы моделирования, анализа и синтеза систем / А. М. Чуднов. СПб.: ВАС, 2021. 193 с.

2. Чуднов А. М. Теоретико-игровые задачи синтеза алгоритмов формирования и приема сигналов // Проблемы передачи информации. 1991. Т. 27. № 3. С. 57–65.

3. Chudnov A. M., Kichko Ya. V., Sapunova L. P. Optimization of the guaranteed rate of information transmission by pseudo-random signals with a randomized base under conditions of deliberate interference // Radio engineering and electronics. 2023. Vol. 68. № 3. PP. 263–270.

4. Анализ помехоустойчивости локальных систем морской навигации в условиях воздействия оптимизированных помех / Е. И. Глушанков, Д. И. Кирик, З. К. Кондрашов [и др.] // Морской вестник. 2025. № 1(93). С. 89-91.

5. Одоевский С. М., Султанов Р. С., Ключников В. О. Оценка помехоустойчивости беспроводных линий связи с адаптивной модуляцией в условиях оптимизированных помех // Радиолокация, навигация, связь: Сборник трудов XXX Международной научно-технической конференции. В 5-ти томах, Воронеж, 16–18 апреля 2024 года. Воронеж: Издательский дом ВГУ, 2024. С. 238-247.

6. Чуднов А. М. Комментарии к статье Н. Н. Плотникова, А. В. Войнова и А. Н. Путилина «Выбор алгоритма адаптации по рабочей частоте в однополосной радиолинии тропосферной связи» // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2024. № 11-12(197-198). С. 20-30.

7. Chudnov A. M., Sazonov V. V., Bikbulatov V. R. Optimization of the decisive rule for a receiver with a Δ-layer of indistinguishability of binary signals in a channel with intentional interference // Problems of Information Transmission. 2025. Vol. 61. № 1. PP. 41-55.

8. Чуднов А. М., Сазонов В. В., Бикбулатов В. Р. Оптимизация области неразличимости приемником двоичных сигналов, передаваемых по каналу с преднамеренной помехой // Проблемы передачи информации. 2025. Т. 61. № 1. С. 47-59.

SYNTHESIS OF A DECISION RULE FOR A RECEIVER WITH A Δ-LAYER OF INDISTINGUISHABILITY OF PSEUDO-RANDOM SIGNALS UNDER NON-COHERENT INFLUENCE OF INTENTIONAL INTERFERENCE

Neguritsa A., Sazonov V.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

For the reception of pseudo-random signals under non-coherent influence of intentional interference, a randomized decision rule with a Δ-layer of signal indistinguishability is introduced. Based on methods from the theory of statistical decisions, information theory, and dynamic programming, the quasi-optimality of the proposed receiver decision rule is demonstrated according to the minimax criterion, when receiving an additive mixture of non-coherent intentional interference and pseudo-random phase-manipulated signals.

Key words: *intentional interference, class of interference with limited average power, signal base, signal-to-noise ratio, energy gain, data transmission system, randomized signal reception algorithm, Kotelnikov receiver*

УДК 654.739
ГРНТИ 49.33.29

ОБ ИНФОРМАТИВНОСТИ ДИНАМИЧЕСКОГО ПОДХОДА К АНАЛИЗУ И ПРИМЕНЕНИЮ ТРАНСПОРТНЫХ СВОЙСТВ ФУНКЦИОНАЛЬНЫХ ДИЭЛЕКТРИЧЕСКИХ МАТЕРИАЛОВ С НЕУПОРЯДОЧЕННЫЙ СТРУКТУРОЙ

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

Показываются и обосновываются возможности, которые открывает применение динамического подхода в целях детализации физической картины транспорта заряда в неупорядоченных диэлектриках и выявления необходимых для характеризации их устойчивости к электрическому разрушению структурной неоднородности. Предлагаются направленные на решение указанных задач методы аналитического и диагностического назначения

неупорядоченные диэлектрики, прыжковый транспорт, нестационарные явления, случайная неоднородность, методы анализа и прогностической диагностики

В ряду используемых и перспективных для создания элементов электронной базы инфокоммуникационных систем материалов видное место занимают диэлектрические материалы с неупорядоченной структурой как обладающие в слоях субмикронных толщин требуемыми свойствами и имеющие обширную технологическую базу получения [1, 2]. Область применения неупорядоченных диэлектриков охватывает конденсаторы, полевые транзисторы, элементы резистивной энергонезависимой памяти, электреты. Прогресс в этой области в значительной степени зависит от уровня знаний отвечающих за транспортные свойства представляющих интерес диэлектрических материалов физических процессов и факторов, для получения которых необходимы информативные методы. В отношении последних имеется ощутимый дефицит. Целый ряд широко и успешно используемых для анализа транспортных свойств кристаллических материалов методов, таких, например, как методы, основанные на измерении холловского напряжения и термо-ЭДС, не позволяют получить необходимую информацию относительно материалов с неупорядоченной структурой [3, 4]. В зна-

чительной степени это связано с сопряженной с неупорядоченностью структуры ее случайной неоднородностью.

Являясь, с одной стороны, ограничивающим фактором, случайная неоднородность структуры неупорядоченных диэлектриков, с другой стороны, ориентирует на изучение могущих быть положенными в основу анализа природы и диагностики транспортных свойств этих материалов физических явлений. К таковым относятся присущие неупорядоченным диэлектрикам долговременные нестационарные явления переноса заряда, что указывает на целесообразность применения к анализу и использованию указанных материалов динамического подхода и отвечающих ему методов, аргументируемую в настоящей работе.

Опорными в обосновании возможностей, которые открывает применение динамического подхода, являются результаты экспериментальных и теоретических исследований транспортных свойств аморфных диэлектрических оксидов тантала и ниобия в структурах емкостных элементов и зарядонакопительных электретных устройств [1, 2, 5]. В качестве рекомендуемых как апробированные, отвечающие динамическому подходу, методов выступают низкочастотная спектроскопия полной проводимости, хроноамперометрия и хроновольтометрия.

Информативной в плане установления механизма электропроводности в неупорядоченных диэлетриках является, как известно, частотная зависимость динамической проводимости [4, 5]. Наблюдаемая в широком диапазоне частот степенная зависимость проводимости на переменном токе является сильным аргументом в пользу прыжкового механизма электропроводности.

По изменению с частотой показателя степенной зависимости, будь оно наблюдаемо в результатах широкодиапазонной спектроскопии, как это имеет место у аморфных оксидов тантала и ниобия, можно судить о размерах кластера локализованных состояний, в пределах которого носители заряда успевают транспортироваться за полупериод переменного сигнала. Заметное понижение показателя степени с уменьшением частоты отражает рост протяженности цепочки задействованных в транспорте локализованных состояний и наличие на самых низких частотах мультиплетной прыжковой электропроводности, фиксация перехода к которой может быть осуществлена следующим образом.

Во-первых, по характеру поведения с понижением частоты отношения реактивной составляющей комплексной проводимости к разности между

активной составляющей и проводимостью на постоянном токе: от постоянства этого отношения в режиме транспорта в пределах кластеров небольших размеров к его падению с понижением частоты в режиме мультиплетной прыжковой электропроводности.

Во-вторых, по поведению динамической проводимости при приложении, наряду с малым переменным сигналом, постоянного напряжения, создающего в диэлектрике сильное электрическое поле. Обусловленный перестройкой путей протекания тока в неупорядоченной системе нелинейный эффект уменьшения проводимости с увеличением напряженности электрического поля может проявляться только при условии транспорта носителей заряда в пределах кластеров больших размеров, то есть в режиме мультиплетной прыжковой электропроводности. Соответственно, фиксируемая в эксперименте верхняя граничная частота указанного эффекта – это частота перехода к мультиплетной прыжковой электропроводности.

На основе температурной зависимости указанной граничной частоты можно получить информацию относительно природы носителей заряда и механизмов их локализации в диэлектрике. Как следует из развитой модели, в случае слабой электрон-фононной связи с ростом температуры граничная частота падает, а при сильной электрон-фононной связи, напротив, возрастает. Последнее, имеющее место в изученных материалах, указывает на поляронную природу носителей заряда [6].

Отмеченное в отношении поведения граничной частоты с изменением температуры обусловлено характеристической температурной зависимостью минимальной (критической), определяющей статическую проводимость, вероятности прыжка W_c. Последняя может быть восстановлена из временной зависимости изотермического релаксационного тока на постоянном сигнале, а именно, следуя модели нестационарной прыжковой проводимости [4], по отсечке графика этой зависимости, линеаризованной в координатах $(\gamma t)^{-1/2} - \lg t$. Располагая данными о зависимости $\gamma(t)$, полученными при различных значениях напряженности электрического поля, можно судить о зависимости $W_c(E)$ и, соответственно, о доказательности представлений о перестройке путей протекания тока в сильных электрических полях.

Динамический подход продуктивен и в плане определения распределения задействованных в прыжковом транспорте локализованных состояний по энергиям. Информативной здесь является зависимость потенциала электретированого диэлектрика от времени, прошедшего после его заряжения [7]. При релаксации потенциала, обусловленной экстракцией носителей за-

ряда, по этой зависимости можно определить положение уровня Ферми и энергетическое расстояние между ним и уровнем максимума плотности локализованных состояний.

Еще одна задача, которая может быть решена на основе динамического подхода – это определение малой подвижности носителей заряда. Один из апробированных способов ее решения основывается на анализе временной зависимости восстанавливаемого после закорачивания электретированного диэлектрика в проводящей среде потенциала [8]. Предпосылкой к тому является пропорциональность скорости ответственного за данное явление изменения электронной релаксационной поляризации подвижности носителей заряда.

Другой способ определения подвижности носителей заряда основывается на анализе изменения частотной зависимости тангенса угла диэлектрических потерь tg δ предварительно подвергнутого оптическому возбуждению диэлектрика в области собственного поглощения со временем. Возникающая при генерации неравновесных носителей заряда в приповерхностной области диэлектрика неоднородность по проводимости отражается в наличии в частотной зависимости максимума, который при распространении носителей в глубь образца смещается в область более низких частот и возрастает по величине. Подвижность носителей заряда, следуя развитой модели этого явления [9], может быть оценена по наклону прямолинейного участка графика зависимости квадрата максимального значения tg δ от времени.

Отметим, что применение указанных независимых методов к изученным материалам дало сходящееся по порядку величины значения подвижности носителей заряда.

Полученные на аморфных оксидах тантала и ниобия результаты изучения их транспортных свойств в структурах емкостных элементов [10] свидетельствуют о ресурсности динамического подхода в плане характеризации устойчивости диэлектрика по отношению к долговременному воздействию сильного электрического поля, что представляет интерес в плане прогностической диагностики.

Фактором первого порядка, определяющим кинетику электрического разрушения, является наличие в структуре неупорядоченного диэлектрика областей локального разрежения, в которых возникают каналы длиннопробежного транспорта ионов; в аморфных оксидах тантала и ниобия – кислородо- и водородосодержащих ионов. Первых – при нормальном включении

полярных емкостных элементов, что проявляется в электростимулированном росте кристаллов металлооксида, замещающих аморфный в исходном состоянии оксид; вторых – при приложении к емкостному элементу обратного напряжения, когда в каналах длиннопробежного транспорта происходит интенсивное восстановление оксидного вещества, а при значительной плотности тока – термическая кристаллизация [11, 12].

Как следует из результатов проведенных исследований, для выявления потенциально опасной структурной неоднородности целесообразно использовать следующие характеристики и параметры:

– частотную зависимость tg δ, обнаруживающую при наличии сильной неоднородности характерный максимум;
– начальную скорость наблюдаемого при структурно-фазовых изменениях роста ионного тока;
– величину обратного напряжения, при которой происходит возрастание граничной частоты перехода к мультиплетной прыжковой электропроводности;
– спектральную плотность низкочастотных избыточных шумов.

В дополнение к сказанному отметим, что динамический подход продуктивен применительно не только к диэлектрическим, но и к полупроводниковым материалам [13-16]. Так, с использованием этого подхода установлены фрактальные свойства временной последовательности импульсов тока при микроплазменном пробое структур светодиодов на основе фосфида галлия, развиты отвечающие этому модельные представления, методика выявления потенциально опасных дефектов и спроектирован генератор фрактальных сигналов.

Список используемых источников

1. Физика и технология наноструктурированных функциональных материалов: Монография / Под ред. С. Д. Ханина и Ю. А. Кумзерова. СПб.: Издательство Военной академии связи. 2023. 392 с.

2. 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.

3. Звягин И. П. Кинетические явления в неупорядоченных полупроводниках. М.: Изд-во МГУ, 1984. 187 с.

4. Bottger H., Bryksin V. Hopping Conduction in Solids. VCH, 1985. 472 p.

5. Khanin S. D. Kinetic Electron Phenomena in Metal Oxide Dielectric Films //Materials Science Forum, 1995. Vol. 185-188. PP. 563-572.

6. Брыксин В. В., Ханин С. Д. Сверхмалые поляроны в аморфном оксиде тантала // Физика твердого тела, 1993. Вып. 8. С. 2266-2270.

7. Брыксин В. В., Дороговцев С. Н., Моргунов М. С., Ханин С. Д. Релаксация поляризованного состояния в аморфных окислах Ta_2O_5 // Физика твердого тела. 1991. Т. 33. № 7. С.2031-2039.

8. Моргунов М. С., Ханин С. Д. Восстановление поверхностного потенциала аморфного оксида тантала // Физика твердого тела, 1984. Т. 26. № 12. С. 3545-3548.

9. Bryksin V. V., Goltsev A. V., Khanin S. D. Relation between the tangent of the angle of dielectric losses and low mobility in dielectric // Philosophical Magazin (b). 1991. Vol. 64. № 1. PP. 91-100.

10. Khanin S. D. Structure Inhomogeneities of the Oxide and the Properties of Tantalum Capacitors // Materials Science Forum. 1995. Vol. 185-188. PP. 573-580.

11. Ханин С. Д. Структурная неоднородность и транспортные свойства некристаллических металлооксидных материалов // Техника радиосвязи. 2023. Вып. 2(57). С. 76-82.

12. Ханин С. Д. Имплантационно-стимулированные процессы в функциональных элементах оксидных конденсаторов // 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. 4. С. 858-863.

13. Khanin S. D., Shashkina A. S. Characterization of microplazma breakdown in semiconductor structures based on fractal analyses // Nanotechnologies Science and Technology. New Materials Preparation, Properties and Applications in the Aspects of Nanotechnology. Nova Science Publishers. 2020. PP. 149-162.

14. Шашкина А. С., Ханин С. Д. Имитационный подход к моделированию лавинного пробоя p-n перехода // Физика и техника полупроводников. 2019. Т. 53. № 6. С. 850-855.

15. Khanin S. D., Shashkina A. S. Fractal Properties of Microplazma Breakdown and Structural Heterogenety of Semiconductor Materials // Environment Technology Resources. Proceedings of the International Scientific and Practical Conference. 2019. Vol. 3. PP. 105-108.

16. Шашкина А. С. Ханин С. Д., Костарев С. В. Фрактальные сигналы как альтернатива хаотическим сигналам в защищенных системах передачи информации // 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. 802-805.

ON THE INFORMATIVE VALUE OF THE DYNAMIC APPROACH TO ANALYSIS AND APPLICATION OF TRANSPORT PROPERTIES FUNCTIONAL DIELECTRIC MATERIALS WITH A DISORDERED STRUCTURE

Ostroumova Yu.[1], Khanin S.[2]

[1] Military Medical Academy of S. M. Kirov

[2] The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The possibilities that the application of the dynamic approach opens up in order to detail the physical picture of charge transport in disordered dielectrics and identify the structural inhomogeneities necessary to characterize their resistance to electrical destruction are shown and justified. Analytical and diagnostic methods aimed at solving these problems are proposed.

Key words: *disordered dielectrics, jump transport, unsteady phenomena, random heterogeneity, methods of analysis and prognostic diagnostics*

УДК 621.391
ГРНТИ 49.43.29

ИССЛЕДОВАНИЕ АЛГОРИТМОВ ЛИНЕЙНОЙ И НЕЛИНЕЙНОЙ ФИЛЬТРАЦИИ СИГНАЛОВ В ГИДРОАКУСТИЧЕСКОМ КАНАЛЕ СВЯЗИ

Д. Р. Сидоркович

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

Гидроакустические каналы связи являются неотъемлемой частью современных подводных коммуникационных систем, обеспечивая передачу данных в условиях, где радиочастотные методы теряют свою эффективность. Для повышения надежности и качества обмена информацией в сложной подводной среде, подверженной рэлеевским замираниям и специфическим шумам, необходимы современные методы обработки сигналов. В данной работе исследуются алгоритмы линейной и нелинейной фильтрации, реализованные на основе фильтра Калмана и расширенного фильтра Калмана, с учетом особенностей различных апертур.

подводная беспроводная связь, фильтр Калмана, распределение Рэлея

Пусть для передачи информации используется гидроакустический канал связи (ГАКС), в котором присутствуют аддитивный белый гауссовский шум, замирания, а также эффект Допплера [1].

Стохастическое дифференциальное уравнение (СДУ) для описания параметров ГАКС имеет следующий вид для распределения Рэлея [2]:

$$dx = \left(\frac{4\sigma^2}{N_0}x(t) + \frac{N_0}{x(t)}\right)dx + dw, \quad (1)$$

где N_0 – односторонняя спектральная плотность мощности белого шума, σ – дисперсия замирающей амплитуды.

Так как в канале шум является аддитивным белым гауссовским, матрица воздействия шума процесса можно принять равной единице.

Тогда априорная матрица ошибок имеет вид:

$$P_{k+1|k} = P_k P_{k|k} F_k^T + Q, \quad (2)$$

где Q – начальная дисперсия шума процесса, вычисляется как:

$$Q = \left(\frac{N_0}{2}\right)\Delta t, \quad (3)$$

Вычисление коэффициента усиления происходит по формуле (4):

$$K = \frac{P_{k+1|k} H_k^T}{H_k P_{k+1|k} H_k^T + R}, \quad (4)$$

В формуле (4) применяются линеаризованные матричные коэффициенты, представленные формулами (5) и (6), а также начальная дисперсия шума измерений R и априорная матрица ошибок (2).

Линеаризованная матрица перехода (5) образуется на основе СДУ для распределения Рэлея:

$$F_k = 1 + \left(\frac{4\sigma^2}{N_0} + \frac{N_0}{x(t)}\right)\Delta t, \quad (5)$$

Линеаризованная матрица наблюдения (6):

$$H_k = cos(\omega t_{k+1} + \varphi_{k+1}) \quad (6)$$

Конечный вид алгоритма фильтрации, использованного для рассматриваемой модели, был выведен на основе [3] и представлен формулой (7):

$$\hat{x}_{k+1|k+1} = \hat{x}_{k+1|k} + K_{k+1}\left(z_{k+1} - H_k \hat{x}_{k+1|k}\right), \quad (7)$$

На основе данных, представленных выше, было проведено сравнение алгоритмов линейной и нелинейной фильтрации для двух видов апертур: линейно и квадратичной.

На рис. 1 представлены результаты моделирования для линейной апертуры для линейного фильтра Калмана (Kalman filtering – KF) и расширенного фильтра Калмана (Extended Kalman filter – EKF).

Численные данные занесены в таблицу 1.

ТАБЛИЦА 1. Значение параметров для линейной апертуры

Оцениваемый параметр	KF	EKF
Среднеквадратичная ошибка (MSE)	0.2164	0.1120
Коэффициент корреляции	0.8133	0.8749
Время сходимости, с	0.0340	0.0206
Скорость сходимости, 1/с	29.41	48.54

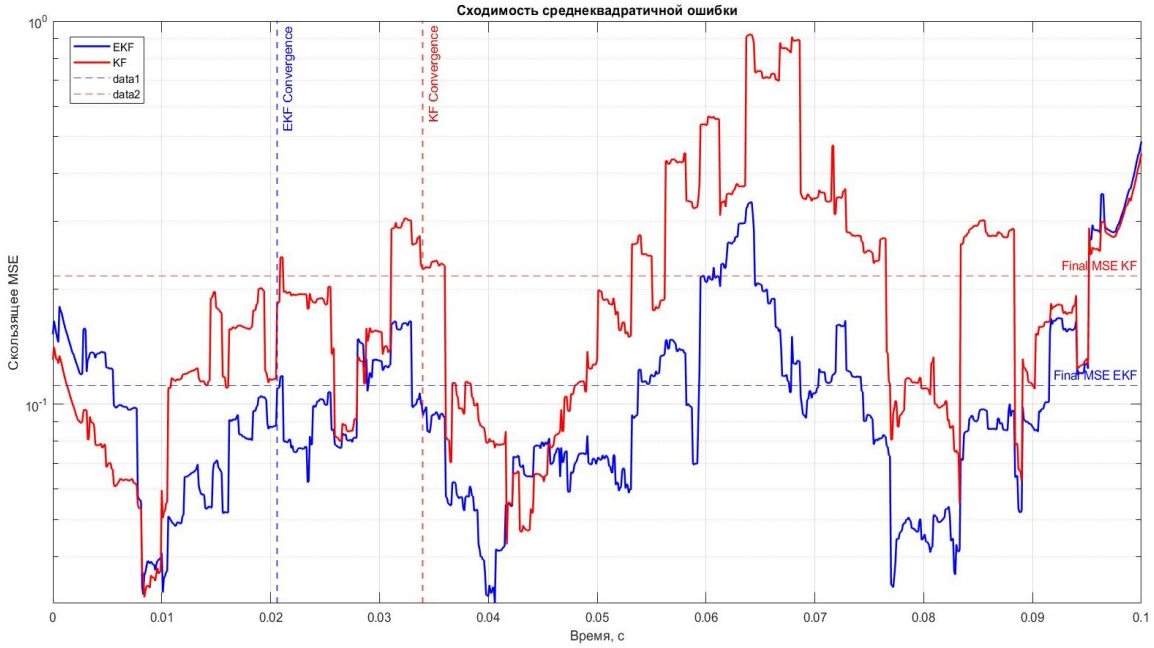


Рис. 1. Сходимость среднеквадратичной ошибки

На рис. 2 представлены результаты моделирования для квадратичной апертуры. В данном варианте также использовались два вида фильтрации: линейная и нелинейная.

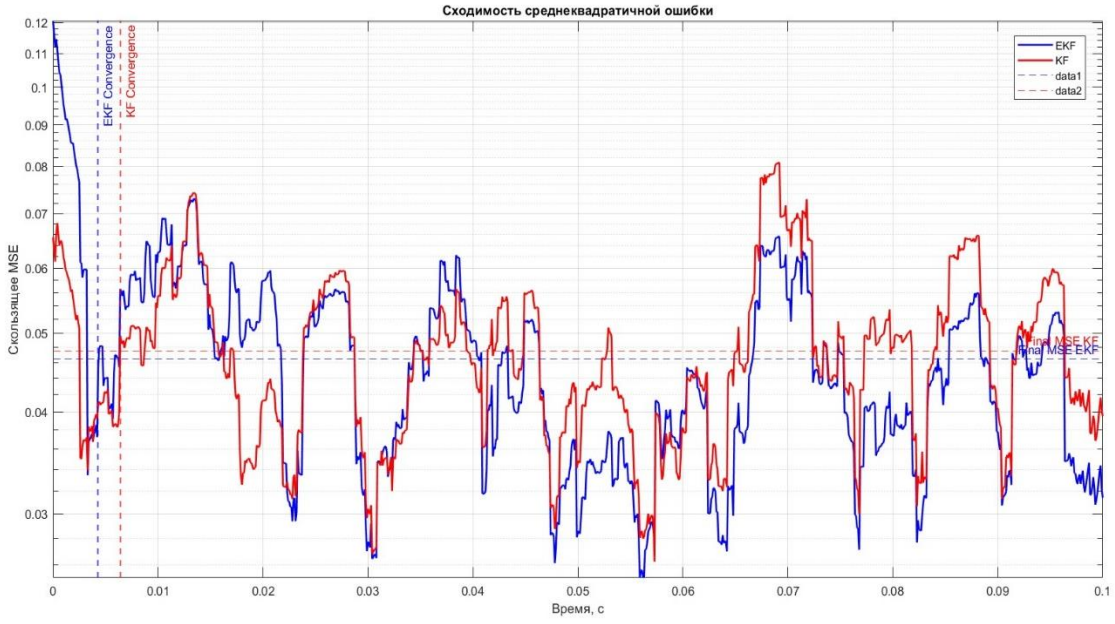


Рис. 2. Результаты моделирования для квадратичной апертуры

Численные данные для данного варианты моделирования занесены в таблицу 2.

ТАБЛИЦА 2. Значение параметров для линейной апертуры

Оцениваемый параметр	KF	EKF
Среднеквадратичная ошибка (MSE)	0.2164	0.1120
Коэффициент корреляции	0.8133	0.8749
Время сходимости, с	0.0340	0.0206
Скорость сходимости, 1/с	29.41	48.54

Анализ таблиц 1 и 2 позволяет сделать следующие выводы:

– точность оценки: EKF на 48 % для линейной апертуры и на 7 % для квадратичной апертуры точнее KF, благодаря учету нелинейной динамики;
– скорость сходимости: EKF быстрее адаптируется к изменениям амплитуды;
– устойчивость: KF менее чувствителен к начальным условиям.

Разработанная модель учитывает особенности гидроакустического канала связи. Благодаря моделированию появляется возможность проследить тенденцию к обеспечению более точной оценки амплитуды сигнала расширенным фильтром Калмана, который является нелинейным, в условиях рэлеевских замираний, что подтверждается снижением MSE на 30-40 % по сравнению с линейным фильтром Калмана в гидроакустических симуляциях.

Список используемых источников

1. Ahmed S. et al. Parameters Affecting Underwater Channel Communication Performance // Parameters. 2018. Т. 9. № 10.

2. 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.

3. Сейдж Э. М. Д. Теория оценивания и ее применения в связи и управлении. 1976.

Статья представлена научным руководителем, профессором кафедры РТ СПбГУТ, доктором технических наук, профессором Глушанковым Е. И.

RESEARCH OF LINEAR AND NONLINEAR SIGNAL FILTERING ALGORITHMS IN A HYDROACOUSTIC COMMUNICATION CHANNEL

Sidorkovich D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Hydroacoustic communication channels are an integral part of modern underwater communication systems, enabling data transmission in environments where radio frequency methods lose their effectiveness. To improve the reliability and quality of information exchange in the challenging underwater environment, which is subject to Rayleigh fading and specific types of noise, modern signal processing methods are required. This work examines algorithms for linear and nonlinear filtering, implemented based on the Kalman filter and the extended Kalman filter, taking into account the characteristics of different apertures.

Key words: *Underwater wireless communication, Kalman filter, Rayleigh distribution*

УДК 621.396.67
ГРНТИ 47.45.29

ДИАГРАММООБРАЗОВАНИЕ АНТЕННОЙ РЕШЕТКИ В СИСТЕМЕ КООРДИНАТОМЕТРИИ БЛИЗКОРАСПОЛОЖЕННЫХ ИСТОЧНИКОВ СИГНАЛОВ ДЛЯ ПОДАВЛЕНИЯ ПОМЕХ

Д. С. Сыроветник

ООО «Амунго»

В данной работе описывается программная реализация алгоритма подавления помех за счет изменения диаграммы направленности антенной решетки. Рассматривается система координатометрии близкорасположенных источников сигналов, в которой используются плоские эквидистантные антенные решетки, состоящие из 4 или 16 элементов типа патч-антенн. К сигналам и помехам, принимаемым антенной решеткой, применяется алгоритм сверхразрешения MUSIC. По результатам его работы устанавливается факт распознавания помехи и относительный уровень ее мощности. В направлении нежелательных сигналов в диаграмме направленности антенной решетки формируются нули. Положительным результатом работы алгоритма подавления помех является полное их отсутствие в итоговом пространственном спектре алгоритма MUSIC или значительное снижение их мощности. Разработанные программно-математические решения будут внедрены в главную программу координатометрии в качестве одной из модификаций и повысят помехоустойчивость системы.

антенная решетка, помеха, диаграмма направленности, координатометрия, алгоритм сверхразрешения MUSIC, MATLAB

История использования преднамеренных помех для радиоэлектронной борьбы берет свое начало еще с первых лет XX века, со времен Русско-японской войны. С тех пор антенно-фидерные устройства и приемопередатчики значительно преображались, параллельно решая две задачи – помехозащищенную передачу и прием информации, а также подавление средств связи противника путем излучения мощного и сложного по сигнатуре помехового радиосигнала. В современное время, особенно в последние годы, задача борьбы с помехами на различных радиоканалах, наверное, находится на одном из своих пиковых значений в вопросе актуальности [1]. Именно поэтому каждая разрабатываемая радиосистема в наши дни должна принимать меры по защите от помех и предлагать алгоритмы, позволившие бы эффективно работать в любой помеховой обстановке. В данной работе будет про-

веден краткий обзор существующих способов борьбы с помехами, выбран и реализован наиболее эффективный из них применительно к разрабатываемой системе координатометрии.

На данный момент была реализована модель системы координатометрии в среде MATLAB, проводящая процесс нахождения угловых направлений (пеленгов) на источники радиоизлучения с помощью алгоритма сверхразрешения MUSIC, а также находя непосредственно координаты целей с помощью алгоритма координатометрии на базе метода наименьших квадратов (МНК) [2]. Разрабатываемая система является динамической, позволяет гибко задавать пространственно-мощностные параметры приемных и передающих объектов, а также их параметры скорости и траектории. В качестве приемных устройств рассматриваются антенные решетки из 4 и 16 антенных элементов, что позволяет реализовать алгоритмы по подавлению до 3 и 15 помех соответственно.

Рассмотрим основные алгоритмы для борьбы с помехами, различающиеся по способу применения и обработки данных [3].

Алгоритмы пространственной фильтрации. Позволяют подавлять помеховые сигналы за счет изменения диаграммы направленности (ДН).

Алгоритмы временной обработки. Позволяют отделить полезный сигнал от помехового за счет накопления и усреднения во времени.

Частотные методы. Используют быстрое преобразование Фурье (БПФ) и анализ частотного спектра, а также режекторную фильтрацию.

Поляризационные алгоритмы. Для подавления помех применяются специальные поляризационные фильтры и матрицы их параметров.

Слепые методы. Используют статистические методы разделения сигнала, слепые деконволюцию, шумоподавление и фильтрацию.

Гибридные методы. Представляют собой комбинацию вышеперечисленных алгоритмов. Эффективны при разнородных помехах.

Среди перечисленных наиболее эффективным подходом для разрабатываемой системы координатометрии является пространственная фильтрация [4]. Благодаря разнесению 4 или 16 антенных элементов появляется возможность гибко изменять диаграмму направленности и формировать «нули» в направления помех. Среди наиболее популярных алгоритмов можно выделить методы формирования луча (DAS, MVDR, LCMV), адаптивные методы (LMS, RLS), гибридные методы (STAP, BSS). Принимая во внимание работу с планарной антенной решеткой, отбрасываются простейшие алгоритмы по диаграммообразованию линейной решетки (Дольфа-Че-

бышева, Тейлора). Так как в разрабатываемой системе уже реализован алгоритм сверхразрешения MUSIC, то можно считать направления на приходящие сигналы (в том числе помеховые) известными. Таким образом, наиболее эффективным вариантом станет применение модификации алгоритма минимизации мощности помех (MVDR) с линейным ограничением LCMV [5].

Алгоритм линейного ограничения минимальной дисперсии сигнала LCMV (Linearly Constrained Minimum Variance) представляет собой поиск таких весовых коэффициентов, при которых выполняется условие минимизации целевой функции:

$J(w) = w^H R_{xx} w \rightarrow min$ *при условии* $C^H w = f$,

где w – вектор комплексных весовых коэффициентов размерности 1xM;

R_{xx} – ковариационная матрица принятого сигнала;

C^H – эрмитово-сопряженная матрица ограничений;

f – желаемый отклик системы;

M – число элементов антенной решетки.

Таким образом, формула для оптимального набора весовых коэффициентов может быть записана следующим образом:

$$w_{opt} = R_{xx}^{-1} C (C^H R_{xx}^{-1} C)^{-1} f.$$

На рисунке 1 представлена схема работы алгоритма LCMV.

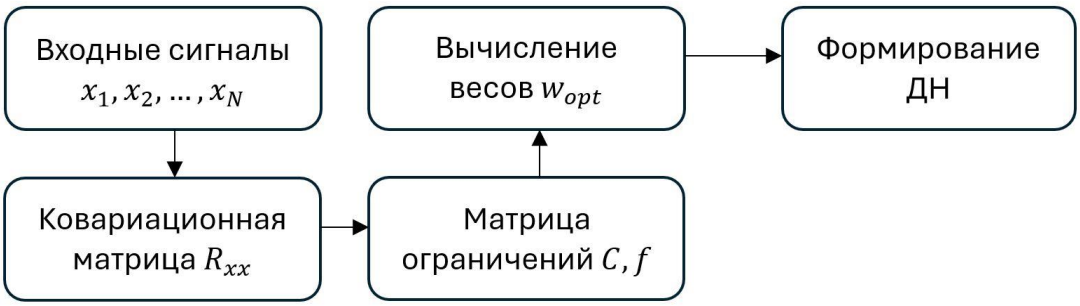


Рис. 1. Схема работы алгоритма LCMV

Ранее в разрабатываемой системе координатометрии использовалась антенная решетка с изотропными элементами, имеющими одну и ту же амплитуду и фазу. Для внедрения алгоритма подавления помех был произведен переход на адаптивную модель приемного устройства с возможностью регулировки комплексных весов. В цикл определения направления на источники излучения был добавлен блок оптимизации диаграммы направленности, принимающий результаты метода MUSIC в виде набора пеленгов и формирующий вектор весовых коэффициентов с целью уменьшения влия-

ния нежелательных сигналов. Для проверки алгоритма LCMV рассматривались пространственные спектр MUSIC со значениями ОСШ до и после оптимизации. На рисунке 2 приведена часть графического интерфейса модели в MATLAB, обновленного для ввода данных о помеховых сигналах, их координат и динамических параметров.

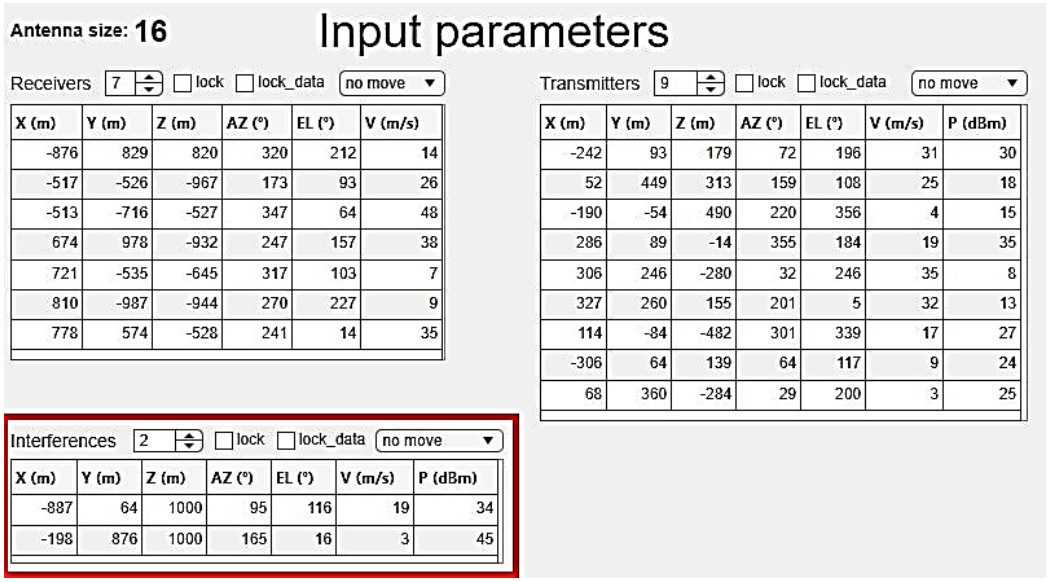


Рис. 2. Интерфейс модели координатометрии в MATLAB с блоком помех

Для антенной решетки из 4 элементов были сформированы следующие диаграммы направленности (стандартная и с нулем в направлении помехи).

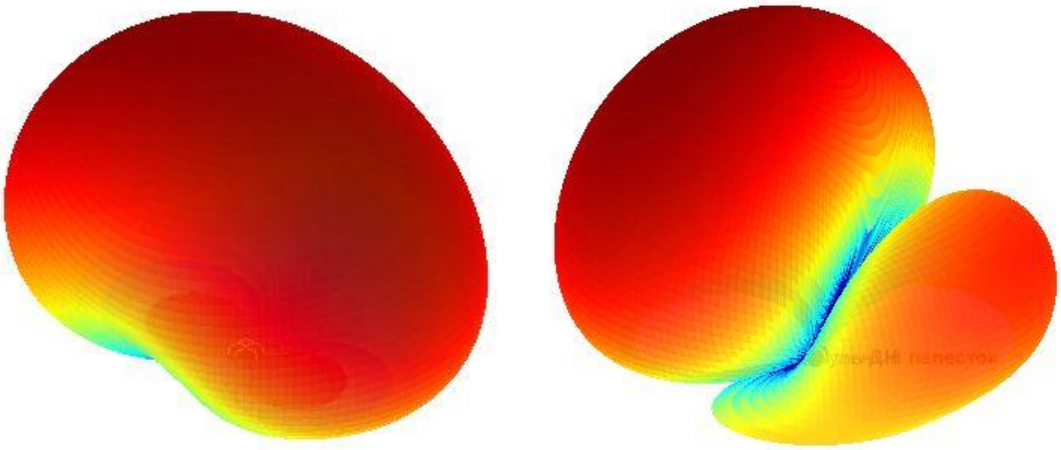


Рис. 3. ДН 4-элементной решетки до и после применения алгоритма LCMV

Из рисунка 3 видно, что на диаграмме направленности сформировался ярковыраженный ноль в одном из направлений. Для оценки численного «выигрыша» в ОСШ приводится рисунок 4 с пространственными спектрами MUSIC до и после применения алгоритма подавления помех.

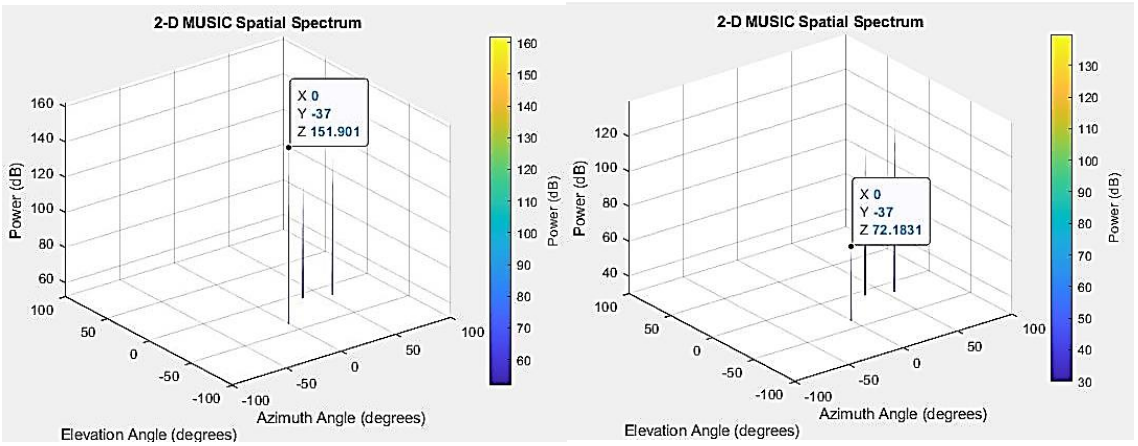


Рис. 4. Пространственные спектры MUSIC до и после алгоритма LCMV

Из рисунка 4 видно, что уровень ОСШ снизился с 151.9 до 72.2, что представляет собой выигрыш в 79.7 дБ по отношению к уровню сигнала в направлении помехи.

Для антенной решетки из 16 элементов был проведен аналогичный тест эффективности алгоритма LCMV. В данном случае формировался не один «ноль» ДН, а сразу три. Далее на рисунках 5 и 6 приведены аналогичные предыдущему варианту графические данные. Из рисунка 5 видно, что новообразованная диаграмма направленности имеет несколько лепестков, между которыми сформированы места наименьшей эффективности приема сигнала. Из рисунка 6 видно, что коэффициент подавления помех для трех нежелательных сигналов составил более 80 дБ и они перестали быть одними из результатов алгоритма MUSIC. Алгоритм LCMV показал свою эффективность для антенных решеток из 4 и 16 антенных элементов.

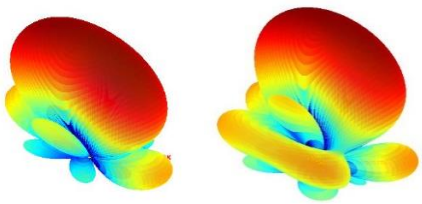


Рисунок 5. ДН 16-элементой решетки до и после применения алгоритма LCMV

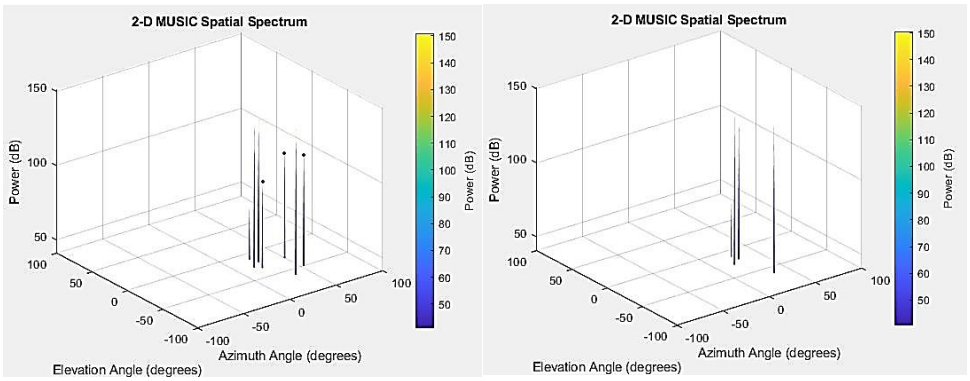


Рисунок 6. Пространственные спектр MUSIC до и после алгоритма LCMV

Результатом данной работы можно считать успешную реализацию и внедрение алгоритма диаграммообразования LCMV в разрабатываемую систему координатометрии близкорасположенных источников сигналов.

Список используемых источников:

1. Матвеев А. М. Современные способы борьбы с помехами в радиоэлектронных системах ракетно-космической техники / А. М. Матвеев, В. С. Конищев // Военная мысль. 2021. № 4. С. 101–105. EDN:OGHCSI

2. Динамическая модель координатометрии близкорасположенных источников сигналов с использованием алгоритма сверхразрешения MUSIC / Е. И. Глушанков, З. К. Кондрашов, Д. С. Сыроветник, Е. А. Рылов // Моделирование, оптимизация и информационные технологии. 2025. Т. 13, № 1(48), 11 с. DOI 10.26102/2310–6018/2025.48.1.004. EDN:IXVGKG

3. Harry L. Van Trees / Optimum Array Processing: Part IV of Detection, Estimation, and Modulation Theory, 2002 p. 1139 – 1194

4. Глушанков Е. И. Адаптивная пространственная фильтрация сигналов в четырехэлементной антенной решетке / Е. И. Глушанков, В. И. Царик // Подготовка профессиональных кадров в магистратуре для цифровой экономики. Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции, Санкт-Петербург, 30 ноября – 02 2021 года. СПб.: СПбГУТ, 2022. С. 60-63. EDN:TKQQPM

5. Яцкин Д. В. Особенности применения метода MVDR для обработки сигнала фазированной антенной решеткой / Д. В. Яцкин, И. А. Калинов, А. А. Кочкаров // Путь в науку. Радиотехнические системы: Материалы конференции, Ярославль, 27 апреля 2018 года / Отв. ред. Л. Н. Казаков; Ярославский гос. университет им. П. Г. Демидова. Ярославль: Ярославский государственный университет им. П. Г. Демидова, 2018. С. 47-57. EDN:OXJQMZ

Статья представлена научным руководителем, профессором кафедры РТ СПбГУТ, доктором технических наук, профессором Глушанковым Е. И.

ANTENNA ARRAY'S RADIATION PATTERN FORMATION IN THE COORDINATEOMETRY SYSTEM OF NEARBY SIGNAL SOURCES FOR INTERFERENCE SUPPRESSION

Syrovetnik D.
LLC "Amungo"

This paper describes a software implementation of an interference suppression algorithm by changing the antenna array radiation pattern. Coordinateometry system of nearby signal sources is considered, which uses planar equidistant antenna arrays consisting of 4 or 16 elements of the patch antenna type. The MUSIC super-resolution algorithm is applied to signals and interference received by the antenna array. Based on the results of its operation, the fact of interference recognition and the relative level of its power are established. Zeros are formed in the direction of unwanted signals in the antenna array radiation pattern. A positive result of the interference suppression algorithm is their complete absence in the final spatial spectrum of the MUSIC algorithm or a significant decrease in their power. The developed software and mathematical solutions will be implemented in the main coordinateometry program as one of the modifications and will increase the system's noise immunity.

Key words: *antenna array, interference, radiation pattern, coordinateometry, MUSIC super-resolution algorithm, MATLAB*

УДК 621.396.67
ГРНТИ 47.45.29

ИССЛЕДОВАНИЕ ВЛИЯНИЯ КОЛИЧЕСТВА ЭЛЕМЕНТОВ АНТЕННОЙ РЕШЕТКИ НА АЛГОРИТМЫ АДАПТАЦИИ ПРИ ВОЗДЕЙСТВИИ МЕРЦАЮЩИХ ПОМЕХ

А. А. Хренов

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

Современные радиотехнические устройства, использующие адаптивные антенные решетки, подвергаются воздействию различных типов помех, в том числе и мерцающих, что сказывается на работоспособности систем. Помехи данного вида могут иметь характеристики, которые не позволяют алгоритмам адаптации антенной решетки сходиться к оптимальному решению. В работе предлагается исследование влияния количества антенных элементов на работоспособность алгоритмов адаптации линейной антенной решетки в условиях воздействия мерцающих помех с различной частотой следования. Полученные результаты позволяют определить границы применимости алгоритмов адаптации, а также их оптимальные параметры в условиях сложной радиоэлектронной обстановки.

линейная антенная решетка, мерцающие помехи, алгоритмы адаптации.

Введение

Современные радиотехнические устройства, зачастую, работают в сложных условиях радиоэлектронной обстановки, подвергаясь влиянию различного рода помех, в том числе и мерцающих. Для улучшения качества приема информации в системах применяются адаптивные антенные решетки (ААР) с различным числом антенных элементов (АЭ) [1].

Целью исследования является оценка эффективности работы алгоритмов адаптации линейной антенной решетки при изменяющемся числе антенных элементов в условиях воздействия мерцающих помех с различным временем переключения.

Для достижения указанной цели были определены следующие задачи:

1. Провести моделирование в программной среде MATLAB случаев воздействия медленно и быстро мерцающих помех на алгоритмы адаптации линейной антенной решетки (АР) с различным количеством элементов.

2. Оценить ошибки на выходе линейной ААР.

3. Определить скорости сходимости алгоритмов адаптации.

4. Выполнить анализ полученных результатов с точки зрения влияния количества элементов ААР на улучшение устойчивости алгоритмов адаптации к мерцающим помехам.

Исследуемые алгоритмы адаптации и параметры моделирования

В качестве исследуемых алгоритмов адаптации были выбраны:

1) LMS (Least Mean Squares) – алгоритм по критерию наименьших квадратов;

2) NLMS (Normalized Least Mean Squares) – адаптивный нормализованный алгоритм по критерию наименьших квадратов;

3) RLS (Recursive Least Squares) рекурсивный алгоритм по критерию наименьших квадратов.

Более подробное математическое описание представленных алгоритмов приводится в работе [1]. Также для сравнения эффективности работы был выбран оптимальный алгоритм Винера-Хопфа [2].

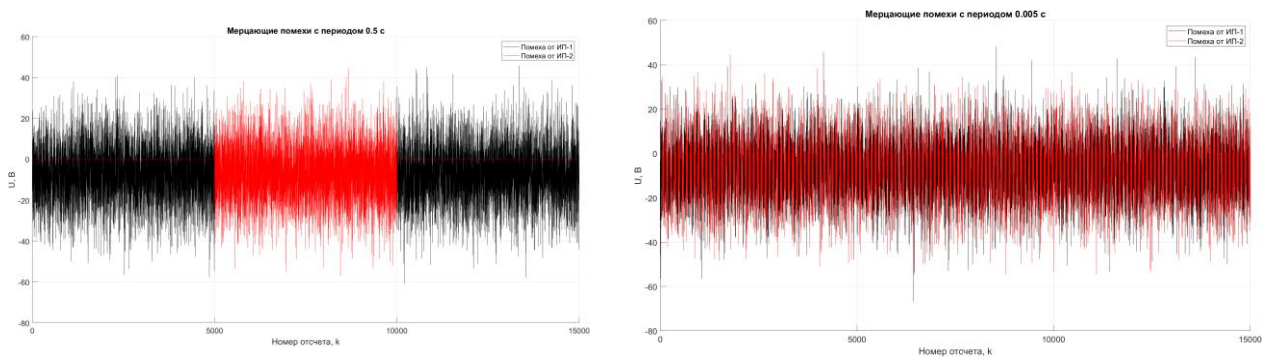
Параметры моделирования были определены следующие:

Антенная решетка: линейная с числом элементов $N = 2^n$, где n = 2, 3, 4, 5, 6, 7 => N = 4, 8, 16, 32, 64, 128 элементов соответственно.

Угол прихода полезного сигнала: 0 °.

Угол прихода помех: 25 ° и -25 °.

В качестве помех выбраны синхронизированные мерцающие, модели которых представлены на рисунке 2. Медленно мерцающие помехи с частотой повторения импульсов 2 Гц (0,5 с) (рис. 1, а) и быстро мерцающие помехи с частотой повторения импульсов 200 Гц (0,005 с) (рис. 1, б).



а) б)

Рис. 1. Модели помех: а) – медленно мерцающих; б) – быстро мерцающих.

Оценка ошибок на выходе линейной адаптивной антенной решетки

Для оценки влияния числа АЭ на ошибки алгоритмов адаптации при воздействии медленно и быстро мерцающих помех были построены графики зависимости квадрата ошибки на выходе ААР от числа антенных элементов (рис. 2) [3, 4].

Из графика видно, что при увеличении числа АЭ ошибки алгоритмов LMS и NLMS стремятся к значениям оптимального алгоритма. RLS показывает хорошие результаты, не уступающие алгоритму Винера-Хопфа, при воздействии медленно мерцающих помех, однако при быстро мерцающих ведет себя менее устойчиво.

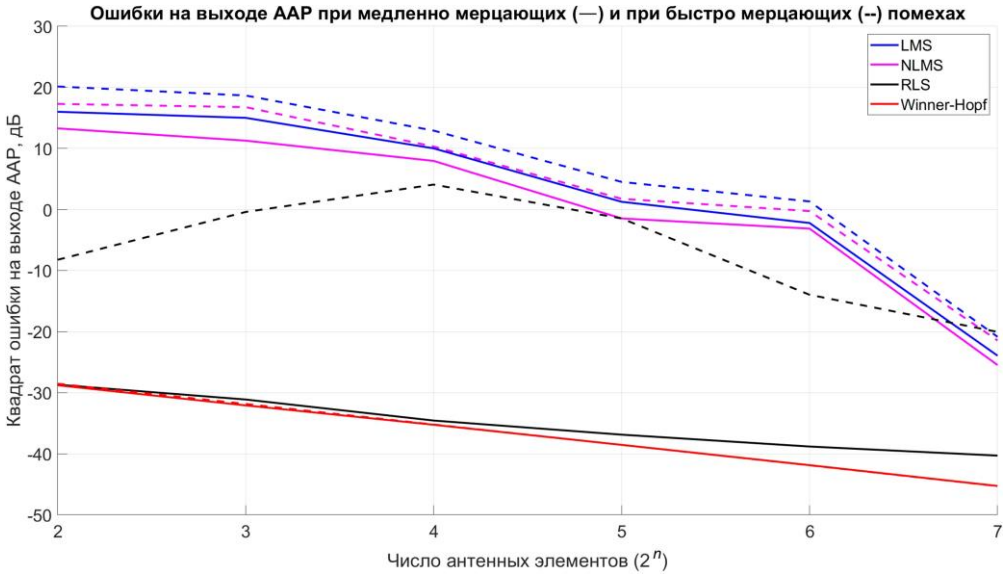


Рис. 2. Графики зависимости ошибки на выходе ААР от числа АЭ

Определение скорости сходимости алгоритмов адаптации

Решая задачу определения скорости сходимости алгоритмов адаптации по результатам имитационного моделирования, были получены графики зависимости скорости сходимости алгоритмов адаптации от числа АЭ (рис. 3) в условиях воздействия медленно и быстро мерцающих помех.

Видно, что алгоритмы LMS и NLMS ведут себя идентично и имеют малую скорость сходимости при воздействии быстро мерцающих помех. Наибольшую скорость сходимости (≈0,002 с) имеют алгоритмы RLS и Винера-Хопфа.

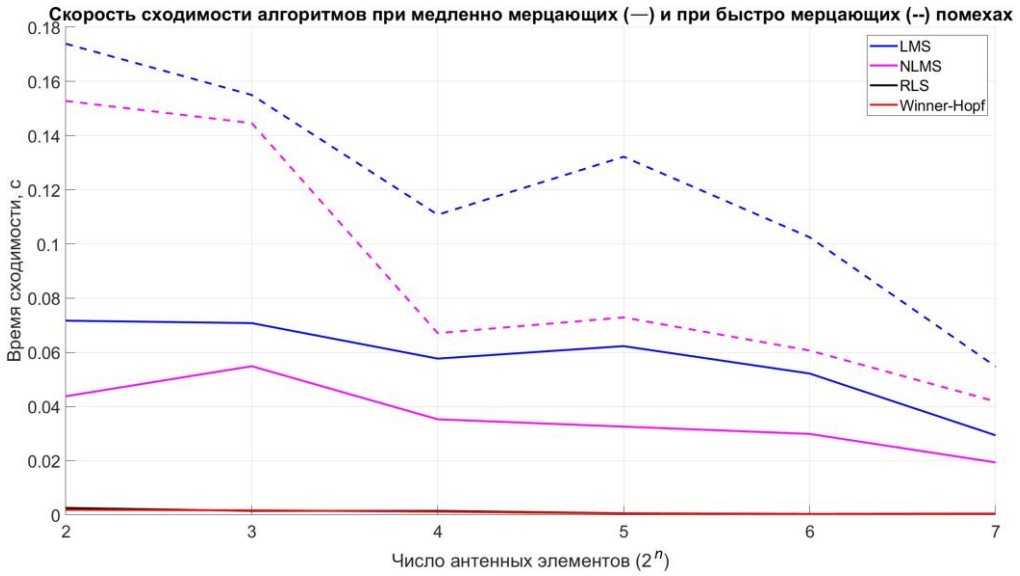


Рис. 3. Графики зависимости скорости сходимости алгоритмов от числа АЭ

Дополнительно было проведено исследование скорости сходимости для алгоритмов LMS и NLMS при увеличенном числе антенных элементов до 4096 (2^{12}). По результатам моделирования построены графики (рис. 4).

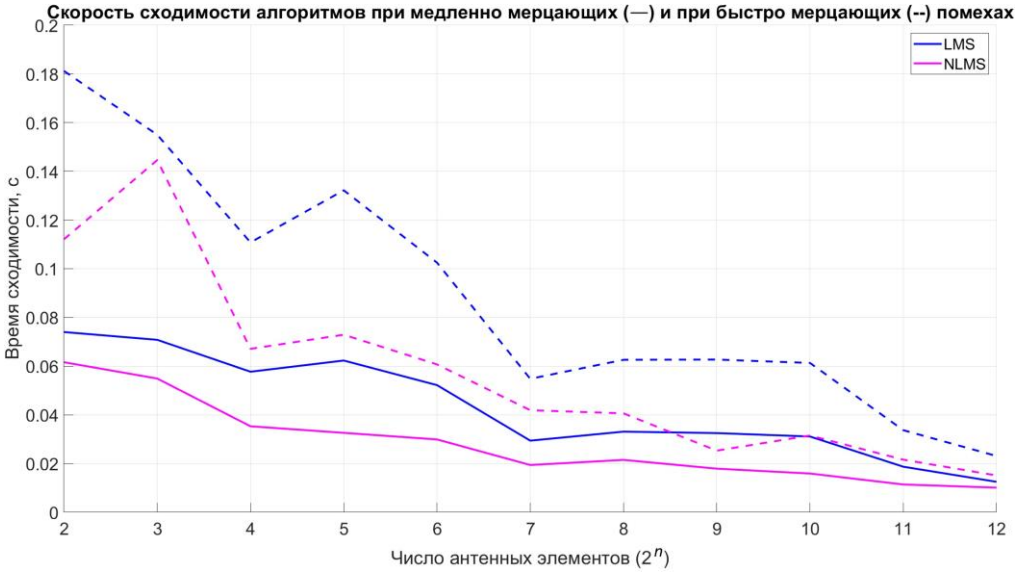


Рис. 4. График зависимости скорости сходимости LMS и NLMS от числа АЭ.

При большом числе антенных элементов скорости сходимости алгоритмов LMS и NLMS составляют ≈0,01 с, приближаясь к значениям алгоритмов RLS и Винера-Хопфа.

Время обработки входного сигнала алгоритмом адаптации

Немаловажным параметром при оценке эффективности алгоритмов адаптации является время обработки входного сигнала алгоритмом ААР,

которое напрямую связано с его вычислительной сложностью и количеством АЭ. Так для LMS и NLMS – это $O(2N)$, RLS – $O(N^2)$, а Винера-Хопфа – $O(N^3)$. В ходе имитационного моделирования построены графики зависимости времени работы алгоритмов от числа АЭ (рис. 5).

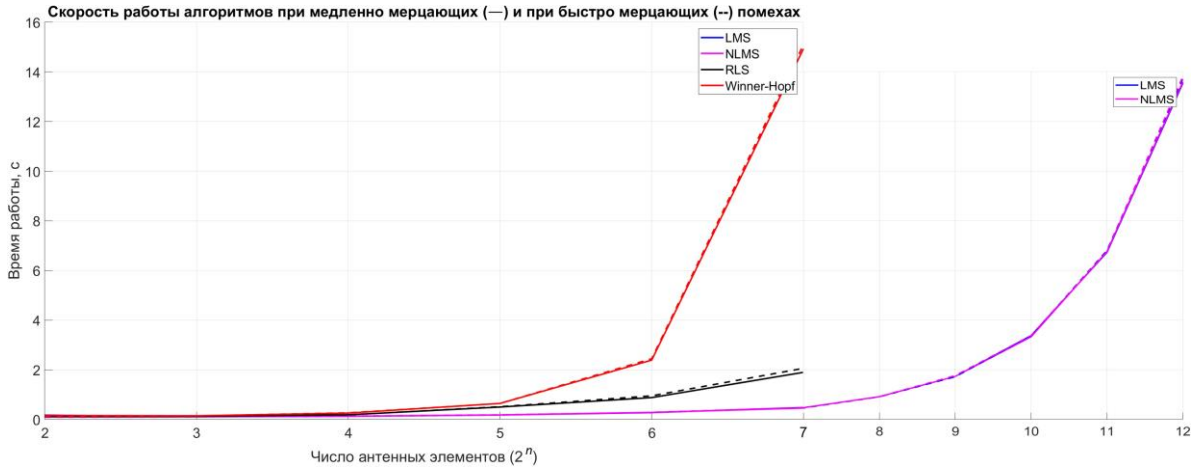


Рис. 5. График зависимости времени работы алгоритмов адаптации от числа АЭ

Из графиков видно, что при малом числе антенных элементов скорость работы всех алгоритмов составляет ≈0,1 с. Разница между работой алгоритмов в условиях быстро и медленно мерцающих помех составляет 0,2 с. Время работы алгоритмов LMS и NLMS при числе антенных элементов 128 и при воздействии мерцающих помех составляет ≈0,48 с, однако по мере увеличения числа АЭ время возрастает и приближается к значениям алгоритма Винера-Хопфа.

Анализ полученных результатов

Увеличение числа элементов линейной адаптивной антенной решетки в условиях воздействия мерцающих помех позволяет:

– во-первых, уменьшить ошибку на выходе ААР;
– во-вторых, увеличить скорость сходимости алгоритмов к оптимальному значению.

При воздействии мерцающих помех алгоритмы LMS и NLMS показывают схожие результаты ошибок на выходе ААР и быстродействия, что касается скорости сходимости, то они отличаются в среднем на 0,02 с в пользу NLMS. При увеличении числа антенных элементов алгоритмы стремятся к значениям оптимального алгоритма Винера-Хопфа.

Алгоритм адаптации RLS не уступает оптимальному алгоритму Винера-Хопфа, однако при быстро мерцающих помехах он менее устойчив.

Преимущество алгоритма RLS перед оптимальным – его быстродействие при большом числе элементов.

Оптимальный алгоритм Винера-Хопфа показывает отличный результат в условиях воздействия мерцающих помех, однако, платой за это является низкая скорость работы при увеличении числа антенных элементов.

Список используемых источников

1. Джиган В. И. Адаптивная фильтрация сигналов: теория и алгоритмы. Москва: Техносфера, 2013. 528 с.

2. Монзинго Р. А., Миллер Т. У. Адаптивные антенные решетки. Пер. с англ. М.: Радио и связь, 1986г. 448 с.

3. Джиган В. И. Линейно-ограниченная адаптивная фильтрация СМ-сигналов с помощью многолучевых антенных решеток // Доклады 13-й Международной конференции «Цифровая обработка сигналов и ее применения (DSPA-2011)» (Российская академия наук: Институт проблем управления им. В. А. Трапезникова, 30 марта – 1 апреля 2011 г.). Москва, 2011. Том 1. С. 97–100.

4. Вечтомов В. А., Исследование характеристик алгоритмов пространственной фильтрации активных помех на основе адаптивных антенных решеток: учебно-методическое пособие / В. А. Вечтомов, В. И. Джиган. Москва: Издательство МГТУ им. Н. Э. Баумана, 2022. 88 с.

Статья представлена научным руководителем, профессором кафедры РТ СПбГУТ, доктором технических наук, профессором Глушанковым Е. И.

RESEARCH OF INFLUENCE OF ANTENNA ARRAY ELEMENT COUNT ON ADAPTATION ALGORITHMS UNDER FLICKERING INTERFERENCE

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

Modern radio engineering devices employing adaptive antenna arrays are exposed to various types of interference, including flicker noise, which affects system performance. Such interference may exhibit characteristics that prevent antenna array adaptation algorithms from converging to an optimal solution. This study investigates the influence of the number of antenna elements on the performance of linear antenna array adaptation algorithms under flickering interference with varying pulse repetition frequencies. The obtained results establish the applicability limits of adaptation algorithms and identify their optimal parameters in complex electronic warfare environments.

Key words: *linear antenna array, flickering noise, adaptation algorithms*

УДК 537.86
ГРНТИ 47.05.03

АНАЛИЗ ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ДВОЙНОГО ЭКСПОНЕНЦИАЛЬНОГО РАСПРЕДЕЛЕНИЯ ДЛЯ ВЫЧИСЛЕНИЯ ПОРОГА ОБНАРУЖЕНИЯ СИГНАЛА

А. В. Элентух

ООО «Специальный технологический центр»

Рассмотрены вопросы расчета плотности распределения вероятностей минимальных и максимальных значений мощности шума, которые получены на основе статистики экстремальных значений. Приведены зависимости вероятности ложной тревоги от величины порога обнаружения сигнала. Получено соотношение, связывающее величину порога с параметрами распределения Гумбеля и позволяющее вычислить порог при заданной вероятности ложной тревоги.

адаптивный порог, распределение Гумбеля, обнаружение сигнала

Одной из важных задач радиотехнического контроля (РТК) является обнаружение сигналов источников радиоизлучений (ИРИ) с целью последующего анализа их параметров. В настоящее время при решении этой задачи применяется метод энергетического детектора [1, 2], основанный на сравнении значений мощности выходных отсчетов с пороговым значением *T*. Порог задается оператором и является неизменным параметром. В связи с вышесказанным представляется актуальным использование адаптивного порога, автоматически подстраиваемого под текущий уровень шума.

Для решения задачи формирования адаптивного порога воспользуемся некоторыми свойствами распределений экстремальных значений.

Известно, что правый «хвост» функции распределения случайной величины *x* можно представить асимптотическим выражением [3, 4]:

$$F(x) = 1 - \frac{1}{n} exp\left(-a_{max}(x - u_{max})\right), \quad (1)$$

где *n* – количество отсчетов случайной величины *x,* из которых выбирается максимальное значение;

α_{max} – параметр масштаба распределения максимальных значений;

u_{max} – параметр сдвига распределения максимальных значений.

Тогда, задав вероятность ложной тревоги $P_{ЛТ}$, можно определить значение порога T по формуле [3]:

$$T = u_{max} - ln\ (nP_{ЛТ})/a_{max}. \quad (2)$$

Метод оценки параметров u_{max} и α_{max} основан на первом предельном распределении Гумбеля [3]. Процедура определения этих величин состоит в следующем. Производится накопление N отсчетов $\{x_i\}_N$ ($i = 1, 2, \ldots, N$) случайной величины x на выходе квадратурного детектора. Полученная числовая последовательность $\{x_i\}_N$ разбивается на m групп по n чисел в каждой группе. В каждой группе определяется максимальное значение. В результате образуется новая числовая последовательность $\{x_{imax}\}_{\text{m}}$ ($i = 1, 2, \ldots, m$). Далее находятся среднее и дисперсия максимальных значений [3]:

$$\mu[x_{max}] = \frac{1}{m}\sum_{i=1}^{m} x_{imax};$$
$$\sigma^2[x_{max}] = \sigma^2_{max} = \frac{1}{m}\sum_{i=1}^{m}(x_{imax} - \mu[x_{max}])^2.$$

И наконец, определяются оценки экстремальных параметров [3]:

$$a_{max} = \frac{\pi}{\sqrt{6\sigma^2_{max}}};$$
$$u_{max} = \mu[x_{max}] - \frac{0{,}5772}{a_{max}}.$$

Как показано в [3], выражение (1) дает возможность достаточно точно рассчитать величину порога обнаружения при условии, если в исходной выборке присутствует только шум. При наличии сигнала оценка искомых параметров распределения будет сильно искажена.

Исключить влияние данного фактора можно с помощью дополнительной оценки параметров распределения минимальных значений x_{min}, полученных из максимальных x_{max}. Для получения случайной величины x_{min}, числовую выборку $\{x_{imax}\}_{\text{m}}$ разбивают на r групп по k чисел в каждой группе. После чего в каждой из полученных групп определяется минимальное значение. Согласно [4], полученная таким образом случайная величина x_{min} имеет распределение Гумбеля для минимальных значений, функция распределения вероятности которой выражается следующим образом [4]:

$$F(x_{min}) = 1 - exp\left[-exp\big(a_{min}(x_{min} - u_{min})\big)\right].$$

где α_{min} – параметр масштаба распределения минимальных значений;

u_{min} – параметр сдвига распределения минимальных значений.

Процедура определения параметров распределения α_{min} и u_{min} состоит в следующем. Находят среднее и дисперсию минимальных значений:

$$\mu[x_{min}] = \frac{1}{r}\sum_{i=1}^{r} x_{imin};$$

$$\sigma^2[x_{min}] = \sigma^2_{min} = \frac{1}{r}\sum_{i=1}^{r}(x_{imin} - \mu[x_{min}])^2.$$

Далее определяют параметры распределения α_{min} и u_{min} [4]:

$$a_{min} = \frac{\pi}{\sqrt{6\sigma^2_{min}}}; \quad (3)$$

$$u_{min} = \mu[x_{min}] + \frac{0{,}5772}{a_{min}}. \quad (4)$$

Параметры α_{max} и u_{max} можно выразить через α_{min} и u_{min} следующим образом [4]:

$$a_{max} = \frac{a_{min}}{ln\,(k)}; \quad (5)$$

$$u_{max} = u_{min} + \frac{ln\,(ln(k))}{a_{max}}. \quad (6)$$

Подставляя полученные выражения (5) и (6) в выражение (2), получаем окончательную формулу вычисления порогового значения T для заданной вероятности ложных тревог $P_{ЛТ}$:

$$T = u_{min} + \frac{ln\,(k)}{a_{min}}\Big(ln\big(ln(k)\big) - ln\,(nP_{ЛТ})\Big). \quad (7)$$

Справедливость формулы была подтверждена методом имитационного моделирования, суть которого заключается в следующем:

1. Формируют выходные отсчеты квадратурного детектора $\{x\}$, плотность распределения вероятности (ПРВ) которых описывается выражением (1). Размер исходной выборки $N = 10^6$, величины n и k были выбраны равными 100.

2. Осуществляют оценку экстремальных параметров распределения Гумбеля для минимальных отсчетов согласно выражениям (3) и (4) при отсутствии сигнала.

3. К отсчетам $\{x\}$ аддитивно добавляют импульсный сигнал со скважностью $q = 2$ и отношением сигнал шум равным 6 дБ. Осуществляется оценка экстремальных параметров распределения Гумбеля для минимальных отсчетов согласно выражениям (3) и (4) при наличии сигнала.

4. На основе оценок экстремальных параметров вычисляют ПРВ максимальных значений шума при отсутствии (рисунок 1) и присутствии (рисунок 2) сигнала. На данных рисунках пунктирная линия – плотность распределения вероятности, параметры которой рассчитаны при помощи выражений (5), (6), а сплошная линия соответствует гистограмме максимальных значений.

5. На основе оценок экстремальных параметров, вычисляют пороговое значение T по формуле (7) для заданной вероятности ложных тревог $P_{ЛТ} = 10^{-5}$.

6. Оценивают реальную вероятность ложных тревог методом Монте-Карло по отсчетам шума [5].

Расхождение гистограммы и расчетной ПРВ отражает отличие полученной в ходе моделирования вероятности ложной тревоги (рисунок 1). При этом на рисунке 2 расчетная плотность вероятности лучше описывает гистограмму. Вероятность ложной тревоги, рассчитанная методом Монте-Карло, для случая шума составила $3 \cdot 10^{-5}$. В случае с сигналом вероятность ложной тревоги составила 10^{-5}. Таким образом, вероятность ложной тревоги снизилась при наличии сигнала (поднялся порог). Такой результат обусловлен исключением отсчетов, которые, в отсутствии сигнала, оказались бы минимальными.

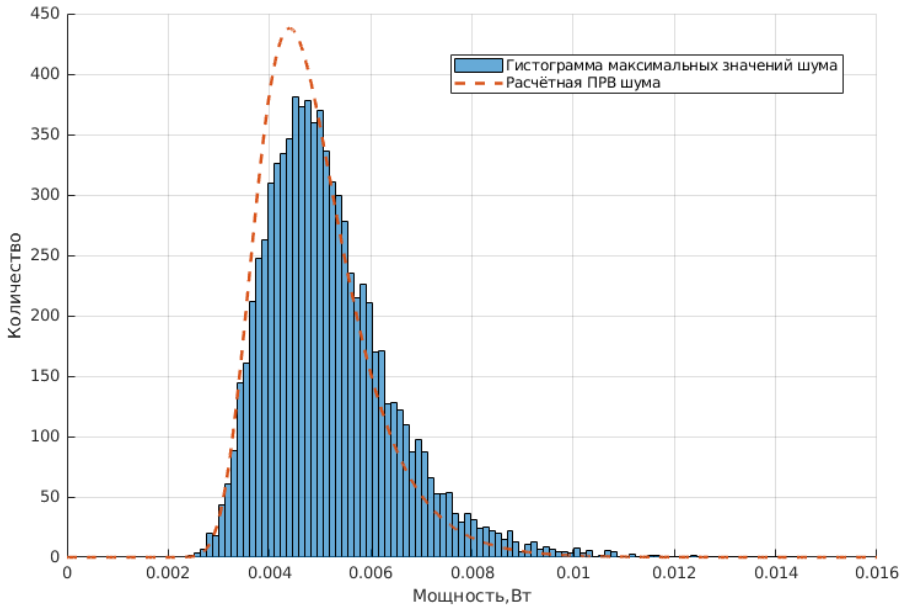


Рис. 1. Гистограмма максимальных значений при отсутствии сигнала

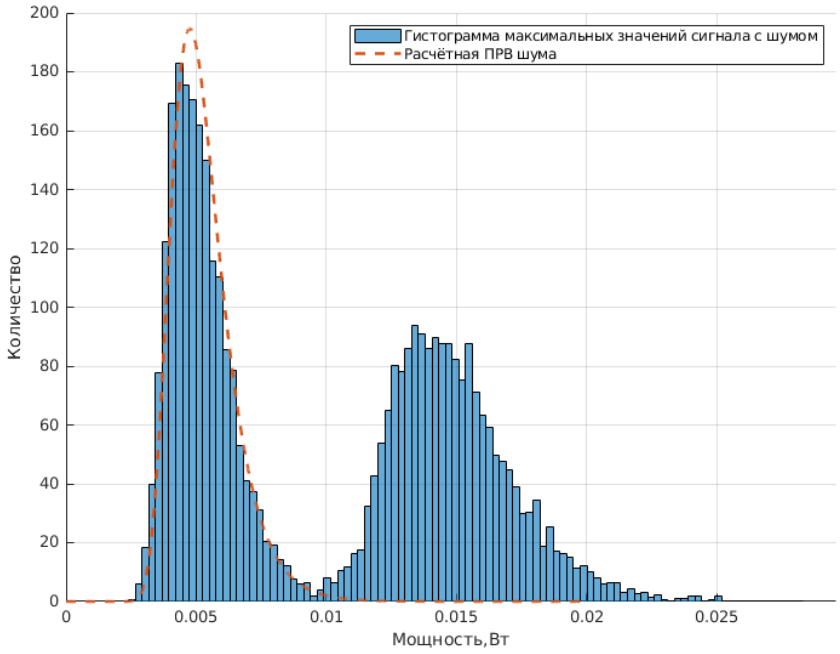


Рис. 2. Гистограмма максимальных значений при наличии сигнала

Анализ зависимостей позволяет качественно оценить степень близости ПРВ и гистограммы распределения максимальных значений шума, а также подтверждает возможность использования приведенных выше аналитических выражений для компенсации влияния сигнала на оценку величины шума.

Последнее утверждение иллюстрирует рисунок 2, на котором представлена гистограмма максимальных значений сигнала с шумом. Из рисунка 2 видно, что расчетная ПРВ, в условиях наличия сигнала, описывает только область значений, относящихся к шуму.

Выполненные исследования позволили получить соотношение для расчета порога обнаружения на основе статистики экстремальных значений для заданного числа отсчетов с выхода квадратурного детектора и требуемой величины вероятности ложной тревоги.

Расчет порога рекомендуется производить по выборке из 106 отсчетов, при этом значения n и k должны быть не менее 100.

Установлено, что наличие сигнала незначительно увеличивает величину порога.

Результаты исследования могут быть использованы в средствах радиотехнического контроля при обнаружении сигналов на фоне шума.

Список используемых источников

1. Atapattu S., Tellambura C., Jiang H. Energy Detection for Spectrum Sensing in Cognitive Radio. New York, Springer. 2014. 83 p.
2. Richards M. A. Fundamentals of Radar Signal Processing. New York: McGraw-Hill, 2005.
3. Литюк Л. В. Метод экстремальных статистик и генерирование «белого» шума на ЭВМ // Инновационная наука 2020. № 12. С. 34–36.
4. Гумбель Э. Статистика экстремальных значений / Пер. с англ. М.: Изд-во МИР, 1965.
5. Nicholas Metropolis, Stanislaw Ulam, The Monte Carlo method, J. Amer. statistical assoc. Vol. 44. № 247. PP. 335-341

Статья предоставлена научным руководителем, главным инженером конструктором проектов ООО "СТЦ", доктором технических наук, старшим научным сотрудником Коротковым В. Ф.

ANALYSIS OF THE APPLICABILITY OF THE DOUBLE EXPONENTIAL DISTRIBUTION FOR COMPUTING THE DETECTION THRESHOLD OF A SIGNAL

Elentukh A.
Special Technology Center

The paper examines the calculation of probability density functions for the minimum and maximum values of noise power obtained using extreme value theory. The dependencies of the false alarm probability on the detection threshold value are presented. A relation connecting the threshold value with the parameters of the Gumbel distribution is derived, allowing the threshold to be computed with an accuracy up to the order of a given false alarm probability.

***Key words**: Adaptive threshold, Gumbel distribution, signal detection*

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

УДК 004.896
ГРНТИ 28.23.29

КОНЦЕПЦИЯ ПРИМЕНЕНИЯ ЦИФРОВЫХ ДВОЙНИКОВ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ СПУТНИКОВОЙ СИСТЕМОЙ ПЕРЕДАЧИ ДАННЫХ

Ю. А. Арланцева, Р. М. Вивчарь, Р. А. Дулаев, К. Д. Зайчиков, К. А. Кульситова, А. В. Пачин, К. А. Шибаленков

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

Появление группировок космических аппаратов на низких орбитах, а также сочетание спутников на разных орбитах со взаимодополняющим функционалом открывает существенные перспективы в повышении результативности спутниковых систем передачи данных. Вместе с тем, задача управления такими системами в условиях присущей их элементам неопределенности является весьма рискованной. В представленной статье приводится концепция снижения рисков решений по управлению спутниковой системой передачи данных с применением цифровых двойников, построенных на основе полимодельных комплексов, включающих искусственные нейронные сети и онтологические модели, а также средства трехмерного интерактивного интерфейса.

искусственный интеллект, цифровые двойники, суперактивное управление, спутниковые системы, онтологические модели, искусственные нейронные сети

В настоящее время значительные ресурсы многих государств и частных компаний выделяются на создание и развитие спутниковых систем передачи данных.

Подобные системы функционируют в США и КНР, перспективы и задачи их построения и совершенствования указаны в стратегии развития отрасли связи Российской Федерации на период до 2035 года [1]. В рамках федерального проекта «Комплексное развитие космических информационных технологий («Сфера»)» и государственной программы Российской Федерации «Космическая деятельность России» и Федеральной космической программы России на 2016–2025 гг. реализуются мероприятия по развитию спутниковой связи.

В рамках Федеральной космической программы 2016–2025 гг. проводятся работы по созданию многофункциональной системы персональной спутниковой передачи данных с космических аппаратов нового поколения на низких орбитах.

Федеральный проект «Комплексное развитие космических информационных технологий («Сфера»)» позволит обеспечить использование спутниковых систем с взаимодополняющим функционалом на разных орбитах, в том числе и геостационарных.

Подобные спутниковые системы являются техническими сложными суперсистемами, включающими сотни тысяч устройств различного назначения, которые с некоторой степенью абстракции можно объединить в три основных комплекса – группировка КА, наземный комплекс управления этой группировкой и целевой комплекс передачи данных.

Управление в таком случае, как процесс обеспечения достижения желаемого состояния системы, требует существенных затрат ресурсов. При этом присущие столь сложной системе значительные неопределенности повышают риск невыполнения задачи [2].

Для преодоления указанного противоречия предлагается разработанная в СПбГУТ концепция, основанная на использовании технологии цифровых двойников в сочетании с методологией суперактивного управления сложными системами.

Анализ объекта исследования позволил выделить ряд актуальных проблемы функционирования спутниковых систем передачи данных (ССПД):

а) деградация элементов бортовых систем КА, в т. ч. из-за воздействия агрессивной среды;

б) воздействие помех на целевой комплекс;

в) отказы оборудования НКУ и ЦК;

Каждое из указанных обстоятельств вызывает негативные ситуации случайным образом, и требует максимально оперативного принятия малорискованных решений, при этом решения не должны вести к нарушению требований безопасности и превышению заданных ограничений по ресурсам. Обоснования подобных решений и является **целью** исследования.

Для достижения цели должна быть решена общая задача исследования, заключающаяся в разработке инструмента получения решений по управлению ССПД с минимальным риском – цифрового двойника ССПД, включающего комплекс аналитических, нейросетевых, онтологических моделей и интерактивный трехмерный интерфейс.

В формальном виде задач исследования выглядит следующим образом. Дано:

U – множество управляемых параметров системы;

Z – множество неуправляемых параметров системы;

E – множество параметров среды;

Y – множество выходных параметров системы;

∏– множество требований к показателям;

U_{hi} – массив исторических данных управляемых параметров системы;

Z_{hi} – массив исторических данных неуправляемых параметров системы;

E_{hi} – массив исторических данных параметров среды.

Найти:

$$U^* = arg \min_{U \in \Delta} (1 - P[Y(U(U_{hi}, t), Z(Z_{hi}, t), E(E_{hi}, t)) \in \Pi])$$

Вербально: известных прогнозных значениях управляемых параметров системы, неуправляемых параметров системы и параметров среды, полученных на основе исторических данных, найти такое рациональное множество значений управляемых параметров (параметров решения на управление), находящихся в области допустимых значений Δ, которое позволит минимизировать риск несоответствия будущего состояния системы всем заданным требованиям.

Требования определяются результативностью, оперативностью и безопасностью функционирования ССПД.

Основой для решения задачи является цифровой двойник (ЦД) всей системы, как комплекс адекватных моделей, связанный с объектом двусторонними каналами передачи данных, отображающий с достаточно низкой задержкой его реальное состояние и транслирующий управляющие воздействия.

ЦД являются одним из инструментов современной индустрии, многократно подтвердившими свою пригодность для решения задач управления сложными техническими системами на разных стадиях жизненного цикла.

Однако, для достижения поставленных целей одного двойника недостаточно, необходимо включение в состав этого комплекса элементов, реализующих технологию суперактивного управления [3-4].

Суперактивное управление – одна из проактивных стратегий управления сложными техническими системами и процессами, обеспечивающих упреждение наступления негативных ситуаций и их исключение в будущем.

Суперактивное управление является результатом конвергенции прогноза и плана (траектории) достижения прогнозируемого будущего состояния, который базируется на реальных знаниях о препятствиях на этом пути – первопричинах возникновения негативных ситуаций. Из-за сложностей долгосрочного прогнозирования ее применение всегда сопряжено с риском и должно сопровождаться оценкой показателей риска выполнения принимаемых решений.

Основные принципы:

– достижение в будущем желаемого состояния объекта управления, позволяющего обеспечить высокую эффективность функционирования;
– в качестве объекта управления рассматривается не только собственно процесс эксплуатации, но и внешние обстоятельства, в которых он протекает;
– формирование у персонала проактивного видения своей деятельности.

В общем виде архитектура разрабатываемого ЦД ССПД представлена на рисунке 1.

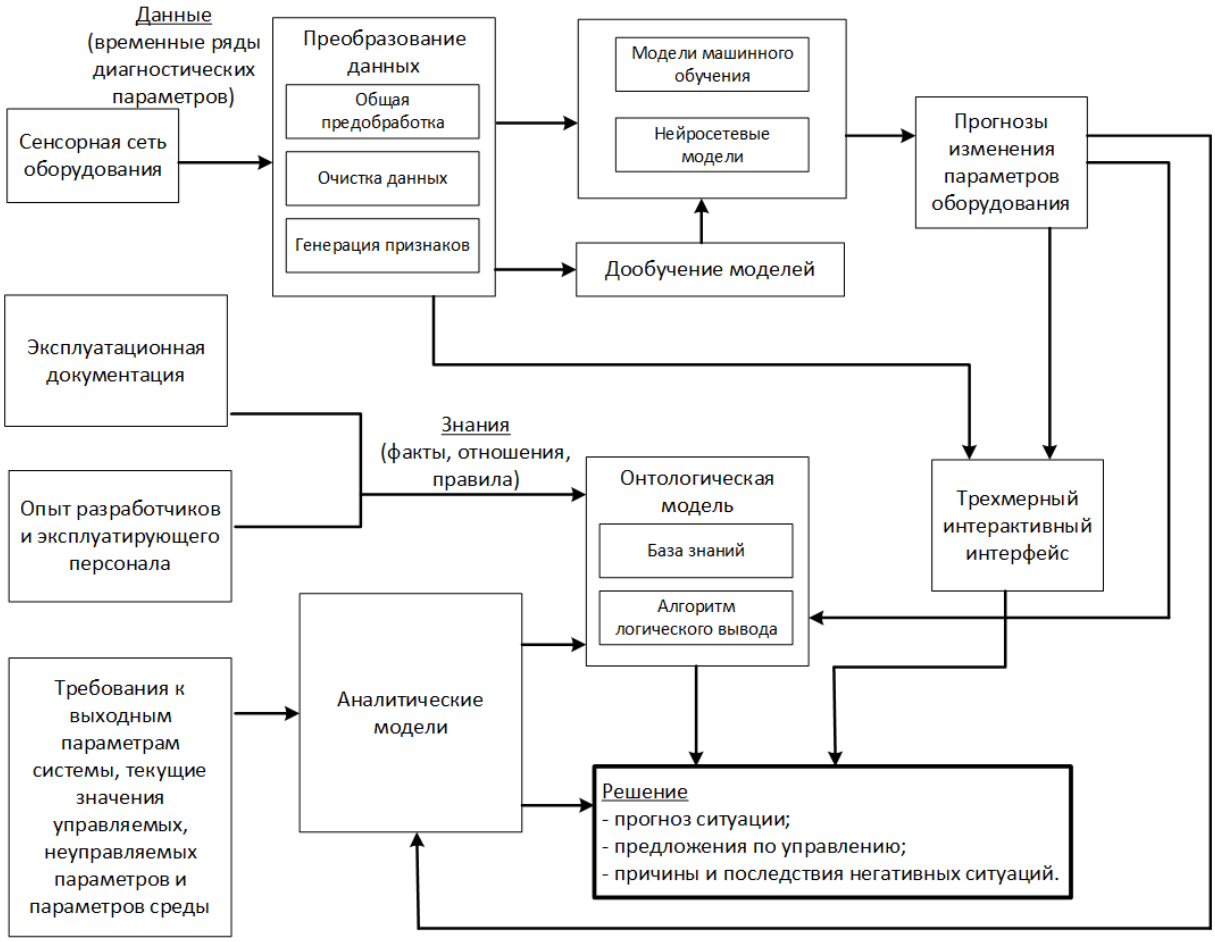


Рис. 1. Архитектура цифрового двойника ССПД

Основными компонентами ЦД являются:

а) полимодельный блок прогнозирования, включающий средства предварительной обработки данных, модели машинного обучения и искусственные нейронные сети, предназначенные для прогнозирования параметров системы и среды. Кроме того, предусмотрены модуль дообучения моделей по результатам реализации прогнозов и поступления новых данных. Исходными данными для прогнозирования являются данные, получаемые от сенсорной сети оборудования ССПД.

б) блок аналитических моделей, решающий на основе классических математических методов ряд задач, для которых подобный подход является наиболее рациональным. Примером может служить применение метода динамического программирования для оптимального управления запасами.

в) блок онтологических моделей ССПД, предназначенный для формализации знаний, получаемых из документации и от персонала, а также обработки знаний и реализации алгоритмов логического вывода.

г) интерактивный трехмерный интерфейс для отображения текущей и прогнозной ситуации.

Комплексное применение приведенного набора методов и технологий позволяет решать задачи прогнозирования ситуаций, подготовки предложений в решения и анализа причин и следствий негативных ситуаций.

На основе полученных от одной из компаний – операторов ССПД реальных телеметрических данных, были выполнены работы подготовительного этапа разработки предиктивных моделей нейросетевых моделей, онтологии и модуля интерактивного трехмерного интерфейса.

Модуль прогнозирования основан на моделях машинного обучения и предобученной нейронной сети, для качественного прогноза на разных горизонтах прогнозирования.

Используется нейронная сеть Tiny Time Mixers (TTM) от IBM – легковесная, основанная на многослойном перцептроне модель временных рядов без механизма внимания с возможностью zero-shot и few-shot предсказаний [5]. TTM основывается на модели TSMixer (также от IBM), однако использует меньше ресурсов и имеет более высокую скорость обучения, что важно при работе с несколькими временными рядами.

На стороне машинного обучения используются и сравниваются следующие модели регрессии: XGBoost, LightGBM и Random Forest. XGBoost и LightGBM – реализация градиентного бустинга, основывающаяся на деревьях решений.

После обучения получены модели, позволяющие прогнозировать значение ряда параметров, в данном конкретном случае – это емкость и напряжение бортовых батарей КА типа Экспресс, результаты моделирования представлены на рисунке 2.

Кроме того, по итогам подготовительного этапа сделаны выводы о мероприятиях, которые в будущем позволят повысить эффективность блока прогнозирования в целом:

а) ансамблирование моделей для объединения технологий;

б) генерация новых признаков с целью создания новых зависимостей для модели;

в) обучение многомерной модели прогнозирования с целью оптимизации ресурсов.

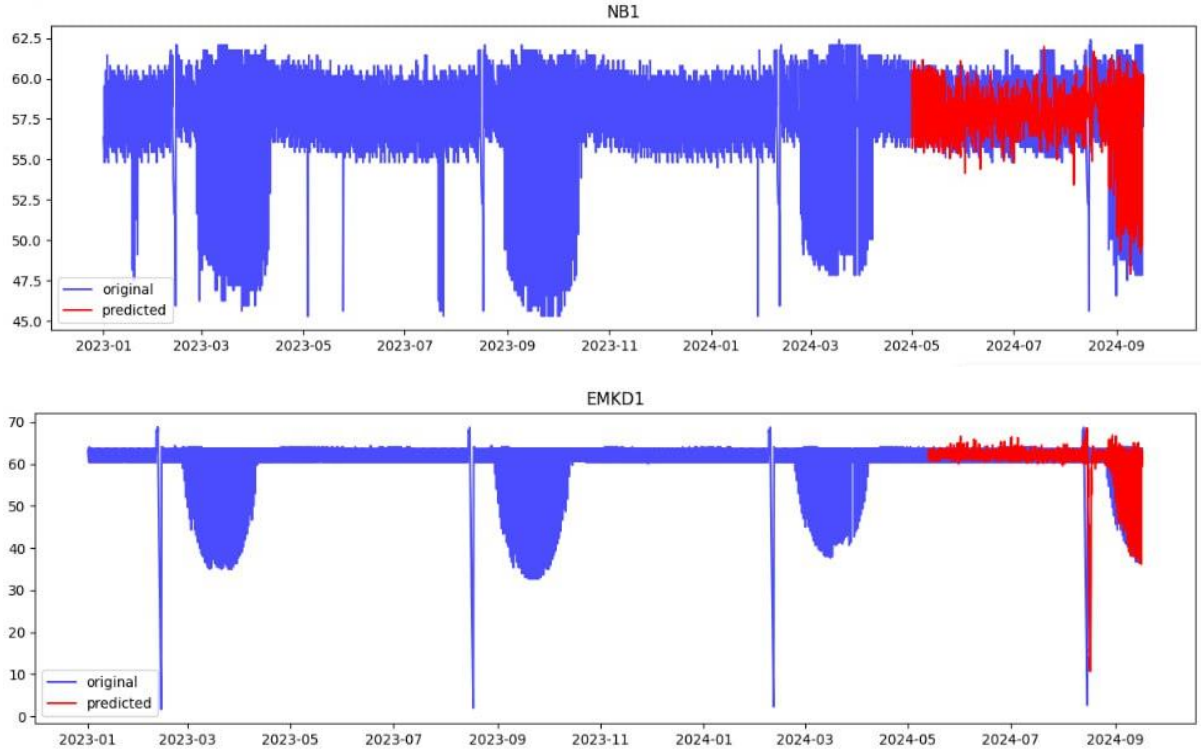


Рис. 2. Результаты работы предиктивных моделей напряжения и емкости бортовой батареи КА

В части онтологического моделирования на подготовительном этапе проведен анализ существующих инструментов.

Онтологическая модель включает классы сущностей (например, «Батарея», «Параметры работы», «Предотказные состояния»), их атрибуты (характеристики, метрики) и отношения (логические и причинно-следственные связи между сущностями) [6].

Модель поддерживает иерархическую организацию данных (например, наследование классов «Работоспособная батарея» → «Батарея») и правила логического вывода (например, «Если напряжение падает ниже порога X, а емкость батареи превышает Y, то состояние классифицируется как Z»).

В качестве входных данных используются текущие параметры отслеживаемого модуля или устройства, результаты аналитического моделирования (например, расчет остаточной емкости). Также для построения логических связей о модулях и параметрах используются референсные данные из технической документации (номинальные параметры, пороговые значения).

На основе входных данных модуль формирует семантически связанную сеть сущностей, позволяющую автоматически классифицировать состояния батареи (норма, риск, предотказ) и выявлять аномалии через сопо-

ставление текущих данных с онтологическими правилами. Генерировать объяснимые выводы (например, «Снижение емкости на 20 % связано с изменением конкретного параметра в узле А»).

Онтологическая модель должна предоставлять интерфейс для передачи структурированных данных в модуль визуализации (например, графы связей) и систему отчетности. Поддерживается возможность ручной корректировки онтологии (добавление новых классов, правил) через административный интерфейс.

Выходные данные представлены в виде JSON-LD или RDF-представление онтологии с актуальными связями и атрибутами. Также логи принятых решений (например, «Состояние ID-1234 отнесено к «Предотказу» на основании правил P1, P2»).

Подготовлена анкета для опроса персонала дежурных смен центра управления полетом КА и центров спутниковой связи для сбора и формализации имеющегося практического опыта по управлению элементами ССПД.

В части разработки трехмерного интерфейса определена архитектура модуля, набор применяемых инструментов (рис. 3). Подготовлена пилотная страница веб-приложения, позволяющая отображать текущие значения ряда параметров КА и прогноз их изменения.

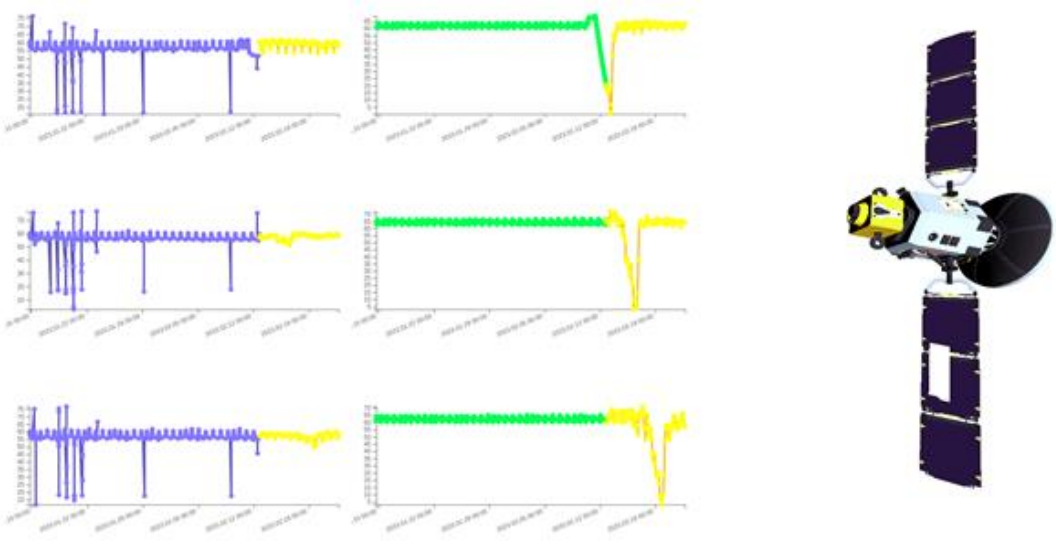


Рис. 3. Веб-приложение трехмерного интерактивного интерфейса

Описанная концепция представляет собой основу для проведения целого ряда теоретических научных исследований и практических действий по реализации результатов, таких как:

а) исследования, обоснование и разработка комплексов предиктивных нейросетевых и ML-моделей для прогнозирования значений параметров системы (управляемых и неуправляемых) и внешней среды (модели параметров оборудования КА, НКУ, КСПД, модели помех, космической погоды, пользователей);

б) исследования, обоснование и разработка онтологических моделей прогнозирования развития ситуаций в системе и подготовки решений, анализа негативных ситуаций, определения следствий и причин;

в) исследование, обоснование и разработка имитационных моделей элементов ССПД всех уровней;

г) разработка методик оценивания эффективности применения элементов ИИ в управлении ССПД;

д) разработка элементов интерактивного интерфейса, в том числе с применением технологий дополненной, виртуальной реальности и телеприсутствия.

Внедрение планируемых результатов в существующие и создаваемые ССПД в перспективе позволит снизить риски решений по управлению системой, и, как следствие, повысить эффективность их функционирования.

Список используемых источников

1. Стратегия развития отрасли связи Российской Федерации на период до 2035 года. Утверждена распоряжением Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р.

2. Вивчарь Р. М. Повышение качества решений по управлению системой обеспечения готовности ракеты космического назначения к пуску на основе риск-ориентированного подхода / Р. М. Вивчарь, А. В. Пачин, В. Ю. Свирский // Труды Военно-космической академии имени А. Ф. Можайского. 2022. № 683. С. 139-143. EDN:YXTTZX.

3. Щербина И. С. Концепция ситуационного риск-ориентированного управления процессами подготовки и пуска ракеты-носителя / И. С. Щербина, Р. М. Вивчарь, В. М. Локтионов // Труды Военно-космической академии имени А. Ф. Можайского. 2024. № 693. С. 213-224. EDN:HQHZNF.

4. Басотин Е. В. Проактивное управление техническим состоянием оборудования критически важных объектов / Е. В. Басотин, Р. М. Вивчарь, А. И. Птушкин // Труды Военно-космической академии имени А. Ф. Можайского. 2024. № 694. С. 150-156. EDN:SEZGGY.

5. Ekambaram V. Tiny Time Mixers (TTMs): Fast Pre-trained Models for Enhanced Zero/Few-shot Forecasting of Multivariate Time Series / V. Ekambaram, A. Jati, P. Dayama et al. URL: https://openreview.net/pdf?id=3O5YCEWETq (дата обращения 25.05.2025).

6. Ontology-Driven Software Development / J. Z. Pan, S. Staab, U. Aßmann, J. Ebert, Y. Zhao. Berlin: Springer, 2012. 355 p.

CONCEPT OF USING DIGITAL TWINS TO IMPROVE THE EFFICIENCY OF SATELLITE DATA TRANSMISSION SYSTEM MANAGEMENT

Arlantseva Yu., Dulaev R., Zaichikov K., Kulsitova K., Vivchar R., Pachin A., Shibalenkov K.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The emergence of low-orbit satellite constellations, combined with satellites in different orbits featuring complementary functionalities, opens significant prospects for enhancing the efficiency of satellite data transmission systems. However, managing such systems under the inherent uncertainty of their components presents considerable risks. This article presents a concept for mitigating decision-making risks in satellite data transmission system management through the use of digital twins based on multi-model complexes. These complexes incorporate artificial neural networks, ontological models, and interactive 3D interface tools.

***Key words**: artificial intelligence, digital twins, hyperactive control, satellite systems, ontological models, artificial neural networks*

УДК 004.8
ГРНТИ 28.23.15

АНАЛИЗ ГИДРОАКУСТИЧЕСКИХ СИГНАЛОВ С ПОМОЩЬЮ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

Н. А. Васильев, Б. С. Лещинский, Д. С. Ситдиков

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

В статье рассматриваются современные методы глубокого обучения, включая сверточные нейронные сети, рекуррентные сети, трансформеры и автоэнкодеры, которые демонстрируют высокую эффективность в задачах анализа гидроакустических сигналов. Приведены результаты эксперимента с моделью ResNet-50, обученной на открытом датасете DeepShip, достигшей точности 95 %. Отмечены ключевые проблемы: дефицит размеченных данных, нестабильность шумов, ограниченная интерпретируемость. Подчеркивается потенциал ИИ в задачах обработки гидроакустических данных и направления дальнейших исследований.

гидроакустические сигналы, CNN, RNN, LSTM, трансформеры, автоэнкодеры, спектрограммы, классификация судов.

Анализ гидроакустических сигналов является важным направлением в морских исследованиях, мониторинге окружающей среды и судоходстве. Особенности подводной среды – высокая зашумленность, нестабильные условия распространения звука, многократные отражения – создают значительные сложности при обработке акустической информации. Традиционные методы, основанные на фиксированных фильтрах и порогах, часто не справляются с адаптацией к изменяющимся условиям. В этих условиях особенно актуальны методы глубокого обучения – они позволяют автоматически извлекать значимые признаки, распознавать объекты даже при низком уровне сигнала и эффективно адаптироваться к динамике подводной обстановки.

Внедрение таких подходов требует соответствующей подготовки входных данных. Прежде чем подать гидроакустические сигналы в нейросеть, необходимо провести их тщательную предобработку: удалить фоновый шум, выделить информативные признаки и преобразовать сигнал в форму, удобную для анализа. Типичные этапы включают фильтрацию и извлечение спектральных характеристик с помощью преобразования Фурье (STFT), мел-спектрограмм, кепстральных коэффициентов MFCC, а также специализированных спектров, таких как LOFAR и Meier [1].

Рассмотрим более подробно применяемые методы.

Сверточные нейронные сети (CNN) эффективно извлекают локальные характеристики акустических сигналов [2]. В исследованиях отмечено, что глубокий CNN демонстрирует высокую обучаемость и адаптивность при классификации акустических данных, особенно при использовании спектральных представлений. Например, CNN применяется к LOFAR-граммам для классификации целей и оценки их параметров. Используются для сегментации гидролокационных изображений (FLS) – автоматически выделяют объекты на сонарных кадрах, улучшая детекцию малых целей и подавление фонового шума. Применяются для оценки направления прихода звука (DOA) с помощью двумерных карт (например, матриц ковариации сигналов) [1].

Рекуррентные нейросети (RNN, LSTM, GRU) учитывают последовательность временных данных, что полезно для анализа изменяющихся во времени гидроакустических сигналов. Комбинация сверточных и рекуррентных блоков (CRNN) позволяет одновременно учитывать пространственную структуру спектрограммы и временную динамику. Применяются для трекинга целей: например, алгоритм, в котором выходы кубатурного фильтра Калмана поступают на вход GRU, смог лучше предсказывать состояние подводного беспилотника (UUV) во времени, чем классические фильтры [3]. LSTM и GRU традиционно успешно используют в задачах предсказания акустических временных рядов, компенсируя затухание градиента при длинных последовательностях.

Трансформеры с механизмом самовнимания позволяет учитывать долгосрочные зависимости во входных данных. Для гидроакустики были предложены модели, превращающие звуковые спектрограммы в последовательность патчей и обрабатывающие их через энкодер трансформера. Впервые подобную модель применили для распознавания подводных целей, и она показала высокую точность на спектрограммах шумов [4]. В задачах обнаружения в изображениях бокового обзора (side-scan sonar) используют гибридные сети на основе YOLO с интегрированным модулем внимания (Swin-Transformer) – это позволяет фокусироваться на релевантных объектах и учитывать глобальный контекст [5].

Автоэнкодеры (AE) применяют для автоматического шумоподавления и выделения признаков. В гидроакустике строятся сверточные денойзинг-автоэнкодеры (ConvDAE) для удаления фонового шума кораблей или эхолокационных отражений. Исследования показали, что такие сети могут повысить отношение сигнал/шум на ~10 дБ, значительно улучшая качество из-

влечения признаков. Также используют двунаправленные автоэнкодеры и гибриды с другими сетями. Денойзинг-автоэнкодеры полностью обучаются на примерах «шум+цель», поэтому не нуждаются в ручном выборе признаков [6].

В рамках исследования возможности использования сверточной нейронной сети для автоматической классификации типов судов на основе гидроакустических сигналов, с опорой на сохранение важной информации о низко- и высокочастотных компонентах сигнала проведена разработка и обучение модели нейронной сети.

Для эксперимента использовался открытый датасет DeepShip, содержащий WAV-записи различных типов судов, записанных на частоте дискретизации 32 кГц.

Каждая аудиозапись преобразовывалась в 3-канальное изображение (RGB). Каналы R и G – две независимые LF-спектрограммы разных диапазонов, канал B – одна HF-спектрограмма. Пример получившихся спектрограмм представлен на рисунке 1.

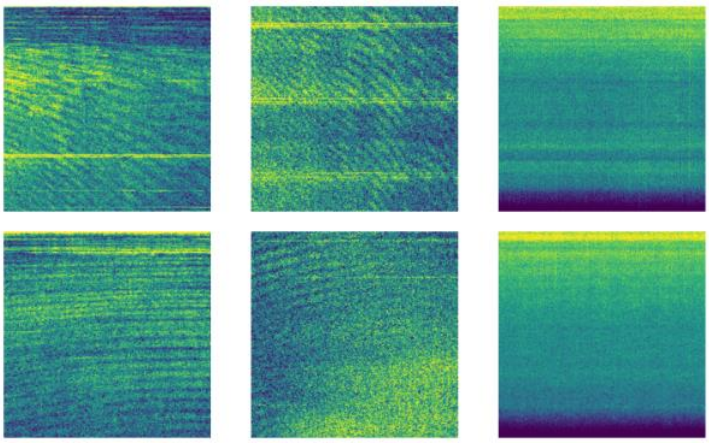


Рис. 1. Спектрограммы сигналов

Спектрограммы нормализовались логарифмически и масштабировались в диапазон (0, 1).

Разделение на обучающую и валидационную выборки производилось случайным образом с сохранением пропорции классов (20 % валидация).

Для классификации использовалась модель ResNet-50, предобученная на ImageNet, с модифицированным входом на 3 канала. В качестве функции потерь применялась бинарная кросс-энтропия, оптимизатор Adam, метрика точности – accuracy_multi.

На рисунке 2 представлены результаты обучения нейронной сети. Обучение выполнялось в течение 200 эпох с автоматическим сохранением луч-

шей модели по метрике точности. Значение точности модели на валидационной выборке составило 95,1 %. На тестовых данных 95 %.

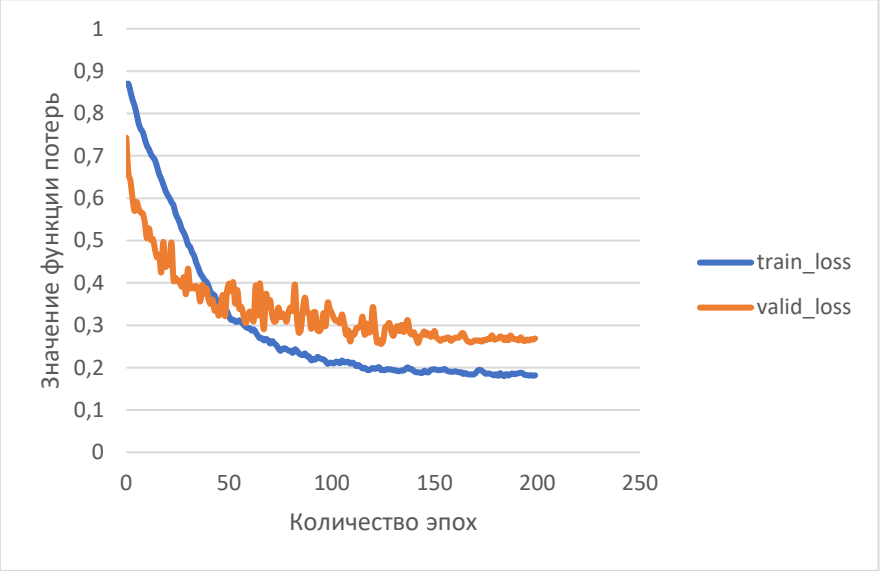


Рис. 2. График функции потерь для обучающей и валидационной выборок

Проведенный эксперимент подтвердил эффективность применения сверточной нейронной сети ResNet-50 для классификации судов по спектральному представлению их гидроакустических сигналов: модель достигла высокой точности при работе с преобразованными RGB-спектрограммами. Однако, несмотря на полученные результаты, при практическом применении подобных моделей в реальной подводной среде возникают некоторые ограничения, напрямую влияющих на стабильность и надежность классификации:

1. Сильные акустические помехи. Морская среда характеризуется шумами разного происхождения – шум самого приемника (автономного аппарата), многопутевыми отражениями, биофоновым и ветряным шумом. Эти факторы искажают целевые сигналы. Даже современные глубокие модели ограничены в борьбе с нестационарным шумом: если SNR очень мал, то результаты денойзинга и классификации ухудшаются. Специальные архитектуры применяются для фильтрации, но остается риск потери важной информации при подавлении шумов.

2. Ограниченность размеченных данных. Учебные наборы гидроакустических данных зачастую скудны и разнородны, сбор реальных данных сложно организовать. Это затрудняет обучение глубоких сетей, требующих больших объемов данных. Вследствие этого применяют перенос обучения (например, сети, предобученные на общих аудио-базах), генеративные мо-

дели для синтеза данных. Однако неизбежна разница между тренировочными наборами и реальным окружением, что требует тщательной проверки обобщаемости моделей.

Подводя итог, хочется отметить, что в настоящее время глубокое обучение становится ключевым инструментом для анализа гидроакустических данных. Современные архитектуры (CNN, RNN, трансформеры) позволяют достигать высокой точности в задачах обнаружения и классификации подводных объектов и шумов. Одновременно с этим сохраняются нерешенные задачи: снижение влияния шумов и расширение объемов размеченных данных. Будущие исследования будут направлены на разработку эффективных методов аугментации, а также на создание гибридных систем, сочетающих нейросетевые алгоритмы с традиционной акустической обработкой.

Список используемых источников

1. Lin X. et al. Efficient ship noise classification with positive incentive noise and fused features using a simple convolutional network // Scientific Reports. 2023. Т. 13. № 1. С. 17905.

2. Lin X., Dong R., Lv Z. Deep learning-based classification of raw hydroacoustic signal: A review //Journal of Marine Science and Engineering. 2022. Т. 11. № 1. С. 3.

3. Wang Y. et al. Passive sonar target tracking based on deep learning //Journal of Marine Science and Engineering. 2022. Т. 10. № 2. С. 181.

4. Li P. et al. STM: Spectrogram transformer model for underwater acoustic target recognition // Journal of Marine Science and Engineering. 2022. Т. 10. № 10. С. 1428.

5. Wen X. et al. Underwater side-scan sonar target detection: YOLOv7 model combined with attention mechanism and scaling factor // Remote Sensing. 2024. Т. 16. № 13. С. 2492.

6. Hummel H. I., van der Mei R., Bhulai S. A survey on machine learning in ship radiated noise // Ocean Engineering. 2024. Т. 298. С. 117252.

ANALYSIS OF HYDROACOUSTIC SIGNALS USING DEEP LEARNING METHODS

Vasiliev N., Leshchinsky B., Sitdikov D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article discusses modern deep learning methods, including convolutional neural networks, recurrent networks, transformers, and autoencoders, which demonstrate high efficiency in the tasks of hydroacoustic signal analysis. The results of an experiment with the ResNet-50 model trained on the open DeepShip dataset, which achieved 95 % accuracy, are presented. Key problems are noted: lack of labeled data, noise instability, limited interpretability. The potential of AI in hydroacoustic data processing tasks and directions for further research are emphasized.

Key words: *hydroacoustic signals, CNN, RNN, LSTM, transformers, autoencoders, spectrograms, ship classification*

УДК 004.8
ГРНТИ 28.23.25

ИНТЕГРАЦИЯ ЗНАНИЙ НЕЙРОСЕТЕВЫХ МОДЕЛЕЙ БЕЗ ДОСТУПА К ДАННЫМ

Н. А. Васильев, Б. С. Лещинский, Д. С. Ситдиков

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

В статье рассматриваются два подхода к объединению знаний нейросетевых моделей без доступа к исходным данным: (1) передача знаний от нескольких моделей-учителей к единой модели-студенту с использованием синтетически сгенерированных данных; (2) прямое объединение параметров моделей без обучения. Первый подход включает методы генерации псевдоданных на основе поведения учителя и позволяет обучать студентов произвольной архитектуры. Второй подход использует специальные алгоритмы для объединения весов предварительно обученных моделей, решая проблему различий в структуре внутренних представлений. В работе обсуждаются условия применения каждого метода, их ограничения и качество объединения по результатам экспериментов на задачах классификации.

объединение нейросетей, Zero-Shot KD, DeepInversion, DFAD, Git Re-Basin, MuDSC, синтетические данные, параметрическое слияние, обучение без доступа к данным

Задача передачи знаний между нейросетями была предложена Хинтоном и соавторами и предполагает обучение компактной модели (студента) на основе более крупной модели (учителя) с сохранением качества. Однако классические методы требуют доступа к исходным данным, что в реальных условиях часто невозможно по причинам конфиденциальности, объема или правовых ограничений [1]. Это породило два направления объединения моделей без данных: передача знаний с синтетическими данными (data-free distillation) и слияние параметров моделей (parameter merging).

В статье проводится обзор методов обоих типов, анализируются их принципы, архитектурные требования и ограничения, а также рассматриваются результаты на задачах классификации.

Передача знаний с синтетическими данными – сначала генерируются искусственные примеры, вызывающие характерные отклики у учителя, затем студент обучается имитировать эти отклики. Рассмотрим более подробно методы данного направления.

Zero-Shot Knowledge Distillation (ZSKD) позволяет генерировать «отрисовки» данных (data impressions) из учителя без реальных примеров [1]. Это

делается путем обратной оптимизации: ищутся такие входы, которые учитель классифицирует с высокой уверенностью, или соответствуют статистике его выходов. Полученные синтетические изображения используются для обучения студента. Преимущество ZSKD – простота идеи и обобщенность; однако такие изображения могут быть малореалистичными. На рисунке 1 представлена структура работы методов данного направления.

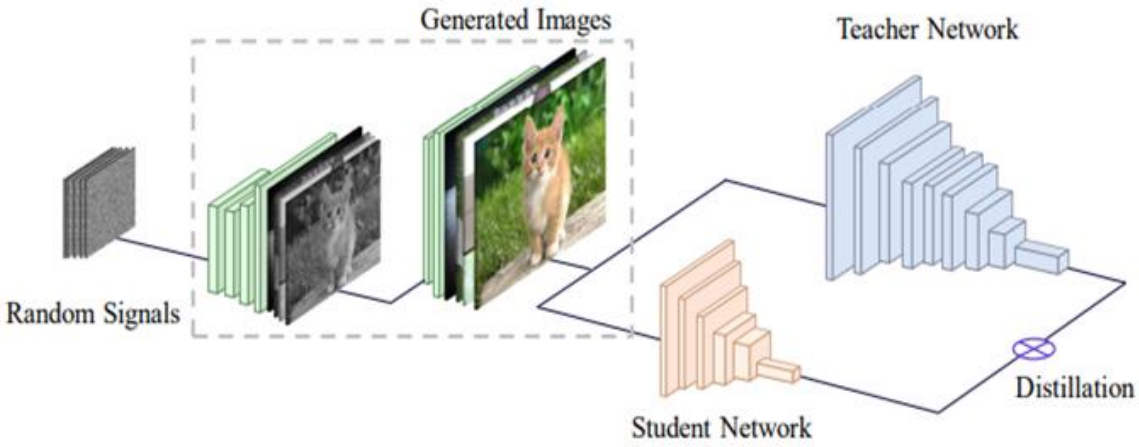


Рис. 1. Общая структура работы методов передачи знаний на основе создания синтетических изображений

Метод Data-Free Adversarial Distillation (DFAD) использует генератор, который обучается создавать изображения, на которых предсказания учителя и студента максимально расходятся [2]. Эти примеры затем служат основой для обучения студента, направленного на сокращение расхождения. В отличие от ZSKD, здесь задействован механизм игры (GAN-подобная схема), что позволяет генерировать более «напряженные» примеры. Авторы демонстрируют, что DFAD обеспечивает сравнимую с классическим подходом обучения точность на задачах классификации. Ограничением является относительно высокая сложность обучения: генератор оптимизируется совместно с двумя сетями (учителем и студентом). Авторы демонстрируют точность 93,3 % для студента на датасете CIFAR-10.

DeepInversion основан на прямой оптимизации изображений без использования генеративных моделей [3]. Процесс начинается со случайного шума, который итеративно обновляется путем минимизации функции потерь. Эта функция включает ошибку предсказания учителя и регуляризующий компонент, заставляющий промежуточные активации сети соответствовать статистике BatchNorm-слоев учителя. Поскольку многие современ-

ные модели содержат BN-слои, их сохраненные статистики (средние и дисперсии) используются в качестве ограничений – это заставляет синтетические изображения иметь естественную «визуальную правдоподобность». Преимуществом DeepInversion является высокое качество синтетических примеров; однако метод требует, чтобы учительская модель содержала статистику BN, и сам процесс оптимизации довольно ресурсоемок.

В методе DAFL (Data-Free Adversarial Learning) учитель выступает в роли фиксированного дискриминатора, а генератор обучается выдавать примеры, вызывающие максимальный отклик у учителя. Затем на выходах учителя для этих примеров обучается студент. Авторы [4] достигли 92,2 % точности на CIFAR-10 и 74,5 % на CIFAR-100 для студента ResNet-18 без использования реальных данных. Метод простой в реализации и эффективно генерирует классовые «абстракции», но генерируемые образы часто однотипны, что ограничивает разнообразие данных.

DiffDFKD основан на использовании диффузионных моделей для синтеза данных [5]. Предобученный диффузионный генератор направляется информацией из учителя, а именно модель учителя помогает оптимизировать условия генерации так, чтобы синтезированные изображения приближали истинное распределение обучающих данных. Для повышения разнообразия был введен прием Latent CutMix – склейка латентных представлений различных сгенерированных изображений. В результате DiffDFKD существенно превзошел существующие подходы по точности обучения модели-студента без использования реальных данных. Преимущество – высокое качество фотогеничных образцов, существенное улучшение финальной точности студента; ограничение – необходимость в предобученной диффузионной модели и значительные вычисления при генерации. На рисунке 2 представлены примеры сгенерированных изображений различных методов. В таблице 1 представлены значения метрики точности для различных методов передачи знаний на основе синтетических данных.

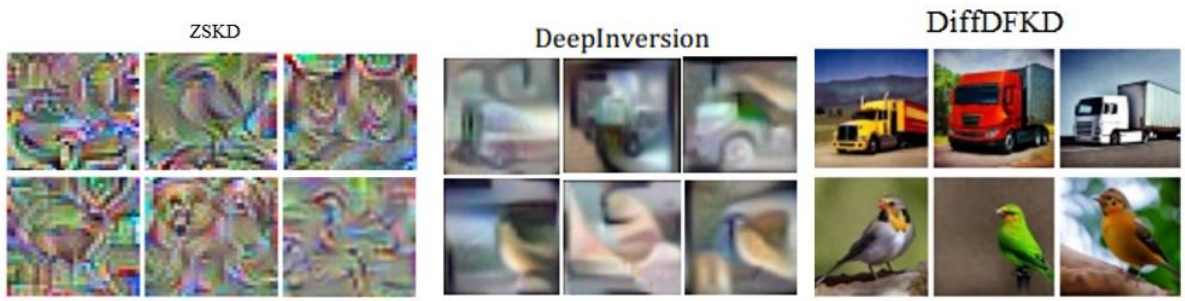


Рис. 2. Примеры сгенерированных изображений

ТАБЛИЦА 1. Значения метрики точности для различных методов передачи знаний на основе синтетических данных

Датасет CIFAR-10					
Метод	R34 R18	V11 R18	W40-2 W16-1	W40-2 W16-2	W-40-2 W40-1
Teacher	95.70	92.25	94.87	94.87	94.87
Student	95.20	95.20	91.12	93.94	93.95
DeepInv	93.26	90.36	83.04	86.85	89.72
DAFL	92.22	81.10	65.71	81.33	81.55
ZSKT	93.32	89.46	83.71	86.07	89.66
DiffDFKD	95.41	92.36	91.10	94.03	93.81

Второе направление – слияние параметров модели. Наиболее распространенные методы включают: Task Arithmetic, Git Re-Basin, ZipIt! и MuDSC.

В методе Task Arithmetic предполагается, что модель (или ее часть) после дообучения на задаче A отличается от исходной только добавлением некоторого вектора задачи (task vector) в весовое пространство [6]. Этот вектор получается вычитанием весов базовой модели из весов модели, дообученной на задаче A. В дальнейшем векторы задач можно суммировать: например, добавление вектора задачи A и вектора задачи B к исходной модели стремится улучшить производительность по обеим задачам одновременно. Преимущество – простота: достаточно знать веса обученных моделей. Однако Task Arithmetic требует, чтобы все модели имели одинаковую архитектуру и происходили от одной инициализации.

Git Re-Basin – метод устранения перестановочной неоднозначности между нейросетями одинаковой архитектуры [7]. Он автоматически подбирает перестановки нейронов скрытых слоев, чтобы привести независимо обученные модели к общему представлению, позволяющему их усреднение без потерь в качестве. Работает при различной инициализации моделей.

ZipIt! – метод объединения моделей с одинаковой архитектурой, обученных на разных задачах [8]. Он реализует частичное слияние нейронов до заданного слоя, после чего сохраняет раздельные выходные ветви для каждой задачи. Это позволяет совместно использовать общие признаки и одновременно сохранять специфику задач.

Метода MuDSC (Merging under Dual-Space Constraints) учитывает сходства нейронов как по весовым параметрам, так и по активациям [9]. В методе строятся матрицы сходства в пространстве весов и активаций, а затем определяются перестановки нейронов, оптимально согласующие обе метрики для более точного объединения моделей в двух пространствах. Однако поиск оптимальных перестановок в двойном пространстве довольно сложен и вычислительно затратный.

В таблице 2 представлены значения метрики точности различных методов на основе слияния параметров модели. Joint – точность модели, обученной на 10 классах, Avg, T.A., T.B. – значения точности объединенной модели на 10 и каждой группы из 5 классов соответственно.

ТАБЛИЦА 2. Значения метрики точности для различных методов передачи знаний на слияния параметров модели

Модель	Resnet20			
Датасет	CIFAR-10			
Метод	Joint	Avg	T.A	T.B
Re-basin	60.61	88.57	88.46	88.68
ZipIt	82.44	94.61	94.22	95.00
MuDSC	83.09	94.88	94.56	95.21

Методы объединения нейросетей без доступа к исходным данным делятся на два типа: дистилляция с синтетическими данными и прямое объединение параметров.

Data-free distillation позволяет переносить знания между разными архитектурами, но требует генерации псевдоданных и обучения студента. Преимущества – гибкость и точность, недостатки – высокая вычислительная сложность и возможное расхождение с реальными данными.

Parameter merging не требует дообучения, но ограничен совместимостью архитектур. Он прост и быстр, однако требует точного выравнивания нейронов и не подходит для сильно разных моделей.

В целом, выбор подхода зависит от условий: если необходим компактный студент на новой архитектуре и можно потратить ресурсы на его обучение – лучше data-free KD; если же нужно быстро получить модель, выполняющую несколько задач без долгого обучения – предпочтителен direct merging (например, ZipIt или MuDSC при сходной архитектуре). Каждая группа методов

имеет свои сильные и слабые стороны, поэтому в практике стоит учитывать размер модели, доступный ресурс, требуемую точность и ограничения на архитектуру. В любом случае, оба направления активно развиваются: появляются более эффективные и универсальные решения, расширяющие возможности объединения нейросетей без доступа к исходным данным.

Список используемых источников

1. Nayak G. K. et al. Zero-shot knowledge distillation in deep networks // International Conference on Machine Learning. PMLR, 2019. С. 4743-4751.

2. Fang G. et al. Data-free adversarial distillation // arXiv preprint arXiv:1912.11006. 2019.

3. Yin H. et al. Dreaming to distill: Data-free knowledge transfer via deepinversion // Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. 2020. С. 8715-8724.

4. Chen H. et al. Data-free learning of student networks // Proceedings of the IEEE/CVF international conference on computer vision. 2019. С. 3514-3522.

5. Qi X. et al. Data-free Knowledge Distillation with Diffusion Models // arXiv preprint arXiv:2504.00870. 2025.

6. Ilharco G. et al. Editing models with task arithmetic // arXiv preprint arXiv:2212.04089. 2022.

7. Ainsworth S. K., Hayase J., Srinivasa S. Git re-basin: Merging models modulo permutation symmetries //arXiv preprint arXiv:2209.04836. 2022.

Stoica G. et al. Zipit! merging models from different tasks without training // arXiv preprint arXiv:2305.03053. 2023.

Xu Z. et al. Training-free pretrained model merging // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2024. С. 5915-5925.

INTEGRATION OF KNOWLEDGE OF NEURAL NETWORK MODELS WITHOUT ACCESS TO DATA

Vasiliev N., Leshchinsky B., Sitdikov D.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The paper considers two approaches to merging the knowledge of neural network models without access to the source data: (1) transferring knowledge from several teacher models to a single student model using synthetically generated data; (2) direct merging of model parameters without training. The first approach includes methods for generating pseudo-data based on the teacher's behavior and allows training students of arbitrary architecture. The second approach uses special algorithms for merging the weights of pre-trained models, solving the problem of differences in the structure of internal representations. The paper discusses the conditions for applying each method, their limitations, and the quality of merging based on the results of experiments on classification problems.

Key words: *neural network fusion, Zero-Shot KD, DeepInversion, DFAD, Git Re-Basin, MuDSC, synthetic data, parametric fusion, data-free learning*

УДК 519.2
ГРНТИ 49.03.11

МЕТОДИКА ПОИСКА КОРНЕВЫХ ПРИЧИН НАРУШЕНИЙ НОРМАЛЬНОГО ФУНКЦИОНИРОВАНИЯ ГИБРИДНОЙ СЕТИ

Р. М. Вивчарь, В. А. Гончаров

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

Гибридные сети, объединяющие как традиционные проводные, так и современные беспроводные технологии, обеспечивают повышенную гибкость и надежность передачи данных. Однако их сложная архитектура также создает множество проблем, особенно в вопросах поддержки эксплуатационной эффективности и надежности. Для решения таких проблем использовалась методология анализа корневых причин проблемы. Дополнив методами из раздела теории вероятностей и математической статистика, был разработан экспертно-статистический метод моделирования и анализа причин нарушений нормального функционирования гибридной сети на основе применения Байесовой сети с использованием типовых шаблонов причинно-следственных связей, позволяющий проводить автоматизированный анализ, диагностику и прогнозирование причин нарушений.

гибридные сети, Байесовые сети, анализ корневых причин, АКП.

В эпоху, характеризующуюся быстрым развитием технологий и растущей зависимостью от взаимосвязанных систем, гибридные сети стали основными инфраструктурами, лежащими в основе связи и обмена данными в различных областях. Эти сети, объединяющие как традиционные проводные, так и современные беспроводные технологии, обеспечивают повышенную гибкость и надежность передачи данных. Однако их сложная архитектура также создает множество проблем, особенно в вопросах поддержки эксплуатационной эффективности и надежности. Нарушения в их нормальном функционировании могут привести к значительным сбоям, влияющим на все: от индивидуального опыта пользователя до критически важных бизнес-операций. Поэтому понимание корней этих нарушений имеет важное значение для обеспечения устойчивости и долговечности гибридных систем связи.

В современном менеджменте качества для обозначения процесса решения проблем на основе поиска и устранения ее корневых причин используется термин анализ корневых причин (root cause analysis, RCA) [1, 2]. Анализ корневых причин (АКП) – это структурированное исследование, целью которого является идентификация истинных причин проблемы и принятие действий, необходимых для устранения этих причин. Поскольку в основе любой проблемы лежат

причины этой проблемы, то для ее решения необходимо вначале идентифицировать причину, а затем выработать и предпринять корректирующее воздействие для устранения этой причины, что в конечном итоге приведет к разрешению проблемы, при этом эффективное решение проблемы невозможно без поиска и устранения ее корневой (системной) причины (root cause) [2].

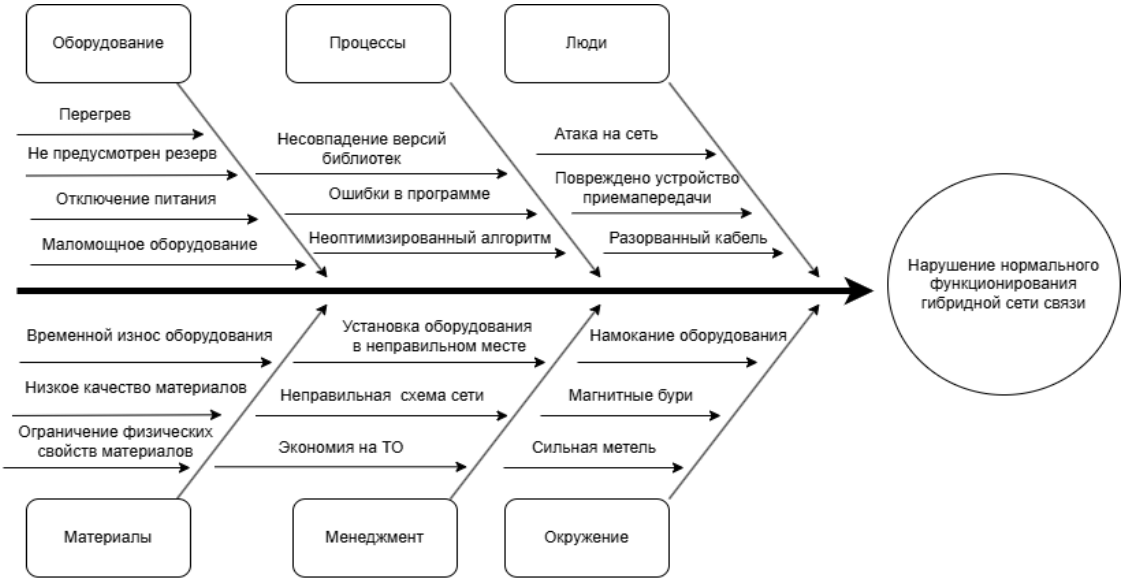


Рис. 1. Диаграмма Исикавы

На рис. 1 представлена диаграмма Исикавы – графический способ исследования и определения наиболее существенных причинно-следственных взаимосвязей между факторами и последствиями, которые ведут к нарушению нормального функционирования гибридной сети.

Зная причины и последствия, можно построить граф, каждую вершину описать в виде дискретной случайной величины и задать множество ее значений с помощью метода Байеса.

Метод Байеса относится к классу статистических методов распознавания причин надежности и является наиболее эффективным [3, с. 11-18]. Он основан на теореме Байеса, которая позволяет рассчитать апостериорную вероятность гипотезы при условии наступления свидетельства; также возможно, как прогнозирование, так и диагностирование дефектов. Данный метод нашел применение и при анализе и диагностике причин несоответствий в области качества [4].

Байесовы сети (БС) – это разновидность графовых моделей, отражающие вероятностные связи между событиями предметной области.

По сравнению с методами анализа корневых причин, обладающими высокой долей субъективизма, в основе БС лежит строгий аппарат теории вероятностей, статистики и теории графов. Следовательно, выводы, получае-

мые на основе БС, можно считать объективными при условии объективности входных данных.

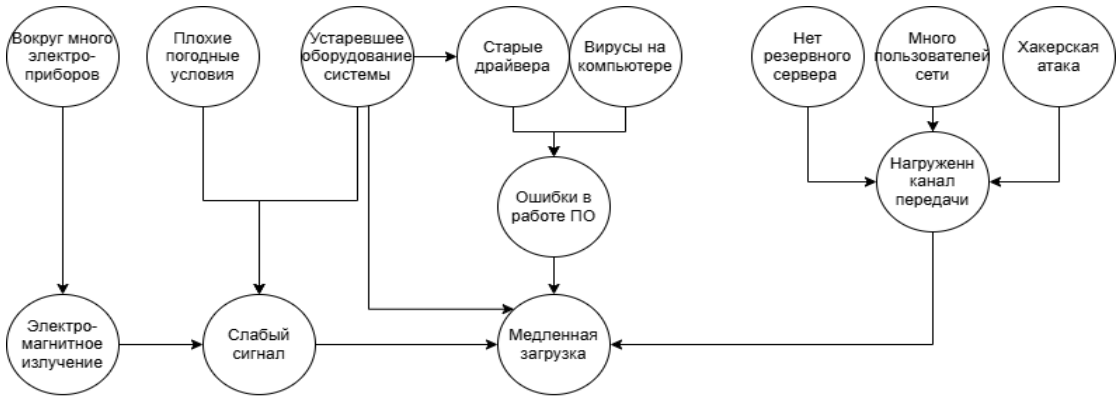


Рис. 2. Байесовая сеть

На рис. 2 изображена Байесовая сеть, описывающая причинно-следственные связи (события), приводящие к возникновению медленной загрузки данных в гибридной сети связи.

При расчетах имеется возможность совместного использования степеней доверия и вероятностей в классической (частотной) трактовке, что является важным преимуществом БС. В частности, это позволяет в единой модели учесть как знания экспертов (субъективную информацию), так и вероятностные распределения (объективную информацию), которые могут быть получены на основе статистических данных либо иных сведений о моделируемой системе:

$$P(A) = \sum_i P(A, B_i),$$
$$P(A, B) = P(B) * P(B) \quad (1)$$

Вероятность любого события A может быть вычислена путем обуславливания на множестве несовместных событий B_i, i = 1, 2, ..., n, образующих полную группу и последующего суммирования:

$$P(A) = \sum_i P(B_i)P(B_i) \quad (2)$$

Декомпозиция (2) представляет собой базу для проведения гипотетических рассуждений. Это означает, что степень доверия к любому событию A представляет собой взвешенную сумму степеней доверия к этому событию во всех случаях, когда осуществление A возможно.

В результате на рис. 3 предложена методика, которая позволяет построить причинную Байесову сеть для анализа и моделирования несоответствий, при этом использование формул и Байесовского подхода позволяет в единой модели учитывать как статистическую информацию о нарушениях, так и знания экспертов, формально представленные в виде графа и субъективных вероятностей.

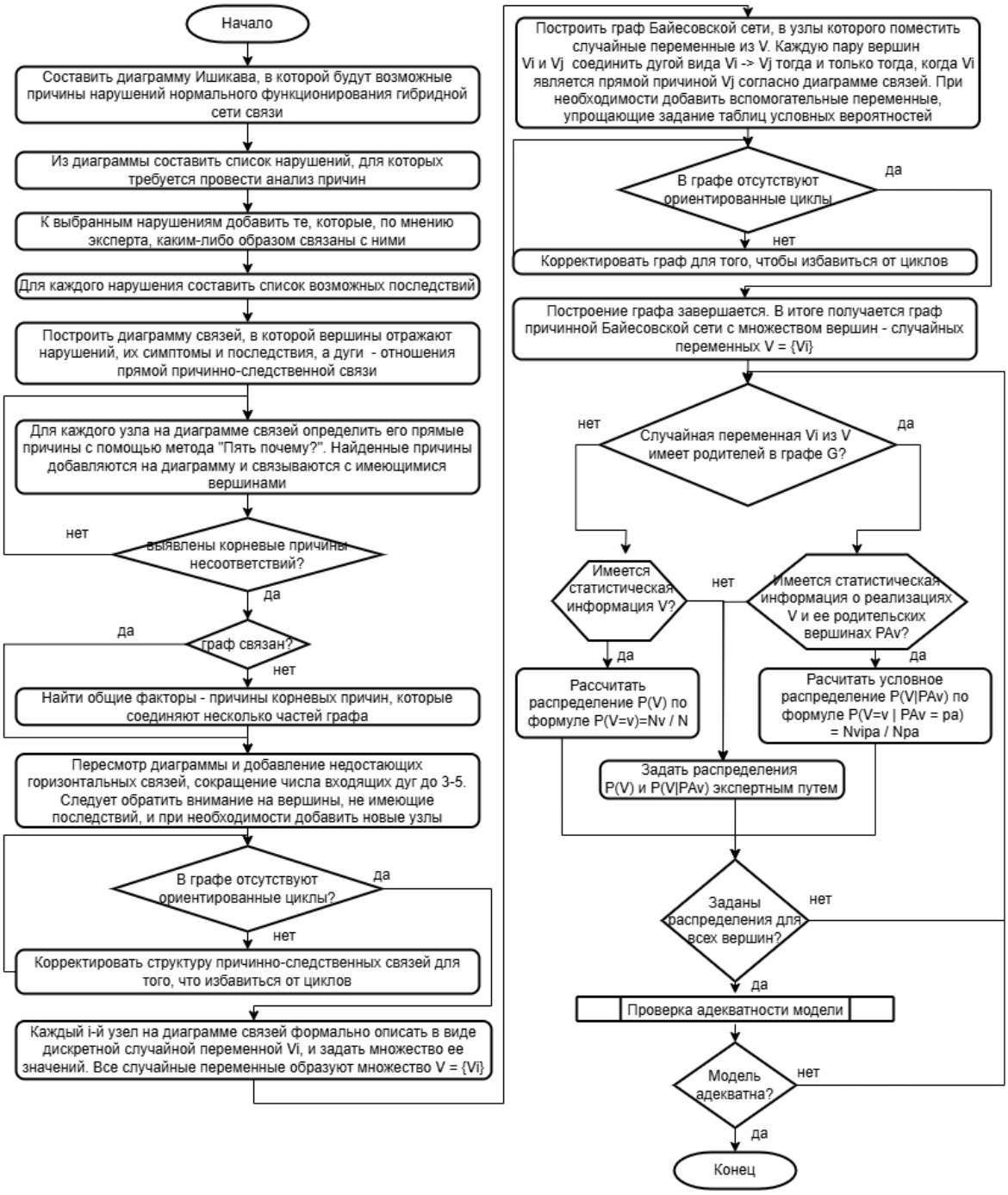


Рис. 3. Схема экспертно-статистического метода моделирования и анализа причин нарушений нормального функционирования гибридной сети

Список используемых источников

1. Савинкина В. А. Анализ корневых причин / по материалам статьи Root Cause Analysis vs. Shallow Cause Analysis by Robert J. Latino, опубликованной на сайте www.reliability.com подготовила В. А. Савинкина; Robert J. Latino // Методы менеджмента качества. 2008. № 8. С. 51-53.

2. Andersen B. Root cause analysis: simplified tools and techniques / B. Andersen, T. Fagerhaug. American Society for Quality, Quality Press, 2006. 240 p.

3. Биргер И. А. Техническая диагностика / И. А. Биргер. М.: Машиностроение, 1978. 240 с.

4. Червяков И. В. Использование методов технической диагностики для поиска причин несоответствий / И. В. Червяков // Методы менеджмента качества. 2009. № 4. С. 40-43.

5. Pearl J. Probabilistic Reasoning in Intelligent Systems / J. Pearl. San Francisco: Morgan Kaufmann, 1988. 520 p.

6. Pearl J. Causality: Models, Reasoning and Inference / J. Pearl. Cambridge University Press. 2-nd edition, 2009. 464 p.

METHOD OF SEARCHING FOR ROOT CAUSES OF DISTURBANCES IN THE NORMAL FUNCTIONING OF A HYBRID NETWORK

Vivchar R., Goncharov V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Hybrid networks, which combine both traditional wired and modern wireless technologies, provide increased flexibility and reliability of data transmission. However, their complex architecture also creates many problems, especially in maintaining operational efficiency and reliability. To solve such problems, the methodology of root cause analysis of the problem was used. Supplemented with methods from the section probability theory and mathematical statistics, an expert-statistical method for modeling and analyzing the causes of disruptions in the normal functioning of a hybrid network was developed based on the application of a Bayesian network using typical patterns of cause-and-effect relationships, allowing for automated analysis, diagnostics and forecasting of the causes of disruptions.

Key words: *hybrid networks, Bayesian network, root cause analysis, RCA*

УДК 621.396
ГРНТИ 49.33.29

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ГИБРИДНЫХ ВЫЧИСЛИТЕЛЬНЫХ АРХИТЕКТУР В V2X СИСТЕМАХ

А. Г. Владыко, П. В. Плотников, Г. И. Тамбовцев

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

Рост требований к пропускной способности и допустимым задержкам в интеллектуальных транспортных системах стимулируют развитие гибридных вычислительных архитектур, сочетающих облачные, граничные и туманные вычисления. Несмотря на ограниченные ресурсы бортовых устройств, их объединение в самоорганизующиеся структуры позволяет эффективно распределять и обрабатывать вычислительно сложные задачи вблизи источника данных. В статье рассматриваются подходы к построению многоуровневой архитектуры Vehicle-to-Everything, включая имен-ориентированную передачу данных (Named Data Networking) и микросервисную организацию вычислений. Проведен сравнительный анализ, выявлены различия и общие черты рассматриваемых архитектур.

сети VANET, V2X-системы, edge, fog, mobile RSU, cluster, NDN

Развитие интеллектуальных транспортных систем (Intelligent Transportation Systems, ITS) и технологий взаимодействия «транспортное средство ко всему» (Vehicle-to-Everything, V2X) повышает требования к вычислительной инфраструктуре транспортных средств [1, 2]. Минимальная задержка, высокая надежность и безопасность соединений необходимы для ряда приложений, начиная от анализа дорожной обстановки до потоковой мультимедиа-передачи [1–3]. Ключевой задачей является минимизация задержек при сохранении высокого уровня качества услуг (Quality of Service, QoS) и качества восприятия (Quality of Experience, QoE). Централизованные облачные решения, хотя и обладают масштабируемостью, сталкиваются с проблемами увеличения задержки из-за удаленности центров обработки, перегрузкой магистралей и уязвимостью к отказам, особенно в условиях высокой мобильности участников дорожного движения и динамически изменяющейся нагрузки.

Децентрализованные подходы – edge и fog computing – направлены на обработку данных ближе к источникам, но бывают ограничены ресурсами или сложностью обеспечения стабильности. В последние годы особое вни-

мание исследователей привлекли гибридные вычислительные архитектуры, сочетающие преимущества облачных, граничных и туманных решений. В частности, перспективным направлением стало использование транспортных средств как элементов туманной инфраструктуры, что открывает новые возможности при решении задач оптимизации задержки и распределения нагрузки.

В рамках настоящей работы проводится сравнительный анализ двух близких, но одновременно концептуально различных подходов к построению гибридных архитектур в V2X-системах:

FoggyEdge [4] – многоуровневая архитектура на основе Named Data Networking (NDN), микросервисов и стационарных узлов Vehicular Fog Computing (VFC) формируемых из припаркованных автомобилей.

Кластеризация придорожных устройств (Roadside Unit, RSU) с мобильными RSU (mRSU) [5] – IP-ориентированный подход с группировкой стационарных RSU и использованием мобильных узлов для формирования динамического тумана, перемещающихся по требованию.

FoggyEdge включает четыре слоя (рисунок 1):

1. Слой транспортных средств (Things layer) – мобильные и припаркованные автомобили, оснащенные бортовыми вычислительными модулями (On Board Unit, OBU).

2. Граничный слой (Edge layer) – дорожные узлы (RSU), обеспечивающие базовую обработку данных и связь с облаком.

3. Слой «vehicular fog» (VF layer) – вычислительные узлы, формируемые из припаркованных автомобилей, интегрированных через VF-шлюз.

4. Облачный слой (Cloud layer) – централизованная обработка долгосрочных и ресурсоемких задач.

Применение NDN обеспечивает маршрутизацию по именам контента, кэширование и агрегацию запросов. Авторы в работе [4] раскрывают подробнее, что для создания такой архитектуры требуется использовать независимые микросервисы, которые могут переноситься между узлами. Это снижает трафик, так как переносится не весь сервис, а лишь необходимые модули. Микросервисная архитектура также соответствует современному подходу разработки. Управление доступом реализуется через HMAC-аутентификацию, защищая микросервисы от несанкционированного использования. VF-шлюз поддерживает таблицу доступных ресурсов и перераспределяет задачи между VF, границей и облаком в зависимости от загруженности.

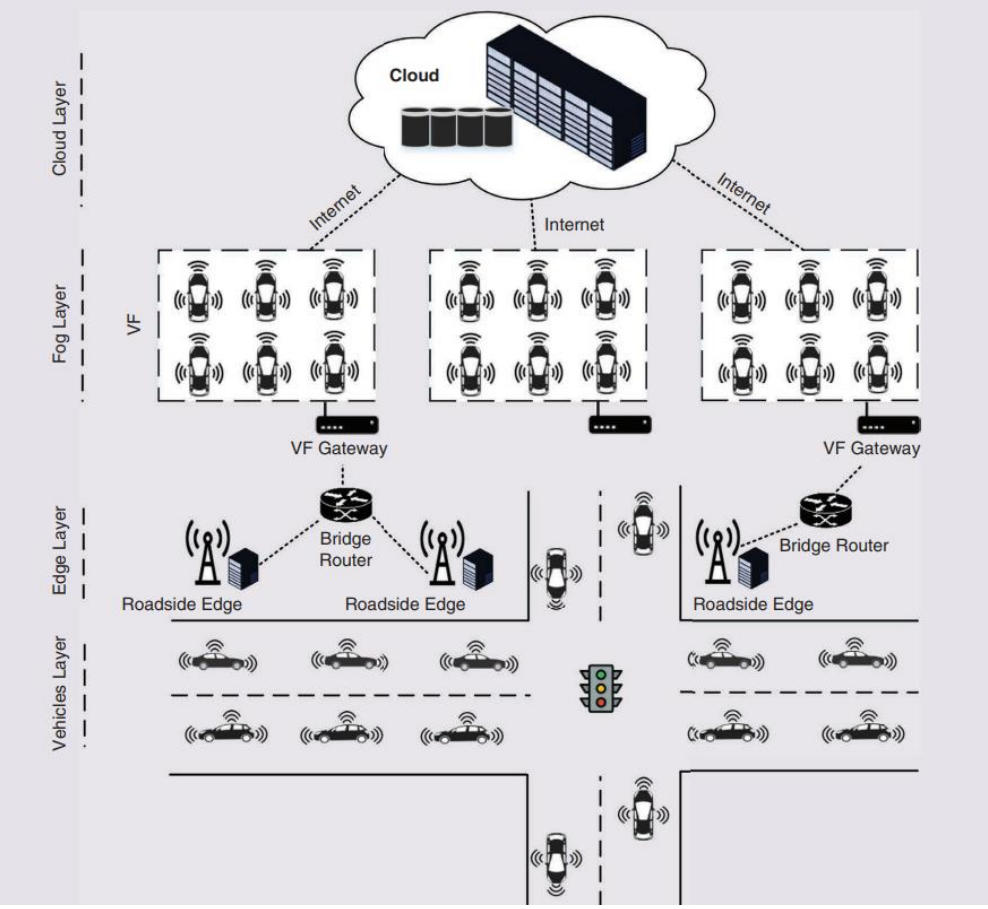


Рис. 1. *FoggyEdge* архитектура [4]

Концепция использования припаркованных автомобилей в качестве VF-узлов вызывает ряд вопросов практического характера. В частности, в представленной работе не рассматривается аспект энергопотребления таких узлов. Выполнение вычислительных задач в автомобиле требует энергии, что может привести либо к разрядке аккумулятора, либо к необходимости работы двигателя. Без механизмов компенсации затрат или обеспечения внешнего питания это ограничение может существенно снизить привлекательность решения для автовладельцев, что, в свою очередь, повлияет на устойчивость всей архитектуры.

Альтернативно, кластеризация RSU с mRSU использует классическую IP-модель. Стационарные RSU объединяются в кластеры с координирующим узлом; mRSU служат временными вычислительными и коммуникационными точками в зонах высокой нагрузки или слабого покрытия. Такой подход не зависит от владельцев транспортных средств и исключает риски, связанные с энергопотреблением их автомобилей.

Использование mRSU позволяет гибко перераспределять нагрузку с зон обслуживания в ответ на пространственно-временные колебания трафика, что позволяет минимизировать вероятность перегрузок и повысить устойчивость системы к отказам отдельных стационарных узлов. При этом подход исключает зависимость от готовности владельцев частных автомобилей предоставлять свои ресурсы и устраняет риски, связанные с энергопотреблением и износом бортовых систем частных транспортных средств. На рисунке 2 в схожей тематике проиллюстрирована рассматриваемая архитектура.

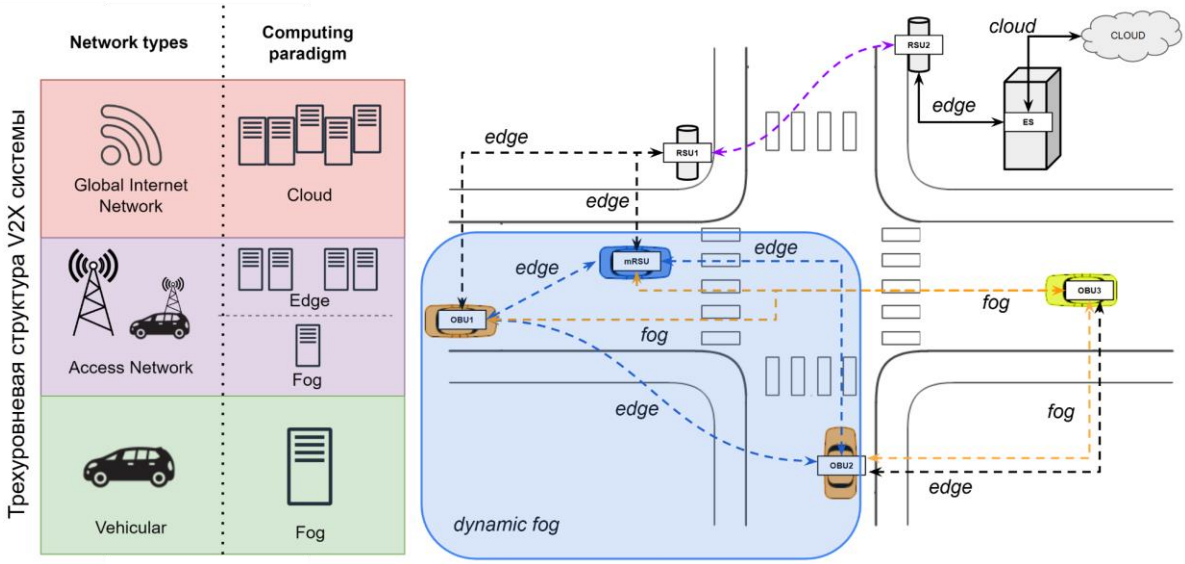


Рис. 2. Представление трехуровневой архитектуры V2X [5]

Обращаясь к рисунку 2, пунктирной линией обозначена беспроводная связь 802.11p/802.11bd [6]. Динамический туман (dynamic fog) достигается за счет наличия RSU/mRSU в кластере из бортовых устройств. Внутри динамического тумана, OBU – это edge (граница), по признаку близости друг к другу. Fog же достигается «от лица» OBU3 (выделено зеленым цветом), поскольку оно может установить соединение с одним из участников динамического тумана (на рисунке 2 – OBU2), однако при этом, оно само не является частью динамического тумана, поскольку ни одно RSU/mRSU не является к нему границей. Авторы в работе [5] не уточняют по какому алгоритму происходит кеширование, тем не менее, проблема кеширования остается актуальной, что гораздо лучше проработано в FoggyEdge.

Сопоставление двух подходов показывает, что их сильные стороны взаимодополняемы. Применение механизмов NDN и микросервисной архитектуры, представленных в FoggyEdge, может существенно повысить эффек-

тивность управления контентом и снизить задержки. При этом использование mRSU в качестве мобильных узлов масштабирования представляется более практичным и энергетически независимым решением по сравнению с VF из припаркованных автомобилей. Таким образом, интеграция этих элементов в единую архитектуру может обеспечить как высокую производительность и эффективность обработки данных, так и устойчивость к эксплуатационным ограничениям.

Исследование выполнено за счет гранта Российского научного фонда № 24-29-00304, https://rscf.ru/project/24-29-00304/.

Список используемых источников

1. Liu L. et al. Vehicular edge computing and networking: A survey // Mobile networks and applications. 2021. Т. 26. № 3. С. 1145-1168

2. Hou X. et al. Vehicular fog computing: A viewpoint of vehicles as the infrastructures // IEEE transactions on vehicular technology. 2016. Т. 65. № 6. С. 3860-3873.

3. Clancy J., et al. Wireless access for V2X communications: Research, challenges and opportunities // IEEE Communications Surveys & Tutorials. 2024. Т. 26. № 3. С. 2082-2119.

4. Rehman M. A. U., et al. FoggyEdge: An information-centric computation offloading and management framework for edge-based vehicular fog computing //IEEE Intelligent Transportation Systems Magazine. 2023. Т. 15. № 5. С. 78-90.

5. Vladyko A., Plotnikov P., Tambovtsev G. Simulation-Based Evaluation of V2X System with Variable Computational Infrastructure // Network. 2025. Т. 5. № 1. С. 4.

6. IEEE Standards Association. URL: https://standards.ieee.org/ieee (lata обращения 20.07.2025).

COMPARATIVE ANALYSIS OF HYBRID COMPUTING ARCHITECTURES IN V2X SYSTEMS

Vladyko A., Plotnikov P., Tambovtsev G.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The growing demands for bandwidth and permissible latency in Intelligent Transportation Systems are driving the development of hybrid computing architectures that combine cloud, edge, and fog computing. Despite the limited resources of on-board units (OBUs), their integration into self-organizing structures enables the efficient distribution and processing of computationally intensive tasks near the data source. This paper examines approaches to building multi-layer Vehicle-to-Everything architectures, including Named Data Networking for data delivery and microservice-based computing organization. A comparative analysis is conducted to identify both the differences and the common features of the architectures under consideration.

Key words: *VANET, V2X systems, edge computing, fog computing, mobile RSU, clustering, Named Data Networking (NDN)*

УДК 378.147:514.18
ГРНТИ 27.21.21

ПРИНЦИП БУЙНЕВИЧА-ШЕСТАКОВА

Д. В. Волошинов

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

В современной геометрии принято считать, что осями (главными направлениями) кривых второго порядка являются прямые линии. Однако, если оси эллипса имеют в пересечении с этой кривой четыре действительные точки, то оси гиперболы пересекаются с ней в двух действительных и двух мнимых точках. Поскольку с точки зрения проективной геометрии кривые второго порядка не различаются, то природа точек пересечения главных направлений этих кривых с самими кониками должна быть однородной, что приводит к противоречию с имеющимся положением дел. Устранить это противоречие можно лишь в том случае, если понимать под осями коник не прямые линии, а окружности особого рода – линии, состоящие из двух ветвей: известных на настоящий момент прямых и бесконечно удаленной прямой – несобственной прямой плоскости. Рассматриваемый в статье принцип Буйневича-Шестакова демонстрирует простое объяснение рассматриваемого феномена и устанавливает конструктивную связь между осями и фокусами кривых.

преобразование инверсии, радикальная ось, кривые второго порядка, фокусы коник

В соответствии с классическим определением преобразования инверсии полагается, что на евклидовой плоскости некоторая выделенная окружность, называемая в дальнейшем окружностью инверсии, устанавливает между точками P и P' инволюционное соответствие, такое, что $\left|OP'\right|\cdot\left|OP\right| = R^2$, где под точкой O понимается центр окружности инверсии [1–3]. Особенность этого преобразования заключается в том, что единственной точке плоскости, совпадающей с центром окружности инверсии, не находится однозначного соответствия, так как при бесконечном удалении точки от центра окружности инверсии по любому направлению ее образ стремится к центру окружности инверсии. Для сохранения однозначности преобразования принято расширять евклидову плоскость единственной бесконечно удаленной точкой, устраняющей проблему неоднозначности.

Однако такой подход имеет и ряд недостатков, которые приводят к нарушению некоторых основополагающих геометрических принципов и затрудняют решение ряда задач, в особенности тех, которые сформулированы в терминах проективной плоскости [4–6], замкнутой на бесконечно удален-

ной прямой, а не точке. В частности, перестают соблюдаться положения о сохранении инцидентности объектов-прообразов и соответствующих им в преобразовании объектов-образов, а также понятие о порядке кривой линии.

Несложно привести примеры таких несоответствий. Так, например, любая прямая линия несет на себе единственную бесконечно удаленную точку (как в случае с преобразованием инверсии, так и в проективном варианте). Но, расширяя плоскость лишь единственной бесконечно удаленной точкой, следует признать, что все прямые линии плоскости проходят через эту бесконечно удаленную точку, тем самым составляя пучок прямых с общим центром. Поскольку в соответствии с аксиоматикой две несовпадающие прямые должны иметь в пересечении общую точку и имеют в то же время общую точку названного пучка, то приходится признать, что все прямые линии плоскости совпадают, что приводит к абсурду.

Второй аспект, который необходимо принимать во внимание, заключается в том, что под порядком кривой линии понимают число пересечений прямой линии с этой кривой (учитывая, разумеется, мнимые решения и их возможную кратность). Прямая линия пересекается с другой прямой линией в одной точке, в результате чего ей приписывается первый порядок. Она же с окружностью пресекается в двух точках, следовательно, окружность понимается как линия второго порядка.

Предположим, что на плоскости имеются прямая линия l и окружность d (рис. 1), которые в пересечении образуют две точки $T_1, T_2 = d \times l$ (действительные или мнимые). Пусть также на плоскости задана окружность инверсии i, относительно которой осуществим преобразование инверсии $d, l, T_1\ T_2$ в $d' = \mathrm{I}_i(d)$, $l' = \mathrm{I}_i(l)$, $T'_1 = \mathrm{I}_i(T_1)$, $T'_2 = \mathrm{I}_i(T_2)$. Понятно, что окружность d преобразуется в окружность d', а прямая линия l – в окружность l', проходящую через центр O окружности i. Но, поскольку окружности являются частным случаям кривых второго порядка, то они должны пересекаться не в двух, а в четырех точках – двух явных и в двух циклических точках, имеющих мнимую природу, через которые проходят все окружности плоскости. В соответствии с принципом сохранения инцидентности в образах и прообразах в обратном преобразовании прямая должна была бы нести на себе прообразы циклических точек, причем все прямые плоскости должны были бы через эти точки проходить, и, значит, совпадать. Это рассуждение снова приводит к противоречию, следовательно, в принятых в основу преобразования инверсии допущениях содержится некоторый логический изъян.

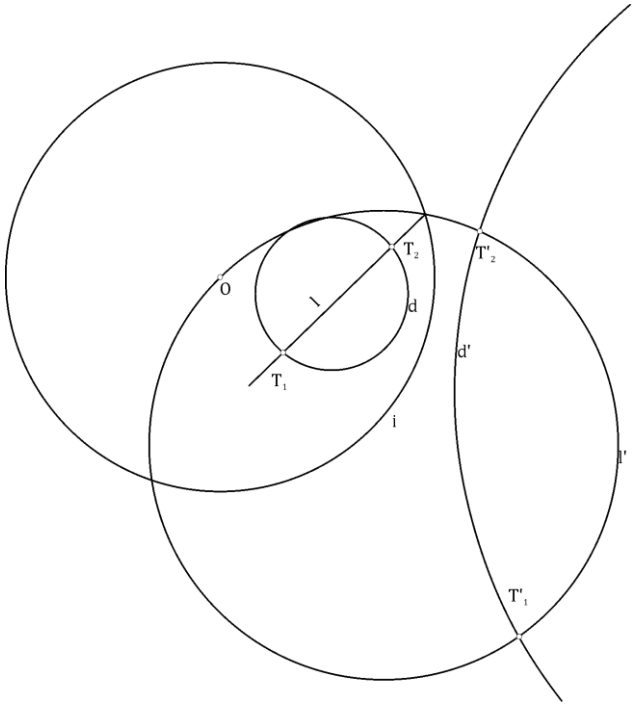


Рис. 1. К пояснению преобразования инверсии

Попытка сопоставить точке центра окружности инверсии бесконечно удаленную прямую линию, расширяющую евклидову плоскость до проективной плоскости, также не приведет к устранению противоречий. Корреляти́вное преобразование, устанавливающее взаимно-однозначное соответствие между пространствами разных размерностей должно было бы быть единым для всех аргументов преобразования, однако в рассматриваемом случае это не так.

Выход из создавшейся ситуации видится в следующем. В литературе при рассуждениях о преобразовании инверсии можно, например, встретить такие понятия как «нуль-окружность» в отношении точки, «обобщенная окружность» в отношении прямой линии [7].

Природа первого термина освещается в литературе достаточно подробно. Часто ассоциация, возникающая от визуального представления о «сжатии окружности в точку» при стремлении ее радиуса к нулю способствует неверному пониманию этого геометрического феномена. Из уравнения $x^2 + y^2 = R^2$ при $R = 0$ становится ясно, что окружность нулевого радиуса представляется двумя мнимыми изотропными прямыми $x + iy = 0$ и $x - iy = 0$, рассматриваемые в совокупности. Здесь особенно важно отметить, что таких прямых две, и, следовательно, в совокупности они пересечении с произвольной прямой образуют две точки, а значит представление о порядке кривой, равным двум, соблюдается.

В то же время под обобщенной окружностью обычно понимают просто прямую линию, замкнутую на себя в бесконечности, а для сохранения порядка ее представляют, как двойную линию. Однако такое допущение приводит к логическим проблемам.

Предположим, на плоскости имеются две несовпадающие точки, которые примем за центры пучка окружностей. Выделив в этом пучке любую окружность и разместив на ней третью точку, начнем изменять радиус этой окружности за счет перемещения этой точки по произвольному направлению. По мере удаления третьей точки от центров пучка окружность будет все более «спрямляться» и при достижении ею бесконечно удаленного положения окружность, проходящая через центры, «выродится» в прямую линию. Получается, что прямая линия проходит через три точки, не лежащие на одной прямой, что противоречит базовой аксиоматике геометрии. Видно, что чисто представление об «обобщенной окружности», исходя из соображений визуальности, в виде прямой линии противоречит логике поставленной задачи. Выходом из создавшегося положения является расчленение «обобщенной окружности» на две прямые линии-ветви, одна из которых проходит через два обозначенных центра, а вторая представляет собой бесконечно удаленную прямую, с которой встречаются все возможные точки, расширяющие окружность пучка до бесконечного радиуса.

Следуя в контексте приведенных рассуждений и отвлекаясь от понятия точки, можно полагать, что исходно в преобразовании инверсии осуществляется парное сопоставление окружностей и оно первично по отношению к другим геометрическим образам. При этом центру инверсии, замещенному на нуль-окружность и представляемому парой изотропных прямых, сопоставляется двойственная бесконечно удаленная прямая линия, которая может также рассматриваться как окружность особого вида.

Предлагаемый подход, получивший название «принцип Буйневича-Шестакова»[1], позволяет по-новому истолковать ряд известных положений и дать объяснение некоторым геометрическим конструкциям.

Так, например, с точки зрения проективной геометрии природа образования всех кривых второго порядка одинакова и поэтому кривые, различаемые в аффинной геометрии, в ней не различаются. Поэтому, например, эллипс и гипербола должны иметь по два главных направления (две оси), ко-

[1] Название обсуждаемому в статье принципу дано в честь коллег автора – профессоров Санкт-Петербургского государственного университета им. М. А.Бонч-Бруевича д.т.н. Буйневича Михаила Викторовича, и д.т.н. Шестакова Александра Викторовича, побудивших его к изучению данного геометрического феномена.

торые пересекаются с этими кривыми в двух парах точек. Поэтому должно существовать коллинеарное преобразование, переводящее такие четыре точки эллипса в соответственные четыре точки гиперболы при сохранении сами кривые друг в друга. Однако, в отличие от эллипса, гипербола имеет две вещественные точки пересечения с одной из осей. Точки пересечения с осью, называемой мнимой (но вещественной по своей природе), мнимы (комплексно сопряжены). Задание коллинеарного преобразования между соответственными парами точек неизбежно приведет к получению мнимого образа для любого вещественного прообраза, чего не должно быть. Поэтому представление о том, что мнимая ось гиперболы – это действительно ось, неверное.

Проблема может быть легко решена, если рассматривать оси кривых второго порядка не как прямые, а как окружности особого рода, речь о которых шла выше. Рассматривая пересечение гиперболы со второй ветвью такой окружности, бесконечно удаленной прямой, действительно получаем пересечение этой коники и прямой в двух точках – местах касания гиперболы с ее асимптотами. Принимая во внимание этот факт, можно установить рассмотренное ранее коллинеарное преобразование, которое однозначно переведет конику-прообраз в конику-образ с сохранением всех геометрических особенностей, свойственным главным направлениям кривых второго порядка.

Тот же принцип позволяет вскрыть геометрическое родство фокусов и осей кривых второго порядка, а также и других объектов, объединенных природой этого родства. Продемонстрируем это утверждение на примере эллиптической кривой.

Пусть на плоскости задан эллипс и найдены его вещественные фокальные точки (рис. 2). Проведем через эти точки произвольную окружность – представитель некоторого пучка окружностей. Эта окружность, как и сам пучок, устанавливает на прямой линии, соединяющей фокусы, инволюцию точечного ряда и определяет другой пучок окружностей, ортогональный к исходному. Несложно увидеть, что фокальные точки являются центрами нуль-окружностей этого пучка, а ось, не содержащая вещественных фокусов, представляет собой одну из ветвей окружности бесконечного большого радиуса из этого пучка. Тем самым демонстрируются, что фокусы и оси кривой второго порядка имеют общую геометрическую природу построения.

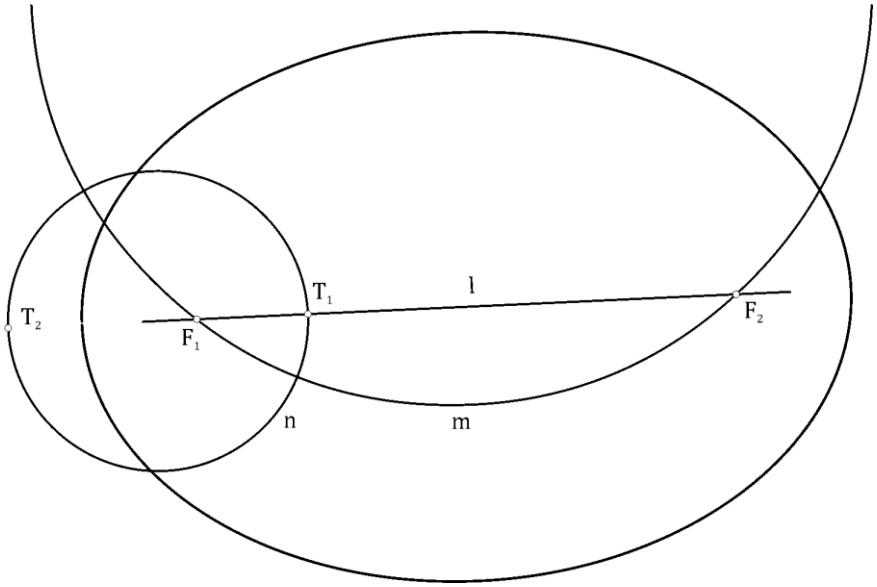


Рис. 2. Зависимость времени передачи от ширины полосы и уровня сигнала

Список используемых источников

1. Жижилкин И. Д. Инверсия. М.: Изд-во МЦНМО. 2009. 72 с.
2. Бакельман И. Я. Инверсия. М.: Наука. 1966. 79 с.
3. Адлер А. Теория геометрических построений. Л.: Учпедгиз. 1940. 232 с.
4. Клейн Ф. Высшая геометрия. Пер. с нем., М.: ОНТИ, 1939.
5. Глаголев Н. А. Проективная геометрия. М.: Высшая школа. 1963. 342 с.
6. Четверухин Н. Ф. Проективная геометрия. М.: Просвещение. 1953. 360 с.
7. Вольберг А. О. Основные идеи проективной геометрии. М.-Л.: Учпедгиз. 1949. 188 с.

BUYNEVICH-SHESTAKOV PRINCIPLE

Voloshinov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In modern geometry, it is generally accepted that the axes (principal directions) of curves of the second order are straight lines. However, if the axes of an ellipse have four real points in their intersection with this curve, then the axes of a hyperbola intersect it at two real and two imaginary points. Since curves of the second order are not distinguished from the point of view of projective geometry, the nature of the intersection points of the principal directions of these curves with the conics themselves must be uniform, which leads to a contradiction with the current state of affairs. This contradiction can be eliminated only if we understand the axes of conics not as straight lines, but as circles of a special kind - lines consisting of two branches: the currently known straight lines and an infinitely distant line - an improper line of the plane. The Buinevich-Shestakov principle considered in the report demonstrates a simple explanation of the phenomenon under consideration and establishes a constructive connection between the axes and foci of curves.

Key words: *inversion transformation, radical axis, second order curves, foci of conics*

УДК 004.273
ГРНТИ 20.15.05

«АРХИТЕКТУРА ИНФОРМАЦИОННЫХ СИСТЕМ» КАК МЕТОД БОРЬБЫ С ШАБЛОНАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В. В. Громов

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

В работе рассматриваются методика обучения студентов с помощью систем виртуальных машин при выполнении учебных заданий по дисциплине «Архитектура информационных систем» в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича.

Приведенная методика основана на многолетнем опыте формирования и эксплуатации Федеральной информационной системы Госавтоинспекции с 1996 по 2013 гг., опыте работы с Windows, Linux и UNIX системами, а так же с опытом эксплуатации российских операционных систем в период с 2013 по 2025 гг. Анализируются перспективы формирования навыков создания информационных систем студентов в условиях современного развития вычислительной техники.

системы виртуальных машин, программные системы, операционные системы

Шесть лет на кафедре информатики и компьютерного дизайна СПбГУТ ведется обучение студентов дисциплине «Архитектура информационных систем» (далее по тексту – АИС). Дисциплина основана на базе экспериментальных работ, проходивших в Москве и Санкт-Петербурге в период с 1996 по 2006 гг. при создании и вводе в промышленную эксплуатацию Федеральной информационной системы Госавтоинспекции России (далее по тексту ФИС ГИБДД). [1]

Курс представляет собой 13 лекционных занятий, в которых рассказывается методика построения корпоративных информационных систем.

Студентам предлагается в рамках курса создать макет корпоративной системы с использованием основных сетевых систем доступа, научиться администрировать Linux системы и объединять Windows и Linux клиентов в единую сеть.

Лабораторный практикум включает в себя 14 лабораторных работ, которые позволят сформировать следующие навыки:

– инсталляции, настройки и эксплуатации Linux/UNUX систем [2];
– создания скрипт-файлов на языке Shell [3];
– формирования сервисов WWW, FTP;
– инсталляции и администрирование сети SAMBA [4];

– конвертации и оптимизации данных для видео-аудио потоков, текстовой информации, фотографических снимков и графической информации;
– формирования дистрибутивов для инсталляции в открытых системах корпоративной информационной системы [5].

Основа курса – практические занятия, в которых студент изучает командную строку Linux, команды и методику их применения, ~~и~~ учится анализировать и подготавливать данные с использованием языка Shell [3].

В 2025 году было выпущено учебно-методическое пособие по дисциплине «Архитектура информационных систем», но данная мера была вынужденной, так как студенты не способны вести конспекты и записывать за преподавателем.

Неспособность вести элементарный конспект пагубно сказывается на последующей работе, формируя «специалиста», который не может творчески мыслить, но может только написать часть кода, не предусмотрев возможные варианты развития событий.

В прошлой работе автору требовалось предусмотреть возможные варианты развития событий и пути их разрешения в случае возникновения внештатных ситуаций.

Анализ и подготовка данных – основные умения при сопровождении любой информационной системы. К глубокому убеждению автора, данный вопрос упущен при обучении студентов работы с базами данных. Преподаватели упускают простейшие моменты, которые впоследствии оказывают воздействие на различные информационные системы.

В этом случае приходится возвращаться к азам дисциплины и на конкретных примерах из жизни объяснять, почему нужно сделать именно так, а не иначе.

В ходе ведения дисциплины было установлено:
– студенты не имеют авторитетов среди учебной литературы, единственный авторитет – «OK! Google»;
– большинство студентов закомплексовано и неспособно креативно мыслить;
– студенты не могут сформулировать логическую цепь рассуждений для формирования комплекса вопросов при решении поставленной задачи;
– повально применяют «искусственный интеллект» для решения поставленных преподавателем задач.

Искусственный интеллект (далее по тексту ИИ) или LLM (Lage Language Model) – большая языковая модель для машинного обучения, позволяющая генерировать ответы на поставленные задачи и вести диалог предугадывая ответы.

В своем обучении автор не разрешает использовать ИИ для подготовки отчетов и программного кода, объясняя это тем, что необходимо мыслить и развивать способности текущего обучения для последующей работы.

Многие студенты пытаются соблюдать необходимые требования, но большинство стараются использовать ИИ, чем читать рекомендованную учебную литературу.

Формально проверка домашнего задания сводится к сортировке работ и выявлению заимствований в программном коде и отчетах.

Современный преподаватель может определить наличие текста сгенерированного нейросетью за счет некоторых косвенных признаков, которые однозначно можно трактовать как искусственно сгенерированный текст. К таким признакам относятся:

– текст отчета, не содержащий стилистических ошибок;
– применение в программах только новых методов написания кода.

Для исключения возможности использования ИИ были сформированы задания для лабораторных работ, которые последовательно формируют навыки работы с системой из-под root, что вводит в некоторое замешательство ИИ.

Методы работы из-под root в Linux системах считаются устаревшими и неправильными, хотя четких рекомендаций, обоснованных в академической среде, не существует. Применение подобного метода позволило выявить студентов, использовавших ИИ для подготовки программного кода итоговой работы.

Следует отметить, что итоговая работа служит ориентиром для оценки за экзамен и является подготовительным процессом, позволяющим определить степень готовности студентов по дисциплине АИС.

Можно заметить, что использование нестандартного метода администрирования UNIX/Linux систем может неправильно сформировать навыки. Автор склонен не согласиться с данным доводом и заметить, что правильное и аккуратное использование прав суперпользователя способно исключить возможность взлома системы.

Работая в риск-зоне, студент формирует навыки соблюдения элементарных правил безопасности эксплуатации системы и формируют навыки критического мышления при эксплуатации системы.

Нейросеть в данном режиме работы не способна принять правильное решение и ошибается при выборе необходимого кода программы, подводя студента, выбравшего «легкий путь» реализации итогового задания.

Студенты, сформировавшие свой уникальный код, поощряются даже при наличии ошибок. Таким образом формируется итоговая оценка, которая позволяет поощрить талантливых студентов, а студентов, склонных к ба-

нальному списыванию, наказать. При этом формируется ощущение справедливости полученной оценки за экзамен.

Подведем небольшой вывод – нестандартные методы позволяют сформировать через ИИ неправильный код, в то время как индивидуально выполненное задание может содержать незначительные ошибки, которые можно пояснить студенту, что существенно сблизит студента и преподавателя и дать возможность студенту реализовать свои идеи самостоятельно и получить чувство уверенности при работе со сложными информационными системами.

Список используемых источников

1. Громов В. В. Информационные системы Госавтоинспекции России // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 250-253.

2. Gnu.org. Сайт сообщества. URL: https://www.gnu.org/ (дата обращения 30.07.2025).

3. Wikipedia. Сайт свободной энциклопедии. URL: https://en.wikipedia.org/wiki/Shell_script (дата обращения 30.07.2025);

4. Группа «Астра». Сайт корпорации. URL: https://astragroup.ru/training/authorized-training/section.php?SECTION_ID=1052 (дата обращения 30.07.2025).

5. Громов В. В. Архитектура Информационных систем. Учебно-методическое пособие по выполнению лабораторных работ. Санкт-Петербург, 2025.

THE REPORT DISCUSSES THE METHODOLOGY FOR TEACHING STUDENTS USING VIRTUAL MACHINE SYSTEMS WHEN PERFORMING EDUCATIONAL TASKS IN THE DISCIPLINE "INFORMATION SYSTEMS ARCHITECTURE"

.

Gromov V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The report discusses the methodology of teaching students using virtual machine systems when performing educational assignments in the discipline "Architecture of Information Systems" at the St. Petersburg State University of Telecommunications. prof. M.A. Bonch-Bruevich. The presented methodology is based on experience in operating UNIX/Linux from 1996 to 2013. The prospects for developing skills in creating information systems for students in the context of modern development of computer technology using short programming code are analyzed.

Key words: *virtual machine systems, software systems, operating systems*

УДК 004.273
ГРНТИ 20.15.05

GNU COBOL – «МЕРТВЫЙ ЯЗЫК» С БОЛЬШИМИ ВОЗМОЖНОСТЯМИ

В. В. Громов

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

В работе рассматривается методика обучения студентов с помощью систем виртуальных машин при выполнении учебных заданий по дисциплине «Архитектура информационных систем» в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича.

Приведенная методика основана на многолетнем опыте формирования и эксплуатации Федеральной информационной системы Госавтоинспекции с 1996 по 2013 гг., опыте работы с Windows, Linux и UNIX системами, а так же с опытом эксплуатации российских операционных систем в период с 2013 по 2025 гг. Анализируются перспективы формирования навыков создания информационных систем студентов в условиях современного развития вычислительной техники.

системы виртуальных машин, программные системы, операционные системы

На протяжении шести лет на кафедре информатики и компьютерного дизайна СПбГУТ ведется обучение студентов дисциплине «Архитектура информационных систем» (далее по тексту – АИС). Дисциплина основана на базе экспериментальных работ, проходивших в Москве и Санкт-Петербурге в период с 1996 по 2006 гг. при создании и вводе в промышленную эксплуатацию Федеральной информационной системы Госавтоинспекции России (далее по тексту ФИС ГИБДД) [1].

Но статья посвящена не ФИС ГИБДД, а языку программирования GNU Cobol, с которым ~~я~~ автор познакомился в 2023 году. Здесь необходимо сделать небольшое отступление.

Вернемся к ФИС ГИБДД и возьмем его основные компоненты:

– СУБД – “ADABAS C”;
– язык манипулирования данными – Natural;
– язык обработки и подготовки данных – REXX;
– операционные системы – OS/2 и Solaris ver. 9-10.

На данных компонентах была построена ФИС ГИБДД и работала вплоть до 2015 года. Необходимо отметить, что на OS/2 система работала до 2006 года. Эти компоненты явно раскрывают процесс модернизации системы и переход от CISC к RISC компьютерам при обработке данных. А данных было не мало – в 2013 году численность записей в БД достигла 500 000 000. На тот момент это было большое достижение [1].

Система отвечала на распределенные запросы в течение 25 секунд, направляя их в 11 межрегиональных центров обработки данных, которые хранили информацию по 10-12 регионам России.

Почему “ADABAS C”? Ответ простой – это надежная, высокопроизводительная СУБД, которая эксплуатируется в критически зависимых приложениях по всему миру. Сейчас в ФИС ГИБДД переключают на Postgres PRO и проблем с эксплуатацией стало значительно больше, чем в “ADABAS C”.

Несколько раз автор направлял запросы в поисковые системы по эксплуатации и жизненного цикла СУБД “ADABAS C” и получал интересные ответы, которые раскрывали суть выбора данной СУБД. Периодические статьи от Software AG показывали жизненный период востребованности базы данных вплоть до 2050 года. Почему Software AG и как оно относится к языку COBOL? Ответ не очевиден, но прост – язык Natural, который является языком манипулирования данных для СУБД “ADABAS C”, создан на базе языка COBOL. Разница в синтаксисе существенна, но не критична, но самое главное – переход от Natural к COBOL прост и логичен.

Студенту или преподавателю, который не работал с REXX, OS/2, COBOL, Solaris, “ADABAS C” и Natural, покажется этот набор продуктов ущербным и несовременным.

Несовременность выбора реализуется надежностью работы всех компонентов вместе и по отдельности включительно. Можно лишь привести пример, что на памяти автора существуют два примера эксплуатации систем без обслуживания более 10 лет и без аварий, и это связано с “ADABAS C”, COBOL и Natural. Подобные решения надежны с точки зрения эксплуатации, но в постгарантийном сопровождении становятся обременительны, т.к. количество специалистов, обладающих знаниями в данной сфере программирования, минимально.

Приведем некоторую статистику компании Rocket Software, которая занимается подготовкой специалистов по языку Visual Cobol. Она представлена на рисунке 1.

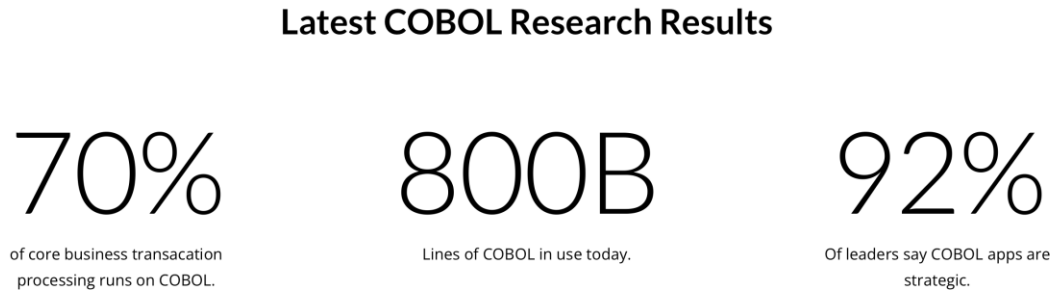


Рис. 1. Статистика по языку COBOL компании Rocket Software

Приведенная статистика показывает, что количество кода и количество бизнес-транзакций является лидирующим в банковской сфере создания прикладного программного обеспечения. Данные были подтверждены в российском портале «ХАБР» в статье «COBOL в XXI веке: почему банки и госслужбы не могут отказаться от языка 1959 года» [2].

Visual Cobol создан для применения новых технологий при обработке данных таких как JSON, XML, .NET, JVM.

Формально существуют следующие основные четыре реализации языка:

– GCC COBOL [3];
– GNU COBOL [3];
– IBM COBOL [3];
– Micro Focus International VisualCobol [4].

Формально представленные четыре диалекта перекрывают все возможные линейки операционных систем и архитектур компьютеров и позволяют создавать приложения с графическим интерфейсом для систем, использующих Windows и классическим терминальным интерфейсом для IBM System Z и UNIX/Linux систем.

В настоящее время мы работаем в рамках импортозамещения и пытаемся всей страной перейти с Windows на Linux (Astra, Alt, Red). Весь этот переход был сделан второпях и как всегда, получил массу негатива и неопределенностей. Возьмем СПбГУТ, где часть лабораторий работают под ОС Windows, часть – под Astra Linux и RedOS, а студенты – под Windows практически 99 % [5].

В таких условиях воспитать хорошего специалиста практически невозможно, т.к. отсутствует долговременная, перспективная программа развития IT-специалистов, которая должна начинаться в школе с азов программирования для развития логики работы в среде UNIX/Linux.

Логика перехода определяется его стоимостью и наличием необходимых компонентов. Идея написать эту статью возникла спонтанно, когда автором была написана программа «Зодиак». Указанная программа была написана в учебных целях для детей автора в качестве примера использования языка GNU COBOL.

Основой программы стала таблица знаков зодиака по китайскому календарю, представленная на рисунке 2.

Крыса	1912	1924	1936	1948	1960	1972	1984	1996	2008
Бык	1913	1925	1937	1949	1961	1973	1985	1997	2009
Тигр	1914	1926	1938	1950	1962	1974	1986	1998	2010
Кролик (Кот)	1915	1927	1939	1951	1963	1975	1987	1999	2011
Дракон	1916	1928	1940	1952	1964	1976	1988	2000	2012
Змея	1917	1929	1941	1953	1965	1977	1989	2001	2013
Лошадь	1918	1930	1942	1954	1966	1978	1990	2002	2014
Коза	1919	1931	1943	1955	1967	1979	1991	2003	2015
Обезьяна	1920	1932	1944	1956	1968	1980	1992	2004	2016
Петух	1921	1933	1945	1957	1969	1981	1993	2005	2017
Собака	1922	1934	1946	1958	1970	1982	1994	2006	2018
Свинья	1923	1935	1947	1959	1971	1983	1995	2007	2019

Рис. 2. Таблица знаков зодиака по китайскому календарю

Написание программы по данным в таблице не составила труда, но следом последовала другая идея – а почему бы не узнать знак зодиака после 2019 года или от самого рождества Христова?

Идея, конечно, не нова. Затея узнать, в каком году ты родился или родилась какая-либо историческая личность, с точки зрения практичности бесполезна, но с точки зрения алгоритмизации – упражнение не из простых за-

дач для первокурсников, особенно не создававших блок схемы и не программировавших на таких языках как C, Pascal, Fortran, BASIC и COBOL.

Написание программы заняло несколько часов, самое ответственное – выбор точки отсчета для определения коэффициентов различных годов.

На протяжении более чем 12 лет автору приходится пояснять студентам, что если двум программистам дать одно и тоже задание и рассадить их по разным комнатам, то они напишут разный код. Так было и в этом случае. Для написания автор использовал циклы и коэффициенты, а сын автора – массивы, используя язык Swift.

Закончилось противостояние COBOL и Swift формально ничьей, но «мертвый» язык выявил одно неоспоримое преимущество, о котором необходимо поговорить.

Преимущество заключается в выборе типа данных, которое позволяет экономить на операциях, что естественно сказывается на скорости вычисления. Примером может служить необходимость вычисления модуля числа, когда следует вводить условие для проверки или же вводить дополнительные действия, а в таком древнем языке, как COBOL, нужно просто правильно определить переменную и можно вычитать из меньшего бОльшее число, получив в ответе положительный результат по модулю.

Учитывая зарубежные результаты и то, что нам придется использовать Linux для программы импортозамещения, использование GNU COBOL видится как перспективное направление обучения студентов для создания бинарных модулей, что необходимо для исключения возможности взлома программного кода в случае использования программ, требующих интерпретаторы.

Список используемых источников

1. Громов В. В. Информационные системы Госавтоинспекции России // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 250-253.

2. habr.com. Сайт издания. URL: https://habr.com/ru/companies/ruvds/articles/918156/ (дата обращения 30.07.2025).

3. Wikipedia. Сайт свободной энциклопедии. URL: https://ru.wikipedia.org/wiki/%D0 %9A %D0 %BE %D0 %B1 %D0 %BE %D0 %BB (дата обращения 30.07.2025);

4. Rosket Software. Сайт компании для обучения по программе Visio COBOL https://www.rocketsoftware.com/en-us/products/cobol/visual-cobol-personal-edition (дата обращения 30.07.2025).

5. Группа «Астра». Сайт корпорации. URL: https://astragroup.ru/training/authorized-training/section.php?SECTION_ID=1052 (дата обращения 30.07.2025).

GNU COBOL – A "DEAD LANGUAGE" WITH GREAT CAPABILITIES

Gromov V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This paper examines a methodology for teaching students using virtual machine systems when completing assignments in the "Information Systems Architecture" course at the Saint Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich. This methodology is based on many years of experience in developing and operating the Federal Information System of the State Traffic Safety Inspectorate from 1996 to 2013, experience working with Windows, Linux, and UNIX systems, as well as experience operating Russian operating systems from 2013 to 2025. The paper analyzes the prospects for developing students' information system creation skills in the context of modern computing technology development.

Key words: *Virtual machine systems, software systems, operating systems*

УДК 004.81
ГРНТИ 28.23.37

ИССЛЕДОВАНИЕ МЕТОДОВ РАСПОЗНАВАНИЯ ЗЕЛЕНЫХ ЗОН ГОРОДСКОЙ ИНФРАСТРУКТУРЫ ПО АЭРОФОТОСНИМКАМ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

Исследованы методы обнаружения и сегментации зеленых зон на городских аэрофотоснимках. Проведен анализ требований с учетом особенностей зеленых зон в городской среде. Изучены существующие методы сегментации изображений в геоинформационных технологиях. Разработана методика обработки аэрофотоснимков и выделения зеленых зон на них. Предложен прототип геоинформационного приложения для автоматической сегментации зеленых зон на аэрофотоснимках. Практическая значимость результатов заключается в том, что предложенное геоинформационное приложение позволит автоматизировать процесс обнаружения и сегментации зеленых зон на городских аэрофотоснимках. Это значительно упростит работу городских планировщиков.

сегментация изображений, аэрофотоснимок, зеленые зоны городской инфраструктуры

Эффективное проектирование городского озеленения требует комплексного анализа существующих насаждений, оценки их состояния и разработки рекомендаций по уходу за ними. Однако, в настоящее время в России отсутствует единое автоматизированное программное обеспечение, специализирующееся на планировании систем озеленения городов, что затрудняет процесс принятия решений и управления зелеными зонами.

Существующие методы управления зелеными насаждениями в городах часто ограничены и не обеспечивают достаточно эффективного анализа и управления. Традиционные подходы, такие как ручная инвентаризация и анализ картографических данных, могут быть трудоемкими, неэффективными и подвержены ошибкам.

В работе проведен анализ существующих нейросетевых архитектур и определены наиболее эффективные для решения поставленной задачи. Для более точного обнаружения и подсчета деревьев выбрана готовая модель DeepForest [1]. Эта модель обучена на данных Национальной экологической обсерватории (NEON) с использованием полуконтролируемого подхода. Исходно модель была предварительно обучена на данных с 22 сайтов NEON с использованием алгоритма LiDAR (технология дистанционного зондирования, которая использует лазерные импульсы для измерения расстояний до

объектов и создания 3D-карт). Эту модель можно использовать для прогнозирования новых данных или как основу для переобучения на новых данных. Пример работы модели DeepForest показан на рис. 1.

Рис. 1. Результат работы DeepForest на аэрофотоснимке

После прогона через модель файла с изображением получим csv файл. Каждая аннотация выделенной области возвращается со своими координатами x_{min}, y_{min}, x_{max}, y_{max} и прогнозируемой вероятностью (рис. 2). Чтобы уменьшить избыточный подсчет перекрывающихся фрагментов, DeepForest сортирует прогнозы по показателям достоверности и удаляет блоки перекрытия с более низкой оценкой. Далее csv файл преобразуется в векторный файл shp для хранения в БД и наложения на карту.

A	B	C	D	E	F	G	H
	xmin	ymin	xmax	ymax	label	score	image_path
0	1694	6179	1827	6313	Tree	0.931897819	tif-0-0.tif
1	13304	2289	13403	2382	Tree	0.9273607731	tif-0-0.tif
2	5887	2819	6018	2947	Tree	0.9174414873	tif-0-0.tif
3	33090	2599	33202	2713	Tree	0.9149394035	tif-0-0.tif
4	23434	6590	23589	6747	Tree	0.9133126736	tif-0-0.tif
5	34179	9515	34294	9619	Tree	0.9096582532	tif-0-0.tif
6	4352	5506	4481	5624	Tree	0.9026683569	tif-0-0.tif
7	13387	9635	13511	9751	Tree	0.902451694	tif-0-0.tif
8	13631	2539	13747	2644	Tree	0.9020348191	tif-0-0.tif
9	13812	2903	13941	3034	Tree	0.9009684324	tif-0-0.tif
10	25140	6067	25257	6196	Tree	0.8995236158	tif-0-0.tif
11	12672	9590	12780	9687	Tree	0.8991969228	tif-0-0.tif
12	853	8640	995	8766	Tree	0.8954501152	tif-0-0.tif
13	1013	4063	1127	4160	Tree	0.894536376	tif-0-0.tif
14	34446	9242	34568	9353	Tree	0.8913664818	tif-0-0.tif
15	22686	7775	22810	7891	Tree	0.8910267353	tif-0-0.tif
16	11908	3281	11972	3344	Tree	0.8903765678	tif-0-0.tif
17	17599	3540	17707	3667	Tree	0.8898863196	tif-0-0.tif
18	23642	6796	23762	6912	Tree	0.889362514	tif-0-0.tif
19	30171	2301	30304	2433	Tree	0.8884024024	tif-0-0.tif
20	27407	2570	27518	2681	Tree	0.887788415	tif-0-0.tif
21	17280	4510	17378	4617	Tree	0.8869450092	tif-0-0.tif
22	6248	2918	6356	3033	Tree	0.8864231706	tif-0-0.tif
23	13209	3360	13357	3497	Tree	0.8860731721	tif-0-0.tif
24	13861	5006	13989	5127	Tree	0.8857985735	tif-0-0.tif
25	33318	8908	33428	9028	Tree	0.8854289651	tif-0-0.tif

Рис. 2. Результаты в виде csv файла

Для сегментации изображения в работе выбрана модель SegFormer. Сегментация изображения – это процесс классификации каждого пикселя изображения. Это задача компьютерного зрения, предназначенная в основном для обнаружения областей на изображении с заданным объектом.

SegFormer – нейронная сеть, полностью основанная на трансформерах [2]. Трансформеры (Transformers) известны своим механизмом внимания, который ускоряет процесс обучения и позволяет модели учитывать контекст в данных. Эта особенность позволяет SegFormer выполнять параллельную обработку данных и эффективно использовать контекстную информацию. Архитектура модели представлена на рис. 3 и 4.

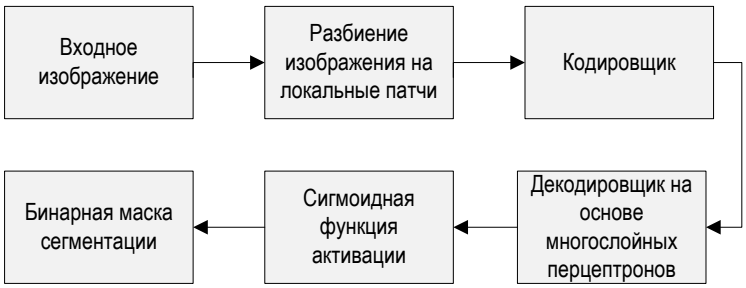


Рис.3. Архитектура SegFormer

Архитектура SegFormer включает в себя кодировщик и декодировщик. Кодировщик извлекает признаки из входного изображения, используя блок разбиения на патчи и несколько блоков-трансформеров. Блок разбиения на патчи делит изображение на патчи размером 4×4 пикселя и передает их на вход блокам-трансформерам. Декодер объединяет многоуровневые признаки для прогнозирования маски сегментации.

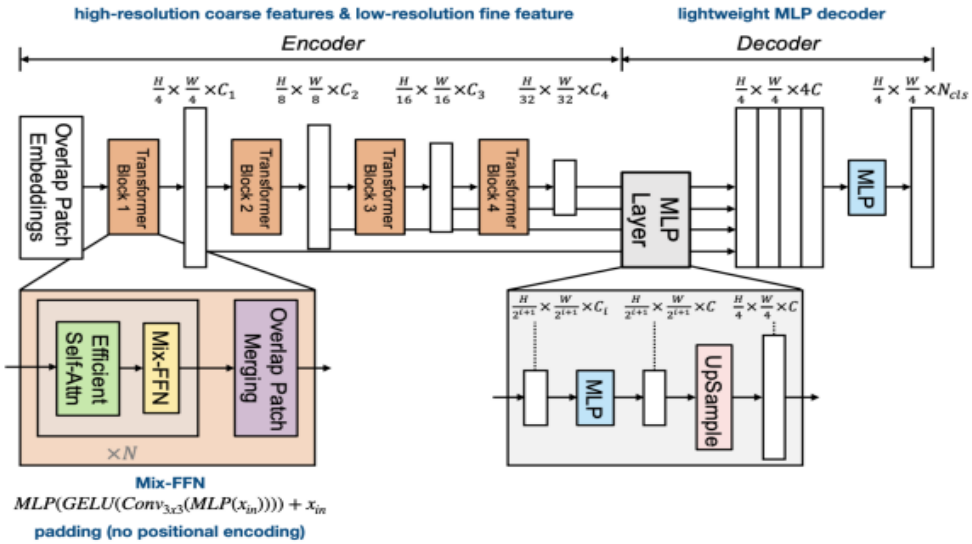


Рис. 4. Архитектура SegFormer, продолжение

На рис.5 показан график точности модели на обучающем наборе данных.

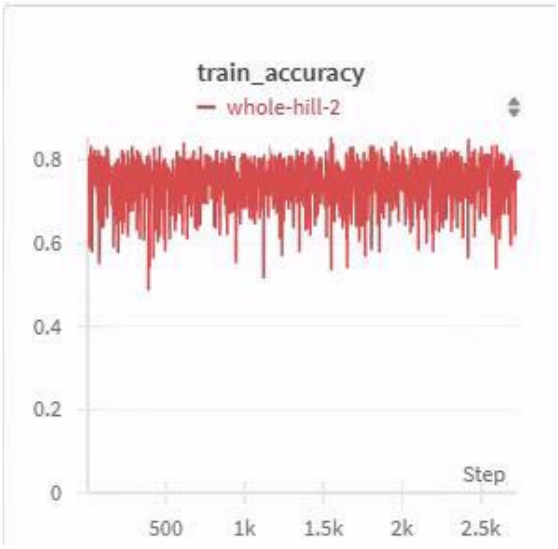


Рис. 5. Точность на обучении

Таким образом, в результате обработки изображения получим два типа файлов: векторные файлы формата Shapefile с метками деревьев и растровые GeoTIFF слои, представляющие местность и маски зеленых зон.

GeoTIFF представляет собой открытый формат, который используется для представления растровых данных в формате TIFF вместе с метаданными о географической привязке, что делает его георефернцированным растром.

Формат "Shape-файл" представляет собой векторный формат для хранения различных типов геометрических объектов, таких как точки, линии, многоугольники и другие. Каждый "Shape-файл" может содержать объекты только одного типа.

Для реализации прототипа геоинформационного приложения выбрана СУБД PostgreSQL с надстройкой PostGIS [3].

Дополнительный модуль PostGIS расширяет возможности PostgreSQL, позволяя, кроме основной, хранить также и пространственную информацию. Кроме того, PostGIS является программным модулем с открытым исходным кодом и предоставляет широкий набор функций для обработки пространственных данных, таких как выполнение пространственных запросов, применение пространственных индексов и т.п.

В качестве веб-сервера выбран GeoServer [4], что обусловлено следующими причинами: возможность стилизации слоев, наличие интерфейса для работы с управлением проекциями, поддержка большого числа растровых и

векторных форматов данных, возможность получения данных из PostGIS, полностью открытый бесплатный компилируемый код на Java.

Пример работы готового приложения показан на рис. 6. Показано, что получается список всех объектов векторного слоя, находящихся внутри выделенной области, и выводится информация о количестве этих объектов.

Рис. 6. Пример работы приложения

Итак, создание цельной геоинформационной системы для управления городскими зелеными насаждениями – важный элемент в формировании комфортной современной городской среды. Внедрение автоматизированных инструментов на базе нейросетевых технологий повысит эффективность планирования и анализа зеленых зон городской инфраструктуры.

Список используемых источников

1. DeepForest documentation. URL: https://deepforest.readthedocs.io/en/v1.5.0/. (дата обращения 11.08.2025).

2. SegFormer: Simple and Efficient Design for Semantic Segmentation with Transformers. URL: https://arxiv.org/abs/2105.15203 (дата обращения 11.08.2025).

3. PostGis documentation. URL: https://postgis.net/ (дата обращения 11.08.2025).

4. GeoServer. URL: https://geoserver.org/ (дата обращения 11.08.2025).

INVESTIGATION OF METHODS FOR RECOGNIZING GREEN AREAS OF URBAN INFRASTRUCTURE FROM AERIAL PHOTOGRAPHS

Gubin A., Litvinov V., Filippov F.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Methods of detection and segmentation of green areas in urban aerial photographs are investigated. The requirements were analyzed taking into account the peculiarities of green areas in the urban environment. The existing methods of image segmentation in geoinformation technologies are studied. A technique has been developed for processing aerial photographs and highlighting green areas on them. A prototype of a geoinformation application for automatic segmentation of green areas in aerial photography is proposed. The practical significance of the results lies in the fact that the proposed geoinformation application will automate the process of detecting and segmenting green areas in urban aerial photographs. This will greatly simplify the work of city planners.

Key words: *image segmentation, aerial photography, green areas of urban infrastructure*

УДК 004.81
ГРНТИ 28.23.37

МЕТОДЫ ВЫЯВЛЕНИЯ КОНФАБУЛЯЦИЙ В ПРОЦЕССЕ ИНФЕРЕНСА БОЛЬШИХ ЯЗЫКОВЫХ МОДЕЛЕЙ

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

Выявление факта генерации ложного контента большими языковыми моделями (LLM) в процессе инференса является критически важным практически для всех областей их применения. В работе исследуется феномен «галлюцинаций» в LLM и методы их обнаружения. Приводится краткий сравнительный анализ различных подходов. Будущие исследования могут сосредоточиться на интеграции методов обнаружения конфабуляций в рабочие процессы LLM. Это особенно важно для областей, требующих высокой точности и надежности, таких как медицина, юриспруденция и финансы.

инференс LLM, конфабуляция, метрики несогласованности, метаморфические отношения, мутации промптов, многоформенные знания, агрегация

Введение

Большие языковые модели демонстрируют впечатляющие возможности в обработке и генерации текста, однако они подвержены "галлюцинациям" – генерации ложного, противоречивого или необоснованного содержания. Человеческая ложь – это намеренное искажение истины для введения в заблуждение. Когда мы говорим о «лжи» LLM, то их генерация, производит аналогичный эффект, что и человеческая ложь, но порождается совершенно иными механизмами. В [1] для описания подобного поведения языковых моделей используется термин – конфабуляция (confabulation). В человеческой психологии конфабуляция происходит, когда в памяти человека есть пробел, и мозг убедительно заполняет остаток, не намереваясь обманывать других. LLM работает не так, как человеческий мозг, но термин «конфабуляция», служит лучшей метафорой, потому что здесь также работает «творческий» принцип заполнения пробелов.

Данное исследование представляет современные методы обнаружения конфабуляций в LLM, от базовых подходов до новейших исследовательских разработок.

Феномен конфабуляций в LLM

Конфабуляции в контексте LLM определяются как "сгенерированный контент, который не соответствует оригинальному предоставленному материалу и не имеет логической ценности" [2]. Исследователи классифицируют конфабуляции на две основные категории: конфабуляции достоверности, когда модель отклоняется от предоставленных инструкций, и фактические конфабуляции, когда существует несоответствие между генерируемым содержанием и проверяемыми фактами [3].

Конфабуляции в LLM возникают по нескольким причинам. Среди них – качество и полнота обучающих данных, которые могут быть неполными или противоречивыми [2]. Кроме того, проблемы переобучения, ошибки в процессах кодирования и декодирования, а также предвзятость обучающих данных существенно влияют на склонность модели к генерации недостоверной информации [4]. Сложная архитектура LLM затрудняет для исследователей выявление и исправление этих базовых причин.

Выявление конфабуляций является критически важным для множества областей применения LLM. Исследователи отмечают, что необоснованные ответы могут препятствовать внедрению этих технологий в медицине, юриспруденции, журналистике и других чувствительных сферах [5]. Достоверность ответов LLM становится особенно важной, когда модели используются для принятия решений, требующих высокой точности и надежности [6].

Методы выявления конфабуляций

Одним из перспективных подходов является использование статистических методов, основанных на оценке энтропии и неопределенности модели. Исследователи из Nature в 2024 году предложили новые методы, основанные на статистике, предлагающие оценки неопределенности на основе энтропии для LLM [5]. Эти методы решают проблему того, что одну и ту же идею можно выразить по-разному, вычисляя неопределенность на уровне смысла, а не конкретных последовательностей слов.

Другой подход использует ансамбли моделей для более эффективного обнаружения конфабуляций. Исследование, представленное в 2023 году, описывает новый метод, который позволяет быстро и эффективно по памяти обучать ансамбли LLM [3]. Авторы демонстрируют, что полученные ансамбли могут обнаруживать конфабуляции и являются жизнеспособным под-

ходом на практике, поскольку для обучения и вывода требуется только один GPU.

Один из самых известных методов обнаружения конфабуляций – SelfCheckGPT, который представляет собой подход, основанный на выборке, который может обнаружить, являются ли ответы, сгенерированные LLM, конфабуляциями или реальными фактами [7]. Основная идея заключается в том, что, когда LLM обучена определенной концепции, сгенерированные ответы, вероятно, будут похожи и будут содержать согласованные факты. Однако, для галлюцинирующих фактов стохастически выбранные ответы, вероятно, будут расходиться и могут противоречить друг другу.

Развитием идеи SelfCheckGPT стал SelfCheckGPT NLI – метрика, измеряющая несогласованности LLM для предсказания галлюцинирующих выходных данных. Исследователи сообщают, что этот индикатор очень точен после определенного порога, то есть любая отмеченная конфабуляция на самом деле является конфабуляцией [6]. Кроме того, уровень обнаружения (recall) хорошо откалиброван с оценкой SelfCheckGPT. Оценка SelfCheckGPT NLI 0,8 соответствует почти 80 % выявленных конфабуляций.

Подход под названием "Grounded in Context" основан на архитектуре RAG (Retrieval-Augmented Generation) и интегрирует извлечение и модели Natural Language Inference (NLI) для прогнозирования фактической согласованности между посылками и гипотезами [8]. Этот метод особенно эффективен для обнаружения необоснованных утверждений, достигая F1-оценки 0,83 в задаче классификации на уровне ответов RAGTruth.

Для промышленных приложений RAG разработан двухуровневый подход на основе энкодеров. Исследователи обнаружили, что предложенные модели превосходят существующие методы и подчеркивают ценность сочетания небольшого количества внутридоменных данных с общедоступными наборами данных [9]. Этот подход особенно ценен для систем обслуживания клиентов, где необходимо обрабатывать как фактические утверждения, так и нефактические элементы, такие как светская беседа или вопросы.

Инновационный подход, представленный в феврале 2025 года, использует метаморфические отношения для обнаружения конфабуляций. MetaQA – это автономный подход к обнаружению конфабуляций, использующий метаморфические отношения и мутации промптов [10]. В отличие от существующих методов, MetaQA работает без внешних ресурсов и совместим

как с открытыми, так и с закрытыми LLM. Метод основан на гипотезе, что "если ответ LLM является конфабуляцией, то разработанные метаморфические отношения будут нарушены".

Исследователи из Университета Иллинойса Урбана-Шампейн представили фреймворк Knowhalu для обнаружения конфабуляций в тексте, генерируемом LLM [11]. Этот фреймворк включает многоэтапный процесс, начинающийся с "проверки конфабуляции без лечения", а затем переходящий к комплексной "фактической проверке", состоящей из пяти шагов: пошаговые рассуждения и запрос, поиск знаний, оптимизация знаний, суждение на основе многоформенных знаний и агрегация.

Сравнительный анализ методов обнаружения конфабуляций

Сравнительный анализ различных методов показывает, что подходы на основе метаморфических отношений, такие как MetaQA, превосходят другие методы обнаружения конфабуляций. Например, MetaQA превосходит SelfCheckGPT с преимуществом от 0,041 до 0,113 (по точности), от 0,143 до 0,430 (по полноте) и от 0,154 до 0,368 (по F1-оценке) [10]. Для модели Mistral-7B MetaQA достигает средней F1-оценки 0,435 по сравнению с F1-оценкой SelfCheckGPT 0,205, что представляет собой улучшение на 112,2 % [10].

Исследователи из NannyML делят методы обнаружения конфабуляций LLM на две категории: методы на основе LLM и методы на основе неопределенности [12]. Методы на основе LLM используют LLM для оценки выходного ответа другой LLM, измеряя согласованность сгенерированного выхода или запрашивая LLM оценить сгенерированный выход по произвольной шкале. Методы на основе неопределенности используют понятие неопределенности для оценки качества ответа LLM.

Заключение

Будущие исследования могут сосредоточиться на интеграции методов обнаружения конфабуляций в рабочие процессы LLM. Разработка систем, которые могут автоматически обнаруживать и корректировать конфабуляции, может значительно повысить доверие к LLM в критически важных приложениях. Дальнейшие исследования также могут сосредоточиться на повышении эффективности и масштабируемости методов обнаружения конфабуляций. Это включает в себя разработку методов, которые работают с

ограниченными вычислительными ресурсами и могут масштабироваться до больших объемов данных. Например, исследователи уже демонстрируют, что их методы обнаружения чрезвычайно эффективны с точки зрения вычислений, с ускорением до 45x и 450x по сравнению с другими базовыми линиями [13].

Обнаружение конфабуляций в больших языковых моделях остается активной областью исследований с множеством перспективных подходов от статистических методов, основанных на энтропии, до подходов, использующих метаморфические отношения. Эти усилия имеют решающее значение для безопасного и эффективного применения LLM в различных областях, особенно тех, где фактическая точность является первостепенной. По мере развития исследований в этой области мы можем ожидать дальнейших инноваций, которые сделают LLM более надежными и заслуживающими доверия инструментами для широкого спектра применений.

Список используемых источников

1. Timmer J. Researchers describe how to tell if ChatGPT is confabulating. URL: https://arstechnica.com/ai/2024/06/researchers-describe-how-to-tell-if-chatgpt-is-confabulating/ (дата обращения 17.07.2025).

2. Как обнаружить галлюцинации в LLM? URL: https://habr.com/ru/companies/bothub/articles/805047/ (дата обращения 17.07.2025).

3. Arteaga G. Y., Schön T. B. Hallucination Detection in LLMs: Fast and Memory-Efficient Finetuned Models. URL: https://arxiv.org/html/2409.02976v1 (дата обращения 17.07.2025).

4. Саджид Х. Искусственный интеллект. Что такое LLM-галлюцинации? Причины, этическая проблема и профилактика. URL: https://www.unite.ai/ru/what-are-llm-hallucinations-causes-ethical-concern-prevention/ (дата обращения 17.07.2025).

5. Farquhar S., Kossen J., Kuhn L., Gal1 Y. Detecting hallucinations in large language models using semantic entropy. URL: https://www.nature.com/articles/s41586-024-07421-0 (дата обращения 17.07.2025).

6. Huynh D. Automatic Hallucination detection with SelfCheckGPT NLI. URL: https://huggingface.co/blog/dhuynh95/automatic-hallucination-detection (дата обращения 17.07.2025).

7. Manakul P., Liusie A., Gales M.J.F. SelfCheckGPT: Zero-Resource Black-Box Hallucination Detection for Generative Large Language Models. URL: https://aclanthology.org/anthology-files/anthology-files/pdf/emnlp/2023.emnlp-main.557.pdf (дата обращения 17.07.2025).

9. Gerner A., Madvil N. et all. Grounded in Context: Retrieval-Based Method for Hallucination Detection. URL: https://arxiv.org/abs/2504.15771 (дата обращения 17.07.2025).

10. Zimmerman I., Tredup J., Selfridge E., Bradley J. Two-tiered Encoder-based Hallucination Detection for Retrieval-Augmented Generation in the Wild. URL: https://aclanthology.org/2024.emnlp-industry.2/ (дата обращения 17.07.2025).

11. Yang B., Mamun M.A.A., Zhang J.M., Uddin G. Hallucination Detection in Large Language Models with Metamorphic Relations. URL: https://arxiv.org/abs/2502.15844 (дата обращения 17.07.2025).

12. Víquez S. Can we detect LLM hallucinations? – A quick review of our experiments. https://www.nannyml.com/blog/llm-hallucination-detection (дата обращения 17.07.2025).

13. Sriramanan G., Bharti S. at all. LLM-Check: Investigating Detection of Hallucinations in Large Language Models. URL: https://openreview.net/ pdf?id=LYx4w3CAgy. (дата обращения 17.07.2025).

METHODS FOR DETECTING CONFABULATIONS IN THE PROCESS OF INFERENCE OF LARGE LANGUAGE MODELS

Gubin A., Litvinov V., Filippov F.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Identifying the fact that large language models (LLM) generate false content in the inference process is critically important for almost all areas of their application. The paper examines the phenomenon of "hallucinations" in LLM and the methods of their detection. A brief comparative analysis of different approaches is provided. Future research may focus on integrating confabulation detection techniques into LLM workflows. This is especially important for areas requiring high accuracy and reliability, such as medicine, law, and finance.

Key words: *LLM inference, confabulation, metrics of inconsistency, metamorphic relationships, mutations of products, multiform knowledge, aggregation*

УДК 004.81
ГРНТИ 28.23.37

ОПРЕДЕЛЕНИЕ РАЗМЕРНОСТИ ЛАТЕНТНОГО СЛОЯ АВТОЭНКОДЕРА НА ОСНОВЕ ОЦЕНКИ ДИВЕРГЕНЦИИ КУЛЬБАКА-ЛЕЙБЛЕРА

А. Н. Губин, В. Л. Литвинов, Ф. В. Филиппов

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

В статье рассматриваются проблемы выбора размерности латентного пространства автоэнкодера, которая является ключевым параметром, влияющим на качество представления данных и эффективность функционирования устройства. Основное внимание уделяется использованию дивергенции Кульбака-Лейблера (KL-дивергенции) как критерия для оценки соответствия распределения скрытых признаков заданным априорным распределениям обрабатываемого сигнала. Анализируются методы, позволяющие на основании значений KL- дивергенции выявлять баланс между переобучением и потерей информативности скрытых представлений.

автоэнкодер, латентный слой, дивергенция Кульбака-Лейблера

Автоэнкодеры представляют собой достаточно мощный инструмент в области машинного обучения и обработки данных, предназначенный для эффективного представления и преобразования данных. Основная задача автоэнкодера заключается в сжатии входных данных в компактное латентное представление, а затем в восстановлении исходных данных из этого представления.

В статье рассматривается задача оценки дивергенции Кульбака-Лейблера (KL-дивергенция) между распределениями входного и выходного сигналов автоэнкодера. Для исследований предложено использовать энтропийную модель автоэнкодера. Полученная оценка KL-дивергенции может быть использована для определения влияния количества разрядов m в латентном слое автоэнкодера на степень различия между входным сигналом x и выходным сигналом y.

Автоэнкодеры состоят из двух основных компонентов: кодера и декодера. Кодер преобразует входные данные x в латентное представление z, а декодер восстанавливает данные из этого представления, создавая выходной сигнал y. Формально, один из вариантов использования автоэнкодера можно представить в виде следующей модели (рис. 1).

Поскольку одним из основных критериев работы автоэнкодера является отличие распределения входных сигналов от распределения выходных сигналов, которое определяется значением *KL*-дивергенции и полностью определяется энтропийными характеристиками сигналов, то целесообразно использовать при решении рассматриваемой задачи энтропийную модель автоэнкодера.

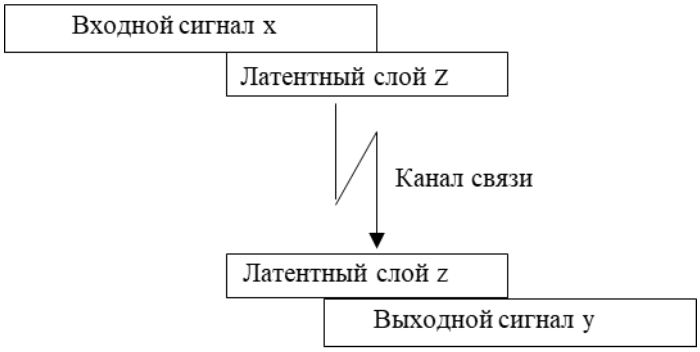


Рис. 1. Использование автоэнкодера

Если допустить, что канал связи не вносит в передаваемый сигнал никаких искажений, то энтропийную модель автоэнкодера можно представить в следующем виде (рис. 2).

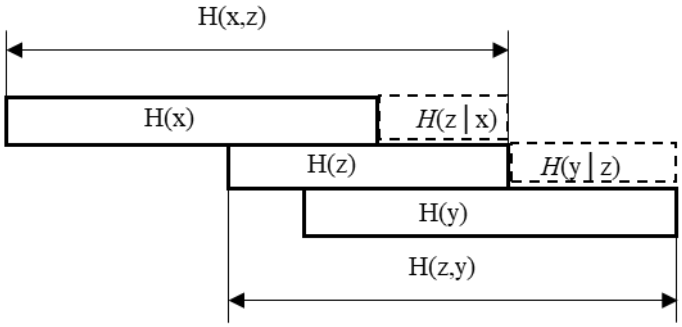


Рис. 2. Энтропийная модель автоэнкодера

На рис. 2 $H(x)$, $H(z)$, $H(y)$ – энтропийные оценки распределения входного, латентного и выходного сигналов; $H(x,z)$ и $H(z,y)$ – перекрестные, а $H(z \mid x)$ и $H(y \mid z)$ – условные энтропии распределений соответствующих сигналов.

Рассматривая указанную модель, необходимо определить степень различия между распределениями входного x и выходного y сигналов. Для оценки использовать соответствующие значения дивергенции Кульбака-Лейблера [1]:

$$D_{KL}(X \parallel Y) = \sum_{i=1}^{n} p(x_i)\, log\left(\frac{p(x_i)}{q(y_i)}\right),$$

где $p(x_i)$ – распределение входных данных, а $q(y_i)$ – распределение выходных данных.

Кроме того, необходимо оценить влияние размера m латентного слоя z на величину дивергенции Кульбака-Лейблера.

Использование энтропийной модели автоэнкодера обосновывается тем, что эта модель достаточно подробно отражает связи KL-дивергенции с кросс-энтропией распределения сигналов, обрабатываемых автоэнкодером, это обстоятельство позволяет использовать указанные характеристики для оценки информационных потерь при реконструкции сигналов.

Исходя из предложенной модели, можно определить

$$D_{KL}(X \parallel Y) = H(X,Y) - H(X)\,,$$

где

$$H(X,Y) = -\sum_{i=1}^{n} p(x_i) log\,(\,q(y_i)$$

представляет собой кросс-энтропию (перекрестную энтропию) входного и выходного сигналов, а

$$H(X) = -\sum_{i=1}^{n} p(x_i) log\,(\,p(x_i) -$$

энтропийную характеристику входного сигнала.

Определение энтропийных характеристик сигналов x, z, y, а также совместных энтропий $H(X,Z)$ и $H(Z,Y)$ не вызывает затруднений, а получить выражение для $H(X, Y)$, пользуясь только указанными выше характеристиками, не представляется возможным. Однако, если предположить, что x, z, y, являясь случайными сигналами, представляют собой марковскую цепочку $x \rightarrow z \rightarrow y$, то это означает, что выход Y зависит от входа X только через латентный слой Z. Это латентное представление обладает меньшей размерностью, чем X, следовательно, знание Z определяет меньше информации об Y, чем знание сигнала X и таким образом, можно записать:

$$H(Y|X) \leq H(Y|Z).$$

Согласно свойствам энтропии и условной энтропии, определим

$$H(X,Y) = H(X,Z,Y) + H(Z|X,Y) \text{ или } H(X,Y) = H(X) + H(Y|X).$$

Преобразуем последнее выражение с учетом полученного ранее неравенства:

$$H(X,Y) \approx H(X) + H(Y|Z).$$

Далее, определим:

$$H(Y|Z) = H(Z,Y) - H(Z),$$

и учитывая, что

$$H(X) = H(X,Z) - H(Z)$$

получим

$$H(X,Y) = H(X,Z) - H(Z) + H(Z,Y) - H(Z).$$

С учетом формулы включения-исключения для энтропий, окончательно определим

$$H(X,Y) = H(X,Z) + H(Z,Y) - H(Z).$$

Кросс-энтропия $H(X,Y)$ связана с KL-дивергенцией $D_{KL}(X \parallel Y)$:

$$H(X,Y) = H(X) + D_{KL}(X \parallel Y).$$

Используя это выражение и аналогичные для $H(X,Z)$ и $H(Z,Y)$:

$$H(X) + D_{KL}(X \parallel Y) = [H(X) + D_{KL}(X \parallel Z)] + [H(Z) + D_{KL}(X \parallel Y)] - H(Z)$$

и далее

$$D_{KL}(X \parallel Y) = D_{KL}(X \parallel Z) + D_{KL}(Z \parallel Y).$$

Полученное выражение для вычисления *KL*-дивергенции между распределениями входного и выходного сигналов автоэнкодера может быть использовано для оценки качества работы автоэнкодеров.

Оценка влияния размерности *m* латентного слоя автоэнкодера на величину *KL*-дивергенции между распределениями входного *x* и выходного *y* сигналами.

Оценка количественного влияния размерности латентного слоя *m* на величину *KL*-дивергенции между распределениями входного *x* и выходного *y* сигналов является достаточно сложной задачей, поскольку указанная зависимость определяется влиянием большого количества факторов, включая архитектуру модели, данные и способы обучения и др. Однако, рассматри-

вая результаты вычислительных экспериментов, можно выделить некоторые общие тенденции изменения *KL*-дивергенции в зависимости от значений *m*.

При фиксированной размерности входного сигнала *n* уменьшение размерности латентного слоя *m* ведет к возрастанию *KL*-дивергенции из-за потери информации.

– При *m* =*n* или больше *KL*-дивергенция минимальна, но риски переобучения и избыточной размерности возрастают.
– Оптимальный размер *m* лежит в компромиссной зоне, позволяющей балансировать между сжатием данных и качеством восстановления.

Для простых наборов входных данных, таких как *MNIST* размерностью *n* = 784 (28×28), размерность латентного слоя может варьироваться от 2 до 100 [2, 3, 4]. При этом значение *KL*-дивергенции и точность восстановления данных изменяется в соответствие со значениями, приведенными в таблице.

ТАБЛИЦА 1. Зависимость значений *KL*-дивергенции и ошибки восстановления данных от размерности *z* латентного слоя

m (размерность *z*)	Значение *KL*-дивергенции	Ошибка восстановления (*MSE*)
2	25,4	0,12
10	17,3	0,08
50	10,7	0,05
100	11,5	0,06

Из примера видно, что при росте *m KL*-дивергенция уменьшается, как и ошибка восстановления, но при очень большом *m* может наступить незначительный рост *KL*-дивергенции из-за эффекта переобучения.

Основные рекомендации по подбору размерности *m* латентного слоя автоэнкодера можно сформулировать следующим образом.

Для изображения *MNIST* (784 пикселя) эффективны значения *m* = 60 [5] или *m* = 100 [6].

В задачах классификации с высокими входными размерностями (до 3000) рекомендуется уменьшать *m* до 10-20 % от исходной размерности *n* [7].

Таким образом, полученные выражения позволяют предварительно вычислить значение *KL*-дивергенции, а затем использовать это значение для

выбора размерности латентного слоя автоэнкодера. Это сокращает количество итераций при настройке работы автоэнкодера.

В будущем планируется провести дополнительные эксперименты с другими архитектурами и наборами данных для более глубокого понимания влияния структуры автоэнкодеров на их производительность.

Список используемых источников

1. Вентцель Е. С., Овчаров Л. А. Теория вероятностей и ее инженерные приложения. М.: Высшая школа, 2007. 491 с.

2. Hinton G. E., Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks // Science, 313(5786), 504-507.

3. Kingma D. P., Welling, M. (2014). Auto-Encoding Variational Bayes. URL: https://arxiv.org/abs/1312.6114 (дата обращения 18.07.2025).

4. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016. 768 p.

5. On the Importance of the Kullback-Leibler Divergence Term in Variational Autoencoders for Text Generation. https://arxiv.org/abs/1909.13668 (дата обращения 18.07.2025).

6. Understanding disentangling in β-VAE. https://doi.org/10.48550/arXiv.1804.03599 (дата обращения 18.07.2025).

7. Variational Lossy Autoencoder. https://arxiv.org/abs/1611.02731 (дата обращения 18.07.2025).

DETERMINATION OF THE HIDDEN LAYER DIMENSION FOR THE AUTOENCODER BASED ON THE KULLBACK-LEIBLER DIVERGENCE ESTIMATION

Gubin A., Litvinov V., Filippov F.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article discusses the problems of choosing the dimension of the hidden space of the autoencoder, which is a key parameter affecting the quality of data representation and the efficiency of the device. The main focus is on using the Kullback-Leibler divergence (KL-divergence) as a criterion for evaluating the correspondence of the distribution of hidden features to the specified a priori distributions of the processed signal. The methods that make it possible, based on the values of the KL divergence, to identify a balance between retraining and loss of information content of hidden representations are analyzed.

Key words: *autoencoder, latent layer, Kullback-Leibler divergence*

УДК 621.391.28
ГРНТИ 49.33.29

ФОРМАЛИЗАЦИЯ ПРОЦЕССА УСТАНОВЛЕНИЯ IPSec-ТУННЕЛЯ

Е. В. Давыдова, Н. Н. Мошак, А. А.Федотов

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

Приводится вербальная модель процесса работы протокола IPSec. Предложено программное приложение для установки IPSec-туннелей в режиме «site-to-site» между узлами сети с использованием платформы .NET 8. Приведены фрагменты кода, демонстрирующие процесс обмена ключами и шифрования данных. Предложена структура библиотеки IPSecCore, которая содержит весь серверный код приложения и централизованно управляет криптографическими операциями, обменом данными и сетевыми функциями.

мультисервисная сеть, инфотелекоммуникационная транспортная система, виртуальная частная сеть, безопасный интернет-протокол IPSec

Введение

Одной из базовых задач построения защищенных мультисервисных сетей (МСС) является проблема защиты информации в процессе ее передачи по открытым каналам связи. Использование технологии защищенных виртуальных сетей (Virtual Private Network, VPN) позволяет обеспечить криптозащиту информации при организации защищенных каналов связи или защищенных туннелей между защищенными локальными вычислительными сетями (ЛВС) МСС. Каждый выделенный виртуальный канал VPN формируется в компьютере пользователя или в пограничных маршрутизаторах с помощью механизмов тунелирования (инкапсуляции) базового примитива протокола логического уровня МСС в примитив защищенного протокола. VPN-агенты могут осуществлять функции шифрования/расшифрования, аутентификации, а также контроль целостности сообщения. Работающее на сетевом уровне семейство протоколов безопасности Internet (далее – семейство протоколов IPSec [RFC 2401]) прозрачно для приложений и может работать практически во всех пакетных IP-сетях [1]. Данная работа является дальнейшим развитием идей, изложенных в [2-4].

Вербальное описание работы семейства протоколов IPSec

Архитектура семейства протоколов IPSec включает в себя: протокол обмена ключевой информацией IKE (Internet Key Exchange); протокол

аутентифицирующего заголовка (Authentication Header, AH); протокол инкапсулирующей защиты содержимого (Encapsulating Security Payload, ESP); домен интерпретации (Domain of Interpretation, DOI), который доопределяя структуру блоков данных и задавая правила именования информации, определяющей безопасность (политики безопасности, криптографические режимы и алгоритмы), связывает IKE с протоколом, защита которого обеспечивается.

В работе IKE можно выделить две основные фазы (phases). На первой фазе работы IKE происходит согласование обязательных параметров общего контекста безопасности IKE SA, выполняется взаимная аутентификация оконечных маршрутизаторов участников мультимедийного соединения и устанавливаются сеансовые ключи. IKE SA определяет, как именно будет обеспечиваться защита последующего трафика, в частности, обменов второй фазы. На второй фазе выполняется взаимная аутентификация участников сессии и согласуются контексты безопасности (которых может быть несколько) для протокола, использующего IKE, т. е. создаются контексты безопасности протоколов семейства IPsec (AH SA и ESP SA).

Протоколы AH и ESP поддерживают работу в двух режимах: туннельный режим и транспортный режим и не зависят от конкретных криптографических алгоритмов [5].

Особенности реализации защищенного IPSec-туннеля

Для реализации VPN выбран туннельный режим IPSec. При реализации защищенного IPSec-туннеля использован комплексный подход, сочетающий высокоуровневые языки программирования с низкоуровневыми системными вызовами. Основой разработки стал язык C# (.NET 8), который обеспечивает необходимый баланс между производительностью и безопасностью. Кроссплатформенность .NET 8 позволяет развертывать решение как на Windows-серверах, так и на Linux-системах, что критично для гетерогенных корпоративных сред. Для работы с эллиптической криптографией (ECDH-384) используется библиотека BouncyCastle.Cryptography 2.1.0. Механизмы управления ключами реализованы с учетом особенностей операционных систем: на Windows-платформах задействован Microsoft Data Protection API (DPAPI). Система логирования построена на базе NLog 5.2.0, обеспечивающего комплексный мониторинг всех этапов работы туннеля.

Реализация программного приложения для установки IPSec-туннелей в режиме «site-to-site» между узлами сети

В рассматриваемой реализации параметры IPSec-соединения между клиентом и сервером предварительно согласованы. Разработанное решение построено по принципу многослойной архитектуры с четким разделением ответственности между компонентами. В основе системы лежит криптографическое ядро, реализованное через статические классы-провайдеры, что обеспечивает максимальную производительность за счет минимизации накладных расходов на создание объектов.

Клиентское приложение начинается с генерации пары ключей для протокола ECDH. Приложение GenerateECDHKeys (рисунок 1) генерирует как приватный, так и публичный ключ для клиента, который будет использоваться в процессе обмена с сервером.

```
// Генерация публичного и приватного ключа для ECDH
Ссылок: 4
public static (byte[] privateKey, byte[] publicKey) GenerateECDHKeys()
{
    using var ecdh = ECDiffieHellman.Create();
    byte[] privateKey = ExportPrivateKey(ecdh); // Экспортируем приватный ключ
    byte[] publicKey = ExportPublicKey(ecdh);  // Экспортируем публичный ключ

    Logger.Debug("[ECDHKeyExchange] Generated ECDH keys.");
    return (privateKey, publicKey);
}
```

Рис. 1. Реализация GenerateECDHKeys

ExportPrivateKey с помощью функции ExportPkcs8PrivateKey экспортирует приватный ключ в формате PKCS#8, который используется для вычисления общего секрета (рисунок 2).

```
// Экспорт приватного ключа (PKCS#8)
Ссылок: 1
public static byte[] ExportPrivateKey(ECDiffieHellman ecdh)
{
    try
    {
        return ecdh.ExportPkcs8PrivateKey();  // Экспортируем приватный ключ в формате PKCS#8
    }
    catch (Exception ex)
    {
        Logger.Error("[ECDHKeyExchange] Error exporting private key: " + ex.Message);
        throw;
    }
}
```

Рис. 2. Экспорт приватного ключа в формате PKCS#8

После того, как публичный ключ клиента отправляется серверу, сервер генерирует свою пару ключей и также отправляет свой публичный ключ клиенту. Клиент и сервер используют свои приватные ключи и публичные ключи друг друга для вычисления общего секрета с помощью CalculateSharedSecret. Общий секрет клиент использует для шифрования сообщений, отправляемых серверу. Для шифрования данных используется алгоритм EncryptDataWithAES, а для расшифрования – алгоритм DecryptDataWithAES. Консольные приложения клиента и сервера служат интерфейсом для взаимодействия с библиотекой IPSecCore и демонстрации ее работы. Весь серверный код приложения сосредоточен в библиотеке IPSecCore (рисунок 3), которая управляет криптографической логикой, обменом данными и сетевыми операциями.

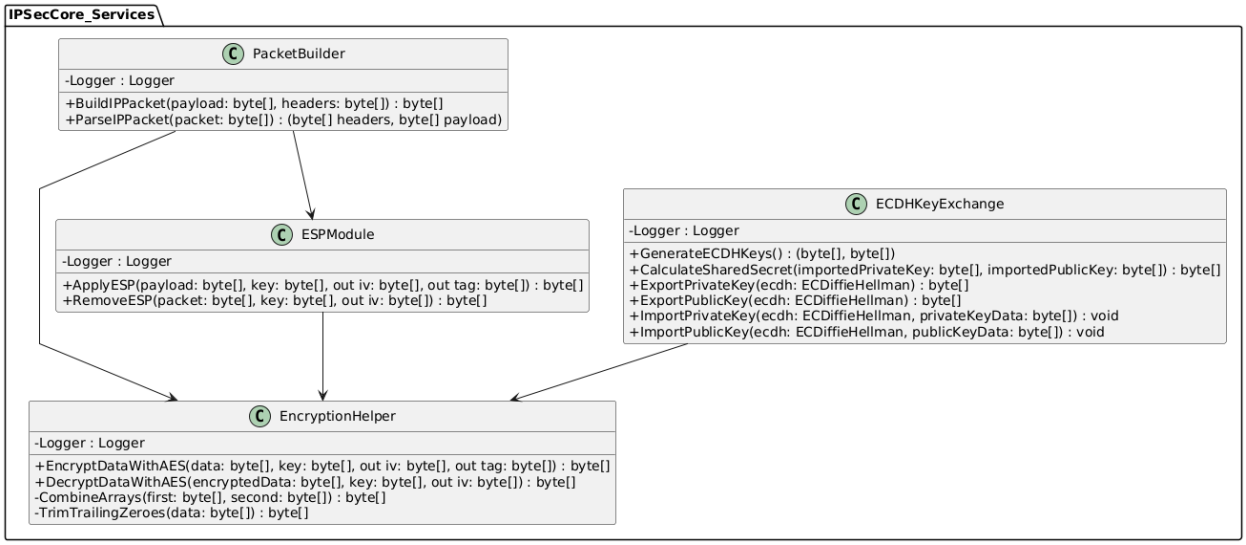


Рис. 3. Архитектура библиотеки IPSecCore

Библиотека IPSecCore представляет собой универсальное решение для организации защищенных соединений, архитектура которого предусматривает несколько сценариев интеграции в различные программные экосистемы. Разработанная с учетом принципов модульности и кроссплатформенности, библиотека может быть адаптирована под требования конкретных проектов и сред выполнения. Архитектура приложения предусматривает независимую работу модулей, отвечающих за различные аспекты системы: обмен ключами, шифрование данных и сетевое взаимодействие. Такая организация позволяет модифицировать отдельные компоненты без изменения всей системы. Решение поддерживает работу в разных средах выполнения.

Централизация криптографической логики в IPSecCore также облегчает процесс тестирования и отладки. Для серверных приложений библиотека предлагает надежный механизм защиты межсерверного взаимодействия, особенно востребованный в распределенных системах обработки данных. Особое внимание уделено совместимости с современными контейнерными решениями, что делает библиотеку применимой в оркестрируемых средах.

Сетевые сервисы могут использовать IPSecCore в качестве промежуточного слоя безопасности, добавляющего криптографическую защиту на транспортном уровне. Для клиентских решений библиотека предоставляет адаптивные механизмы управления соединением, включая поддержку нестабильных сетевых условий и роуминга между точками доступа. Это делает ее применимой для мобильных приложений, требующих постоянного защищенного соединения с бэкенд-системами.

Архитектура библиотеки предусматривает несколько уровней абстракции для интеграции, начиная от простого высокоуровневого API для быстрого внедрения базовой функциональности, до детализированного доступа к криптографическим примитивам для специализированных решений. Подсистема плагинов расширяет возможности интеграции с альтернативными системами аутентификации, нестандартными транспортными протоколами и специализированными хранилищами ключей.

Техническая реализация предусматривает seamless-интеграцию с системами мониторинга и управления, предоставляя точки для сбора метрик производительности и событий безопасности. Это особенно важно для корпоративных решений, где требуется централизованный контроль над защищенными соединениями. Поддержка стандартных протоколов логирования позволяет интегрировать библиотеку в существующие системы аудита безопасности без дополнительных адаптеров.

Заключение

Предложено программное приложение для установки IPSec-туннелей в режиме «site-to-site» между узлами сети с использованием платформы .NET 8. Приведены фрагменты кода, демонстрирующие процесс обмена ключами и шифрования данных. Разработанная библиотека IPSecCore, представляющая собой универсальное решение для организации защищенных соединений, содержит весь серверный код приложения и централизованно управ-

ляет криптографической логикой, обменом данными и сетевыми операциями.

Список используемых источников

1. Мартыненков И. В. Основные этапы развития криптографических протоколов SSL/TLS и IPSec // ПДМ. 2021. № 51. С.31–65.

2. Мошак Н. Н. Оценка влияния протоколов VPN сетевого уровня на параметры транспортной системы инфокоммуникационной сети на технологии IP-QoS / Н.Н. Мошак, Д.Б. Цветков // Информационные сети, системы и технологии: материалы Международной научн. конф. МКИССиТ-2006 30 октября - 02 ноября 2006 г. С. 33–35.

3. Кириллов В. В., Кокаева Р. С., Мошак Н. Н. Формализация протоколов строгой аутентификации на основе ассиметричных алгоритмов шифрования в мультисервисной сети на технологии IP-QoS. // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Междун.науч.-техн. и научн.-метод.конф.,сб. научн. ст. в 4 т. / под ред. С. В. Бачевского, СПб.: СПбГУТ, 2018, Т. 2. С. 393–398.

4. Яшин А. И., Мошак Н. Н., Цветков Д. Б. Модель системы сигнализации пакетной мультисервисной сети военно-морского флота РФ с учетом трафика безопасности // Морская радиоэлектроника. 2016. 2 (56). С. 14–17.

5. Андрусенко Ю. А., Кузьменко Г. С., Ржевская Н. В., Лагунова С. А. Исследование протоколов сетевой безопасности // Auditorium. 2023. № 1 (37). С. 21–26.

FORMALIZING THE IPSEC TUNNEL ESTABLISHMENT PROCESS

Moshak N., Fedotov A., Davydova E.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

A verbal model of the IPSec protocol operation process is provided. A software application is proposed for establishing IPSec tunnels in site-to-site mode between network nodes using the .NET 8 platform. Code fragments are provided that demonstrate the process of key exchange and data encryption. The structure of the IPSecCore library is proposed, which contains all the server code of the application and centrally manages cryptographic operations, data exchange and network functions.

Key words: *Multiservice network, Infotelecommunication Transport System, Virtual Private Network, IPSec protocol*

УДК 004.89
ГРНТИ 28.23.01; 68.01.11

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СЕЛЬСКОМ ХОЗЯЙСТВЕ ЗАРУБЕЖНЫХ СТРАН

В. А. Журавлев

Белорусская государственная академия связи

В данной статье рассматривается мировой опыт развития искусственного интеллекта в сельском хозяйстве зарубежных стран, что позволяет определить дальнейший этап эволюции сельскохозяйственной отрасли, открывая новые возможности для сельскохозяйственных предприятий и способствуя становлению сельского хозяйства.

Применение искусственного интеллекта в сельском хозяйстве подразумевает интеграцию инновационных решений, включая машинное обучение, компьютерное зрение, робототехнику и Интернет вещей, с целью модернизации сельского хозяйства, увеличения рентабельности и обеспечения устойчивости сельского хозяйства. Искусственный интеллект позволяют аграриям аккумулировать и обрабатывать информацию, автоматизировать рутинные операции и принимать взвешенные решения, что в свою очередь способствует увеличению продуктивности и оптимизации использования ресурсов.

искусственный интеллект, предприятия, рентабельность, устойчивость, сельское хозяйство, технологии.

Целью данной статьи является: рассмотреть и изучить мировой опыт развития инновационных методов и технологий с использованием искусственного интеллекта (далее – ИИ) в сельском хозяйстве; выявить преимущество ИИ для сельского хозяйства.

В 2024 году мировой рынок ИИ в сельском хозяйстве достиг 2,14 млрд долларов США. По прогнозам, к 2035 году рынок достигнет 20,96 млрд долларов США, а среднегодовой темп роста составит 23,06 % в период с 2024 по 2035 год [1, 2]. Рынок демонстрирует стабильный рост, обусловленный растущей потребностью в технологиях точного земледелия для повышения урожайности, оптимизации использования ресурсов и снижения воздействия на окружающую среду, а также растущим распространением устройств и датчиков, интернета вещей для ведения сельского хозяйства на основе данных, спросом на передовые алгоритмы искусственного интеллекта и модели машинного обучения для анализа обширных сельскохозяйственных данных [2]. По данным [3], ИИ становится ключевым драйвером изменений, в частности, более половины мировых компаний, а именно 58

%, рассматривают возможности интеграции ИИ для осуществления преобразований в своей деятельности. Охват ИИ в сельском хозяйстве мира пока невелик (около 12 %), но эта технология быстро развивается и уже демонстрирует значительный потенциал для трансформации аграрного сектора [4].

Государства по всему миру признают потенциал ИИ в революционном преобразовании сельского хозяйства и поэтому оказывают существенную поддержку в виде инициатив и финансирования, делая его более доступным и полезным для сельскохозяйственной отрасли в целом. Инициативы часто включают субсидии на сельскохозяйственные технологии на основе ИИ, гранты на исследования и разработки, а также образовательные программы для сельхозпроизводителей, что стимулирует рост рынка и поощряет инновации и внедрение ИИ в сельском хозяйстве.

По использованию ИИ Северная Америка доминирует на рынке благодаря развитой технологической инфраструктуре, пристальному вниманию к точному земледелию и масштабным инвестициям во внедрение ИИ. В данном регионе присутствуют ведущие компании, исследовательские институты и стартапы – разработчики решений на основе ИИ, инновационные технологии которых внедряются в сельскохозяйственный сектор, а именно ИИ для мониторинга урожая, анализа почвы и автономных машин. Данная инициатива поддерживается государством. Сельскохозяйственные предприятия в этом регионе используют ИИ для оптимизации всего: от посадки и полива до борьбы с вредителями и сбора урожая, повышая урожайность и снижая воздействие на окружающую среду. Кроме того, надежная цифровая инфраструктура региона обеспечивает бесперебойный сбор и анализ данных, что крайне важно для эффективного внедрения ИИ.

Латинская Америка становится перспективным рынком для ИИ в сельском хозяйстве, а такие страны, как Бразилия и Аргентина, лидируют по внедрению ИИ. Богатые сельскохозяйственные ресурсы региона и растущее понимание преимуществ ИИ способствуют его распространению. Латиноамериканские сельскохозяйственные предприятия используют ИИ для оптимизации выращивания культур, выявления болезней и прогнозирования урожайности, стремясь повысить производительность и обеспечить продовольственную безопасность.

В Европе рынок демонстрирует стабильный рост, при этом такие страны, как Германия, Франция и Нидерланды, лидируют по внедрению ИИ. В этом регионе особое внимание уделяется устойчивым методам ведения сельского хозяйства и сохранению окружающей среды, что делает ИИ

ценным инструментом для оптимизации использования ресурсов и минимизации воздействия на окружающую среду. Европейские сельскохозяйственные предприятия все чаще используют ИИ для управления посевами, мониторинга скота и прогнозной аналитики для повышения общей производительности сельского хозяйства.

В Азиатско-Тихоокеанском регионе наблюдается значительный рост рынка ИИ в сельском хозяйстве, обусловленный обширным сельскохозяйственным сектором, ростом населения и увеличением спроса на продовольственную безопасность. Такие страны, как Китай и Индия, внедряют технологии на основе ИИ для точного земледелия, мониторинга урожая и «умного» сельского хозяйства. Инновации в сельском хозяйстве региона в сочетании с государственной поддержкой делают Азиатско-Тихоокеанский регион важным игроком на мировом рынке ИИ в сельском хозяйстве.

Ближний Восток и Африка постепенно внедряют ИИ в сельское хозяйство, уделяя особое внимание решению проблемы нехватки воды и экстремальных климатических условий. Решения на основе ИИ для точного орошения и управления сельскохозяйственными культурами набирают популярность в засушливых регионах. Кроме того, правительства и международные организации инвестируют в проекты на основе ИИ для улучшения методов ведения сельского хозяйства и обеспечения продовольственной безопасности в этом регионе [2, 5-8].

Структура рынка ИИ в сельском хозяйстве в разбивке по регионам за 2023 год представлена на рисунке 1.

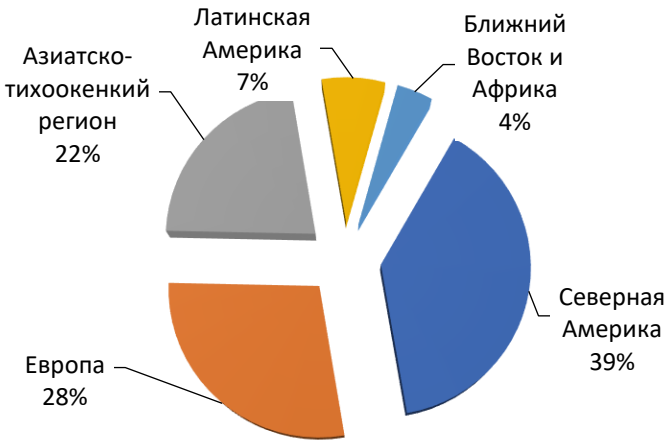


Рис. 1. Доля искусственного интеллекта на рынке сельского хозяйства в разбивке по регионам за 2023 год, %

Ведущие ключевые игроки на рынке в области искусственного интеллекта в сельском хозяйстве активно участвуют в стратегических инициативах. Эти инициативы включают в себя исследования и разработки для улучшения алгоритмов искусственного интеллекта, адаптированных для сельского хозяйства. Кроме того, они запускают новые решения и платформы на базе искусственного интеллекта, которые предлагают сельскохозяйственным организациям передовые инструменты для мониторинга урожая, прогнозной аналитики и автономной техники. Также они предоставляют услуги по обучению и поддержке для эффективного использования технологий искусственного интеллекта в сельском хозяйстве, способствуя их более широкому внедрению [9].

В период с 2021 по 2022 гг. в России, благодаря федеральной инициативе «Искусственный интеллект», было поддержано свыше 600 проектов, направленных на создание и ускоренное внедрение ИИ-технологий. Кроме того, на базе ведущих вузов страны было основано шесть научно-исследовательских центров, а также утверждено 85 магистерских программ по ИИ в 16 ведущих вузах. Следующей важной задачей в рамках реализации национальной стратегии в области ИИ является разработка практических решений на базе искусственного интеллекта и их широкое распространение среди компаний, представляющих наиболее значимые отрасли экономики страны [10].

В России активно внедряется ИИ в агропромышленный комплекс и за последние годы реализованы десятки проектов, охватывающих различные направления, более подробно о внедрении ИИ изложено в [11].

Важность широкого использования ИИ рассматривается в Республике Беларусь и одним из первоочередных приоритетных направлений научной, научно-технической и инновационной деятельности на 2026-2030 гг. утвержденные Указам Президента Республики Беларусь от 01.04.2025 № 35 «О приоритетных направлениях научной, научно-технической и инновационной деятельности на 2026 - 2030 годы», является технологии искусственного интеллекта. Также в Указе большое внимание уделяется инновационным технологиям в агропромышленном комплексе и пищевой промышленности.

Приоритетные направления, обозначенные в Указе, обеспечат технологический суверенитет страны, консолидацию научного, образовательного и производственного потенциала, концентрацию материальных и интеллекту-

альных ресурсов на реализации наиболее значимых направлений научной, научно-технической и инновационной деятельности.

Использование ИИ в сельском хозяйстве позволят разработать и внедрить инновационные методы, модели и технологи, которые могут решать сложные задачи, ранее недоступные для традиционных подходов.

На заседании Совета по проектам в сфере цифрового развития при Министерстве связи и информатизации Республики Беларусь 3 мая 2024 г. было принято решение о реализации мероприятия «Создание информационно-аналитической системы «Цифровая платформа точного земледелия» (первая очередь)» [4].

Цель данного мероприятия: формирование основы Цифровой платформы точного земледелия, входящий в состав инфраструктуры ведения пространственных данных, базовых подсистем и комплексов аппаратно-программных средств, с поэтапным эволюционным развитием к технологиям точного земледелия для сельскохозяйственных предприятий Республики Беларусь. Данная платформа будет обеспечивать автоматизацию и поддержку принятия решений для специалистов сельхозпредприятий.

Опыт реализации в Республике Беларусь технологий с использованием ИИ был представлен в проведенных ранее работах [12].

В заключении можно сделать вывод, что развитие ИИ в сельском хозяйстве становится ключевым фактором повышения эффективности агропромышленного комплекса во многих странах. Внедрение ИИ-технологий позволяет оптимизировать использование ресурсов, повышать урожайность, снижать экологическую нагрузку и минимизировать риски. Однако уровень развития и применения ИИ в аграрном секторе значительно различается в зависимости от экономических, технологических и политических условий каждой страны.

США и Канада: активно используют ИИ для точного земледелия, мониторинга состояния почв, прогнозирования урожайности и автоматизации сельхозтехники. Крупные компании (John Deere, IBM, Microsoft) разрабатывают AI-решения для фермеров.

Китай: делает ставку на масштабное внедрение ИИ благодаря государственной поддержке (программа «Цифровое сельское хозяйство»). Используются дроны, роботы для сбора урожая и системы анализа данных.

Европейский Союз: развивает «умные фермы» с акцентом на устойчивое развитие. Германия, Нидерланды и Франция лидируют в применении ИИ для контроля качества продукции и снижения пестицидной нагрузки.

Израиль: несмотря на небольшие территории, активно внедряет ИИ в капельное орошение и управление теплицами, демонстрируя высокую эффективность.

Россия: Внедряет ИИ в крупных агрохолдингах (например, «Русагро», «Мираторг»), основные направления – прогнозная аналитика и автоматизация.

Бразилия и Аргентина: Используют ИИ для мониторинга состояния почв и управления крупными плантациями.

Индия: начинает активно внедрять ИИ-решения для мелких фермеров (например, прогнозирование погоды через мобильные приложения), но масштабы пока ограничены.

Несмотря на огромный потенциал, внедрение ИИ в сельском хозяйстве большинства стран сталкивается с рядом проблем, таких как высокая стоимость технологий, недостаток квалифицированных кадров, необходимость сбора и обработки больших объемов данных, защиты данных и конфиденциальности, а также необходимостью в развитой цифровой инфраструктуре в сельской местности.

Список используемых источников

1. AI in Agriculture Market – Mode of access: https://www.rootsanalysis.com/ai-in-agriculture-market. (дата обращения 27.02.2025).

2. Artificial Intelligence In Agriculture Market Size, Share, and Trends 2024 to 2034 – Mode of access: https://www.precedenceresearch.com/artificial-intelligence-in-agriculture-market. (дата обращения 06.03.2025).

3. Цифровая трансформация в компаниях // tadviser. URL: https://www.tadviser.ru/index.php/. (дата обращения 11.03.2025).

4. Цифровое сельское хозяйство Республики Беларусь / под общ. ред. В. Г. Гусакова; Нац. акад. наук Беларуси, Ин-т систем. исслед. в АПК/ Минск: Беларуская навука, 2024. 553 с.: ил.

5. AI in Agriculture Future of Farming. Mode of access: https://www.geeksforgeeks.org/ai-in-agriculture-future-of-farming/. (дата обращения 04.03.2025).

6. Agriculture Use Cases & Machine Learning Applications. Mode of access: https://vitalflux.com/agriculture-use-cases-machine-learning-applications (дата обращения 04.03.2025).

7. AI in Agriculture – Present Applications and Impact. Mode of access: https://emerj.com/ai-agriculture-present-applications-impact/. (дата обращения 05.03.2025).

8. Artificial Intelligence in Agriculture: Farming for the 21st Century. Mode of access: https://apro-software.com/artificial-intelligence-in-agriculture (дата обращения 05.03.2025).

9. Как искусственный интеллект помогает сельскому хозяйству // dzen. URL: https://dzen.ru/a/YEkyzrEBrkLWMtD2. (Дата доступа: 05.03.2025).

10. «Умные» фермы: как искусственный интеллект меняет сельское хозяйство // rbc. URL: https://www.rbc.ru/technology_and_media/14/06/2023/64802aae9a7947c6121756b7???history=0&pfid=1&sample=33&ref=2 (дата обращения 14.03.2025).

11. Применение ИИ в сельском хозяйстве [Электронный ресурс] // digitalocean. URL: https://digitalocean.ru/n/polevye-usloviya???history=0&pfid=1&sample=33&ref=0. (дата обращения 12.03.2025).

12. Журавлев, В. А. Цифровизация сельского хозяйства в Республике Беларусь: технологические решения для развития / В. А. Журавлев // Аграрная экономика. 2024. № 3 (346). С.60–70.

APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN FOREIGN COUNTRIES' AGRICULTURE

Zhuravlev V.
Belarusian State Academy of Telecommunications

This article examines the global experience of developing artificial intelligence in agriculture in foreign countries, which allows us to determine the next stage of the agricultural industry's evolution, opening up new opportunities for agricultural enterprises and contributing to the development of agriculture.

The application of artificial intelligence in agriculture involves the integration of innovative solutions, including machine learning, computer vision, robotics, and the Internet of Things, with the aim of modernizing agriculture, increasing profitability, and ensuring the sustainability of agriculture. Artificial intelligence allows farmers to accumulate and process information, automate routine operations, and make informed decisions, which in turn helps to increase productivity and optimize resource utilization.

Key words: *artificial intelligence, enterprises, profitability, sustainability, agriculture, and technology*

УДК 004.855.5
ГРНТИ 28.23.15

ОБУЧЕНИЕ НЕЙРОСЕТЕВОЙ МОДЕЛИ МАШИННОГО ЗРЕНИЯ RT-DETRv2, ДЛЯ РАСПОЗНОВАНИЯ СПЕЦИАЛЬНОЙ ИНДИВИДУАЛЬНОЙ ЗАЩИТЫ

Д. Е. Карпенко, К. С. Курочка

Гомельский Государственный технический университет им. П. О. Сухого

Рассматривается применение модели RT-DETRv2 для автоматизированного контроля наличия средств индивидуальной защиты (СИЗ) на производстве с использованием компьютерного зрения. Проведено сравнение RT-DETRv2 R18 с моделями YOLOv8 и YOLOv11 на датасете D900. Оценка по метрикам mAP и mAR показала, что RT-DETRv2 обеспечивает хорошее соотношение точности и скорости, что делает ее подходящей для задач мониторинга СИЗ в реальном времени. Отмечены пути улучшения качества детекции редких объектов.

нейронные сети, искусственный интеллект, охрана труда, техника безопасности, RT-DETRv2, СИЗ

В современных промышленных системах безопасности все большую значимость приобретают автоматизированные средства контроля на основе компьютерного зрения. Основной задачей является выявление нарушений требований охраны труда, в частности, отсутствие средств индивидуальной защиты (СИЗ) у персонала на производственных объектах. Для этого применяется подход объектной детекции, позволяющий определить местоположение и класс объектов на изображении или в видеопотоке. В данном исследовании задача сводится к обнаружению работников и проверке наличия у них обязательных СИЗ: касок, жилетов, очков и других элементов, определенных политикой предприятия [1].

Одной из новейших моделей для детекции объектов является RT-DETR (Real-Time Detection Transformer). В отличие от традиционных методов, основанных на сверточных нейронных сетях (CNN), таких как YOLO, RT-DETR использует механизмы внимания (attention) и другие возможности трансформеров для более эффективной обработки данных. Основой для RT-DETR послужила модель DETR (Detection Transformer), которая отказалась от этапов выбора анкоров и прямо предсказывает ограничивающие рамки и классы объектов. RT-DETR оптимизирует эту идею для достижения высо-

кой производительности в реальном времени [2], сохраняя при этом точность трансформерных архитектур.

Архитектура RT-DETR представляет собой структуру Encoder-Decoder. Encoder извлекает признаки из изображения, а Decoder генерирует прогнозы ограничивающих рамок и классов, используя запросы, которые через слои внимания становятся «осведомленными» об объектах. Это позволяет RT-DETR эффективно работать в реальном времени, что критически важно для применений в видеонаблюдении, автономных транспортных средствах и робототехнике.

Для сравнительного анализа были выбраны следующие архитектуры: YOLOv8 (Small, Medium), YOLOv11 (Small, Medium), RT-DETRv2 R18. Целью исследования было нахождение оптимальной модели, сочетающей высокую скорость работы и точность маркирования объектов, оцениваемую метриками mAP и mAR). Наиболее популярной архитектурой на рынке и среди исследователей является модели архитектуры YOLO. Модель используется в различных задачах: трекинг автотранспорта [3], поиск дефектов [4], распознавание позвонков [5] и др. задачах. Информация об используемых моделях представлена в таблице 2.1.

ТАБЛИЦА 1. Информация о моделях машинного зрения

Архитектура	Название	Параметры (млн)	Тип
YOLO 8	YOLO 8 Small	11.2	Одностадийный детектор
YOLO 8	YOLO 8 Medium	25.9	Одностадийный детектор
YOLO 11	YOLO 11 Small	9.4	Одностадийный детектор
YOLO 11	YOLO 11 Medium	20.1	Одностадийный детектор
RT-DETRv2	RT-DETRv2 R18	20.2	Одностадийный детектор

Эффективность моделей машинного зрения напрямую зависит от качества и репрезентативности обучающих данных. Для данной задачи был сформирован набор данных D900, содержащий 900 изображений с аннотациями для 8 классов СИЗ (каска, лямка каски, спецовка, человек передом/задом, без каски, без лямки, без спецовки). Для обеспечения обобщающей способности модели, данные были разнообразны по ракурсу, освещению и фону.

Обучение и валидация моделей проводились в среде Windows 10 с использованием Python 3.10.6 на компьютерной конфигурации с процессором AMD Ryzen 7 5700X и видеокартой NVIDIA GeForce RTX 3060 (12 ГБ). Для ускорения вычислений все модели обучались в точности FP16. Ключевые параметры обучения представлены в таблице 2.

ТАБЛИЦА 2. Основные параметры моделей

Название модели	Размер батча	Входное разрешение
YOLO8 Small	6	1280x736
YOLO8 Medium	4	1280x736
YOLO 11 Small	4	1280x736
YOLO 11 Medium	2	1280x736
RT-DETRv2 R18	12	600x600

Разрешение 1280x736 выбрано, исходя из распространенности Full HD камер. Для RT-DETRv2 R18 использовалось квадратное разрешение 600x600 пикселей для сохранения пропорций и возможности идентификации мелких объектов, таких как лямки касок.

Тестирование производительности проводилось на GPU RTX 3060 и CPU R7 5700X. По результатам валидации, большинство моделей показали отличные значения mAP и mAR (от 0.88 до 0.99). Метрики mAP и mAR по классам представлены в таблицах 3 и 4 соответственно.

ТАБЛИЦА 3. Метрики mAP по классам

Класс	8S	11S	8M	11M	R18
Строительная каска	0.978	0.986	0.994	0.987	0.9771
Нет строительной каски	0.992	0.994	0.994	0.992	0.9901
Нет лямки	0.976	0.991	0.99	0.99	0.9504
Нет спецовки	0.990	0.994	0.994	0.994	0.9901
Лямка каски	0.891	0.787	0.948	0.818	0.7253
Спецовка	0.986	0.99	0.995	0.991	0.9699
Человек передом	0.981	0.985	0.989	0.985	0.9900
Человек спиной	0.983	0.994	0.995	0.994	0.9895

ТАБЛИЦА 4. Метрики mAR по классам

Класс	8S	11S	8M	11M	R18
Строительная каска	0.977	0.98	0.997	0.98	0.9809
Нет строительной каски	0.990	0.99	0.988	0.987	0.9951
Нет лямки	0.994	0.992	0.993	0.993	0.9515
Нет спецовки	0.995	0.994	0.995	0.997	0.9983
Лямка каски	0.703	0.7	0.908	0.733	0.7359
Спецовка	0.987	0.986	0.995	0.987	0.9734
Человек передом	0.973	0.974	0.979	0.975	0.9993
Человек спиной	0.997	0.995	0.996	0.995	0.9961

YOLO Small (8S и 11S) обнаруживают практически все объекты на высоком уровне, за исключением лямок касок. Это связано с тем, что лямки касок встречаются реже всего в наборе данных, а сами модели YOLO Small являются самыми компактными 11.2 и 9.4 млн параметров по сравнению с YOLO Medium 25.9 и 20.1 млн параметров, что сказывается на их обобщающей способности при распознавании малопредставленных классов.

RT-DETRv2 R18 показала себя неплохо, но, как и у моделей YOLO Small, у нее есть проблемы с детекцией лямок касок. RT-DETRv2 R18 является самой малой моделью в семействе RT-DETRv2, 20.2 млн параметров, что эквивалентно nano-моделям в линейке YOLO по производительности (не в кадрах).

Среди всех моделей YOLOv8 Medium показала наилучшие результаты в распознавании всех классов объектов, преодолев проблемы, характерные для YOLOv8 Small, RT-DETRv2 R18, YOLO11 Small/Medium. В таблице 5 представлено сравнение производительности в кадрах в секунду на обработку видеопотока.

ТАБЛИЦА 5. Производительность для RTX3060 + R7 5700X

Модель	Кадры в секунду	На ГПУ/ЦПУ	Точность вычисления
YOLO 8 Small	200 кадр/сек.	ГПУ	FP16
YOLO 8 Small	12,5 кадр/сек.	ЦПУ	FP32
YOLO 8 Medium	136 кадр/сек.	ГПУ	FP16

Модель	Кадры в секунду	На ГПУ/ЦПУ	Точность вычисления
YOLO 8 Medium	5,81кадр/сек.	ЦПУ	FP32
YOLO11 Small	212,7 кадр/сек.	ГПУ	FP16
YOLO 11 Small	12,8 кадр/сек.	ЦПУ	FP32
YOLO 11 Medium	123,9 кадр/сек.	ГПУ	FP16
YOLO 11 Medium	5,5 кадр/сек.	ЦПУ	FP32
RT-DETRv2 R18	84.09 кадр/сек.	ГПУ	FP16
RT-DETRv2 R18	3,7 кадр/сек.	ЦПУ	FP32

В производительности на GPU, YOLO11 Small лидирует с 212.7 FPS, за ней следует YOLO8 Small с 200 FPS. RT-DETRv2 R18 показывает достойные 84.09 FPS, что является хорошим результатом для трансформерной архитектуры и обеспечивает работу в реальном времени. На CPU производительность всех моделей значительно падает.

В ходе сравнительного анализа RT-DETRv2 R18 показала достойные результаты как по точности (mAP и mAR), так и по скорости инференса. Хотя она и имела некоторые трудности с детекцией наименее представленного класса («лямка каски»), что обусловлено ее компактным размером (модель R18 является самой малой в линейке RT-DETRv2, аналогичной nano-версиям YOLO), ее общая производительность в 84.09 FPS на GPU (FP16) является вполне достаточной для большинства применений в реальном времени, таких как видеонаблюдение.

В сравнении с другими моделями, такими как YOLOv8 Medium, которая показала наилучшую точность по всем классам, RT-DETRv2 R18 демонстрирует баланс между производительностью и возможностями трансформерных архитектур. Ее способность к работе на относительно низком разрешении (600x600 пикселей) и сохранению деталей для мелких объектов является значимым преимуществом.

В целом, RT-DETRv2 представляет собой мощный инструмент для систем мониторинга СИЗ, предлагая высокоточную и эффективную детекцию. Для дальнейшего улучшения производительности, особенно в отношении редких и мелких объектов, может быть рассмотрено обучение более крупных моделей из семейства RT-DETRv2 или использование дополнительных методов аугментации данных, направленных на увеличение репрезентативности малочисленных классов.

Список используемых источников

1. Курочка К. С. Локализация позвонков на КТ-изображениях в условиях ограниченности вычислительных ресурсов / К. С. Курочка, К. А. Панарин // Новые горизонты 2021: сб. материалов VIII Белорусско-Китайского молодежного инновационного форума, 11-12 ноября 2021 года / Белорусский национальный технический университет. Минск: БНТУ, 2021. Т. 1. С. 177–179.

2. Lv W. RT-DETR: DETRs Beat YOLOs on Real-time Object Detection / W. Lv, S. Xu, Y. Zhao, G. Wang, J. Wei, Y. Yong, Q. Dang, Y. Liu // Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV): materials of the Intern. Conf., Paris, France, Oct. 2-6, 2023 / IEEE Computer Society. Paris: IEEE, 2023. PP. 6716–6726.

3. Huang Z., Li L., Krizek G. C., Sun, L. Traffic Sign and Vehicle Detection Based on Improved YOLOv8 for Autonomous Driving // 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS). 2023. PP. 226–232.

4. Брехт Э. А., Коншина, В. Н. Применение нейронной сети YOLO для распознавания дефектов // Интеллектуальные технологии на транспорте. 2022. № 2. С. 41–47.

5. Kurachka K. S., Luchshava, T. V., Panarin, K. A. Localization of human percentages on X-ray images with use of Darknet YOLO // Doklady BGUIR. 2018. Vol. 113. № 3. P. 32–38.

TRAINING OF THE NEURAL NETWORK MODEL OF MACHINE VISION RT-DETRV2, FOR DISCOVERING SPECIAL INDI-VIDUAL PROTECTION

Karpenko D., Kurochka K.
Sukhoi State Technical University of Gomel

The application of RT-DETRv2 model for automated control of personal protective equipment (PPE) availability at production facilities using computer vision is considered. A comparison of RT-DETRv2 R18 with the YOLOv8 and YOLOv11 models on the D900 dataset is made. Evaluation on mAP and mAR metrics showed that RT-DETRv2 provides a good ratio of accuracy to speed, making it suitable for real-time PPE monitoring tasks. Ways to improve the quality of rare object detection are highlighted.

Key words: *neural networks, artificial intelligence, occupational health and safety, RT-DETRv2, PPE*

УДК 004.451.3
ГРНТИ 05.14.21

СРАВНЕНИЕ МЕТОДОВ УПРАВЛЕНИЯ ПАМЯТЬЮ В JVM С ТОЧКИ ЗРЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ И ЭКОНОМИКИ ДАННЫХ

Н. В. Кваша, Е. А. Михайлик

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

В статье проводится сравнительный анализ производительности сборщиков мусора JVM (G1GC, Parallel GC, Serial GC) при использовании генератора фрактального пламени с позиции их влияния на экономическую эффективность эксплуатации программных систем. Оценка времени отклика, загрузки процессора, длительности и частоты пауз позволяет определить оптимальный баланс между производительностью и затратами на вычислительные ресурсы. На основе результатов даны рекомендации по выбору сборщика мусора для приложений с различными требованиями, что способствует снижению операционных расходов и повышению рентабельности ИТ-инфраструктуры.

память, производительность, экономика программных систем, Java, JVM, GC, G1GC, Parallel GC, Serial GC.

Исследование посвящено управлению памятью в JVM с анализом трех сборщиков мусора – G1GC, Parallel GC и Serial GC – с точки зрения их экономической эффективности. Производительность и предсказуемость работы JVM напрямую влияют на снижение операционных расходов, минимизацию простоев и повышение рентабельности инфраструктуры [1].

В ходе тестирования с генератором фрактального пламени оценивались ключевые показатели: время отклика, загрузка CPU, частота и длительность пауз. На основе результатов разработаны рекомендации по выбору сборщика мусора, позволяющие оптимизировать затраты без потери качества обслуживания. Сравнение рассматриваемых методов управления памятью представлено в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ методов управления памятью

Характеристика	Serial GC	Parallel GC	G1GC
Многопоточность	Нет	Да	Да
Время пауз	Долгие	Короткие	Предсказуемые
Использование CPU	Низкое	Высокое	Среднее
Адаптивность	Нет	Ограниченная	Высокая

Выбор сборщика мусора (GC) в JVM влияет на технические и экономические показатели приложений, включая использование памяти, загрузку процессора, время отклика, частоту пауз, стоимость инфраструктуры, масштабирование и потери от простоев [2]. Оптимизация управления памятью под конкретный сценарий эксплуатации позволяет снизить совокупную стоимость владения (TCO) и повысить возврат на инвестиции (ROI) за счет более эффективного использования ресурсов [3].

Для исследования использовался генератор фрактального пламени на Java, создающий интенсивную нагрузку на CPU и управление памятью. Приложение генерирует сложные визуальные структуры, что приводит к частому выделению и освобождению объектов, создавая условия для объективного сравнения сборщиков мусора.

Такой подход позволяет оценить поведение G1GC, Parallel GC и Serial GC в реальных нагрузках, включая стабильность времени отклика, частоту и длительность пауз, а также влияние на загрузку процессора и потребление памяти, что служит основой для рекомендаций по выбору оптимального GC в зависимости от требований приложений [4].

Основные критерии оценки:

– время отклика: время генерации одного фрактала;
– использование CPU: средний процент использования процессора;
– время сборки мусора: общее время, затраченное на GC;
– частота и длительность пауз: количество и продолжительность пауз из-за GC.

Тестовая среда:

– ОС: Windows 11;
– Процессор: Intel Core i7-9700K (8 ядер, 3.60 GHz);
– ОЗУ: 16 GB DDR4;
– JVM: OpenJDK 11.

Тестирование проводилось в идентичных условиях для всех сборщиков мусора: G1GC, Parallel GC и Serial GC. Для корректного сравнения различных сборщиков мусора использовались параметры JVM, указанные в таблице 2.

ТАБЛИЦА 2. Настройка параметров JVM для каждого GC

GC	Настройка параметров
G1GC	java -Xmx4g -Xms4g -XX:+UseSerialGC -jar fractal-flame-generator.jar
Parallel GC	java -Xmx4g -Xms4g -XX:+UseParallelGC -jar fractal-flame-generator.jar
Serial GC	java -Xmx4g -Xms4g -XX:+UseG1GC -jar fractal-flame-generator.jar

Код генератора фрактального пламени был собран в исполняемый JAR-файл, а параметры JVM настроены под тестируемый сборщик мусора. Методология позволила объективно сравнить производительность G1GC, Parallel GC и Serial GC, обеспечивая основу для практических рекомендаций по управлению памятью в JVM.

На графиках (рис. 1-3) показаны динамика использования кучи и частота пауз для каждого сборщика, позволяя оценить эффективность, стабильность отклика, нагрузку на процессор и поведение памяти в реальном времени. Эти данные служат основой для сравнения производительности и выбора оптимального GC для разных сценариев эксплуатации.

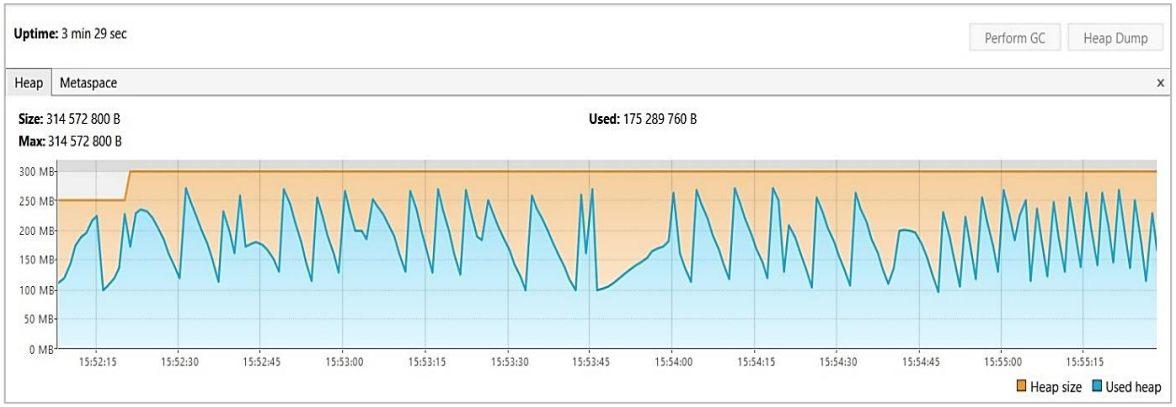


Рис. 1. Результаты тестирования работы G1GC

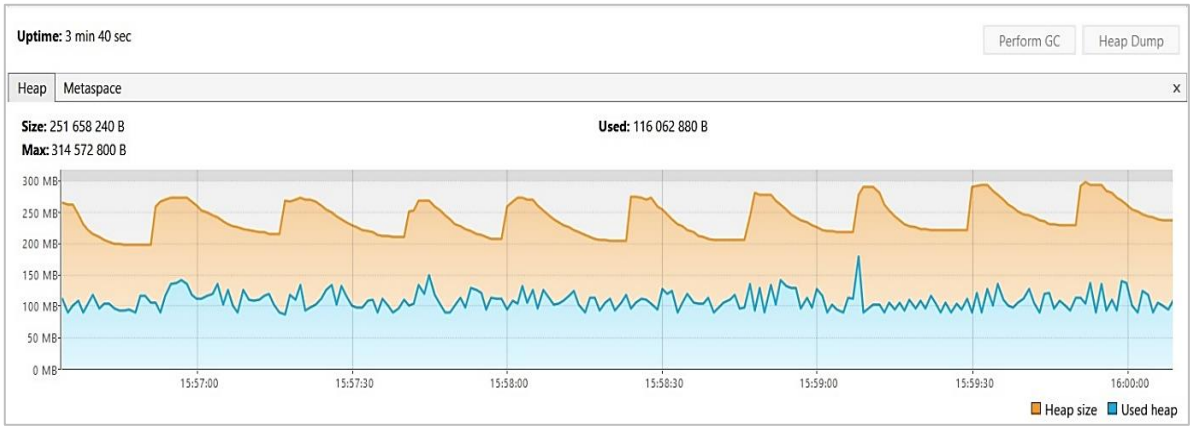


Рис. 2. Результаты тестирования работы Parallel GC

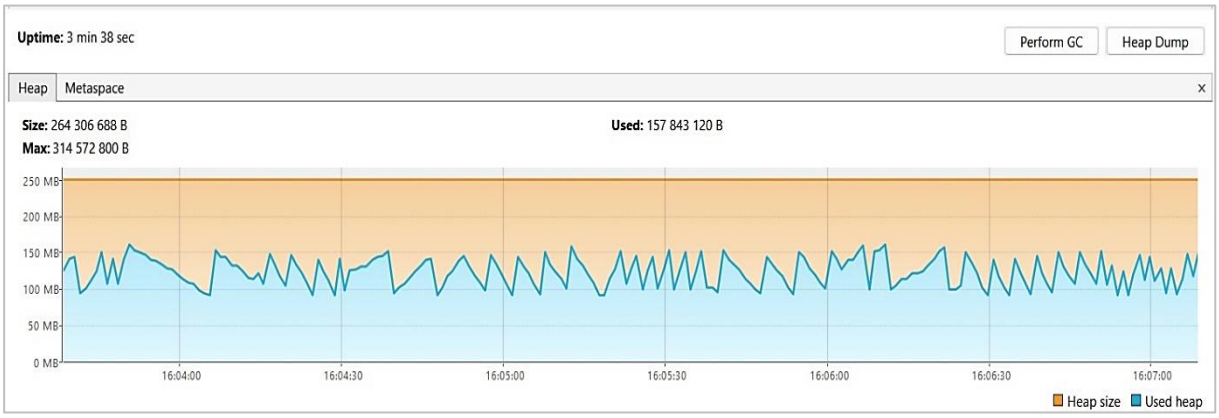


Рис. 3. Результаты тестирования работы Serial GC

В таблице 3 представлено детальное сравнение G1GC, Parallel GC и Serial GC. Для каждого из них указаны ключевые характеристики: размер кучи, используемая память, частота и длительность пауз, влияние на время отклика, нагрузка на CPU, а также области применения, преимущества и недостатки. Такая структура позволяет быстро оценить, какой сборщик мусора наиболее подходит для конкретного типа приложения и условий эксплуатации.

ТАБЛИЦА 3. Сравнение работы сборщиков мусора

Характеристика	G1GC	Parallel GC	Serial GC
Heap Size	315 МБ	252 МБ	264 МБ
Используемая память	100–250 МБ	50–150 МБ	100–200 МБ
Частота пауз	3–5 с	10–15 с	3–5 с
Длительность пауз	Короткие	Короткие	Короткие
Влияние на время отклика	Стабильное	Стабильное	Частые паузы ↑ отклик
Использование CPU	Фоново	Все ядра	Однопоточно
Область применения	Интерактивные приложения	Серверные приложения	Ограниченные ресурсы
Преимущества	Низкие задержки	Быстрый Memory Cleanup	Простота, низкая нагрузка
Недостатки	Возможны паузы	Высокая нагрузка	Частые паузы

Экономический анализ сборщиков мусора JVM показывает, что их выбор влияет на совокупную стоимость владения (TCO) и возврат на инвестиции (ROI) Java-приложений [5].

G1GC стабилен при использовании 100–250 МБ памяти с короткими паузами каждые 3–5 секунд, что важно для интерактивных приложений, минимизирует финансовые потери от задержек и снижает нагрузку на ресурсы. Parallel GC использует 50–150 МБ памяти с паузами каждые 10–15 секунд и активно задействует все ядра CPU, обеспечивая высокую пропускную способность серверов, но повышая затраты при облачной тарификации. Serial GC использует 100–200 МБ, работает однопоточно с паузами каждые 3–5 секунд, выгоден для бюджетных и встроенных систем, экономя на оборудовании, но может увеличить время отклика.

Выбор GC влияет не только на технические показатели, но и на экономику – от затрат на ресурсы до потерь от простоев. Оптимальная настройка под конкретный сценарий позволяет снизить расходы и повысить доходность, улучшая SLA-показатели [6]. Расчеты показали, что корректный подбор GC снижает потребность в дополнительном оборудовании и облачных ресурсах, минимизируя риски и затраты. Экономическая эффективность каждого из рассматриваемых в работе сборщиков мусора указана в таблице 4.

ТАБЛИЦА 4. Экономический эффект от выбора сборщика мусора

Сборщик мусора	Экономия	Потеря от простоев	Экономический эффект
G1GC	до 15 %	низкая	Высокий
Parallel GC	до 20 %	средняя	Положительный
Serial GC	до 30 %	высокая	Положительный

Таким образом, можно сформулировать ряд рекомендаций по выбору оптимального с экономической точки зрения сборщика мусора. G1GC подходит для интерактивных приложений с жесткими SLA, минимизирует паузы и стабилизирует отклик, снижая риск штрафов и сокращая расходы на масштабирование до 15 %. Parallel GC эффективен для высоконагруженных серверов, ускоряет обработку запросов и может дать до 20 % экономии, но высокая нагрузка на CPU увеличивает расходы при перегрузке. Serial GC целесообразен для малых и встроенных систем, снижает капитальные за-

траты до 30 % за счет дешевого оборудования, но при росте нагрузки возможны косвенные потери.

Экономическая целесообразность применения конкретного GC зависит от масштаба системы, профиля нагрузки и бизнес-приоритетов. Грамотный выбор позволяет получить значимый финансовый эффект – от снижения эксплуатационных расходов до роста доходов за счет повышения стабильности и производительности систем.

Список используемых источников

1. Блох Д. Эффективное программирование на Java // Addison-Wesley Professional. 2018. С. 15–32.

2. Венкат С. Программирование конкуренции на JVM: освоение синхронизации, STM и акторов // Pragmatic Bookshelf. 2014. С. 23–41.

3. Госнелл Дж., Джой Б., Стил Г., Браха Г. Спецификация языка Java // Addison-Wesley Professional. 2005. С. 10–56.

4. Джонс Р., Линс Р. Сборка мусора: алгоритмы для автоматического динамического управления памятью // John Wiley & Sons. 1996. С. 5–48.

5. Линдхольм Т., Йеллин Ф., Браха Г., Бакли А. Спецификация виртуальной машины Java, издание для Java SE 8 // Addison-Wesley Professional. 2014. С. 12–60.

6. Ченг П., Харпер Р., Херц М. Поколенческая сборка мусора и виртуальная машина HotSpot // IBM Research Report. 2012. С. 10–75.

COMPARATIVE ANALYSIS OF MEMORY MANAGEMENT METHODS IN JVM FROM THE PERSPECTIVE OF PERFORMANCE AND DATA ECONOMICS

Kvasha N., Mikhaylik E.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This study provides a comparative evaluation of Java Virtual Machine (JVM) garbage collectors, namely G1GC, Parallel GC, and Serial GC, employing a flame fractal generator as a computational benchmark. The analysis focuses on both technical performance and economic efficiency of software systems, assessing metrics such as response time, CPU utilization, and the frequency and duration of pause events. The results enable the identification of an optimal balance between computational performance and operational costs. Based on these findings, recommendations are formulated for selecting the most appropriate garbage collector for applications with varying workload profiles, thereby contributing to reduced infrastructure expenditure and enhanced return on investment in IT systems.

Key words: *memory management, system performance, software economics, Java, JVM, garbage collection, G1GC, Parallel GC, Serial GC*

УДК 004.048
ГРНТИ 28.23.29

ИССЛЕДОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАБОТКЕ БОЛЬШИХ ДАННЫХ

Е. В. Коровкина, Д. А. Молоков

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

В статье проводится исследование применения технологий искусственного интеллекта в обработке больших данных. Приведена актуальная статистика использования ИИ российскими компаниями и в каком соотношении этапов обработки больших данных используется данная технология. Рассмотрены преимущества ИИ-аналитики по сравнению с ее традиционным подходом. Особое внимание уделено перспективам интеграции ИИ в СУБД в виде оптимизации и поддержки запросов на естественном языке, а также возможным рискам такого решения.

ИИ, системы обработки данных, СУБД, большие данные

Искусственный интеллект все активнее применяется не только в повседневной жизни, но и в корпоративных целях для сокращения трудозатрат. Особенно значима его роль в сфере обработки больших данных.

Согласно исследованию, 24 % российских компаний используют искусственный интеллект [1]. Анализ показал, что 49 % компаний применяет ИИ ежедневно, а 30 % – 2-4 раза в неделю. Для детального анализа представлена диаграмма на рисунке 1.

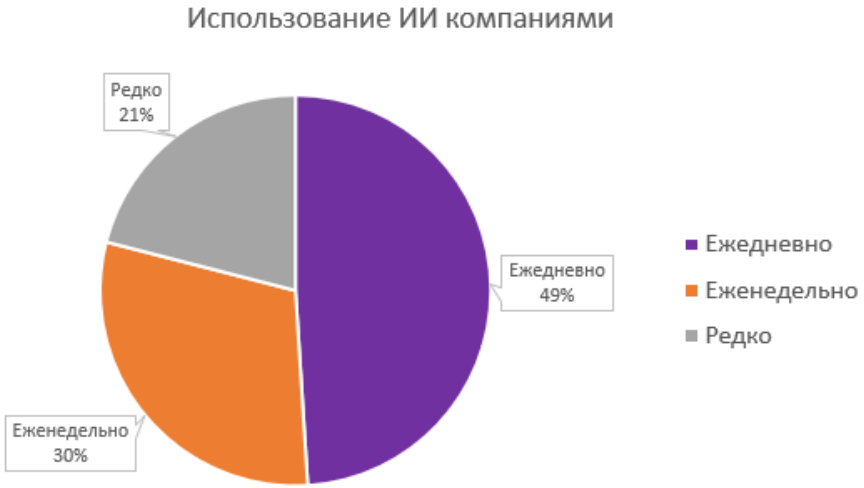


Рис. 1. Использование ИИ компаниями

Актуальность использования ИИ в сфере больших данных подтверждается проведенным исследованием, результатом которого стало, что объем работ, выполняемых ИИ, стремится уже к половине, как показано на рисунке 2 [1]. Среди представленной статистики для данной статьи особенную важность имеют задачи, используемые в системах обработки данных, а именно сбор информации (36 %), вычисления (32 %) и обработка запросов (32 %).

Рис. 2. Использование ИИ в задачах

Каждый день создается более 400 млн терабайт данных [2]. Безусловно, эта цифра будет стремительно расти, поэтому использование технологии ИИ в сфере обработки больших данных является перспективным направлением. Эту тенденцию мы уже можем наблюдать на рисунке 2.

Обработка с помощью ИИ позволяет:

– эффективно собирать данные из большого пула неоднородных источников и затем обрабатывать данные, очищая и упорядочивая;
– выявлять скрытые закономерности, неочевидные для человека при ручном анализе;
– помогать аналитикам интерпретировать тенденции, предоставляя инсайты, прогнозы и рекомендации на основе данных.

Это значительно упрощает анализ больших данных, приводит к эффективному анализу и более обоснованным решениям.

Интегрирование ИИ в системы управления базами данных является одной из ключевых перспектив в обработке больших данных [3]. Можно выделить два направления: интеграция компонентов ИИ непосредственно в СУБД и поддержка запросов на естественном языке [4].

Первое направление позволит анализировать данные и логи самой СУБД, а затем выполнять соответствующие действия, что не только повысит эффективность, но и безопасность базы данных.

Реализация второго направления позволит работать с СУБД пользователям без технической подготовки и оптимизировать запросы. Это позволит уменьшить расходы средств на обучение персонала.

Данная технология ускоряет анализ данных и повышает его точность, но интеграция может вызвать новые риски, как это видно в современных примерах использования, когда ИИ начинает вести не так, как его задумывали:

1. Человеческий фактор. Сделать автономный ИИ на данном этапе развития технологий не представляется возможным, что означает совместную работу ИИ с человеком, а значит, и различные проблемы, например, повышенная сложность интерпретации решений ИИ, а также недоверие или чрезмерное доверие к ее решениям.

2. Повышенный контроль за обучением модели – необходимость тщательной валидации и мониторинга моделей ИИ, так как в функционал инструмента входит обработка данных, в том числе и заполнение пустых значений, ошибки в обучении могут привести к серьезным убыткам.

3. Повышение нагрузки на СУБД – обработка запросов на естественном языке, постоянный мониторинг может затребовать значительных вычислительных ресурсов.

4. Необходимость развивать у сотрудников новые компетенции по работе с инструментами на основе ИИ, что требует времени и средств.

Интеграция искусственного интеллекта постепенно становится не просто преимуществом, а необходимостью для компаний, стремящихся оставаться конкурентоспособными в условиях стремительно растущего объема данных. Дальнейшее использование данной технологии в системах обработки данных и в анализе больших данных – следующий шаг в развитии данной области.

Список используемых источников

1. Четверть российских компаний применяют искусственный интеллект в работе. URL: https://realnoevremya.ru/news/336870-chetvert-rossiyskih-kompaniy-primenyayut-iskusstvennyy-intellekt-v-rabote (дата обращения 10.06.2025).

2. Как изменится рынок big data в 2025 году: 5 ключевых трендов. URL: https://trends.rbc.ru/trends/industry/cmrm/67a5781b9a7947a772708fdf?from=copy (дата обращения 10.06.2025).

3. Рынок систем управления и обработки данных в России: текущее состояние и перспективы развития до 2031 года. URL: https://www.csr.ru/upload /iblock/2cc/cq1atw03el2s4ymd1cuqb00nqo7cj9lf.pdf (дата обращения 11.06.2025).

4. Переход из Oracle в Postgres Pro: не просто смена СУБД, а сдвиг подхода. Интервью с Марком Ривкиным. URL: https://postgrespro.ru/blog/media/5971899 (дата обращения 13.06.2025).

Статья представлена научным руководителем, заведующим кафедрой СОД СПбГУТ, кандидатом технических наук, доцентом Ю. М. Бородянским.

RESEARCH ON ARTIFICIAL INTELLIGENCE IN BIG DATA PROCESSING

Korovkina E., Molokov D.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article studies the use of artificial intelligence technologies in big data processing. It provides current statistics on the use of AI by Russian companies and the ratio of big data processing stages in which this technology is used. The advantages of AI analytics are considered compared to its traditional approach. Particular attention is paid to the prospects for integrating AI into DBMS in the form of optimization and support for natural language queries, as well as the possible risks of such a solution.

Key words: *AI, data processing systems, DBMS, big data*

УДК 004.89:004.912:069
ГРНТИ 28.23.39, 18.41.35

ИССЛЕДОВАНИЕ ПРОБЛЕМЫ ФОРМИРОВАНИЯ СЕМАНТИЧЕСКОГО ЯДРА АТРИБУЦИОННЫХ ДАННЫХ ПРЕДМЕТОВ В РАМКАХ ЦЕНТРАЛИЗОВАННОГО УЧЕТА МУЗЕЙНОГО ФОНДА

М. В. Котлова[1], Р. Я. Лабковская[2]

[1]Военно-исторический музей артиллерии, инженерных войск и войск связи
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье обосновывается актуальность цифровизации процессов музейного учета. Рассмотрен протокол обмена данными между локальными музейными системами и государственной централизованной системой учета предметов. Предложено сочетание базовых компонент при централизованной процедуре регистрации предметов. Определена основная проблема, препятствующая цифровой трансформации систем учета в контексте формирования набора атрибутов объектов. Предложена концептуальная структура семантического ядра для стандартизации схем описания и определения набора атрибутов предметов на основе онтологического подхода.

информационные системы, системы учета, музейные предметы, цифровая трансформация

Тенденции развития современных информационных технологий смещают цифровой вектор национальной политики в области искусства и музейного дела в сторону интеграции электронного учета и документооборота. Большинство процессов в музеях в настоящее время не обходятся без автоматизации и сопровождения профессиональных информационных экспертных систем. Все процедуры, начиная от простого оформления нового предмета в собрание музея, его перемещения в экспозицию, реставрацию/консервацию и заканчивая его исключением или передачей в другое музейное собрание, не только имеют цифровые протоколы, отраженные в локальных музейных системах, но и требуют получения электронного разрешения в государственной централизованной системе.

Таким образом, задача цифровизации и автоматизации процессов музейного учета успешно решается за счет реализации специализированных музейных информационных систем, однако ввиду множества вариаций подобных решений возникает проблема, связанная с отсутствием стандартизации параметров и набора семантических атрибутов. В настоящее время существует порядка шести крупных семейств музейных систем, каждая из которых имеет уникальную настройку и пространство имен, отражающую

индивидуальный подход музея к вопросам учета, тем самым порождая множество различных моделей и наборов атрибуционных данных.

Государственный учет объектов Музейного фонда – музейных предметов предполагает несколько ступеней: первичный учет, который проводится музеем при оформлении новых предметов в локальной информационной системе; и централизованный учет, который проводится в федеральной государственной информационной системе Министерства культуры Российской Федерации – Государственном каталоге. Наборы полей между локальной и централизованной системами отличаются не только в контексте декомпозиции значений, но и с точки зрения сематического контекста, при этом централизованная система контролирует только наличие значения, исключая контроль содержимого набора принимаемых атрибутов предметов. Такой подход, основанный на базе разрозненности информационных систем, разностороннем подходе музеев и отсутствии единого семантического ядра атрибутов, создает ненормированный массив данных, который содержит как логические, так и структурные ошибки.

Взаимодействие между локальными автоматизированными информационными системами и централизованной системой Государственного каталога регламентируется с помощью XML-протокола, который определяет набор обязательных и вспомогательных параметров, передаваемых в систему [1]. На рис. 1 представлена концептуальная модель данных, передаваемых между системами, где оранжевым цветом определены обязательные параметры.

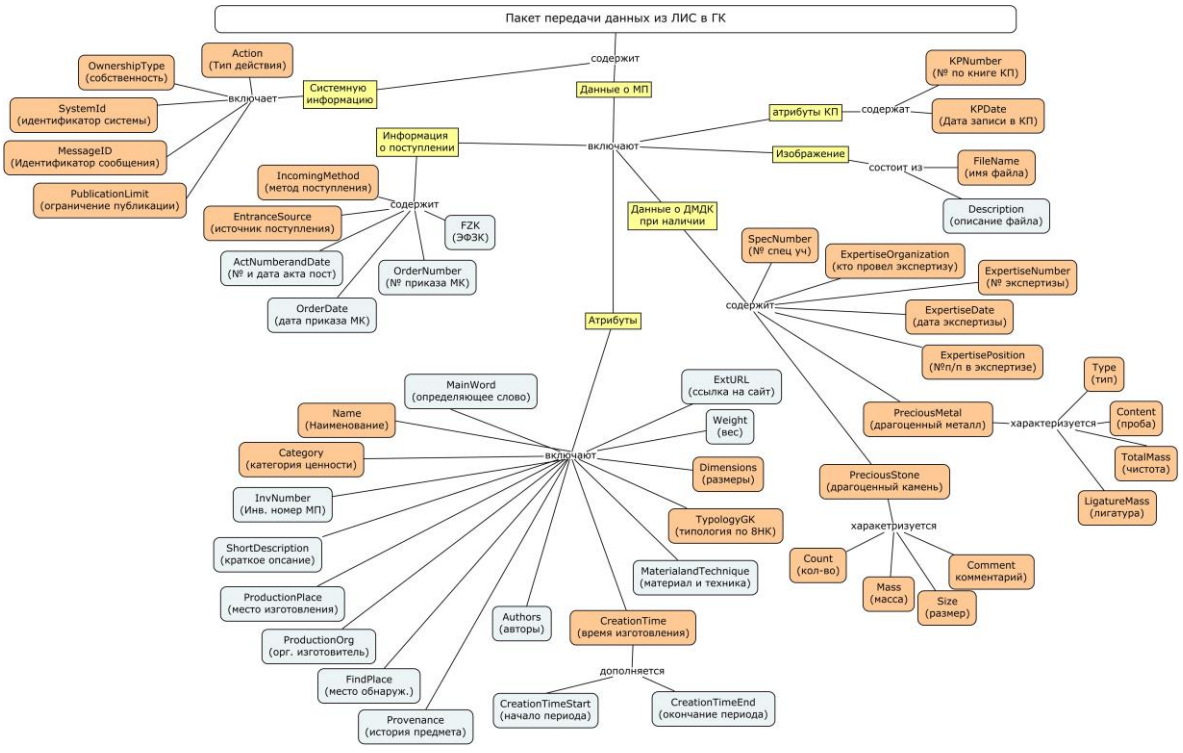


Рис. 1. Концептуальная модель данных

Основная проблема в настоящее время заключается в разностороннем подходе к определению контекста атрибутов предметов со стороны музеев. Централизованная система четко определяет набор параметров: наименование, размер, автор и т.д., в то время как в каждой отдельной локальной информационной системе может содержаться массив разнообразных значений, которые можно как интерпретировать в рамках одного параметра, так и в рамках нескольких, которые определяются в зависимости от типологии и статуса музейного предмета. Таким образом, для каждого типа предметов в каждом музее и музейном образовании формируется своя уникальная парадигма выбора атрибутов, под которую настраивается установленная версия музейной информационной системы [2].

Основная идеология централизованного учета, заключаемая в представлении целостного музейного фонда в парадигме единого подхода к изучению и учету, может быть достигнута при четком определении семантического ядра атрибутов предметов.

Учитывая разнообразие настроек реплик различных информационных музейных автоматизированных систем, необходимо стандартизировать набор и содержание основных компонентов, обеспечивающих атрибуцию и регистрацию предметов. Визуальное представление набора компонентов, смоделированное с учетом технологической последовательности процедуры учета, отраженной в нормативно-правовом поле, отражено на рис. 2.

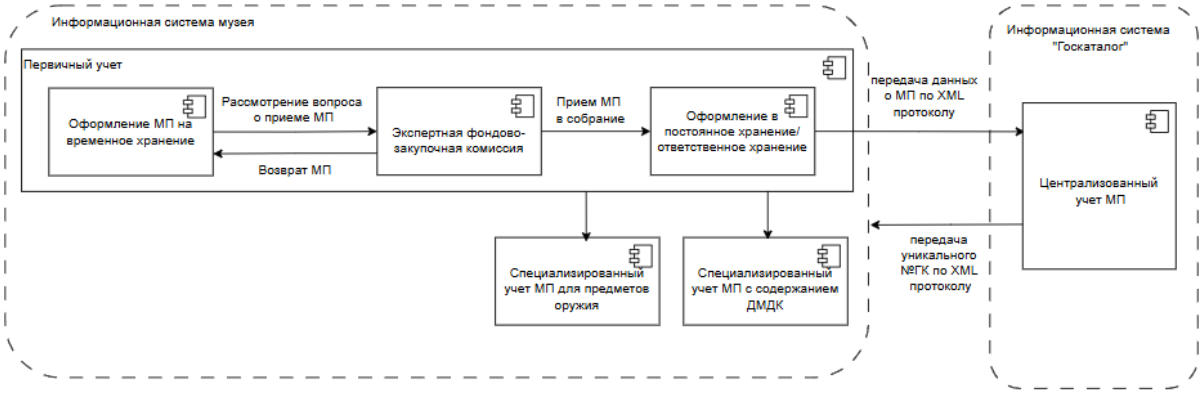


Рис. 2. Взаимодействие основных компонентов информационных систем

Стандартизация компонентного подхода определяет необходимость пересмотра текущего подхода к процедурам учета и контроля и формирует вектор в сторону единой распределенной системы учета, сформированной на базе единого пространства имен.

Задача формирования структуры семантического ядра для стандартизации схем описания и определения набора атрибутов предметов может быть решена только при эффективном взаимодействии специалистов областей музейного дела и информационных технологий, но, несмотря на трудоемкость этой задачи, можно определить концептуальную компоненту этого набора атрибутов.

На рис. 3 представлено графическое отображение концептуальной структуры семантических компонентов стандартизированного ядра атрибутов музейных предметов, определяемых при поступлении музейных предметов в собрание музея в рамках онтологического подхода.

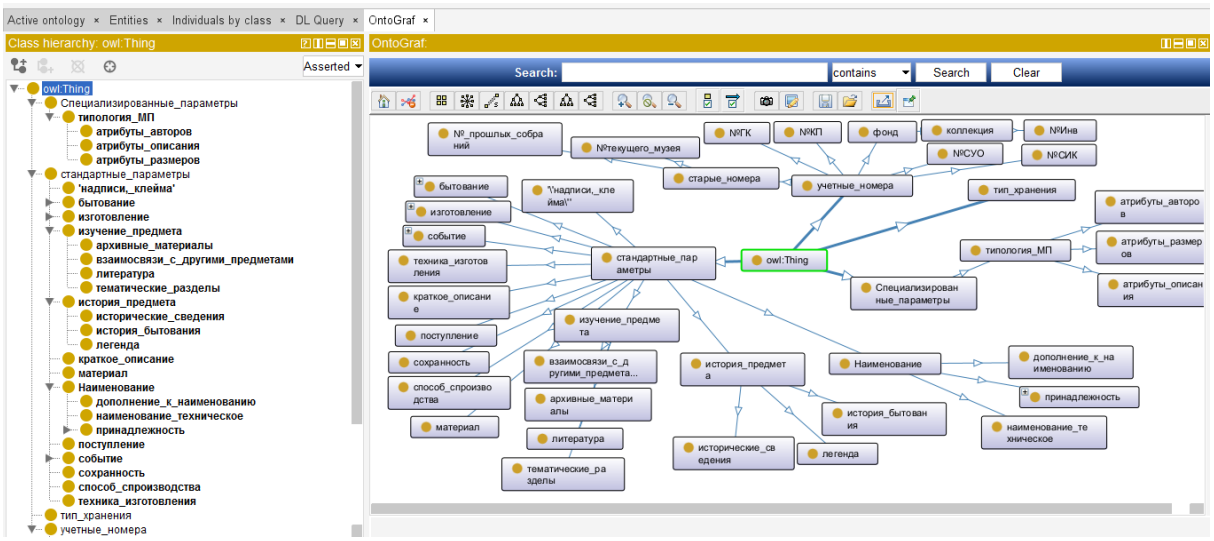


Рис. 3. Онтология концептуального набора атрибутов

Полномасштабное ядро атрибуционных параметров должно включать в себя справочники значений, раскрывающие каждый компонент, а также правила выбора и определения атрибутов. Важно учитывать, что для каждой типологии предмета необходим индивидуальный подход, обеспечивающий полноценное и корректное описание, исключающее человеческий фактор выбора методологии описания. Таким образом, вопрос интеграции аспектов стандартизации подходов к изучению и атрибуции предметов, позволяет определить вектор цифровой трансформации музейных информационных систем в контексте представления единого массива музейного собрания российской Федерации.

Список используемых источников

1. Протокол обмена данными о музейных предметах информационной системы Государственного каталога. URL: https://goskatalog.ru/portal/#/for-museums/docs?id= (дата обращения 29.06.2025 г.)

2. Птицына Л. К., Котлова М. В. Генерация онтологических моделей коллекций экспонатов// Информационные системы и технологии в моделировании и управлении: сборник материалов всероссийской научно-практической конференции (23-24 мая 2016 г.): сб. мат. конференции. / отв. Секретарь Н. Н. Олейник.Симферополь: ИТ «АРИАЛ», 2016. С. 63-68

STUDY OF THE PROBLEM OF FORMING A SEMANTIC CORE OF ATTRIBUTION DATA OF OBJECTS IN THE FRAMEWORK OF CENTRALIZED ACCOUNTING OF A MUSEUM FUND

Kotlova M.[1], Labkovskaya R.[2]
[1]Military History Museum of Artillery, Engineering Troops and Signal Corps
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article substantiates the relevance of digitalization of museum accounting processes. The data exchange protocol between local museum systems and the state centralized system of accounting of objects is considered. A combination of basic components in the centralized procedure of registration of objects is proposed. The main problem hindering the digital transformation of accounting systems in the context of forming a set of attributes of objects is identified. A conceptual structure of the semantic core for standardization of description schemes and definition of a set of attributes of objects based on the ontological approach is proposed.

Key words: *information systems, accounting systems, museum objects, digital transformation*

УДК 004.89:004.94:069
ГРНТИ 28.23.15, 18.41.35

ФОРМИРОВАНИЕ МОДЕЛИ РАСПРЕДЕЛЕННОЙ ГОСУДАРСТВЕННОЙ СИСТЕМЫ УЧЕТА МУЗЕЙНЫХ ПРЕДМЕТОВ

М. В. Котлова[1], Р. Я. Лабковская[2]

[1]Военно-исторический музей артиллерии, инженерных войск и войск связи
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматривается формирование концепции распределенной системы государственного учета музейных предметов. Сформулирован набор основных требований. Предложена модель единой распределенной системы учета предметов Музейного фонда Российской Федерации. Представлена концептуальная структура комплексной автоматизированной информационной системы и сформулировано обоснование приоритетности интеграции единой системы, в условиях динамически развивающегося законодательства. Определены перспективы эволюции функциональных возможностей распределенной системы.

модель информационной системы, распределенная система учета, музейные предметы

Прогрессивное развитие цифрового учета музейных предметов в Российской Федерации способствует активной трансформации специализированных информационных систем. В условиях необходимости решения актуальных задач и интеграции современных информационных технологий с элементами искусственного интеллекта, разрабатываются новые цифровые сервисы, автоматизированные системы и активно модернизируются индивидуальные информационные решения, созданные под конкретные требования крупного музея.

Развитие нормативно-правовых актов в области музейного законодательства определило необходимость проведения централизованного государственного учета для музеев, хранящих государственную часть Музейного фонда Российской Федерации. Для этих целей разработана и успешно внедрена федеральная государственная информационная система «Государственный каталог». Взаимодействие музейных информационных систем и государственной информационной системы определяется в соответствии с протоколом передачи данных, который определяется на законодательном уровне. Важно отметить, что развитие структуры «Государственного ката-

лога» требует доработки, модернизации, а иногда и разработки новых компонентов локального музейного программного обеспечения.

С каждым годом растет количество компаний, разрабатывающих специализированное музейное программное обеспечение. Число вариаций музейных информационных систем стремится к количеству музеев в Российской Федерации, таким образом, практически не существует двух одинаковых программ. Такая вариативность обусловлена возможностью адаптации коммерческого программного обеспечения под все тонкости и нюансы работы музея, что в свою очередь формирует множество подходов к технологическому исполнению процедур учета и контроля музейных предметов, а также формированию семантических искажений терминологии при описании музейных предметов. На рис. 1. представлена модель учета предметов музейного фонда.

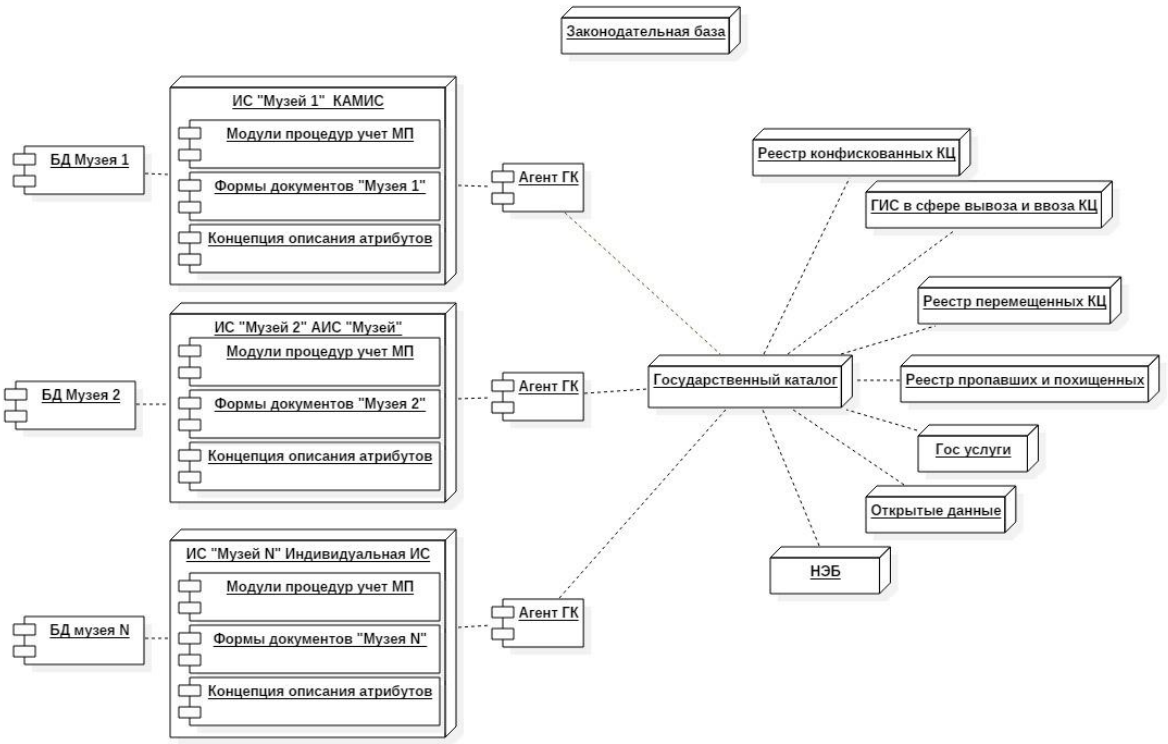


Рис. 1. Модель учета музейных предметов

Данная модель наглядно демонстрирует разрозненность подходов, когда у каждого музея различное автономное программное обеспечение, индивидуальный набор форм документов, авторская концепция описания атрибутов объектов.

Принимая во внимание, что Музейный фонд Российской Федерации разделен на части и хранится в музеях разного уровня подчинения, необходимо выработать единообразный подход к учету, атрибуции и контролю.

Предлагаемая модель единой распределенной системы государственного учета представлена на уровне компонентов на рис. 2.

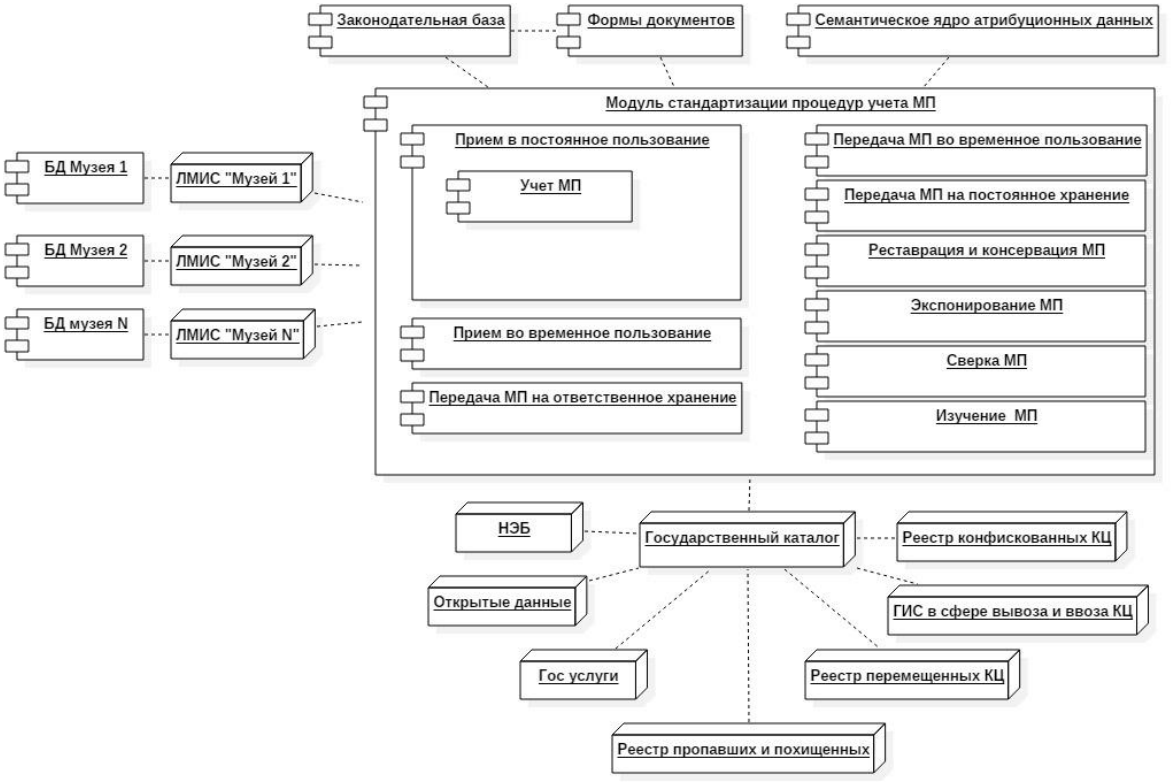


Рис. 2. Модель единой распределенной музейной информационной системы

Распределенная музейная информационная система в своем подходе основана на стандартизации всех основных технологических операций, при этом должно соблюдаться соответствие с актуальными требованиями законодательства, формами и семантическим ядром атрибуционных данных, позволяющих использовать единый подход при описании предмета. В настоящее время система Государственного каталога уже интегрирована в единую коммуникационную среду с порталом Государственных услуг, а атак же других государственных реестров и систем [1].

Важным аспектом является сохранение индивидуальных, изолированных от общего доступа баз данных каждого музея, при этом основная структура базы данных должна соответствовать требованиям централизованной системы для беспрепятственной передачи данных о музейных предметах.

К основным требованиям распределенной информационной системы относятся: обеспечение доступности компонентов музейной информационной системы, стандартизация протоколов операций с музейными предметами, устойчивое взаимодействие с централизованной системой Государственного каталога, соответствие действующему законодательству, своевременная модернизация компонентов и формирование отказоустойчивой базы программной платформы.

Инновационный подход к формированию распределенной мультиагентной системы, реагирующей на изменения внешней среды в режиме реального времени [2], в данном случае основан на концептуальной структуре исполнения процессов комплексной автоматизированной информационной системы (рис. 3).

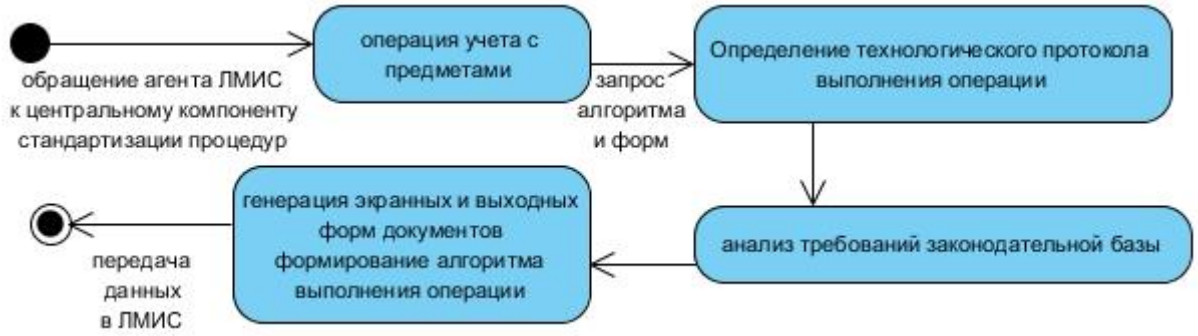


Рис. 3. Концепция исполнения процессов

Такой подход позволяет решить сразу несколько проблем и формировать единый подход к учету музейных коллекций, предоставить возможность перехода на электронный документооборот для всех участников системы, организовать прозрачный контроль за исполнением требований действующего законодательства и упростить процесс согласования и подготовки межмузейных выставочных проектов.

Интеграция модуля стандартизации цифровых протоколов операций с музейными предметами и объединение всех организаций, хранящих музейные предметы, в единую распределенную систему, предоставляет возможность не только осуществлять мониторинг всевозможных статистических аспектов в режиме реального времени, но и проводить анализ качества полноты Музейного фонда за счет интеграции интеллектуальных агентов.

Список используемых источников

1. Методические материалы портала «Госкаталог.РФ». URL: https://goskatalog.ru/portal/#/for-museums/docs (дата обращения 01.07.2025 г.)

2. Лабковская Р. Я., Тарасов В. А. Исследование подхода к интеллектуализации управления корпоративной информационной инфраструктурой // 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. 455-457.

MODEL FORMATION OF THE DISTRIBUTED STATE SYSTEM OF ACCOUNTING OF MUSEUM OBJECTS

Kotlova M.[1], Labkovskaya R.[2]
[1]Military History Museum of Artillery, Engineering Troops and Signal Corps
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article considers the concept formation of the distributed State system of accounting of museum objects. Has been formulated a set of basic requirements. The model of the unified of the distributed State system of accounting of museum objects of the Museum Fund of the Russian Federation is proposed. The conceptual structure of an integrated automated information system is presented and a justification for the priority of integration of the unified system in the context of dynamically developing legislation is formulated. Prospects of evolution of functional capabilities of the distributed system are determined.

Key words: *information system model, distributed accounting system, museum objects*

УДК 004.62+616.3+664
ГРНТИ 50.53, 50.31, 76.29

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ УЛУЧШЕНИЯ КАЧЕСТВА ЖИЗНИ ЛЮДЕЙ С НЕПЕРЕНОСИМОСТЬЮ ЛАКТОЗЫ

Р. Я. Лабковская

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

Обеспечение безопасного и персонализированного питания для лиц с непереносимостью лактозы является актуальной задачей, требующей комплексных решений в области информационных технологий. В статье продемонстрировано применение технологий искусственного интеллекта для решения социально значимой проблемы, с целью улучшения качества жизни целевой группы пользователей. Применены методы обработки естественного языка для семантического анализа, подходы построения онтологий для классификации продуктов, алгоритмы рекомендательных систем, а также интеграция данных через внешние интерфейсы программного взаимодействия.

анализ данных, непереносимость лактозы, искусственный интеллект, ИИ, обработка естественного языка, рекомендательные системы

Непереносимость лактозы – распространенное состояние, обусловленное дефицитом фермента лактазы, приводящее к неспособности полноценно переваривать молочный сахар (лактозу). По оценкам, непереносимость лактозы затрагивает до 65-70 % взрослого населения мира, с вариациями в зависимости от региона и этнической принадлежности [1]. На рис. 1 и 2 изображено визуальное представление непереносимости лактозы взрослого населения в %. Данное состояние вызывает не только физические симптомы (вздутие, диарея, боли в животе), но и существенно снижает качество жизни, создавая постоянный стресс при выборе пищи и ограничивая социальную активность. Основная сложность заключается в необходимости постоянного мониторинга состава продуктов, так как лактоза содержится не только в очевидных молочных продуктах, но и во множестве скрытых источников (хлеб, колбасы, соусы, лекарства). Традиционные методы контроля (изучение этикеток, использование списков) являются трудоемкими, подверженными ошибкам и не учитывают индивидуальную чувствительность. Технологии искусственного интеллекта (ИИ) предлагают мощный

инструментарий для преодоления этих барьеров и кардинального улучшения повседневной жизни целевой группы.

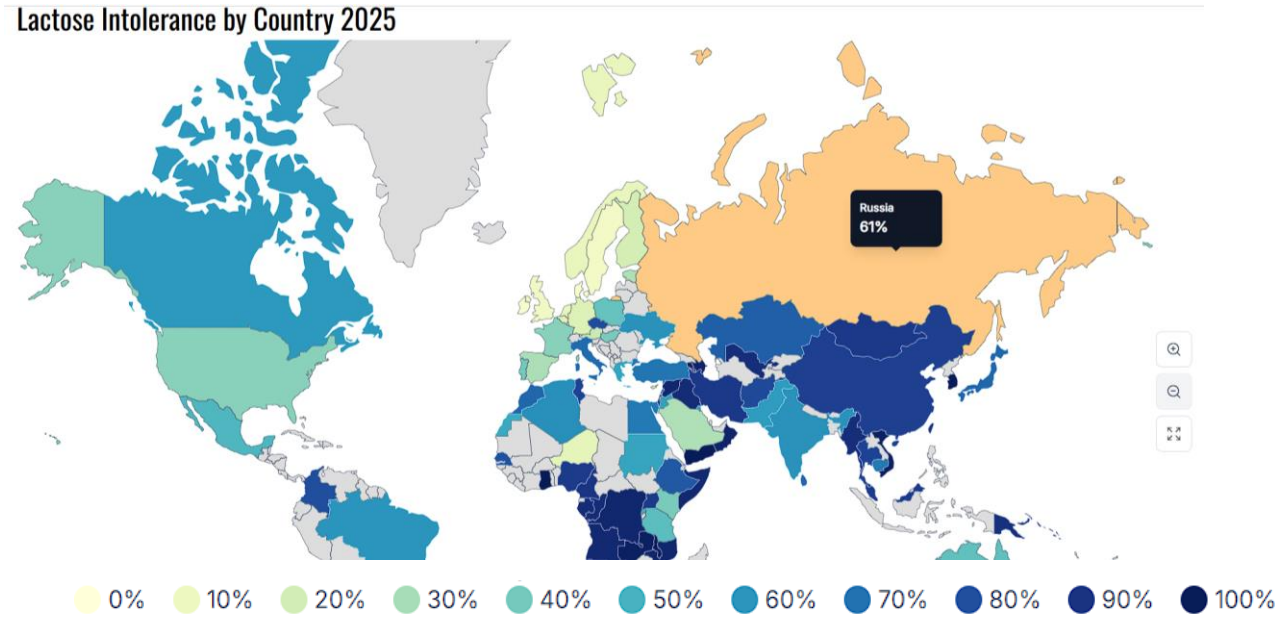


Рис. 1. Непереносимость лактозы (% населения)

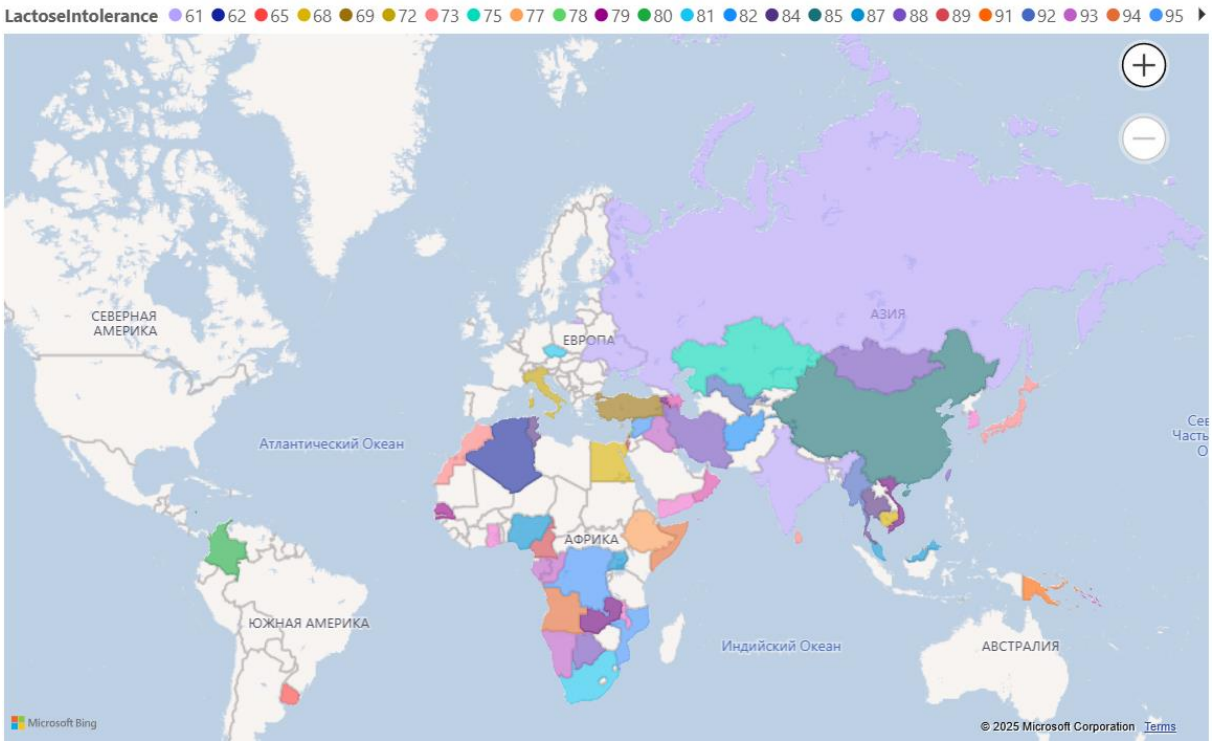


Рис. 2. Непереносимость лактозы (% населения) с порогом свыше 60 %

Методы ИИ в решении проблемы

Ключевым направлением применения методов ИИ является семантический анализ состава продуктов с использованием методов обработки естественного языка (NLP). Задача заключается в автоматическом извлечении и точной интерпретации информации [2] о составе из текста этикеток, описаний в интернет-магазинах или баз данных производителей. Для этого применяются передовые модели NLP, такие как BERT или Transformer, способные выполнять распознавание именованных сущностей (NER) для идентификации ингредиентов, проводить глубокий семантический анализ для понимания синонимов («молочный сахар» = лактоза), производных терминов («сыворотка», «сухое молоко») и контекста (например, фраз «может содержать следы молока»), а также оценивать неопределенность в формулировках. Результатом является точная идентификация наличия и потенциальных источников лактозы, исключающая человеческую ошибку при чтении мелкого шрифта или интерпретации сложных названий [3].

Для систематизации знаний и логического вывода о содержании лактозы, особенно в сложных случаях, критически важно построение и использование специализированных продуктовых онтологий [4]. Онтология представляет собой структурированную базу знаний, включающую классы (Продукты, Ингредиенты, Категории продуктов, Молочные компоненты с указанием содержания лактозы), свойства (содержитсяЛактоза, производноеОт, содержаниеЛактозы) и отношения (иерархические являетсяПодклассом, ассоциативные содержитИнгредиент). Такая онтология (рис. 3) позволяет системе логически выводить наличие лактозы в продукте, даже если она не указана явно, но присутствует через производный ингредиент. Например, система может определить, что колбаса содержит лактозу из-за добавления сухого молока, не упомянутого в основном описании, но связанного через онтологические отношения. Это обеспечивает основу для точной классификации и расширенного поиска безопасных продуктов.

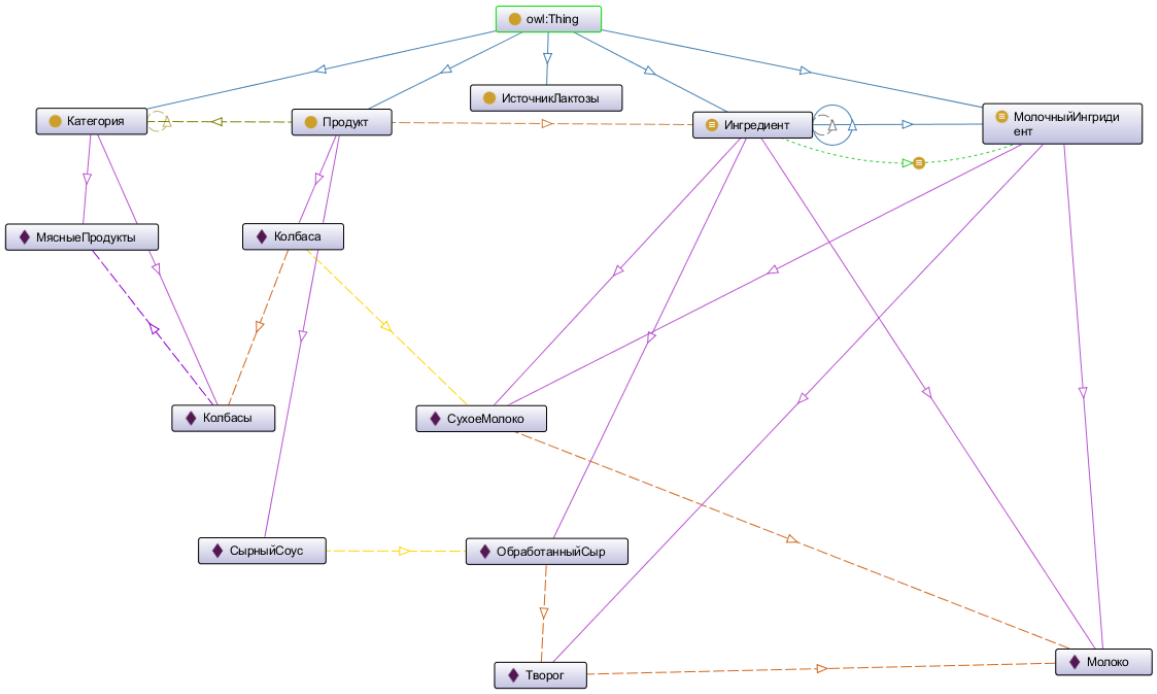


Рис. 3. Продуктовая онтология

На практике для пользователя наиболее важным компонентом являются персонализированные рекомендательные системы, задача которых заключается в подборе не просто безопасных, но и релевантных продуктов, рецептов и целых рационов с учетом уникальных особенностей каждого человека. Для решения данной задачи можно применять:

– коллаборативную фильтрацию, которая анализирует предпочтения «похожих» пользователей (с аналогичной степенью непереносимости, вкусами, целями);
– контентную фильтрацию, основанную на характеристиках продуктов (отсутствие лактозы, категория, пищевая ценность) и профиле пользователя (любимые блюда, дополнительные ограничения – вегетарианство, аллергии);
– гибридные подходы, комбинирующие методы для повышения точности и преодоления проблемы «холодного старта» для новых пользователей;
– учет индивидуального порога толерантности через интеграцию данных о самочувствии пользователя после приема пищи.

Таким образом, применение комплекса методов искусственного интеллекта – семантического анализа (NLP), онтологического моделирования и рекомендательных систем – открывает революционные возможности для решения проблемы непереносимости лактозы. В

настоящее время ведется разработка ИИ-решения для людей с непереносимостью лактозы, способное трансформировать повседневный опыт миллионов людей, избавляя от постоянного страха перед едой и пищевых ограничений. Данное решение обеспечит безопасность питания, возвратит чувство контроля и свободы выбора, что в совокупности приведет к значительному повышению общего качества жизни.

Список используемых источников

1. Lactose Intolerance by Country 2025 // World Population Review URL: https://worldpopulationreview.com/country-rankings/lactose-intolerance-by-country (дата обращения 08.07.2025).

2. Казачкова Ю. А. Разрешение семантической неоднозначности: использование контекстуальных моделей BERT и GPT для точного анализа текста / Ю. А. Казачкова, А. Д. Евсеева // Актуальные проблемы современной лингвистики: Сборник научных статей к юбилею доктора филологических наук, профессора Евгении Александровны Нильсен. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2024. С. 121-126.

3. Зупарова, В. В. Эволюция обработки текста: роль трансформеров и современных языковых моделей / В. В. Зупарова, Т. И. Озеров, М. А. Кирюшина // Научные открытия: междисциплинарный взгляд на исследования: сборник статей Международной научно-практической конференции, Таганрог, 01 мая 2025 года. Уфа: ООО «Аэтерна», 2025. С. 50-52.

4. Ontology-Based Design of Intelligent Systems User Interface / A. S. Boriskin, D. N. Koronchik, I. I. Zhukau [et al.] // Открытые семантические технологии проектирования интеллектуальных систем. 2017. № 7. PP. 95-106.

THE APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS TO IMPROVE THE QUALITY OF LIFE FOR PEOPLE WITH LACTOSE INTOLERANCE

Labkovskaya R.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Providing safe and personalized nutrition for individuals with lactose intolerance is an urgent task that requires comprehensive solutions in the field of information technology. The article demonstrates the application of artificial intelligence technologies to solve a socially significant problem, in order to improve the quality of life of the target group of users. Natural Language Processing methods for semantic analysis, ontology construction approaches for product classification, recommendation systems algorithms, and data integration through external interfaces of software interaction were applied.

Key words: *data analysis, lactose intolerance, artificial intelligence, AI, Natural Language Processing, NLP, recommendation systems*

УДК 519.876.5
ГРНТИ 28.27.00

СРАВНИТЕЛЬНЫЙ АНАЛИЗ РЕЗУЛЬТАТОВ РАБОТЫ СИСТЕМ СИНТЕЗА ЗВУКОВЫХ СИГНАЛОВ

В. Е. Малахов[1,2]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] Институт проблем транспорта им. Н. С. Соломенко Российской академии наук

В статье представлен сравнительный анализ существующих аналоговых, цифровых и гибридных систем синтеза звуковых сигналов, а также исследование разработанной модульной системы синтеза и обработки звука. Рассмотрены актуальные проблемы, связанные с задержками, совместимостью версий и масштабированием. Описана архитектура разработанной системы с поддержкой выполнения на ЦПУ, ГПУ и ПЛИС. Проведены тесты производительности и стабильности, включающие измерения времени генерации, скорости сигнала, потерь данных и утечек памяти. Полученные результаты подтверждают эффективность предложенного решения. Представлена математическая модель модульной архитектуры, позволяющая формализовать расчет задержек, производительности и устойчивости системы.

синтез звука, модульная архитектура, ЦПУ, ГПУ, ПЛИС, производительность, стабильность

Синтез звука является одной из важных задач в музыкальном производстве, звуковом дизайне, телекоммуникациях и системах человеко-машинного взаимодействия. Рост требований к качеству и универсальности систем синтеза звука, а также появление новых процессорных архитектур создают предпосылки для разработки решений, обеспечивающих минимальные задержки при высоком качестве звука. Пользователи ожидают от ПО качества и скорости отклика как у аналоговых систем. Это требует не только точного моделирования, но и снижения задержки до физически достижимых уровней (<1 мс) [1]. С появлением новых процессорных архитектур (ПЛИС, GPU-ускорение) открываются возможности для более эффективной реализации алгоритмов синтеза.

Общее описание проблемной области

Каждый модуль обработки звука вносит задержку из-за алгоритмов ЦОС и аппаратной составляющей (память, АЦП/ЦАП, CPU). В сложных си-

стемах задержки накапливаются и критичны для реального времени [1], они требуют точной синхронизации [2, 3]. Ключевой компромисс: системы с упором на качество и гибкость «жертвуют» производительностью из-за сложных алгоритмов, тогда как высокопроизводительные решения (узкоспециализированные, упрощенные) «жертвуют» адаптивностью.

Цель исследований

Для сравнительного анализа были выбраны популярные цифровые рабочие станции (DAW):

1. Ableton Live;
2. FL Studio;
3. Logic Pro X.

Проведенный обзор показал, что цифровые системы обеспечивают высокое качество и гибкость, но часто уступают аналоговым по скорости отклика, что критично для интерактивных приложений. Для решения данной проблемы разработана модульная система синтеза и обработки звуковых сигналов, способная выполнять задачи на различных вычислительных архитектурах (ЦПУ, ГПУ, ПЛИС), обеспечивающей минимальные задержки и высокую стабильность работы при длительных нагрузках. Целью исследования является проведение тестов работы данной системы.

Описание разработанной системы

Разработанная система реализована в виде набора функционально обособленных модулей, объединенных единым управляющим ядром. Архитектура поддерживает:

– адаптивную буферизацию (минимизация задержек);
– асинхронное выполнение задач (точный временной контроль);
– многопоточность для работы с ПЛИС;
– оптимизированные математические вычисления;
– стандартизированные API для подключения внешних модулей;
– кроссплатформенность (Windows, Linux, macOS).

Проведение тестирования

Оценка производилась на эталонном устройстве со следующими параметрами конфигурации:

– ЦПУ: эталонное устройство Intel Core i5-10400 (6 ядер, 65W TDP);

– ГПУ: тестовое устройство NVIDIA GTX 1060 (1280 CUDA ядер);
– ПЛИС: платформа Xilinx Artix-7 XC7A100T.

Тестирование проводилось по двум направлениям: производительность и стабильность.

Задержка определялась путем измерения времени ответа в режиме реального времени [4]. Нагрузка измерялась по среднему пиковому значению (в % от одного потока) в тестовом проекте из 3–5 пресетов [5-7].

Целью теста производительности являлось измерение времени генерации сигнала, количества операций в секунду и скорости обработки при изменении нагрузки. Тест стабильности ставил задачей измерение задержек, потерь данных и утечек памяти при длительной работе.

Для эффективной оценки проведены тесты нескольких сценариев с изменением нагрузки в виде изменения количества обрабатываемой информации.

Для оценки скорости обработки звуковых событий введена метрика скорости сигнала, выраженная формулой 1.

$$P = \frac{N}{T}, \tag{1}$$

где N – количество операций;

T – время их выполнения, сек.

Для оценки деградация производительности используем сравнение времени на одну генерацию (формула 2), увеличение показателя будет свидетельствовать о деградации процесса.

$$D = \frac{T}{N}, \tag{2}$$

где N – количество генераций;

T – общее время выполнения задачи.

Если $D > 0{,}1$ сек/генерацию, это свидетельствует о существенном ухудшении производительности [8].

Тесты производительности

Задача данного теста – это оценка времени генерации сигналов и загрузки системы в разных реализациях (ЦПУ, ГПУ, ПЛИС), согласно метрикам: количество операций, общее время генерации, скорость сигнала (табл. 1, 2).

ТАБЛИЦА 1. Тесты производительности. Время генерации, сек

Система / Количество синусоид	Генерация на ЦПУ	Генерация на ГПУ	Генерация на ПЛИС	Ableton Live	FL Studio.плагин 3xOSC	Logic Pro X
1	0,000104	0,001600	0,000100	0,000030	0,004000	0,074000
10	0,001008	0,002100	0,000200	0,000290	0,006000	7,200000
100	0,010051	0,007800	0,001000	0,002200	0,005000	0,710000
1000	0,100372	0,058000	0,005000	0,027000	0,005000	75,000000
10000	1,003892	0,510000	0,050000	0,250000	0,052000	743,000000
100000	10,040210	5,200000	0,500000	2,900000	0,531000	7124,000000

ТАБЛИЦА 2. Тесты производительности. Скорость сигнала, сигн/сек

Система / Количество синусоид	Генерация на ЦПУ	Генерация на ГПУ	Генерация на ПЛИС	Ableton Live	FL Studio. плагин 3xOSC	Logic Pro X
1	9615,38460	625,00000	10000,00000	33333,33300	250,00000	13,51351
10	9920,63500	4761,90480	50000,00000	34482,75900	1666,66670	1,38889
100	9949,25880	12820,51300	100000,00000	45454,54500	20000,00000	140,84507
1000	9962,93790	17241,37900	200000,00000	37037,03700	200000,00000	13,33333
10000	9961,23090	19607,84300	200000,00000	40000,00000	192307,69000	13,45895
100000	9959,95100	19230,76900	200000,00000	34482,75900	188323,92000	14,03706

Тесты стабильности

Недостатки, проявляющиеся при длительной нагрузке, такие как утечки памяти, накопление ошибок или падение производительности, не могут быть обнаружены при коротких функциональных тестах. Поэтому

особую актуальность приобретает долговременное тестирование стабильной работы. Метрики данного тестирования – это: время работы (мс), число генераций, средняя задержка (мкс), деградация работы системы (сек/генерацию) (табл. 3-5).

ТАБЛИЦА 3. Тесты стабильности. Количество генераций

Система / Время работы (мс)	Генерация на ЦПУ	Генерация на ГПУ	Генерация на ПЛИС	Ableton Live	FL Studio.плагин 3xOSC	Logic Pro X
1,00	7	63	7	46	44	49
10	390	720	90	441	446	443
100	1045	8614	7045	4412	4413	4445
1000	10000	98045	16454	44015	44142	44101
6000	102767	612472	145377	264621	264612	264624
60000	6002472	6012564	6576731	2646154	2646234	2646124
600000	64572371	58152456	60057630	26461264	26461234	26467423

ТАБЛИЦА 4. Тесты стабильности. Средняя задержка, мкс

Система / Время работы (мс)	Генерация на ЦПУ	Генерация на ГПУ	Генерация на ПЛИС	Ableton Live	FL Studio.плагин 3xOSC	Logic Pro X
1	120,0	160,0	120,0	230,0	210,3	220,7
10	115,0	150,0	115,0	230,0	210,2	220,7
100	112,0	145,0	112,0	230,0	210,3	220,7
1000	110,0	142,0	110,0	230,1	210,4	220,7
6000	113,0	148,0	113,0	230,3	210,4	220,7
60000	118,0	160,0	118,0	240,0	210,5	220,7
600000	130,0	185,0	130,0	270,0	210,8	130,0

ТАБЛИЦА 5. Тесты стабильности. Деградация работы системы, мс/генерацию

Система Время работы (мс)	Генерация на ЦПУ	Генерация на ГПУ	Генерация на ПЛИС	Ableton Live	FL Studio.плагин 3xOSC	Logic Pro X
1	0,143	0,016	0,143	0,022	0,023	0,020
10	0,026	0,014	0,111	0,023	0,022	0,023
100	0,096	0,012	0,014	0,023	0,023	0,022
1000	0,100	0,010	0,061	0,023	0,023	0,023
6000	0,058	0,010	0,041	0,023	0,023	0,023
60000	0,010	0,010	0,009	0,023	0,023	0,023
600000	0,009	0,010	0,010	0,023	0,023	0,023

Заключение

Анализ результатов показал, что разработанная система на ПЛИС демонстрирует минимальное время генерации и задержку, опережая цифровые рабочие станции в среднем в 4-6 раз. Использование ГПУ позволяет снизить задержки на 40-50 % по сравнению с ЦПУ. Стабильность системы при длительной работе выше благодаря адаптивной буферизации и контролю утечек памяти.

Разработанная модульная архитектура обеспечивает высокую гибкость, масштабируемость и совместимость с различными вычислительными архитектурами.

Переход на ГПУ и ПЛИС позволяет существенно снизить задержки и время генерации сигналов.

Система может применяться как в музыкальном производстве, так и в телекоммуникационных и интерактивных системах реального времени.

Список используемых источников

1. Roads C. The Computer Music Tutorial. Cambridge: MIT Press, 2022. 1234 p.

2. Dannenberg R. B., Brandt E., McAvinney P. Real – time software synthesis on superscalar architectures // Computer Music Journal. 1998. Vol. 22. № 2. PP. 49–64.

3. Золотарев В. А., Козлов И. А. Цифровая обработка сигналов. М.: Радио и связь, 2019. 384 с.

4. Чистяков Д. А. Звукорежиссура в цифровой среде: учебное пособие. М.: МГУКИ, 2020. 276 с.

5. Зельцер У. Цифровые звуковые эффекты / У. Зельцер; пер. с англ. М.: ДМК Пресс, 2012. 532 с.

6. Борвик Дж. Практика звукозаписи. М.: РадиоСофт, 2014. 495 с.

7. Пронский А. В. Цифровая музыка: технологии и производство. М.: ДМК Пресс, 2021. 312 с.

8. Попов В. Е., Иванов Д. Ю. Производительность вычислительных систем: проблемы оценки и обеспечения. СПб.: СПбГЭТУ «ЛЭТИ», 2019. 208 с.

Статья представлена научным руководителем, доктором технических наук, профессором, заведующим кафедрой ИКД, Д. В. Волошиновым

COMPARATIVE ANALYSIS OF THE RESULTS OF SOUND SIGNAL SYNTHESIS SYSTEMS

Malakhov V.[1, 2]
[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
[2.] N. S. Solomenko Institute of Transport Problems of the Russian Academy of Sciences

The article presents a comparative analysis of existing analog, digital and hybrid sound signal synthesis systems, as well as a study of the developed modular sound generation and processing system. The current problems associated with delays, version compatibility and scaling are considered. The architecture of the developed system with support for execution on the CPU, GPU and FPGA is described. Performance and stability tests are carried out, including measurements of generation time, signal speed, data loss and memory leaks. The obtained results confirm the effectiveness of the proposed solution. A mathematical model of the modular architecture is presented, allowing to formalize the calculation of delays, performance and stability of the system.

Key words*: sound synthesis, modular architecture, CPU, GPU, FPGA, performance, stability*

УДК 004.89
ГРНТИ 28.23

ПРИМЕНЕНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ СИСТЕМЫ КОНТРОЛЯ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ УНИВЕРСИТЕТА

Т. В. Матюхина, О. В. Раковский

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

Рассматриваются возможности применения мультиагентных систем и методов искусственного интеллекта для автоматизации контроля учебной деятельности в университете. Предложена архитектура интеллектуальной системы, включающей агентов, выполняющих функции мониторинга, анализа и управления учебным процессом. Описаны основные методы машинного обучения и обработки данных, применяемые для адаптации образовательных программ и повышения эффективности контроля.

мультиагентные системы, искусственный интеллект, контроль учебной деятельности, автоматизация, адаптивное обучение.

Современное образование в университетах характеризуется высокой динамичностью, разнообразием учебных программ и значительным объемом информации, связанной с учебной деятельностью студентов и преподавателей. Эффективный контроль учебного процесса является ключевым фактором обеспечения высокого качества образования и своевременного выявления проблем в обучении.

Традиционные методы контроля, основанные на ручном сборе и анализе данных, зачастую не обеспечивают необходимой оперативности и точности. В последние годы наблюдается активное развитие технологий искусственного интеллекта (ИИ) и мультиагентных систем (МАС), которые способны автоматизировать процессы мониторинга, анализа и управления учебной деятельностью, обеспечивая при этом адаптивность и масштабируемость решений.

Представляется целесообразным провести исследование возможностей применения мультиагентных систем и методов искусственного интеллекта для создания системы контроля учебной деятельности в университете, способной повысить качество управления образовательным процессом, снизить нагрузку на преподавателей и обеспечить персонализированный подход к обучению.

Мультиагентные системы представляют собой совокупность автономных программных агентов, взаимодействующих для решения комплексных задач [1-3]. В образовательной сфере МАС применяются для моделирования учебного процесса, поддержки принятия решений и адаптивного обучения. Агенты могут выполнять роли студентов, преподавателей и администраторов, обеспечивая сбор и анализ данных, координацию и управление.

Методы машинного обучения, обработки естественного языка и интеллектуального анализа данных позволяют выявлять закономерности в образовательных данных, прогнозировать результаты и формировать рекомендации. Классификация и регрессия используются для оценки успеваемости и адаптации программ, а NLP – для анализа текстовых ответов и обратной связи.

Существующие системы контроля часто ограничены функционально и плохо интегрируются с другими образовательными сервисами. МАС обеспечивают гибкость и масштабируемость, однако требуют решения задач координации агентов и безопасности данных.

Современные мультиагентные системы в образовании строятся на базе интеллектуальных агентов, обладающих следующими основными свойствами:

– автономность. Агент способен самостоятельно принимать решения и выполнять действия без постоянного контроля извне;
– чувствительность. Агент воспринимает изменения в окружающей среде и реагирует на них;
– активность. Агент проявляет инициативу в достижении поставленных целей;
– социальность. Агент взаимодействует с другими агентами, обмениваясь информацией и координируя действия;

Эти свойства позволяют агентам эффективно функционировать в распределенной системе, моделируя поведение участников образовательного процесса – студентов, преподавателей, администраторов и других.

Интеллектуальный агент в образовательной мультиагентной системе обычно включает следующие компоненты:

– сенсоры (датчики) получают информацию из среды и от других агентов (например, данные о посещаемости, успеваемости, активности);
– база знаний хранит накопленные знания, модели поведения, опыт и правила принятия решений;

– планировщик задач формирует планы действий для достижения целей агента с учетом изменяющихся условий;
– эффекторы осуществляют воздействие на среду и взаимодействие с другими агентами (например, отправка сообщений, формирование рекомендаций).

В образовательных системах можно выделить следующие роли интеллектуальных агентов.

Агент студента отвечает за сбор данных о студентах, посещаемости, активности, выполнении заданий и тестов. Взаимодействует с обучающими платформами и системами учета, передавая информацию в систему.

Агент преподавателя анализирует данные, выявляет проблемные зоны в обучении, формирует отчеты и рекомендации для студентов и администрации по корректировке учебного процесса.

Агент администратора управляет расписанием занятий, ресурсами и координирует взаимодействие между участниками учебного процесса.

Агент-координатор обеспечивает синхронизацию действий всех агентов, контролирует обмен сообщениями и поддерживает целостность данных.

В таблице 1 представлены основные свойства интеллектуальных агентов и их функции.

ТАБЛИЦА 1. Основные свойства интеллектуальных агентов и их функции

Свойство	Описание	Функции в образовательной системе
Автономность	Самостоятельное принятие решений	Обработка данных, формирование рекомендаций
Чувствительность	Восприятие изменений в среде	Сбор информации о прогрессе и активности
Активность	Проявление инициативы	Инициирование взаимодействий и корректировок
Социальность	Взаимодействие с другими агентами	Обмен данными, координация действий

Предлагаемая мультиагентная система (МАС) для контроля учебной деятельности университета представляет собой распределенную платформу, состоящую из множества специализированных агентов, каждый из которых выполняет определенные функции в рамках образовательного процесса (рис. 1).

Взаимодействие агентов реализуется через стандартизованные протоколы обмена сообщениями, например, FIPA-ACL (Foundation for Intelligent Physical Agents - Agent Communication Language). Это обеспечивает:

– согласованность действий агентов;
– оперативный обмен информацией;
– возможность масштабирования и интеграции новых агентов.

Каждый агент обладает автономией в принятии решений, однако учитывает информацию, полученную от других агентов, что позволяет коллективно достигать целей контроля и управления учебным процессом.

Для анализа учебных данных применяются следующие методы машинного обучения:

– классификация – для распределения студентов по группам по уровню знаний и активности (например, «успешные», «рисковые», «нуждающиеся в поддержке»);
– регрессия – для прогнозирования итоговых оценок и вероятности успешного завершения курса.
– кластеризация – для выявления скрытых закономерностей и групп студентов с похожими образовательными потребностями.

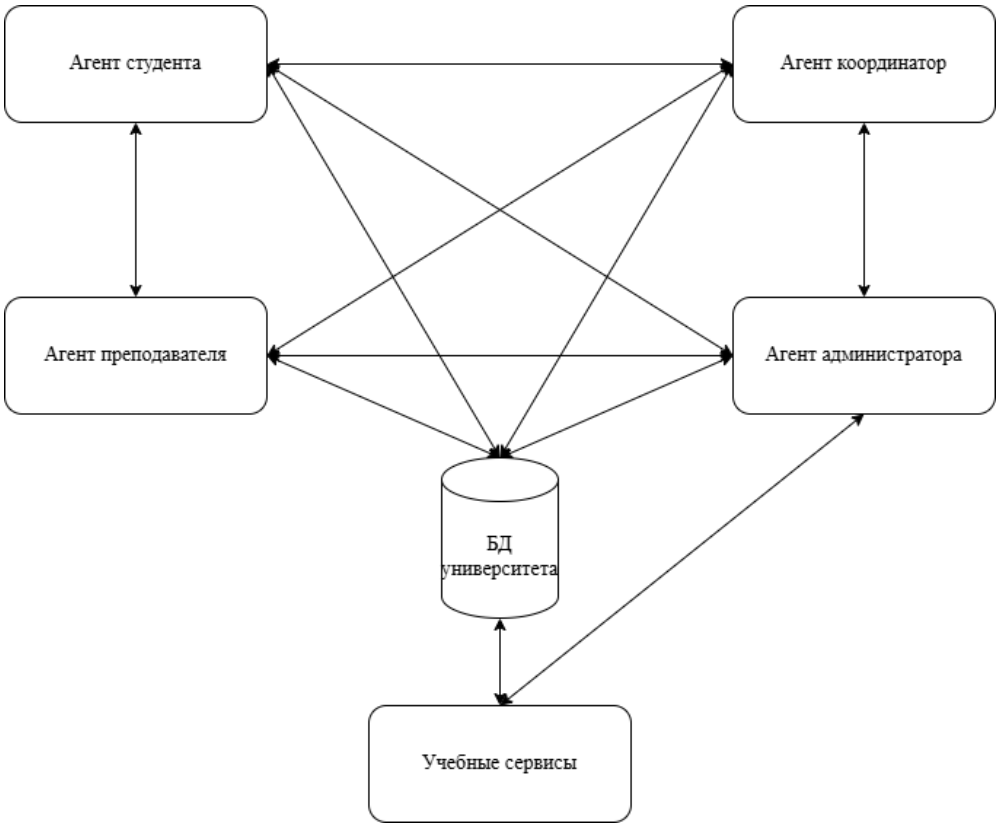


Рис. 1. Архитектура мультиагентной системы контроля учебной деятельности

На основе анализа данных система формирует рекомендации:
– индивидуальные учебные планы;
– дополнительные материалы и задания;
– корректировка расписания и нагрузки.

Таким образом, обеспечивается персонализация обучения и повышение эффективности учебного процесса.

Для анализа текстовых данных (ответы на открытые вопросы, отзывы студентов) применяется обработка естественного языка:
– выделение ключевых тем и проблем;
– анализ эмоциональной окраски отзывов;
– автоматическое формирование отчетов для преподавателей и администраторов.

В рамках интеграции с информационными системами университета система подключается к следующим ресурсам:
– электронным журналам и системам учета посещаемости;
– платформам дистанционного обучения (например, Moodle);
– базам данных успеваемости и расписания.

При разработке системы особое внимание следует уделять:
– защите персональных данных студентов и преподавателей;
– соответствию требованиям законодательства (например, ФЗ-152 «О персональных данных»);
– использованию защищенных каналов связи и аутентификации агентов.

Применение мультиагентных систем и искусственного интеллекта для контроля учебной деятельности университета позволяет:
– автоматизировать сбор и анализ данных;
– повысить качество управления учебным процессом;
– индивидуализировать обучение и повысить мотивацию студентов;
– снизить нагрузку на преподавателей и административный персонал.

В качестве направлений дальнейшей работы можно отметить:
– расширение функционала агентов;
– внедрение нейросетевых моделей для более точного прогнозирования;
– интеграция с системами больших данных и облачными сервисами.

Список используемых источников

1. Wooldridge M. An Introduction to MultiAgent Systems. Wiley, 2009. 484 c. ISBN: 978-E-UDT-E0055-3.

2. Золотов О. И., Матюхина Т. В., Раковский О. В. О роли искусственного интеллекта в системах принятия решения, применительно к управлению структурами с обратной связью // Актуальны проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2024. Т. 2. 636 с. С. 318-321.

3. Бондаренко И. Б., Пелих Д. А., Раковский О. В. Профилирование агентов при разработке мультиагентной системы управления городом // Международный научно-исследовательский журнал. 2025. № 2 (152). DOI: 10.60797/IRJ.2025.152.34.

APPLICATION OF MULTI-AGENT SYSTEMS AND ARTIFICIAL INTELLIGENCE FOR THE MONITORING SYSTEM OF UNIVERSITY EDUCATIONAL ACTIVITIES

Matyukhina T., Rakovskii O.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The possibilities of using multi-agent systems and artificial intelligence methods to automate the control of educational activities at the university are considered. The architecture of an intelligent system is proposed, including agents performing the functions of monitoring, analyzing and managing the educational process. The main methods of machine learning and data processing used to adapt educational programs and improve the effectiveness of control are described.

Key words: *Multi-agent systems, artificial intelligence, control of learning activities, automation, adaptive learning*

УДК: 510.633
ГРНТИ 27.03.19

ДВА ВАРИАНТА МИНИМАЛИСТИЧНОЙ АКСИОМАТИЗАЦИИ ИСЧИСЛЕНИЯ ВЫСКАЗЫВАНИЙ

С. А. Медведев

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

Разработан генератор аксиом-семантических фильтров. С помощью него построена аксиоматизация пропозициональной логики, основанная на операции Шеффера. Разработан семантический объект для описания унарных и бинарных операций Булевой алгебры, являющийся альтернативой таблицам истинности или диаграммам Венна. Он использует те же самые графические элементы, что и синтаксические диаграммы Вирта, которые иначе интерпретируются.

пропозициональная логика, Булева алгебра, операция Шеффера, эквиваленционная логика, аксиоматизация, визуализация

Впервые функционально полная логическая операция была открыта Чарльзом Пирсом в 1881 году. В 1913 году Генри Шеффер открыл еще одну функционально полную логическую операцию и популяризировал оба открытия [1]. Функционально полные логические операции позволяют выразить всю пропозициональную логику минимальными средствами, поэтому неоднократно осуществлялись попытки аксиоматизации всей логики с их использованием [2, 3]. Настоящая работа посвящена проблемам аксиоматизации пропозициональной логики с использованием функционально полной операции Шеффера.

Как правило, аксиомы в логике предназначены для синтаксического вывода. Однако очень часто на практике более эффективной с вычислительной точки зрения является семантическая проверка, использующая таблицы истинности, которые можно рассматривать просто как определенные неотрицательные целые числа, записанные в двоичной системе [4]. Поэтому предлагаемый подход к аксиоматизации рассчитан не на синтаксический вывод, а на семантическую фильтрацию. Аксиома при таком подходе представляют собой уравнение, единственным решением которого является определяемая логическая операция. Для автоматизации поиска аксиом был разработан специальный генератор аксиом. Он перебирает все синтаксические деревья и проверяет, является ли определяемая операция при данной структуре синтаксического дерева единственной, при которой соответству-

ющая формула тождественно истинна, или, если указано в настройках, тождественно ложна. На выходе эта программа выдает список сгенерированных аксиом. С использованием данного генератора было найдено 48 аксиом минимальной сложности, позволяющих однозначно определить эквиваленцию через операцию Шеффера, среди которых была выбрана такая:

$$((\top \barwedge (\bot \Leftrightarrow \top)) \barwedge ((\bot \Leftrightarrow (\top \Leftrightarrow \bot)) \Leftrightarrow \top)) \barwedge \top. \quad (1)$$

Эта формула тождественно истинна. Если эквиваленцию в ней заменить любой другой бинарной логической операцией, она станет тождественно ложной. Эквиваленция нужна для того, чтобы писать определения всех остальных логических операций: в левой части эквиваленции пишется определяемая операция, в правой части – эквивалентное этой операции выражение, которая включает в себя только операцию Шеффера. Например, определение конъюнкции через операцию Шеффера будет выглядеть следующим образом:

$$a \wedge b \Leftrightarrow (a \barwedge b) \barwedge (a \barwedge b).$$

То, что аксиомы тождественно истинны по определению, позволяет через операцию Шеффера определить истинностные константы, используемые в аксиоме эквиваленции (1), следующим образом:

$$\top;\ \bot \barwedge \bot. \quad (2)$$

Неопределяемым при таком подходе является концепт аксиомы как тождественно истинной формулы, а также сама операция Шеффера. Для ее определения было разработано два решения.

Во-первых, можно выразить классическое правило Modus ponens через эту операцию и доопределить ее аксиомой, найденной с помощью генератора аксиом:

$$a \barwedge (b \barwedge b), a \therefore b; \quad (3)$$

$$(a \barwedge a) \barwedge a. \quad (4)$$

Формула (4) останется тождественно истинной, только если операцию Шеффера заменить тривиальной операцией, всегда возвращающей истину, или обратной импликацией. Правило Modus ponens, выраженное через операцию Шеффера (3), исключает операцию, всегда возвращающую истину, потому что гарантирует, что если a истинно, а b ложно, выражение $a \barwedge (b \barwedge b)$ тоже должно быть ложным, а значит, операция $\barwedge$ не может быть тривиальной операцией, всегда возвращающей истину. Обратную импликацию это правило тоже исключает, и единственной возможной интерпретацией символа $\barwedge$ остается классическая операция Шеффера.

Во-вторых, можно использовать найденную с помощью генератора аксиом формулу, которая является тождественно ложной только для операции Шеффера и тривиальной операции, всегда возвращающей ложь:

$$\big(a \barwedge (a \barwedge a)\big) \barwedge \big((b \barwedge b) \barwedge b\big).$$

Тривиальная операция, всегда возвращающая ложь, будет исключаться аксиомой (2), через которую определяется константа лжи.

Единственность решения в обоих случаях соблюдается только при выполнении предположения о бинарности логики. Но бинарность можно рассматривать не только как предположение, но и как метатеорему. Например, если взять определение операции Шеффера, заданное формулами (3) и (4), и предположить, что существует третье истинностное значение U, этим формулам будут соответствовать разные возможные интерпретации. В одной из них определяемая операция возвращает истину во всех случаях, когда правая часть имеет значение U; в другой интерпретации операция возвращает истину, только если левая часть ложна, а правая имеет значение U. В результате в зависимости от выбранной интерпретации, формула $\top \barwedge U$ может быть как истинной, так и ложной. Это может рассматриваться противоречие, исходя из которого можно сделать вывод, что предположение о существовании значения U неверно. Дальнейшее добавление истинностных значений лишь увеличит эту неоднозначность. При необходимости работать с третьим значением «неизвестно» можно заменить его свободной пропозициональной переменной. Тождественно истинные формулы будут возвращать истину, тождественно ложные – ложь, а выполнимые – значение «неизвестно».

Оба этих решения имеют недостатки. Использование правила вывода Modus ponens в системе, рассчитанной на семантические проверки, выглядит избыточным. Использование тождественно ложной формулы требует метатеоретического отрицания, которое после определения функционально полной операции становится ненужным. В связи с этим возникла задача создать отдельный семантический объект, определяющий операцию Шеффера до ее использования в формулах.

Разработанный семантический объект представляет собой диаграммы, использующие те же самые элементы, что и синтаксические диаграммы Вирта [5], но с другой интерпретацией. Как и в случае диаграмм Вирта, любая диаграмма истинности имеет один входной порт и один выходной порт; порты обозначаются стрелками, показывающими направления движения. Как и в случае диаграмм Вирта, прохождение диаграммы истинности осуществляется от входного порта к выходному по плавным

линиям с разнообразными развилками, резкие изломы запрещены. Как и в случае диаграмм Вирта, линии могут проходить через овалы и прямоугольники, внутри которых написан текст. Но значение того, что написано внутри овалов и прямоугольников, в диаграммах истинности другое. Внутри овалов пишутся имена пропозициональных переменных. Если путь от входного порта к выходному проходит через переменную, ее значение истинно. В противном случае ее значение ложно. Внутри прямоугольников пишутся формулы, содержащие Булеву операцию, примененную к этим переменным. Если путь от входного порта к выходному проходит через операцию, она возвращает истину. В противном случае она возвращает ложь. Прохождение или непрохождение через овал или прямоугольник имеет однозначную семантику истинностных значений, с которыми работает пропозициональная логика: да или нет.

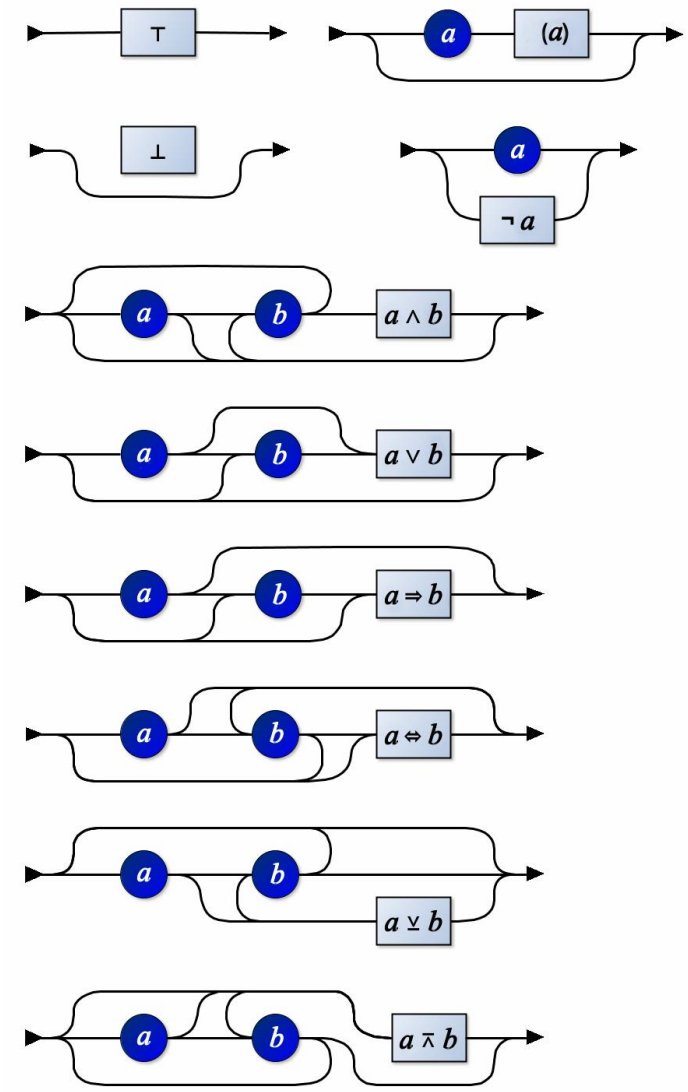


Рис. 1. Диаграммы истинности для основных Булевых операций

На рис. 1 показаны такие диаграммы для основных Булевых операций. Самая первая диаграмма описывает константу «Истина»: путь всегда проходит через прямоугольник с надписью «⊤». Под ней находится диаграмма с константой «Ложь»: путь никогда не проходит через прямоугольник с надписью «⊥». Еще чуть ниже расположена конъюнкция. Путь от входного порта к выходному по горизонтальной линии проходит через переменные *a* и *b*, а также через прямоугольник с надписью «$a \wedge b$». Это означает, что при обоих истинных операндах конъюнкция возвращает истину. Если от входного порта свернуть наверх, то путь к выходному порту пройдет только через переменную *b*. Это означает, что если *b* истинно, а *a* ложно, то конъюнкция вернет ложь. Если от входного порта свернуть вниз, то путь к выходному порту пройдет мимо обеих переменных и мимо прямоугольника с конъюнкцией. Это означает, что если оба операнда конъюнкции ложны, то конъюнкция тоже ложна. Наконец, если после прохождения переменной *a* свернуть вниз, то дальше на пути к выходному порту не встретится ни переменная *b*, ни прямоугольник с конъюнкцией. Это означает, что если *a* истинно, а *b* ложно, то конъюнкция вернет ложь. Аналогичным образом можно разобрать все остальные операции Булевой алгебры, семантика которых описана в виде таких диаграмм.

Получившийся семантический объект не специализирован для операции Шеффера и представляет собой альтернативу таблицам истинности или диаграммам Венна [6]. Логика, которую он описывает, однозначно бинарна. Кроме того, эти диаграммы могут быть прообразами электрических схем логических устройств: можно рассматривать их не как железнодорожные пути, а как кабели, по которым электричество идет от входных портов к выходным, проходя через овалы и прямоугольники. С другой стороны, созданный в ходе данного исследования генератор аксиом открывает возможности для разработки более эффективных алгоритмов обработки цифровых сигналов и их верификации. Полученные с помощью него результаты подтверждаются современными философскими представлениями о первичности различия (операции Шеффера) и вторичности тождества (эквиваленции) [7].

Список используемых источников

1. Sheffer H.M. A Set of Five Independent Postulates for Boolean Algebras, with Application to Logical Constants // Transactions of the American Mathematical Society. 1913. Vol. 14. № 4. PP. 481–488.

2. Гильберт Д., Аккерман В. Основы теоретической логики: пер. с нем. М.: Государственное издательство иностранной литературы, 1947. 304 с. ISBN 978-5-484-01144-5.

3. Quine W.V.O. Methods of Logic: 4th ed. Cambridge, MA: Harvard University Press, 1982. 344 p. ISBN 978-0674571761.

4. Kleene S.C. Introduction to Metamathematics. Amsterdam: North-Holland, 1952. 550 p. ISBN 978-0720421033.

5. Wirth, N. The Programming Language Pascal // Acta Informatica, 1971. Vol. 1. PP. 35 – 63.

6. Eric M. Hammer. Logic and Visual Information (Studies in Logic, Language, and Information): Center for the Study of Language and Inf, 1995, 124 p. ISBN 1881526992.

7. Делез Ж. Различие и повторение: пер. с франц. СПб.: ТОО ТК «Петрополис», 1998. 384 с. ISBN 5-86708-110-9.

TWO VARIANTS OF MINIMALISTIC AXIOMATIZATION OF PROPOSAL CALCULUS

Medvedev S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

A generator of axiom-semantic filters has been developed. With its help, an axiomatization of propositional logic based on the Sheffer operation has been constructed. A semantic object has been developed for describing unary and binary operations of Boolean algebra, which is an alternative to truth tables or Venn diagrams. It uses the same graphical elements as Wirth's syntax diagrams, which are interpreted differently.

Key words: *Propositional logic, Boolean algebra, Sheffer operation, equivalence logic, axiomatization, visualization.*

УДК: 510.624
ГРНТИ 27.03.19

ИСПОЛЬЗОВАНИЕ RAILROAD-ДИАГРАММ ДЛЯ ФИКСАЦИИ СЕМАНТИКИ

С. А. Медведев

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

При работе с формальными системами одним из важнейших инструментов являются формальные грамматики, которые могут быть визуализированы с использованием Railroad-диаграмм. Для задания семантики выражений, которые описываются формальными грамматиками, как правило, используются отдельные инструменты. В работе предлагается подход, позволяющий задавать семантику, используя только инструментарий формальных грамматик, что потенциально может оптимизировать разработку технически сложного оборудования.

пропозициональная логика, Булева алгебра, контекстно-свободная грамматика, атрибутная грамматика

Формальные системы широко используются при разработке технически сложного оборудования для автоматизации доказательства корректности его работы. Любая формальная система имеет синтаксис и семантику. При их описании, как правило, используются разные инструменты. Для описания синтаксиса используется либо нотация Бэкуса-Наура [1], либо railroad-диаграммы Вирта [2]. Для описания семантики используются разные инструменты в зависимости от конкретной формальной системы. В случае пропозициональной логики это таблицы истинности, диаграммы Венна или диаграммы решений [3]. Данная формальная система является фундаментом для любых других формальных систем: на ее базе строится логика предикатов, на базе логики предикатов строится теория множеств, на базе теории множеств строятся сама теория формальных систем [4]. При этом семантика классической пропозициональной логики достаточно проста для того, чтобы ее можно было выразить, используя только синтаксические инструменты. Это позволяет построить основание для любой формальной системы, используя абсолютный минимум неопределяемых понятий. Настоящая работа посвящена одному из возможных решений этой задачи.

В качестве инструмента описания синтаксиса предлагается использовать диаграммы Вирта в связи с их большей интуитивностью, достигаемой благодаря метафоре железной дороги. Еще одно преимущество диаграмм Вирта перед различными вариантами нотации Бэкуса-Наура состоит в том, что это не текстовая нотация, описывающая текст, а графическая нотация, описывающая текст. Это гарантированно позволяет избежать неоднозначностей в ситуациях, когда специальные символы, используемые для описания синтаксиса, встречаются в описываемом языке.

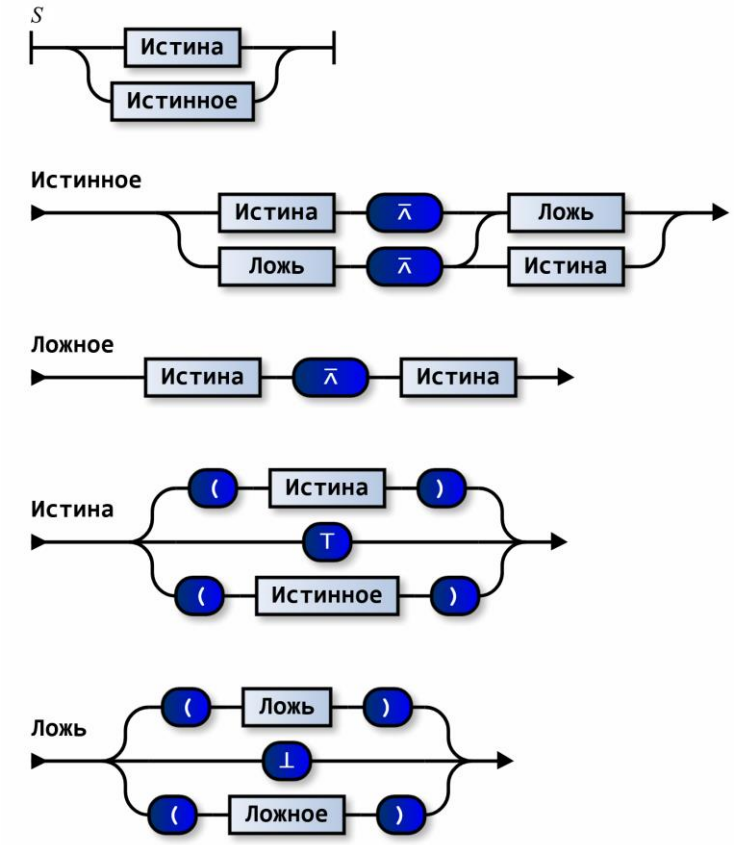


Рис. 1. Определение операции Шеффера через диаграмму Вирта

На рис. 1 показана диаграмма Вирта, описывающая семантику операции Шеффера через грамматику. Входной и выходной порты стартового нетерминала обозначены вертикальными линиями, чтобы отличить его от остальных нетерминалов, в которых они обозначены стрелками. Данная грамматика является контекстно-свободной и рекурсивной. Нетерминалы «Истинное» и «Ложное» описывают, при каких операндах операция Шеффера возвращает истину, а при каких ложь; нетерминалы «Истина» и «Ложь» описывают варианты истинных или ложных операндов операции Шеффера; стартовый нетерминал *S* допускает только истинные выражения.

При такой грамматике синтаксически корректными будут выражения «⊤», «⊤ ⊼ ⊥», «(⊥ ⊼ ⊥) ⊼ (⊤ ⊼ ⊤)», но не «⊥» или «(⊥ ⊼ ⊥) ⊼ (⊤ ⊼ ⊥)», потому что в ней синтаксическая корректность совпадает с семантической истинностью: ложные формулы некорректны синтаксически.

Нетерминалы «Истинное» и «Ложное», описывающие поведение конкретной операции, могут быть расширены на любые другие операции Булевой алгебры. На рис. 2 показано, как они будут выглядеть, если к операции Шеффера добавить эквиваленцию.

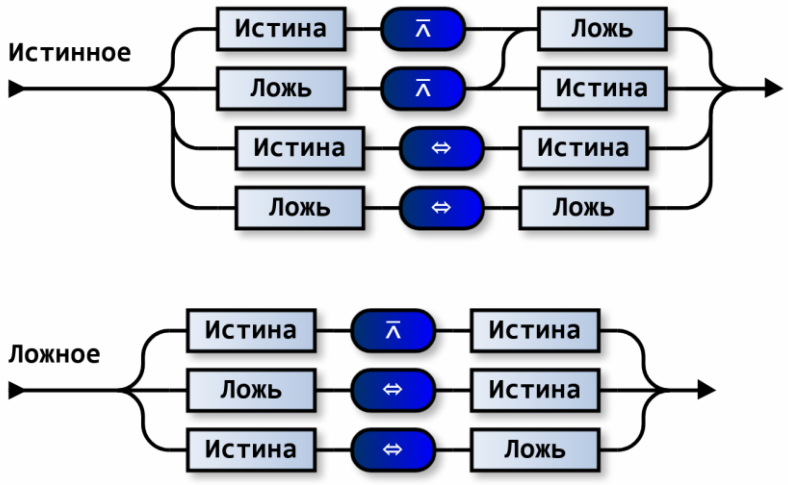


Рис. 2. Расширение формального языка эквиваленцией

Эти нетерминалы могут быть расширены и дальше.

Помимо истинностных значений, скобок и символов для обозначений операций, в пропозициональной логике используются переменные. Кроме того, все операции имеют определенный приоритет, а любые инфиксные операции еще имеют ассоциативность. Из предложенной грамматики приоритет и ассоциативность сознательно исключены, поскольку это сильно усложнило бы ее без увеличения выразительной силы. Вместо этого, если операнд любой операции не является константой, в рассматриваемой грамматике он всегда берется в скобки. Если же приоритет и ассоциативность операций по каким-либо причинам необходимы, предлагается создать вспомогательную грамматику, в которой они есть, и транслятор, добавляющий пропущенные скобки, чтобы преобразовывать исходные выражения к тому виду, в котором они могут быть проверены рассматриваемой грамматикой.

Семантика переменных принципиально не может быть выражена через классические контекстно-свободные грамматики, потому что все вхождения одной переменной в выражении при его вычислении должны быть за-

менены одним и тем же значением [5]. Однако нотация Бэкуса-Наура содержит часто требующееся расширение, которое позволяет решить эту задачу, – исключения. Это расширение предназначено для определения нетерминалов вида «*A*, но не *B*», что позволяет описать пропозициональные переменные, значение которых ложно.

При вычислении истинности выражения с пропозициональными переменными, помимо самого выражения, требуется список истинных пропозициональных переменных, который будет обозначен буквами *TV*. Если пропозициональная переменная находится в этом списке, то она имеет истинное значение. В противном случае она имеет ложное значение. Это позволяет сделать переменные вариантами нетерминалов «Истина» и «Ложь», использующими исключения. Описания этих нетерминалов, расширенные пропозициональными переменными, показаны на рис. 3.

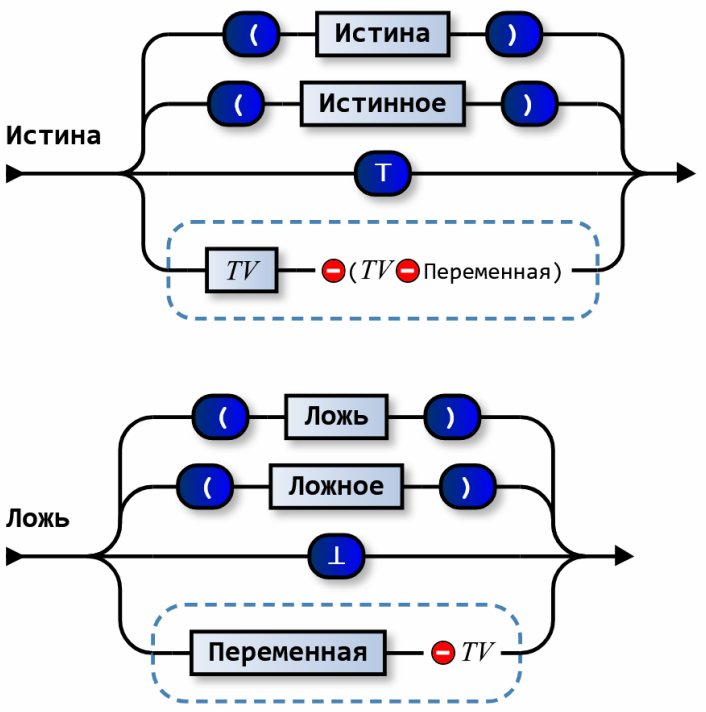


Рис. 3. Расширение формального языка пропозициональными переменными

Любые переменные, присутствующие в списке *TV*, являются вариантами нетерминала «Истина». Любые переменные, отсутствующие в списке *TV*, являются вариантами нетерминала «Ложь». Для того чтобы описать конструкцию «Переменная, но не *TV*», используется исключение, которое в нотации Бэкуса-Наура обозначается символом «минус»; на диаграмме для большей наглядности этот символ помещен в красный круг. Противоположная ситуация, «Переменная и *TV* одновременно», выражена через двойное

исключение. Если список *TV* гарантированно не содержит строк, которые могут быть распознаны как выражения с логическими операторами, то двойное исключение избыточно и достаточно просто списка *TV*. Сам нетерминал «Переменная» тривиален, поэтому его определение в настоящей работе не рассматривается. В простейшем случае переменная – это одна из букв латинского алфавита.

Как видно из диаграммы, список *TV* тоже является нетерминалом. Варианты данного нетерминала – это пропозициональные переменные, которые имеют значение «истина». Например, если при анализе некоторой формулы значение «истина» имеют переменные *b*, *c* и *f*, то нетерминал *TV* будет выглядеть так, как показано на рис. 4.

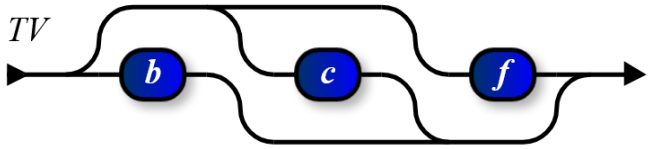


Рис. 4. Нетерминал для списка истинных переменных

В зависимости от конкретных значений переменных, этот нетерминал будет иметь разное определение, но его принципиальная структура будет именно такой, как показано на диаграмме. Поскольку нетерминал *TV* устроен предельно просто, использование исключений в нетерминалах «Истина» и «Ложь» никогда не будет приводить к парадоксам. Таким образом, вся семантика Булевой алгебры может быть описана с применением инструментария контекстно-свободных грамматик, минимально расширенного общепринятым механизмом исключения.

Предложенное решение позволяет свести к синтаксическому разбору часть семантического анализа, что потенциально позволяет строить более легковесные системы, например, при работе с протоколами обмена данными по сети [6]. Разработанная грамматика является синтаксическим и семантическим объектом одновременно. Традиционные семантические объекты в случае пропозициональной логики из необходимых дополнений к синтаксису становятся наглядной иллюстрацией. Рассмотренный подход может быть применен не только к Булевой алгебре, но и к конечным ординалам, а также к схемам аксиом исчисления высказываний. Другие сферы его применения могут быть предметом дальнейших исследований.

Список используемых источников

1. ISO/IEC 14977:1996. Information Technology - Syntactic Metalanguage - Extended BNF. Cambridge: University of Cambridge, 1996. 12 p.

2. Wirth N. The Programming Language Pascal // Acta Informatica, 1971, Vol. 1. PP. 35-63.

3. Eric M. Hammer. Logic and Visual Information (Studies in Logic, Language, and Information): Center for the Study of Language and Inf, 1995, 124 p. ISBN 1881526992.

4. Mendelson E. Introduction to Mathematical Logic. 6th ed. Boca Raton, FL: CRC Press, 2015, 514 p. ISBN 9781032919140.

5. Spicer M. Introduction to the Theory of Computation: Cengage Learning, 2012. 504 p. ISBN 113318779X.

6. Таненбаум Э., Уэзеролл Д., Фимстер Н. Компьютерные сети. 6-е издание: пер. с англ.: СПб: Питер, 2012, 1906 с. ISBN 978-5-4461-1766-6.

USING OF RAILROAD SYNTAX DIAGRAMS AS SEMANTIC OBJECT

Medvedev S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

When working with formal systems, one of the most important tools is formal grammars, which can be visualized using Railroad diagrams. To specify the semantics of expressions described by formal grammars, additional tools are usually used. The paper proposes an approach that allows defining semantics using only formal grammar tools, which can potentially optimize the development of technically complex equipment.

Key words: *propositional logic, Boolean algebra, context-free grammar, attribute grammar*

УДК: 510.622
ГРНТИ 27.03.19

РАСШИРЕНИЯ КОНТЕКСТНО-СВОБОДНЫХ ГРАММАТИК ДЛЯ ОПИСАНИЯ ФОРМАЛЬНЫХ СИСТЕМ

С. А. Медведев

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

Классические аксиомы исчисления высказываний представляют собой шаблоны грамматических конструкций поверх контекстно-свободной грамматики. Работа посвящена исследованию возможности того, как нужно минимальными средствами расширить инструментарий описания контекстно-свободных грамматик, чтобы полностью описать эту формальную систему с помощью него.

пропозициональная логика, Булева алгебра, атрибутная грамматика, семантические объекты, конечные ординалы, метапеременные

Для описания семантики Булевой алгебры достаточно возможностей расширенной нотации Бэкуса-Наура, которая предназначена для описания контекстно-свободных грамматик, дополненных исключениями. Это позволяет минимизировать систему фундаментальных понятий при построении формальных систем и свести их к терминалам, нетерминалам и исключениям. Но помимо алгебраического подхода, в логике существует аксиоматический подход [1]. В отличие от Булевой алгебры, аксиомы исчисления высказываний не могут быть описаны контекстно-свободными грамматиками даже с такими общепринятыми нестандартными расширениями, как исключения. Для решения этой задачи необходимы другие, специализированные расширения.

Помимо контекстно-свободных грамматик, существуют атрибутные и PEG-грамматики [2]. Однако проблема в том, что эти виды грамматик опираются на сложный аппарат, предназначенный для автоматического разбора текста, и не подходят для определения фундаментальных понятий, которые должны в основе этого аппарата лежать. Поэтому необходимы расширения, которые по структуре не сложнее стандартных инструментов построения контекстно-свободных грамматик и являются минимальной надстройкой над ними, позволяющими решать поставленные задачи.

Суть первого из разработанных расширений состоит в том, чтобы дать вхождениям одного и того же нетерминала имена, представляющие собой греческие буквы. Нетерминалы, имеющие одно и то же имя, должны совпа-

дать. Рассмотрим работу этого расширения на примере формальной грамматики для записи конечных ординалов, показанной на рис. 1.

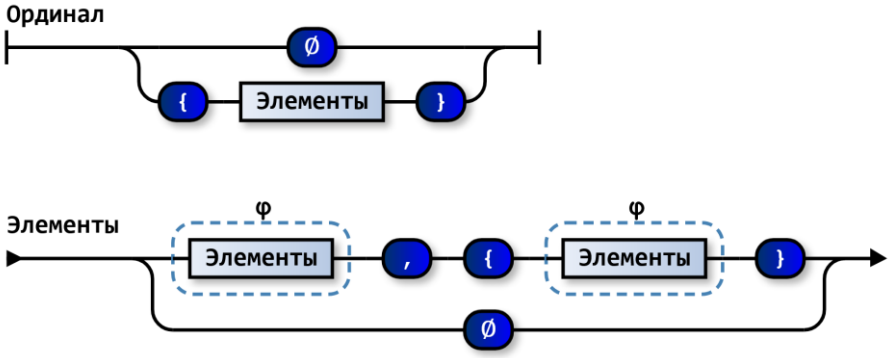


Рис. 1. Формальная грамматика для записи конечных ординалов

Приведенная грамматика состоит из двух нетерминалов. Стартовым является нетерминал «Ординал», представляющий собой либо терминал «∅», либо нетерминал «Элементы», взятый в фигурные скобки, заданные парными терминалами. Простейшим случаем нетерминала «Элементы» тоже является терминал «∅». Более сложный случай состоит из четырех частей: сначала идет нетерминал «Элементы», затем запятая и открывающая фигурная скобка, затем еще один такой же нетерминал «Элементы», затем закрывающая фигурная скобка. Запятая и фигурные скобки задаются соответствующими терминалами. Совпадение вложенных вхождений нетерминала «Элементы» задается с помощью имени φ.

Простейшим выражением данного языка будет выражение, состоящее из символа начального ординала «∅». Это описывается верхней веткой стартового нетерминала. Все остальные выражения будут содержать нетерминал «Элементы» в фигурных скобках. Так как простейшим вариантом нетерминала «Элементы» тоже является символ пустого множества, простейший вариант ординала с фигурными скобками будет выглядеть так: «{ ∅ }». Поскольку нетерминал «Элементы» является рекурсивным, этот же символ является простейшим вариантом вложенного нетерминала «Элементы» в нижней ветке, что даст следующее выражение: «{ ∅, { ∅ } }». Подвыражение «∅, { ∅ }» является простейшей рекурсивной версией нетерминала «Элементы». Оно снова может фигурировать к качестве вложенного нетерминала, что даст выражение «{ ∅, { ∅ }, { ∅, { ∅ } } }». Если бы грамматика была контекстно-свободной, допустимым выражением было бы и такое: «{ ∅, { ∅, { ∅ } } }». Но такое множество не является ординалом [3]. Пометка одинаковых вхождений нетерминала делает конструкции, не являющиеся ординалами, синтаксически некорректными.

Это же расширение позволяет описать такое понятие, как метапеременная в схемах аксиом исчисления высказываний. Метапеременная – это символ, заменяющий собой произвольную формулу. В то же время, формула – это нетерминал в грамматике пропозициональной логики или логики первого порядка. Это позволяет рассматривать любую схему аксиом как нетерминал, в котором вхождения нетерминала «Формула» помечены символами соответствующих метапеременных. Возьмем для примера схему аксиом Гильберта A1 для исчисления высказываний:

$$\varphi \Rightarrow (\psi \Rightarrow \varphi).$$

Эту формулу в рамках контекстно-свободной грамматики, расширенной именованными вхождениями нетерминалов можно представить в виде определения нетерминала, показанного на рис. 2.

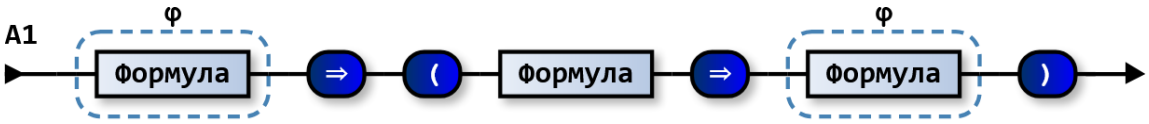


Рис. 2. Схема аксиом A1 в виде описания нетерминала.

Аналогичным образом можно описать все остальные схемы аксиом. Все исчисление высказываний как формальная система при этом может быть описано в виде стартового нетерминала, включающего в себя все схемы аксиом и правило вывода Modus ponens в качестве нетерминалов. Кроме того, в грамматике стандартным образом должен быть определен нетерминал «Формула». Стартовый нетерминал предлагается обозначить символом «⊢», который принято использовать в логике для обознчения выводимости. Примерная структура этого нетерминала показана на рис. 3.

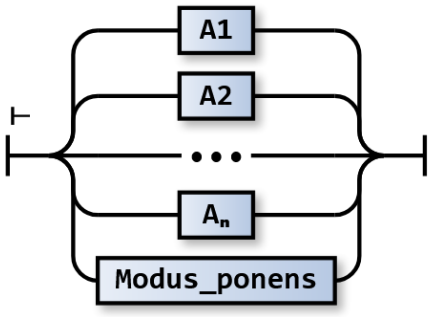


Рис. 3. Структура стартового нетерминала.

Еще одним нетерминалом, который будет дополнительной ветвью этого стартового нетерминала, могут быть гипотезы, из которых требуется сделать логические выводы. Такой нетерминал может называться Г.

Правило вывода Modus ponens, представленное как нетерминал, должно описывать любые формулы, которые с помощью этого правила можно вывести из схем аксиом. Описание такого нетерминала тоже потребует именованных вхождений нетерминала «Формула», но этого недостаточно. Как правило, в контекстно-свободных грамматиках нет информации, поступающей на вход описаний нетерминалов, есть только варианты формируемых последовательностей символов. Но правило вывода Modus ponens на вход принимает две посылки: импликацию и ее антецедент. Поэтому данное правило требует более серьезных расширений.

Расширение, которое предлагается ввести, состоит в том, что требуется существование определенного нетерминала, который, с одной стороны, является вариантом нетерминала «⊢», а с другой стороны, имеет вид импликации. Описание этой конструкции требует серьезного расширения стандартной нотации Вирта. Чтобы создать необходимые блоки, был доработан генератор Railroad-диаграмм Tabatkins. Описание получившегося нетерминала показано на рис. 4.

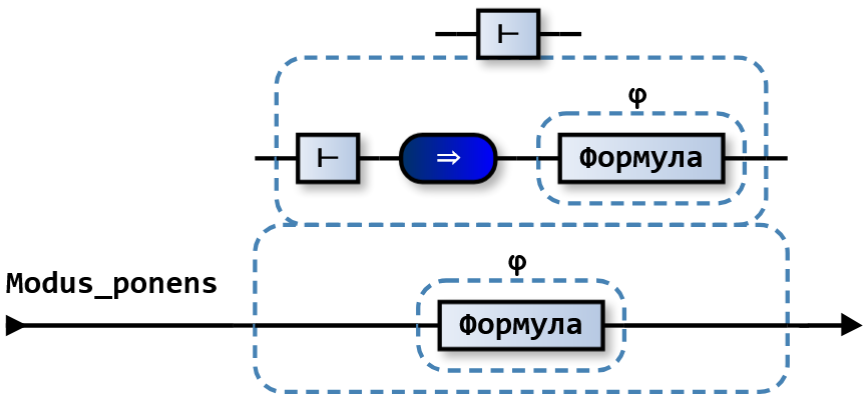


Рис. 4. Правило вывода Modus ponens, описанное как нетерминал.

Нетерминалом Modus_ponens может быть любая формула, но на нее накладывается дополнительное ограничение, показанное сверху в отдельном блоке. Формула, имеющая вид импликации с выводимым антецедентом и произвольным консеквентом, сама должна быть выводима, т.е. быть вариантом нетерминала «⊢». Структура этой импликации показана в верхнем блоке как анонимный нетерминал. Ее выводимость показана обозначением

соответствующего нетерминала над этим блоком. То, что формула, являющаяся вариантом нетерминала Modus_ponens, должна совпадать с консеквентом импликации, показано с помощью имени φ.

В отличие от меток, расширение, подразумевающее существование некоторой неизвестной формулы, не является конструктивным [4]. Оно не позволяет сформулировать алгоритм, позволяющий доказать, что импликация в верхнем блоке и ее антецедент выводимы. Поэтому, хотя формально нетерминал Modus_ponens необходим, чтобы полностью описать исчисление высказываний как формальную систему в виде грамматики, его определение, строго говоря, не является грамматическим по своей сути. При переходе к логике первого порядка требуется учитывать еще более сложные конструкции – свободные и связанные переменные, а также подстановки. Все это, скорее всего, потребует более сложных расширений контекстно-свободных грамматик. Целесообразность использования рассмотренного подхода для описания таких формальных систем может быть предметом дополнительных исследований.

Список использованных источников

1. Гильберт Д., Аккерман В. Основы теоретической логики: пер. с нем. М.: Государственное издательство иностранной литературы, 1947. 304 с. ISBN 978-5-484-01144-5.

2. Ford B. Parsing expression grammars: a recognition-based syntactic foundation: ACM SIGPLAN Notices, Volume 39, Issue 1, 2004. Pages 111 - 122

3. Jech T. Set Theory: The Third Millennium Edition, revised and expanded: Springer, 2013. 786 p. ISBN 978-3642078996

4. Bishop E., Bridges D. Constructive Analysis: Springer, 1985. 477 p. ISBN 978-3-642-61667-9

EXTENSIONS OF CONTEXT-FREE GRAMMARS FOR DESCRIBING FORMAL SYSTEMS

Medvedev S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The classical axioms of propositional calculus are templates of grammatical constructions on top of a context-free grammar. The paper is devoted to investigating the possibility of how to minimally extend the toolkit of describing context-free grammars in order to fully describe this formal system with its help.

Key words: *propositional logic, Boolean algebra, context-free grammar, attribute grammar*

УДК 004.7:004.422.8
ГРНТИ 28.29.01

ИНТЕЛЛЕКТУАЛЬНЫЕ ПОДХОДЫ К ОБЕСПЕЧЕНИЮ QoS В МУЛЬТИСЕРВИСНОЙ АРХИТЕКТУРЕ 5G

Н. Н. Мошак, Н. Эль Сабаяр Шевченко

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

Развитие мультисервисных архитектур в сетях пятого поколения 5G сопровождается повышенными требованиями к согласованному обеспечению параметров качества обслуживания QoS при значительном разнообразии пользовательских запросов и условий функционирования сети. Рассматриваются интеллектуальные подходы, обеспечивающие выбор и композицию сервисов с учетом характеристик среды, политик обслуживания и ограничений инфраструктуры. Предлагается регрессионная модель функции распределения задержки, позволяющая прогнозировать квантиль задержки в мультисервисной архитектуре 5G с учетом состояния сети. Регрессионная модель строится с применением машинного обучения, при этом распределение задержек участвует в процессе косвенно – через формирование обучающей выборки.

5G, QoS, мультисервисная сеть, квантиль задержки, машинное обучение, регрессионная модель

В архитектурах мультисервисных сетей NGN, в частности LTE, механизмы обеспечения QoS основывались на априорных предположениях о распределении задержек и фиксированных конфигурациях сети [1]. При этом ключевой метрикой для изохронных потоков (речь, видео) становится не среднее значение задержки, а ее вероятностная характеристика – квантиль задержки, то есть такое значение, которое не превышается фактической задержкой с заданной вероятностью. Классический расчет квантиля требует фиксировать распределение задержек (например, гамма-распределение для цепочки экспоненциальных звеньев) [1, 2].

В данной работе предлагается заменить явное моделирование плотности вероятности регрессионной моделью машинного обучения. Данная модель обучается на исторических данных, где истинный квантиль t_q рассчитывается эмпирически, а затем в реальном времени предсказывается на основе наблюдаемых признаков сети. Такой подход позволяет прогнозировать квантиль, что удобно для online-мониторинга QoS и интеллектуального контроля SLA (Service Level Agreement), т. к. изохронный трафик требует не

только приоритезации, но и адаптивного управления сетевыми ресурсами с учетом текущего состояния канала [3-6] Задача прогнозирования квантиля задержки в мультисервисной архитектуре 5G сводится к построению модели, способной учитывать совокупное влияние динамических факторов сети и выдавать в реального времени оценку t_q. Ниже приводится ее математическая формализация.

Пусть T – случайная величина, отражающая задержку пакета. Тогда квантиль t_q порядка q (например, 0.95) определяется как:

$$P\{T \le t_q\} = F_T(t_q) = q$$

где t_q – это такое значение задержки, при котором вероятность того, что задержка будет меньше или равна t_q, составляет q, $P\{T \le t_q\}$ – вероятность того, что наблюдаемое значение задержки T окажется меньше или равно пороговому значению t_q.

В классических моделях t_qнаходится аналитическими методами по известной функции распределения. В отличие от классического подхода, где квантиль задержки t_q определяется на основе функции распределения $F_T(t_q)$, в машинном обучении данная функция не используется явно. Распределение задержек участвует в процессе косвенно – через формирование обучающей выборки, но не требует явного задания или аппроксимации. Это позволяет применять модель вне зависимости от конкретной формы распределения и обеспечивает универсальность подхода. В дальнейшем регрессионная модель приближает отображение от признаков текущего состояния сети к ожидаемому значению квантиля, что делает ее пригодной для быстрого прогнозирования в режиме реального времени:

$$\hat{t}_q = f(X), X \in \mathbb{R}^n,$$

где $\hat{t}_q$ – предсказанное значение квантиля задержки t_q, получаемое в результате применения регрессионной модели $f(X)$, к вектору признаков X. Вектор $X \in \mathbb{R}^n$, где n – это количество входных признаков, описывающих текущее состояние сети. Каждый элемент вектора $X = \langle x_1, x_2, \dots, x_n \rangle$представляет собой признаки состояния сети, таких как коэффициент загрузки канала, глубина очереди, среднее время отклика или Round-TripTime (RTT), джиттер, тип трафика или слайса и другие параметры. Таким образом, модель $f(X)$ аппроксимирует неизвестную зависимость между состоянием

сети и соответствующим квантилем задержки, что позволяет прогнозировать его без прямого измерения самих задержек. Параллельно с этим существует пороговое значение квантиля t_q^{SLA} определенное в соглашении об уровне обслуживания (SLA). Если выполнено неравенство $\hat{t}_q \leq t_q^{SLA}$, то SLA считается выполненным. В противном случае, если $\hat{t}_q > t_q^{SLA}$, система должна инициировать перераспределение сетевых ресурсов, изменение параметров обслуживания или адаптацию маршрутов, направленные на восстановление требуемого уровня качества обслуживания в соответствии с заданными ограничениями по задержке.

В качестве регрессионной модели предлагается использовать многослойный перцептрон, способный аппроксимировать сложные нелинейные зависимости между признаками состояния сети и соответствующим квантилем задержки. Модель принимает на вход вектор признаков $X = \langle x_1, x_2, \dots, x_n \rangle$, отражающий текущее состояние мультисервисной сети, и выдает предсказание $\hat{t}_q$, соответствующее оценке квантиля порядка q. В отличие от среднеквадратичной ошибки, которая приближает математическое ожидание целевой переменной, в данной работе предлагается использовать квантильную функцию потерь, позволяющая настраивать модель на такое значение задержки, которое не превышается в $q \times 100\ \%$ случаев. Локальная ошибка для одного примера определяется следующим образом:

$$\phi_q(t, \hat{t}) = \begin{cases} q \cdot (t - \hat{t}), \text{если } t \geq \hat{t} \\ (1 - q) \cdot (\hat{t} - t), \text{если } t < \hat{t} \end{cases}.$$

Общая функция потерь на обучающей выборке из m наблюдений определяется как:

$$\mathcal{L}(\beta) = \frac{1}{m} \sum_{i=1}^{m} \phi_q\left(t^{(i)}, \hat{t}^{(i)}\right).$$

Применение такой модели обеспечивает высокую скорость оценки, независимость от конкретной формы распределения и возможность интеграции в механизмы мониторинга в режиме реального времени и SLA-контроля. Это открывает перспективы для построения адаптивных систем управления ресурсами в сетях 5G, способных своевременно реагировать на угрозу нарушения SLA без необходимости полного наблюдения за выборкой задержек.

В данной работе рассмотрен интеллектуальный подход к обеспечению качества обслуживания (QoS) в мультисервисной архитектуре 5G на основе

прогнозирования квантиля задержки с использованием регрессионной модели. Предложенная модель позволяет выполнять предсказание квантиля задержки на основе текущего состояния сети, без необходимости построения аналитической модели распределения. Такой подход обеспечивает гибкость, высокую скорость работы и применимость в режиме реального времени.

Список используемых источников

1. Мошак Н. Н. Особенности архитектуры сети LTE // Волновая электроника и инфокоммуникационные системы. Материалы XXIII международной научной конференции, в 2 ч. Санкт-Петербург, 2020. С. 320-330.

2. Мошак Н. Н. механизмы обеспечения QoS в сети LTE / Н. Н. Мошак, Г. Д. Харитонов // Региональная информатика (РИ-2020): XVII Санкт-Петербургская международная конференция. Материалы конференции, Санкт-Петербург, 28–30 октября 2020 года. Том Часть 2. Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2020. С. 296-297.

3. Dahlman E., Parkvall S., Skold J. 5G NR: Fundamentals. Academic Press, 2021. 466 p.

4. Малышев А. Н. Сетевые срезы и управление трафиком // Радиосвязь. 2022. № 5. С. 28–36.

5. Fattah S., et al. End-to-End Latency in 5G Networks: Analysis and Modeling // IEEE Internet of Things Journal. 2021. V. 8, № 4. PP. 2602–2615. DOI:10.1109/JIOT.2020.3016346.

6. Смирнов А. П., Киреев С. В. Сетевые срезы в 5G и задачи их поддержки в радиодоступе. Инфокоммуникационные технологии, 2021. № 8, с. 44–50.

INTELLIGENT APPROACHES TO ENSURING QOS IN 5G MULTI-SERVICE ARCHITECTURE

Moshak N., El Zabayar Shevchenco N.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The development of multiservice architectures in fifth-generation (5G) networks is accompanied by increased requirements for the coordinated provision of quality of service (QoS) parameters with a significant diversity of user requests and network operating conditions. This article considers intelligent approaches that ensure the selection and composition of services taking into account the characteristics of the environment, service policies, and infrastructure constraints. Particular attention is paid to the formalization of QoS consistency criteria for the interaction of services of different nature, as well as to the mechanisms of adaptive routing and configuration of network components that ensure the stability of the architecture to changes in external load and application requirements.

Key words: *5G networks, QoS, adaptability, multiservice architecture, delay quantile*

УДК 519.852
ГРНТИ 27.25.19

АНАЛИЗ ПОДХОДОВ К РЕШЕНИЮ МИНИМАКСНЫХ ЗАДАЧ РАЗМЕЩЕНИЯ

П. В. Плотников

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

Статья посвящена анализу современных подходов к решению минимаксных задач размещения, возникающих в логистике, сетевом планировании, управлении и телекоммуникациях. Основной целью таких задач является минимизация максимального значения целевой функции, что означает обеспечение наилучших условий в наихудшем сценарии. Рассматриваются различные методы, такие как: классические аналитические и геометрические подходы, алгоритмы дискретной оптимизации на графах, а также методы, основанные на тропической оптимизации. В статье проведен сравнительный анализ указанных методов, выделены основные преимущества и ограничения. Обобщение представленных решений формирует основу для разработки универсальных стратегий размещения и подчеркивает актуальность дальнейших теоретических и прикладных исследований в данной области.

задача размещения, минимакс, сетевое планирование, тропическая оптимизация

Минимаксные задачи размещения представляют собой важный класс оптимизационных задач, возникающих при проектировании и управлении различными системами, в том числе в логистике, телекоммуникациях, транспортных сетях и системах управления [1, 2]. Их специфика заключается в том, что целью является минимизация максимального значения некоторой целевой функции, что требует создания наилучших условий в наихудшем сценарии функционирования системы. Такой подход особенно востребован при решении задач в условиях высокой неопределенности, ограниченности ресурсов и необходимости обеспечения высокого качества обслуживания.

Классическим примером минимаксной задачи является задача размещения объектов (складов, центров обработки данных, аварийно-спасательных подразделений) таким образом, чтобы минимизировать максимальное расстояние или время отклика до обслуживаемых пунктов. Аналогичные постановки встречаются при проектировании телекоммуникационных се-

тей, где требуется обеспечить минимальную задержку передачи данных для наиболее удаленного узла сети [3].

Существует ряд подходов к решению минимаксных задач размещения. Отметим лишь некоторые, наиболее часто используемые методы, такие как: аналитические и геометрические методы, дискретная оптимизация на графах, а также использование численных методов – в частности, выпуклого и линейного программирования. Важно отметить и ряд перспективных направлений решения: эвристические и метаэвристические алгоритмы и методы тропической (идемпотентной) оптимизации, предоставляющие новые аналитические инструменты для работы с минимаксными критериями.

Несмотря на большое количество работ в данной области, проблема выбора оптимального метода решения остается актуальной. Это связано как с высокой вычислительной сложностью многих предлагаемых решений, так и с необходимостью учитывать специфику прикладной области, включая особенности геометрии пространства, ограничения на ресурсы и условия эксплуатации системы.

В настоящей работе приведен обзор и анализ преимуществ и недостатков наиболее популярных и перспективных подходов к решению минимаксных задач размещения.

Классические минимаксные задачи размещения формулируются как оптимизационные задачи, в которых необходимо выбрать положение одного или нескольких обслуживающих объектов (центров), минимизируя максимальное расстояние или иной показатель между объектом и множеством обслуживаемых точек. В наиболее известной постановке (задаче 1-центра) требуется найти точку x_{opt} в пространстве $\mathbb{R}^n$, минимизирующую функцию:

$$\min_{X} \max_{i \in I} d(x, a_i),$$

где a_i – координаты обслуживаемых пунктов, $d(\dots, \dots)$ – метрика (чаще всего евклидова, Чебышева или прямоугольная).

В зависимости от метрики искомое решение может иметь геометрическую интерпретацию:

1) в евклидовой метрике (L_2) задача сводится к нахождению центра наименьшей окружности (или сферы в многомерном случае), охватывающей все точки a_i;

2) в метрике Чебышева (L_∞) решение находится как центр наименьшего гиперкуба, покрывающего все точки;

3) в прямоугольной метрике (L_1) задача может быть решена независимо по каждой координате, что упрощает вычисления.

Для случая нескольких центров (p-центров) задача усложняется: необходимо минимизировать максимальное расстояние между точкой исходного набора объектов и ближайшим центром:

$$\min_X \max_{i\in I} \min_{j\in J} d(x_j, a_i),$$

где $X = \{x_j\}$ – множество координат центров.

Ключевые особенности классического (аналитический и геометрический методы) подхода можно сформулировать следующим образом:

1. Прямое решения часто строятся через выпуклые оболочки и пересечения геометрических областей.

2. При решении задачи в условиях малых размерностей, есть возможность получить явные алгоритмы с полиномиальной сложностью. Например, алгоритм Вельцля для минимальной окружности.

3. При увеличении числа объектов и измерений задача достаточно быстро становится NP-трудной, что требует поиска приближенных решений или перехода к другим методам.

В задачах размещения, возникающих на практике, часто отсутствует полная информация о параметрах, таких как местоположение пунктов спроса, интенсивность нагрузки, уровень затрат или конфигурация сети. В этих условиях классические минимаксные модели могут давать решения, неустойчивые к изменению исходных данных. Для устранения этого недостатка применяют робастные и стохастические модели минимаксного размещения.

В тех случаях, когда задача размещения может быть представлена в виде дискретной модели, используют подход, основанный на теории графов. Пространство представляют графом $G = (V, E)$ с некоторой метрикой (обычно кратчайшего пути). Точки спроса и/или кандидаты под размещение берутся в качестве вершин графа. Типичная задача p-центров на графе может быть сформулирована следующим образом:

$$\min_{X\subseteq V, |X|=p} \max_{v\in V} \min_{x\in X} d_G(v, x),$$

где $d_G(\dots, \dots)$ – длина кратчайшего пути в G.

Выделяя основные особенности подхода, основанного на теории графов, можно отметить следующее:

1. Если в задаче размещения задано конечное множество потенциальных точек прибытия, то задача может быть сформулирована, как комбинаторная задача (часто целочисленная).

2. Структура графа (дерево, планарный граф, общая сеть) задачи оказывает существенное влияние на сложность и применимость алгоритмов решения.

3. Часто при работе с графом системы предварительно необходимо вычислить матрицу кратчайших расстояний (Декстра / Флойд-Варшал / многократный Декстра). При этом вычислительная сложность алгоритма может оказаться $O(n^2)$, где $n -$ число исходных точек задачи.

Известно достаточно много алгоритмические подходов к решению задач размещения с использованием графов. Приведем лишь некоторые:

1. Параметрический/Радиусный поиск (binary search on radius).

2. Жадный алгоритм Гонсалеса (Gonzalez).

3. Алгоритмы Хочбаума–Шмойса (Hochbaum & Shmoys).

4. Целочисленное программирование (MILP/IP).

Несмотря на все преимущества и широкий выбор алгоритмических решений, подход с использованием графов требует проведения дискретизации задачи размещения, что порождает неточность полученных решений.

Один из подходов, позволяющих получать точное явное решение задачи размещения – это тропическая оптимизация. Это направление математической оптимизации, основанное на так называемой тропической алгебре (или идемпотентной математике). В ней операции сложения и умножения заменяются на операции максимума/минимума и сложения соответственно [4, 5], что позволят переписать задачу по-новому, сводя ее к уже известной, но в новых обозначениях. В контексте минимаксных задач размещения этот подход особенно привлекателен, так как сама структура задачи часто предполагает использование операций максимума и минимума, что напрямую соответствует тропическим операциям.

В тропической алгебре оптимизационные модели записываются в виде линейных уравнений или неравенств в макс-плюс или мин-плюс арифметике. Это позволяет формулировать задачи размещения в компактной алгебраической форме, избегая громоздких традиционных нелинейных выражений. Методы тропической оптимизация оказывается особенно полезными при моделировании сетевых и транспортных структур. Использование идемпотентной алгебры позволяет сводить такие задачи к решению систем линейных уравнений и неравенств в тропической арифметике, что зачастую

упрощает вычислительные процедуры и делает возможным применение эффективных матричных алгоритмов [6].

Применение рассматриваемого подхода особенно эффективно при анализе и проектировании больших сетей (логистических, коммуникационных), поскольку он позволяет решать задачи в условиях, когда классические методы линейного или целочисленного программирования сталкиваются с проблемами экспоненциальной сложности. Важно отметить, что тропическая формализация тесно связана с теорией графов, так как матричные операции в тропических полукольцах соответствуют вычислению кратчайших путей. Это дает возможность использовать развитый аппарат алгоритмов на графах.

Важным преимуществом тропической оптимизации является возможность аналитического описания решения без перебора всех комбинаций, что особенно актуально для реальных приложений с динамически изменяющимися условиями. Однако данный подход требует специфических знаний в области идемпотентного анализа и пока еще не получил широкого распространения в инженерной практике, что определяет перспективность его дальнейших исследований.

Ограничения подхода, основанного на тропической оптимизации, связаны с тем, что он наилучшим образом подходит к решению задач с четкой структурной. В случае, если задача содержит сложные вероятностные зависимости, применение тропической модели требует дополнительных преобразований. Тем не менее, в логистике и телекоммуникационных сетях, тропическая оптимизация становится мощным инструментом моделирования и анализа.

Преимущества и недостатки рассмотренных подходов к решению минимаксных задач размещения показал, что классические методы линейного и целочисленного программирования остаются универсальным инструментом для задач небольшого и среднего масштаба, однако для крупномасштабных и динамически изменяющихся систем перспективными являются методы, опирающиеся на идемпотентный анализ и специализированные алгоритмы графовой оптимизации.

Проведенный анализ показывает, что выбор оптимального метода определяется как характером исходных данных, так и требованиями к надежности и вычислительной эффективности.

Таким образом, интеграция классических, графовых и тропических методов в рамках единой методологии позволяет формировать более гибкие и устойчивые алгоритмы, способные эффективно решать широкий спектр минимаксных задач размещения в условиях неопределенности и ограниченных ресурсов. Дальнейшие исследования в данном направлении целесооб-

разно сосредоточить на разработке гибридных моделей, объединяющих сильные стороны каждого из подходов и обеспечивающих практическую применимость в реальных индустриальных сценариях.

Список используемых источников:

1. Eiselt H. A., Marianov V. (ed.). Foundations of location analysis. – Springer Science & Business Media, 2011. T. 155.

2. Saldanha-da-Gama F., Wang S. Facility location under uncertainty // International Series in Operations Research and Management Science. 2024.

3. Москвин А. А., Максимов Р. В., Горбачев А. А. Модель, оптимизация и оценка эффективности применения многоадресных сетевых соединений в условиях сетевой разведки // Вопросы кибербезопасности. 2023. № 3(55). С. 13–22.

4. Butkovič P. Max-linear systems: Theory and algorithms. Springer, 2010.

5. Cuninghame-Green R. A. Minimax algebra and applications // Advances in Imaging and Electron Physics. Ed. by P. W. Hawkes. San Diego: Academic Press. 1994. Vol. 90. P. 1-121.

6. Плотников П. В. Подход к решению задачи размещения в трехмерном пространстве методами тропической оптимизации // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8, № 1(26). С. 6-13.

ANALYSIS OF APPROACHES TO SOLVING MINIMAX LOCATION PROBLEMS

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

The article is devoted to the analysis of modern approaches to solving minimax location problems arising in logistics, network planning, management and telecommunications. The main goal of such tasks is to minimize the maximum value of the objective function, which means ensuring the best conditions in the worst-case scenario. Various methods are considered, such as: classical analytical and geometric approaches, discrete optimization algorithms on graphs, as well as methods based on tropical optimization. The article provides a comparative analysis of these methods, highlights the main advantages and limitations. The generalization of the presented solutions forms the basis for the development of universal placement strategies and emphasizes the relevance of further theoretical and applied research in this area.

Key words: *location problem, minimax, network planning, tropical optimization*

УДК 004.7
ГРНТИ 28.23

ИСПОЛЬЗОВАНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ И ПРЕДОТВРАЩЕНИЯ РАСПРОСТРАНЕНИЯ ФЕЙКОВЫХ НОВОСТЕЙ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

О. В. Раковский

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

В эпоху цифровых технологий распространение фейковых новостей стало серьезной проблемой, влияющей на общественное мнение, политические процессы и социальную стабильность. В статье исследуется возможность применения методов машинного обучения для выявления и предотвращения распространения фейковых новостей в онлайн-среде. Рассматриваются методы обработки естественного языка и анализа настроений. Выявляются ограничения при использования машинного обучения.

машинное обучение, фейковые новости, обнаружение фейковых новостей, обработка естественного языка, анализ настроений, онлайн-среда

Введение

Распространение фейковых новостей в интернет-пространстве стало серьезной проблемой. Фейковые новости можно определить как ложную или вводящую в заблуждение информацию, представленную в виде новостей. Легкость, с которой фейковые новости могут быть созданы и распространены через социальные сети и другие онлайн-платформы, привела к их широкому распространению и потенциально серьезным последствиям [1].

Влияние фейковых новостей можно наблюдать в различных аспектах общества. Это может повлиять на общественное мнение, политические процессы и социальную стабильность. Например, фейковые новости использовались для влияния на выборы, разжигания социальной розни и нанесения ущерба репутации отдельных лиц и организаций.

Традиционные методы выявления фейковых новостей, такие как проверка фактов и ручной анализ, оказались недостаточными для борьбы с огромным количеством создаваемых и распространяемых фейковых новостей. Поэтому для решения этой проблемы были разработаны автоматизированные подходы, основанные на машинном обучении [2-5].

Машинное обучение, подмножество искусственного интеллекта, предлагает многообещающие решения для выявления и предотвращения распространения фейковых новостей. Используя большие объемы данных и алгоритмы, машинное обучение может помочь распознавать закономерности и характеристики, связанные с фейковыми новостями, что позволяет автоматизировать их обнаружение и смягчение последствий.

В последние годы было проведено значительное количество исследований по выявлению фейковых новостей с использованием методов машинного обучения [2]. Такие исследования касаются способов обработки естественного языка (ОЕЯ или NLP), методов машинного обучения и др.

Методы обработки естественного языка направлены на выявление в тексте особенностей грамматики, синтаксиса и заголовков. Анализ тональности статьи и субъективности изложения позволяет выявить эмоциональную составляющую статьи. Чаще всего фейковые новости имеют сенсационный характер. Также при выявлении нежелательных новостей может оказаться полезным применение методов машинного обучения, которые помогают выявлять различия достоверных и фейковых данных, опираясь на имеющиеся размеченные наборы.

Несмотря на многообещающие результаты, использование машинного обучения для выявления фейковых новостей сталкивается с рядом проблем и ограничений. К ним относятся сложность обработки меняющегося характера фейковых новостей, предвзятость, присутствующая в обучающих данных, и необходимость в интерпретируемых и объяснимых моделях.

Методология

На первом этапе собираются данные, содержащие как фейковые, так и достоверные новостные статьи. Набор данных составляется из различных источников, включая платформы социальных сетей, новостные веб-сайты и базы данных для проверки фактов. Он тщательно отбирается, чтобы обеспечить репрезентативность различных тем, стилей написания и источников.

После сбора данных подборка подвергается предварительной обработке для подготовки к анализу машинного обучения. Этапы предварительной обработки включают:

1. Очистка текста с удалением ненужных символов, HTML-тегов и знаков препинания из текста.

2. Разбиение текста на отдельные слова или токены (токенизация).

3. Понижение размерности данных (стемминг) за счет выделения основной формы слов.

4. Удаление частиц, союзов, предлогов, не несущих особой смысловой нагрузки.

В моделях машинного обучения полезными для решения поставленной задачи представляются следующие функции.

1. Статистическая мера TF-IDF, оценивающая важность слова в документе относительно всего набора текстов.

Формула TF-IDF для термина *t* в документе *d* выглядит следующим образом:

$$TF\text{-}IDF(t,d) = TF(t,d) \times IDF(t),$$

где

$$TF(t,d) = \frac{f_{t,d}}{\sum_k f_{k,d}},$$

$f_{t,d}$ – количество вхождений термина *t* в документ *d*, а знаменатель – общее количество слов в документе *d*.

$$IDF(t) = log\ \frac{N}{|\{d \in D : t \in d\}|},$$

где *N* – общее число документов в выборке, а $|\{d \in D : t \in d\}|$ - количество документов, содержащих термин *t*.

2. Функции анализа настроений используется для определения эмоционального тона и субъективности новостной статьи. Она опирается на оценку полярности текста, например, на основе взвешенного суммирования словарных значений.

$$S = \frac{1}{n}\sum_{i=1}^{n} s(w_i),$$

где $s(w_i)$ – оценка настроения слова w_i, а *n* – количество слов в тексте.

3. Логистическая регрессия.

Логистическая регрессия моделирует вероятность принадлежности объекта к классу «фейковая новость» следующим образом:

$$P(y = 1|x) = \sigma(z) = \frac{1}{1+e^{-z}},$$

где

$$z = \beta_0 + \sum_{j=1}^{m} \beta_j x_j,$$

$x = (x_1,x_2,...,x_m)$ - вектор признаков, β_j - параметры модели, $\sigma(\cdot)$ – сигмоидная функция.

4. Метод Байеса.

Вероятность принадлежности новости к классу C_k вычисляется по формуле Байеса:

$$P(C_k|x) = \frac{P(C_k)\prod_{j=1}^{m} P(x_j|C_k)}{P(x)},$$

где $x = (x_1,x_2,...,x_m)$ - признаки новости.

5. Метод опорных векторов (SVM).

SVM ищет гиперплоскость, разделяющую классы, решая задачу оптимизации:

$$\min_{w,b} \frac{1}{2}\|w\|^2$$

при ограничениях:

$$y_i(w \cdot x_i + b) \geq 1, i = 1,\ldots,n$$

где w – вектор весов, b – смещение, $y_i \in \{-1,1\}$ – метки классов.

6. Нейронные сети.

Нейронные сети используют композицию нелинейных функций. Для одного слоя:

$$a^{(l)} = \sigma(W^{(l)}a^{(l-1)} + b^{(l)})$$

где $a^{(l)}$ – выход слоя l, $W^{(l)}$ – матрица весов, $b^{(l)}$ – вектор смещений, σ – функция активации (например, ReLU или сигмоида).

Производительность моделей машинного обучения можно оценить с использованием различных показателей, включая точность, прецизионность, полноту и F1-меру, которые позволяют оценить способность моделей правильно классифицировать фейковые и достоверные новостные статьи.

1. Точность:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

2. Прецизионность:

$$\text{Precision} = \frac{TP}{TP + FP}$$

3. Полнота:

$$\text{Recall} = \frac{TP}{TP + FN}$$

4. F1-мера:

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}},$$

где *TP* – истинно положительные, *TN* – истинно отрицательные, *FP* – ложноположительные, *FN* – ложноотрицательные классификации.

Выводы

Несмотря на эффективность применения методов машинного обучения для выявления фейковых новостей, следует отметить, что имеется большое количество трудностей, связанных с развитием индустрии вбросов информации, наличием определенной предвзятости при подготовке обучающих наборов данных.

Поэтому дальнейшие исследования представляются перспективными в следующих направлениях.

1. Развитие методов обработки естественного языка с анализом лингвистических особенностей фейковых новостей.

2. Анализ мультимедийной составляющей информации, включая аудио и видеоданные.

3. Разработка интерпретируемых и объяснимых моделей машинного обучения для обеспечения прозрачности и подотчетности.

4. Исследование использования методов активного обучения для снижения предвзятости, присутствующей в обучающих данных.

5. Разработка механизмов защиты от состязательных атак, направленных на обман моделей машинного обучения.

Выполняя отмеченные направления исследований, мы сможем улучшить возможности машинного обучения, для выявления и предотвращения распространения фейковых новостей, тем самым способствуя формированию более достоверной и надежной онлайн-среды.

Список используемых источников

1. Григорян Д. К. Фейковые новости в эпоху цифровизации: технологии противодействия распространению. URL: https://cyberleninka.ru/article/n/feykovye-novosti-v-

epohu-tsifroizatsii-tehnologii-protivodeystviya-rasprostraneniyu (дата обращения 06.06.2025).

2. Хотин Д. Ю., Иванова Г. С. Выявление фейковых фрагментов в текстовых новостных сообщениях с помощью машинного обучения. URL: https://cyberleninka.ru/article/n/vyyavlenie-feykovyh-fragmentov-v-tekstovyh-novostnyh-soobscheniyah-s-pomoschyu-mashinnogo-obucheniya (дата обращения 06.06.2025).

3. Роль ИИ и машинного обучения в кибербезопасности в 2025 году. URL: https://lazarusalliance.com/ru/the-role-of-ai-and-machine-learning-in-cybersecurity-in-2025/ (дата обращения 06.06.2025).

4. Зачем ученому ML? / Machine Learning Podcast. Выпуск 065. URL: https://podcasts.apple.com/ru/podcast/065-ml-авторы-курса-msu-ai-зачем-ученому-ml/id1495052772?i=1000677311387 (дата обращения 06.06.2025).

5. Кравецкий Л. AGI (ИИ общего назначения) уже здесь?! / Machine Learning Podcast. Выпуск 066. URL: https://podcasts.apple.com/ru/podcast/066-ml-лекс-кравецкий-agi-ии-общего-назначения-уже-здесь/id1495052772?i=1000678412638 (дата обращения 06.06.2025).

USING MACHINE LEARNING METHODS TO IDENTIFY AND PREVENT THE SPREAD OF FAKE NEWS ON THE INTERNET

Rakovskii O.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the digital age, the spread of fake news has become a serious problem affecting public opinion, political processes, and social stability. The article explores the possibility of using machine learning methods to identify and prevent the spread of fake news in an online environment. The methods of natural language processing and sentiment analysis are considered. The limitations of using machine learning are revealed.

Key words: *Machine learning, fake news, fake news detection, natural language processing, sentiment analysis, online environment*

УДК 004.056
ГРНТИ 81.93.29

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛИТЕЛЬНЫХ СРЕДАХ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

О. В. Раковский

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

С активным развитием облачных вычислительных сред для хранения и обработки данных растет и количество угроз информационной безопасности. Облачные инфраструктуры все чаще становятся мишенью для сложных кибератак. В статье рассмотрены вопросы обеспечения информационной безопасности в облачных вычислительных средах с акцентом на применение искусственного интеллекта для автоматического обнаружение аномалий и предотвращение утечек данных.

информационная безопасность, облачные вычисления, искусственный интеллект, машинное обучение, шифрование, многофакторная аутентификация, Zero Trust, мониторинг безопасности

Введение

С ростом использования облачных вычислительных сред для хранения и обработки данных увеличивается и количество угроз информационной безопасности. Облачные инфраструктуры становятся мишенью для сложных кибератак, включая фишинг, атаки на гипервизоры, компрометацию API и внутренние угрозы. В 2025 году наблюдается тенденция к усилению проактивных мер защиты с применением искусственного интеллекта (ИИ) и машинного обучения (МО) для автоматического обнаружения и предотвращения угроз [1-3].

Основные угрозы облачной безопасности включают [4]:

– угрозы на уровне гипервизора (гиперджекинг);
– уязвимости API и сервисов облака;
– внутренние угрозы и ошибки пользователей;
– атаки на сетевые соединения (Man-in-the-Middle);
– утечки данных и компрометация хранилищ.

Ключевыми технологиями обеспечения безопасности являются [1-5]:

– Шифрование данных. Обязательное шифрование на всех этапах – в состоянии покоя и при передаче – с использованием современных алгоритмов (AES-256, RSA, ECC) обеспечивает защиту данных даже при компрометации инфраструктуры;
– Многофакторная аутентификация (MFA). Использование MFA снижает риски взлома учетных записей и несанкционированного доступа, комбинируя пароли, биометрию и токены;
– Сегментация сети и минимизация прав доступа. Изоляция ресурсов и принцип наименьших привилегий ограничивают распространение атак и внутренние угрозы;
– Мониторинг и автоматическое обнаружение угроз с применением ИИ. Анализируются логи, поведение пользователей и сетевой трафик для выявления аномалий и подозрительной активности в реальном времени, позволяя предотвращать атаки на ранних стадиях.

Представим современные рекомендации по безопасности облачных сред в виде таблицы 1.

ТАБЛИЦА 1. Основные рекомендации по безопасности облачных сред в 2025 году

№	Компонент безопасности	Рекомендации
1	Шифрование	Использовать сквозное шифрование, защищать данные в покое и при передаче
2	Аутентификация	Внедрять многофакторную аутентификацию (MFA)
3	Сегментация и права доступа	Минимизировать права, изолировать сети и ресурсы
4	Мониторинг и ИИ	Автоматическое обнаружение аномалий, анализ поведения пользователей и сетевого трафика
5	Соответствие стандартам	Сертификация по ISO 27001, SOC 2, GDPR

Применение искусственного интеллекта в облачной безопасности

Представляется целесообразным интегрировать модуль ИИ в облачную инфраструктуру, включающую сбор данных, предобработку, обучение моделей и автоматическое реагирование. Для анализа безопасности могут быть использованы следующие методы машинного обучения:
– классификация аномалий с помощью алгоритмов случайного леса, градиентного бустинга и нейросетей;

– обнаружение аномалий во временных рядах с использованием рекуррентных нейронных сетей (LSTM);
– обработка больших данных с применением распределенных вычислительных платформ для масштабируемого анализа.

Для оценки аномалии в поведении пользователя или процесса используем следующую функцию:

$$S(x) = \frac{1}{N}\sum_{i=1}^{N} |x_i - \mu_i|/\sigma_i,$$

где x_i – наблюдаемое значение признака, μ_i и σ_i – среднее и стандартное отклонение по историческим данным.

В качестве примера представим реализацию модели обнаружения аномалий с использованием рекуррентной сети LSTM для прогнозирования временных рядов на Python (рис. 1).

```python
import numpy as np
import tensorflow as tf
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import LSTM, Dense

# Генерация синтетических данных (например, сетевой трафик)
def generate_data(timesteps, features, samples):
    normal_data = np.random.normal(loc=0.0, scale=1.0, size=(samples, timesteps, features))
    anomalies = normal_data.copy()
    anomalies[0:5] += 5  # искусственные аномалии
    labels = np.zeros(samples)
    labels[0:5] = 1
    return anomalies, labels

X, y = generate_data(timesteps=50, features=10, samples=1000)

# Модель LSTM для обнаружения аномалий
model = Sequential([
    LSTM(64, input_shape=(50, 10), return_sequences=False),
    Dense(1, activation='sigmoid')
])

model.compile(optimizer='adam', loss='binary_crossentropy', metrics=['accuracy'])
model.fit(X, y, epochs=10, batch_size=32, validation_split=0.2)
```

Рис. 1. Пример обнаружения аномалий с использованием сети LSTM

Результаты выполнения программы с использованием LSTM-модели для обнаружения аномалий (рис. 2) показывают, насколько эффективно модель способна классифицировать входные данные на нормальные и аномальные.

```
Epoch 1/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 5s 79ms/step - accuracy: 0.7652 - loss: 0.6034 - val_accuracy: 1.0000 - val_loss: 0.0206
Epoch 2/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 2s 53ms/step - accuracy: 1.0000 - loss: 0.0114 - val_accuracy: 1.0000 - val_loss: 0.0012
Epoch 3/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 2s 29ms/step - accuracy: 1.0000 - loss: 0.0015 - val_accuracy: 1.0000 - val_loss: 6.3726e-04
Epoch 4/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 27ms/step - accuracy: 1.0000 - loss: 8.4235e-04 - val_accuracy: 1.0000 - val_loss: 4.8184e-04
Epoch 5/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 25ms/step - accuracy: 1.0000 - loss: 6.4613e-04 - val_accuracy: 1.0000 - val_loss: 3.9218e-04
Epoch 6/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 31ms/step - accuracy: 1.0000 - loss: 7.3730e-04 - val_accuracy: 1.0000 - val_loss: 3.3059e-04
Epoch 7/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 25ms/step - accuracy: 1.0000 - loss: 6.0686e-04 - val_accuracy: 1.0000 - val_loss: 2.8493e-04
Epoch 8/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 25ms/step - accuracy: 1.0000 - loss: 4.2338e-04 - val_accuracy: 1.0000 - val_loss: 2.5001e-04
Epoch 9/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 26ms/step - accuracy: 1.0000 - loss: 4.3776e-04 - val_accuracy: 1.0000 - val_loss: 2.2225e-04
Epoch 10/10
25/25 ━━━━━━━━━━━━━━━━━━━━ 1s 26ms/step - accuracy: 1.0000 - loss: 3.7847e-04 - val_accuracy: 1.0000 - val_loss: 1.9960e-04
```

Рис. 2. Результаты выполнения программы обнаружения аномалий

В частности, программа генерирует синтетический набор данных, где часть примеров содержит искусственные аномалии (искажения данных). Модель обучается распознавать эти аномалии, минимизируя функцию потерь бинарной классификации.

После обучения программа выводит метрики точности (accuracy) на тестовой выборке, отражая долю правильно классифицированных примеров. Высокое значение accuracy будет свидетельствовать о том, что модель успешно выявляет аномалии в данных, что в контексте информационной безопасности означает возможность автоматического обнаружения подозрительной активности или угроз.

Выводы

Результаты эксперимента показывают эффективность применения LSTM для анализа временных рядов и выявления аномалий в потоках данных, что актуально для мониторинга безопасности в облачных вычислительных средах и других задачах кибербезопасности.

Интеграция автоматизированного мониторинга, шифрования, многофакторной аутентификации и сегментации сети позволяет эффективно противостоять современным киберугрозам. Внедрение ИИ-модулей для анализа поведения и обнаружения аномалий обеспечивает проактивную защиту и минимизацию рисков.

Список используемых источников

1. Смирнов А. Принципы защиты данных в 2025 году. URL: https://companies.rbc.ru/news/efq5uTUy3u/printsipyi-zaschityi-dannyih-v-2025-godu/ (дата обращения 4/06/2025).

2. Тренды в борьбе с киберпреступностью 2025 – мнение эксперта. URL: https://ak152.ru/news/tpost/vubjmb0yc1-trendi-v-borbe-s-kiberprestupnostyu-2025 (дата обращения 4/06/2025).

3. Эксперты Serverspace выделили принципы защиты данных в 2025 году/ URL: https://safe.cnews.ru/news/line/2025-03-06_eksperty_serverspace_vydelili (дата обращения 4/06/2025).

4. Главные киберугрозы для облаков: как защищать свои данные в 2025. URL: https://blog.colobridge.net/2022/05/top-cloud-cyber-threats/ (дата обращения 4/06/2025).

5. Защита облаков в России: основные тенденции и тренды киберугроз в 2025 году/ URL: https://yandex.cloud/ru/blog/posts/2025/04/cloud-protection (дата обращения 4/06/2025).

ENSURING INFORMATION SECURITY IN CLOUD COMPUTING ENVIRONMENTS USING ARTIFICIAL INTELLIGENCE

Rakovskii O.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

With the active development of cloud computing environments for data storage and processing, the number of information security threats is also growing. Cloud infrastructures are increasingly becoming a target for sophisticated cyber attacks. The article discusses the issues of information security in cloud computing environments with an emphasis on the use of artificial intelligence to automatically detect anomalies and prevent data leaks.

Key words: *Information security, cloud computing, artificial intelligence, machine learning, encryption, multifactor authentication, Zero Trust, security monitoring*

УДК 004.725.5
ГРНТИ 20.51.19

ПРИМЕНЕНИЕ ЭЛЕМЕНТОВ ИНТЕЛЛЕКТУАЛИЗАЦИИ В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРОЙ

В. А. Тарасов

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

Эффективное управление современной информационной инфраструктурой в рамках крупной и даже средней организации представляется непростой задачей. Обусловлено это как большим количеством оборудования и программного обеспечения, так и необходимостью отлеживать и корректировать параметры системы в реальном времени. Управление такой системой требует большой нагрузки на административный персонал, и количество его должно быть значительным, особенно если система функционирует в круглосуточном режиме. В этой связи представляется целесообразным вводить в систему управления элементы интеллектуализации, способные как предлагать персоналу варианты управленческих решений в реальном времени, так и оказывать управляющие воздействия непосредственно на информационную инфраструктуру.

информационная система, информационная инфраструктура, система управления сетью, трафик, информационная безопасность

Задачи обслуживания и управления информационной инфраструктурой возникают в любой информационной системе, каков бы ни был ее масштаб. Но особенно актуальны они в крупных корпоративных сетях, системах провайдеров информационных услуг, центрах обработки данных и облачных платформах, где проблема эксплуатации инфраструктуры обусловлена значительным количеством оконечного и коммутационного оборудования различных уровней (доступа, распределения, магистрального), сложностью топологической структуры, гетерогенностью, необходимостью оперативного реагирования на изменения в системе – отказы оборудования, перегрузки каналов, проведение регламентных работ и т. д.

Оказать содействие в решении задач управления информационной инфраструктурой призван класс программных средств – системы управления сетью или NMS (Network Management System), решающие широкий круг задач.

Представляет интерес один из представителей данного класса – система Zabbix. Следует отметить, что система бесплатна, лицензия GPLv2 [1].

Продукт предназначен для использования под управлением операционной системы UNIX, а аппаратные средства выбираются в соответствии с конкретными потребностями.

В составе данной системы можно выделить следующие компоненты:

– Zabbix-сервер, центральный элемент системы, обеспечивающий сбор, обработку и хранение информации посредством агентов либо без них;
– Zabbix-агент призван собирать сведения об узле, на котором он находится – параметры компонентов сервера или рабочей станции;
– Zabbix-прокси обеспечивает сбор информации с узлов для передачи ее серверу для случаев, когда необходимо разгрузить последний либо избежать проблем с системой безопасности;
– Web-интерфейс – средство получения мониторинговой информации и задания опций конфигурирования.

Следует отметить следующие особенности данной NMS [2]:

– наличие системы мониторинга, позволяющей информировать административный персонал о происходящих в сети событиях в реальном времени;
– присутствие предупреждений о критических состояниях системы, дающее возможность оказывать корректирующие воздействия;
– хранение в базе статистики, на основе которой возможно проследить динамику работы сети, построить соответствующие графики (можно отслеживать сразу несколько параметров);
– возможность добавления (без ограничений) процесса мониторинга аппаратных и программных компонентов, для облегчения процедуры конфигурирования и экономии времени удобно использовать шаблоны (имеются готовые, которые можно редактировать).

Zabbix позволяет контролировать ниже указанные параметры:

– базовые – загрузка процессора, занятость оперативной памяти, загрузка накопителей, скорость их работы, параметры файлов, статистика сервера;
– сервера – показатели датчиков температуры и напряжения, значения скоростей вращения вентиляторов;
– сетевого оборудования – значения входящего и исходящего трафика, состояние интерфейсов, включая ошибки;

– служб – справочная информация, параметры;
– сертификатов – срок службы.

К достоинствам системы можно отнести следующие [2-4]:

– система не требует финансовых затрат на приобретение;
– наличие русскоязычной локализации;
– открытая архитектура;
– широкий функционал;
– высокая производительность;
– централизация процессов управления;
– гибкость конфигурирования, включающая шаблоны и настройку оповещений;
– масштабируемость;
– широкие возможности анализа статистики событий системы.

Из недостатков можно выделить:

– громоздкость продукта;
– не очень удобный пользовательский интерфейс;
– проблема со структурированностью параметров тестирования.

Подводя итог, следует отметить, что рассмотренный продукт является как достаточно удобным и эффективным средством управления информационной инфраструктурой, так и элементом информационной безопасности, хотя и требует более высокого уровня автоматизации управления.

Список используемых источников

1. Денисов Ю. Знакомьтесь, Zabbix! Обзор системы и ее установка на ОС Linux. Часть 1 // Системный администратор. 2010. № 5(90). С. 36-38.

2. Смушкин В. А. Zabbix для мониторинга в IT-инфраструктуре // Форум молодых ученых. 2019. № 4(32). С. 958-962.

3. Апанасик П. И. Использование системы мониторинга Zabbix в корпоративной сети // Управление информационными ресурсами: Материалы XX Международной научно-практической конференции, Минск, 29 марта 2024 г. Минск: Академия управления при Президенте Республики Беларусь, 2024. С. 247-248.

4. Зотов С. В. Использование Zabbix для мониторинга гетерогенной сети с работой по проводным и радиоканалам // Научно-исследовательские публикации. 2017. № 1(39). С. 30-39.

THE USE OF INTELLECTUALIZATION ELEMENTS IN INFORMATION INFRASTRUCTURE MANAGEMENT

Tarasov V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Effective management of modern information infrastructure within a large and even medium-sized organization is not an easy task. This is due to both the large amount of hardware and software, and the need to monitor and adjust system parameters in real time. Managing such a system requires a lot of administrative staff, and the number of them should be significant, especially if the system operates around the clock. In this regard, it seems advisable to introduce intellectualization elements into the management system that can both offer staff options for management decisions in real time and exert control effects directly on the information infrastructure.

Key words: *information system, information infrastructure, network management system, traffic, information security*

КИБЕРБЕЗОПАСНОСТЬ

УДК 004.056
ГРНТИ 81.93.29

ПРИМЕНЕНИЕ ИСТОЧНИКОВ ДАННЫХ МАТРИЦЫ MITRE ATT&CK ПРИ ПОИСКЕ СЛЕДОВ КИБЕРПРЕСТУПЛЕНИЙ

Е. А. Антонюк, А. А. Чечулин

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Для поиска следов киберпреступлений применяются различные методы, направленные на обнаружение, изучение и анализ данных, оставленных злоумышленниками после совершения атаки. В статье рассматривается сопоставление тактик, техник и процедур злоумышленников с источниками данных матрицы MITRE ATT&CK, необходимыми для их обнаружения.

информационная безопасность, расследование информационных инцидентов, матрица MITRE ATT&CK

Матрица MITRE ATT&CK – мощный инструмент, который позволяет систематизировать действия злоумышленников, выявлять их тактики и техники, а также связывать инциденты с известными хакерскими группами.

Первый и один из самых важных этапов расследования киберпреступлений заключается в сборе исходных данных [1]. Сам сбор доказательств заключается в анализе объекта и результата атаки, а также оставленных нарушителем следов [2]. Этот процесс позволяет определить ключевые области, откуда потребуется извлечь необходимые данные для дальнейшего разбирательства, а также сформировать массив необработанных сведений, используемых на последующих этапах следствия.

Для использования системного подхода при выявлении следов киберпреступлений, может помочь матрица MITRE ATT&CK, которая представляет собой структурированную базу знаний для описания тактик

и техник, используемых злоумышленниками при проведении атак, и по сути является алгоритмом действий злоумышленника и используемых им инструментов [3]. С ее помощью можно систематизировать информацию о том, какие методы могут использовать хакеры на разных этапах атаки, начиная от первоначального доступа до закрепления в системе и уничтожения следов [4].

Применение модели MITRE ATT&CK на стадии сбора данных позволяет структурировать процесс расследования, снизить вероятность упущения важных доказательств и ускорить распознавание активности злоумышленников. Это особенно важно в условиях ограниченного времени и ресурсов при работе с современными сложными кибератаками.

Источники данных матрицы MITRE ATT&CK (Data Sources) – это категории данных, которые собираются и анализируются для выявления техник ATT&CK и охватывают типы собираемой и исследуемой информации, необходимой для идентификации тех или иных техник ATT&CK. Эти категории отражают разные виды сведений, фиксируемых средствами защиты информации или журналами событий. Помимо общих категорий, существуют также компоненты данных, уточняющие специфические характеристики и значения каждого источника, важные для детектирования конкретной техники или подтехники матрицы MITRE ATT&CK.

Каждая техника в матрице ATT&CK имеет атрибут Data Sources, указывающий, какие данные нужны для ее обнаружения. Например, техника T1059 (Command-Line Interface) использует Data Sources: Process, Command-Line Monitoring, что в свою очередь позволяет обнаружить следы анализируя команды в командной строке (cmd.exe), PowerShell или Bash [5].

Применение Data Sources на этапе сбора данных при расследовании киберпреступлений предполагает структурированное использование информации о типах данных, необходимых для обнаружения конкретных техник атак. Это позволяет точно определить, какие данные собирать, основываясь на тактиках, техниках и процедурах, описанных в матрице MITRE ATT&CK.

Различные источники данных отличаются своей универсальностью и степенью покрытия техник матрицы MITRE ATT&CK. Определение наиболее значимых источников данных помогает установить приоритетность мониторинга и повысить общую эффективность системы информационной безопасности. Чем больше количество релевантных источников задействовано, тем выше точность обнаружения и качественнее аналитиче-

ская корреляция событий. Например, Data Source Process (DS0009) покрывает большое количество техник – около 255, самые распространенные из которых: Process Injection (T1055), File and Directory Discovery (T1083), Modify Authentication Process (T1556), а источник данных Kernel (DS0008) указывает только на 2 техники: Boot or Logon Autostart Execution (T1547) и Escape to Host (T1611), что говорит о низком покрытии техник. Это может, помочь определить, какие источники данных обеспечат большую видимость и, следовательно, являются хорошим кандидатом для поиска следов. Т.е. чем больше обнаружено источников, тем точнее обнаружение и качество корреляции.

В результате исследования источников данных матрицы MITRE ATT&CK разработан алгоритм поиска следов с применением Data Sources (рисунок 1). Алгоритм представляет собой метод, базирующийся на сопоставлении тактик, техник и процедур злоумышленников с соответствующими категориями данных, позволяющими обнаружить такие следы.

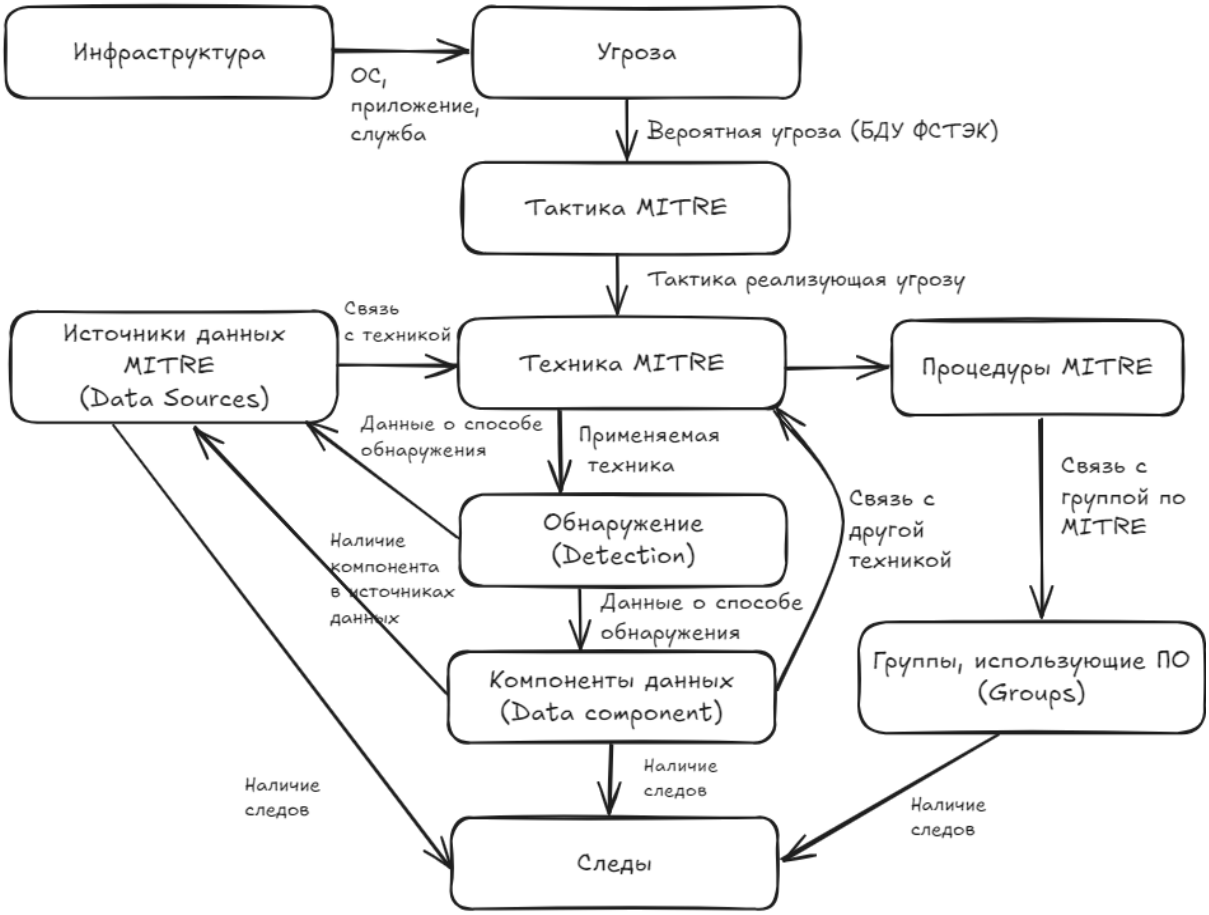


Рис. 1. Алгоритм поиска следов с применением Data Source

Работу алгоритма можно описать следующим образом:

Различная инфраструктура информационных систем порождает уникальные потенциальные угрозы. Каждая угроза связана с определенными тактиками матрицы MITRE ATT&CK. Особенности инфраструктуры и применяемых тактик определяют набор применяемых техник. После определения техник осуществляется анализ связанных компонентов данных (Data Components) и источников данных согласно матрице MITRE ATT&CK. Также выявленные техники содержат практические инструкции и программы, используемые различными группами злоумышленников. Коррелируя данные о источниках данных, компонентах данных и группах, эксплуатирующих программное обеспечение, можно существенно сузить пространство поиска подозрительных следов.

На основе изложенного можно сделать определенные выводы.

1. Применение источников данных матрицы MITRE ATT&CK на этапе сбора данных способствует формированию системного подхода к проведению расследований киберпреступлений.

2. Такой подход минимизирует риск нехватки ключевых данных и ускоряет процесс выявления следов атаки, что крайне актуально в условиях активного сокрытия злоумышленниками своих действий и огромного объема потенциальных свидетельств.

3. Сопоставление полученных данных с известными тактиками и техниками облегчает выявление аномальных активностей и повышает точность определения следов пребывания злоумышленников [6].

4. Разработанный алгоритм обеспечивает последовательную связь между тактиками матрицы MITRE ATT&CK и фактическими объектами, подлежащими сбору и последующему анализу, что исключает избыточность информации, сосредотачиваясь исключительно на данных, соответствующих известным техникам.

5. Поскольку алгоритм основан на абстрактных концепциях, независимых от конкретных технологий его можно применять независимо от особенностей IT-инфраструктуры.

Исследование выполнено за счет гранта Российского научного фонда № 25-11-20028, https://rscf.ru/project/25-11-20028/

Список используемых источников

1. Чечулин А. А., Горда М. Д., Модель расследования киберпреступлений // Науч.-аналит. журн. «Информатизация и Связь». 2023. № 3. С. 92–97. DOI:10.34219/2078-8320-2023-14-3-92-97

2. 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.

3. Сагитов Р. Ф., Сайгафарова А. А. Как MITRE ATT&CK помогает при расследовании киберпреступлений? // Сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием. Уфа, 2021«Информационные технологии обеспечения комплексной безопасности в цифровом обществе». 2023. С. 259-262.

4. Заболотнюк Е. В., Горохова В. Ф., Методика реагирования на кибератаки с использованием матрицы MITRE ATT&CK // Сборник трудов Всероссийской научно-технической конференции. Ижевск, 2023 «Информационные технологии в науке, промышленности и образовании. молодежный научный форум». 2023. С. 439-443.

5. Ihab Mohamed, Hesham A. Hefny and Nagy R. Darwish, Enhancing cybersecurity defenses: a multicriteria decision-making approach to MITRE ATT&CK mitigation strategy //«International Journal of Computer Networks & Communications (IJCNC) Vol.16, No.4, July 2024» DOI: 10.5121/ijcnc.2024.16402.

6. Дойникова Е. В., Чечулин А. А., Котенко И. В. Оценка защищенности компьютерных сетей на основе метрик CVSS // Информационно управляющие системы. 2017. № 6 (91). С. 76–87.

THE USE OF MITRE ATTACK MATRIX DATA SOURCES IN THE SEARCH FOR TRACES OF CYBERCRIME

Antonyuk E., Chechulin A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

To search for traces of cybercrime, various methods are used aimed at detecting, studying and analyzing data left by intruders after the attack. The article examines the comparison of the tactics, techniques and procedures of intruders with the data sources of the MITRE ATT&CK matrix necessary for their detection.

Key words: *Information security, information incident investigation, MITRE ATT&CK matrix*

УДК 004.8
ГРНТИ 20.51.19

АНАЛИЗ УЯЗВИМОСТЕЙ В ЭКОСИСТЕМЕ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ И ПРЕДЛОЖЕНИЯ ПО ИХ УСТРАНЕНИЮ

В. В. Билан, Р. А. Перов

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

Статья рассматривает актуальные аспекты монетизации объектов, связанных с современными автомобилями, и выявляет основные категории активов, привлекающих внимание киберпреступников. В качестве перспективного решения предлагается применение федеративного обучения – подхода, при котором обработка данных происходит непосредственно в устройствах, а на серверы передаются лишь обобщенные обновления алгоритмов, что существенно повышает уровень конфиденциальности и кибербезопасности. В заключение выделяются три ключевые группы рисков: информационные активы, физический доступ к транспортным средствам и их вычислительные ресурсы, подчеркивая необходимость комплексного подхода к обеспечению безопасности в эпоху интеллектуального транспорта.

киберпреступность, федеративное обучение, утечка данных, автономные автомобили, облачные сервисы, интеллектуальные транспортные системы, конфиденциальность данных

Для успешной монетизации объекта его наличие должно нести непосредственную или потенциальную экономическую выгоду, включая возможности перепродажи. В контексте подключенных транспортных средств возникает актуальный вопрос о том, какие именно аспекты этих автомобилей привлекают внимание киберпреступников с целью их несанкционированного использования. Важно выделить основные целевые данные и активы, которые могут быть объектами интереса:

– защита конфиденциальной информации. Синхронизация мобильного устройства с автомобилем позволяет передавать данные о звонках, контактах, приложениях и SMS. Автомобиль также фиксирует местоположение и маршруты передвижения водителя. Такие интеллектуальные авто аккумулируют значительный объем данных о владельце, которые могут стать товаром на нелегальных рынках [1];
– информация пользователя (за исключением личных данных). Технологически продвинутые автомобили с возможностью подключения предла-

гают функциональность использования приложений как непосредственно через встроенную мультимедийную систему, так и через интеграцию с Apple CarPlay или Android Auto. Эти приложения подключаются к облачным сервисам, обеспечивая взаимодействие с различными программами. Модели, такие как Tesla, оснащенные функцией Sentry Mode47, способны записывать происходящее вокруг автомобиля при активации режима. В результате в автомобилях накапливается значительный объем пользовательских данных, что может привлекать к себе интерес злоумышленников с целью их кражи [2];

– само транспортное средство. Безусловно, автомобиль как материальный актив, обладает определенной стоимостью, и в случае, если злоумышленник способен дистанционно разблокировать, завести и похитить транспорт, подобное преступление может быть реализовано не только в отношении этой конкретной модели, но и потенциально адаптировано к автомобилям других марок [3];
– предметы, оставленные в салоне автомобиля, привлекают внимание преступников, поскольку взлом авто и последующее хищение имущества становятся менее затратными по времени и усилиям. В случае с автономными грузовыми автомобилями такая активность может стать еще более выгодной для воров, учитывая ценность транспортируемых грузов.

Услуги профессионального водителя могут обрести новый спрос в эпоху распространения автономных автомобилей. С ростом использования беспилотного транспорта риски, связанные с его взломом, применением для транспортировки запрещенных грузов, осуществлением преступных операций, или выполнением анонимных перемещений могут усложнить процесс идентификации нарушителей для органов правопорядка, повышая ценность услуг квалифицированных водителей как гаранта легальности и безопасности транспортных операций [4].

– аккумулированная энергия. В рамках глобального перехода на экологически чистые транспортные средства, в частности электромобили, технология автомобильных батарей значительно продвинулась, достигая вместимости вплоть до 100 киловатт-часов. Это обеспечивает их владельцев внушительным резервом энергии. В некоторых государствах проводятся пилотные проекты по интеграции запасаемой в транспортных средствах энергии в общую электросеть в качестве дополнительного источника питания. С течением времени, такой объем накопленной энергии в батареях электромобилей может превратиться в объект желания для кражи.

– сетевые и вычислительные мощности, охватывающие все от безвозмездного доступа к интернету, использования передачи данных через сеть, до интеграции с облачными вычислениями, а также взаимосвязь с системами Vehicle-to-Grid (V2G) и Vehicle-to-Vehicle (V2V) коммуникаций, не говоря уже о выделении процессорного времени и других аспектах. Злоумышленники имеют потенциал для внедрения вредоносных программ типа ботнет в системы связанных автомобилей, эксплуатируя сетевые и вычислительные ресурсы транспортного средства в период его простоя, например, в ночное время в домашних условиях.

По данным Федеральной торговой комиссии, электронная система автомобиля может хранить:

– телефонные контакты;
– данные для входа в мобильное приложение;
– данные о местоположении;
– коды гаражных ворот.

Таким образом, возникает серьезная проблема кибербезопасности для автомобильной промышленности. Если центральный сервер сети автомобилей будет взломан, будет ли это означать, что личная информация каждого водителя в этой сети будет захвачена?

«Конфиденциальность – это первая из многих проблем, с которыми мы столкнемся при применении классических алгоритмов искусственного интеллекта к транспортным средствам».

Вместо этого многие обязанности по вычислениям и обучению будут оставлены на усмотрение отдельных автомобилей. Автомобили сами обрабатывали данные и выдвигали предложения по улучшению своих алгоритмов.

Эти предложения, не содержащие необработанных данных, затем передавались на серверы, которые помогали улучшить общий алгоритм для всех устройств в сети. Результат: сеть ИИ, из которой труднее украсть личную информацию. Подобные вычислительные алгоритмы используются уже около десяти лет. Сегодня этот тип ИИ наиболее известен как федеративное обучение – название, которое Google придумала в 2016 году.

Может не только защитить конфиденциальность водителей, но и обеспечить более эффективные и масштабируемые вычисления с растущим числом автомобилей.

Следовательно, на основе проведенного исследования, возможно выделить три принципиальные группы активов и сервисов, которые подвержены

риску эксплуатации и превращения в источник дохода для субъектов киберпреступности:

1. Информация, собранная, произведенная, хранимая и обмениваемая между автомобилями.

2. Физическое присутствие при транспортных средствах, в том числе доступ к услугам по управлению.

3. Ресурсы сети и процессора в автомобильной сфере.

Список используемых источников

1. Gao L., Gu Z., Qiu C., Lei L., Li S. E., Zheng S., Jing W., and Chen J. Cola-HRL: Continuous-lattice hierarchical reinforcement learning for autonomous driving // in Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS). 2022. PP. 13143–13150.

2. Wang J., Shi T., Wu Y., Miranda-Moreno L., and Sun L. Multiagent graph reinforcement learning for connected automated driving // in Proc. 37th Int. Conf. Mach. Learn. 2020. PP. 1–6.

3. Mo S., Pei X., and Wu C. Safe reinforcement learning for autonomous vehicle using Monte Carlo tree search // IEEE Trans. Intell. Transp. Syst. 2022. Vol. 23. № 7. PP. 6766–6773.

4. Tian Y., Cao X., Huang K., Fei C., Zheng Z., and Ji X. Learning to drive like human beings: A method based on deep reinforcement learning,'' IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6357–6367, Jul. 2022.

ANALYSIS OF VULNERABILITIES IN THE AUTONOMOUS VEHICLE ECOSYSTEM AND PROPOSALS FOR ELIMINATION

Bilan V., Perov R.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

This article examines current aspects of monetizing assets associated with modern automobiles and identifies the main asset categories that attract the attention of cybercriminals. Federated learning is proposed as a promising solution – an approach in which data processing occurs directly on devices, with only generalized algorithm updates transmitted to servers, significantly increasing privacy and cybersecurity. Finally, three key risk groups are identified: information assets, physical access to vehicles, and their computing resources, emphasizing the need *for a comprehensive approach to ensuring security in the era of intelligent transportation.*

Key words: *cybercrime, federated learning, data breaches, autonomous vehicles, cloud services, intelligent transportation systems, data privacy*

УДК 004.8
ГРНТИ 20.51.19

ИССЛЕДОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ И ВЫЯВЛЕНИЕ СЛАБЫХ МЕСТ В УПРАВЛЕНИИ АВТОНОМНЫМ ТРАНСПОРТНЫМ СРЕДСТВОМ

В. В. Билан, Р. А. Перов, В. Д. Шевяков

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

Современные автомобили становятся не просто средствами передвижения, но полноценными цифровыми устройствами, интегрированными в экосистему интернета вещей. В статье рассматриваются ключевые аспекты кибербезопасности в контексте "умных" и подключенных транспортных средств, включая уязвимости мобильных приложений, обновлений прошивок и беспроводных коммуникаций. Особое внимание уделено технологии C-V2X (Vehicle-to-Everything), обеспечивающей связь автомобиля с другими транспортными средствами, дорожной инфраструктурой и пешеходами, а также риску кибератак, таких как DoS, DDoS и внедрение вредоносного ПО. Статья призывает к комплексному подходу к защите подключенных автомобилей, чтобы обеспечить не только удобство, но и безопасность пользователей в условиях растущих цифровых угроз.

беспилотный автомобиль, C-V2X, 5G, Bluetooth-уязвимости, искусственный интеллект, кибербезопасность.

Операторы транспортных средств уже не могут игнорировать аспекты безопасности, связанные с цифровыми сервисами и коммуникационными технологиями, интегрированными в автомобили новой эры, называемые «подключенными». Это вовсе не ограничивается функцией упрощения парковки; сфера включает в себя функционал социальных медиа, электронную почту, синхронизацию со смартфоном, навигацию, различные авто-аппликации и другое. Хотя эти инновации предоставляют значительные удобства для пользователей, они одновременно влекут за собой угрозы кибербезопасности и другие опасности для современного автовладельца. Поэтому критически важно изучать и оценивать потенциальные угрозы, которые могут спровоцировать кибернападения, ДТП или даже мошенничество при обслуживании машины.

Защита персональной информации, обновления программного обеспечения в реальном времени и совместимость с приложениями для смартфонов превращаются в ключевые аспекты, уязвимые к кибернетическим ата-

кам в контексте усовершенствованных автомобильных технологий. С появлением «умных» автомобилей, оснащенных передовыми функциями связи, возрастает потенциал для вторжений, схожих с теми, что уже знакомы пользователям ПК и мобильных устройств [1].

При использовании мобильного приложения для дистанционного доступа к автомобилю, вы, по сути, генерируете альтернативный электронный ключ для транспортного средства. Однако отсутствие адекватных мер безопасности может привести к тому, что в случае кражи смартфона злоумышленник способен получить контроль над вашим авто. Это достигается за счет возможности модификации данных в базе данных приложения и обхода систем аутентификации, таких как PIN-код, что значительно облегчает несанкционированную активацию удаленных функций автомобиля.

Обновление прошивки Bluetooth осуществляется посредством скачивания файла с официального сайта производителя и его последующей установки через USB-устройство хранения. Отсутствие криптографической защиты и цифровой подписи в данном файле делает его подверженным рискам, учитывая, что он содержит обширные сведения о функционировании систем автомобиля [2].

C-V2X, являясь ключевым элементом 5G-инфраструктуры, обеспечивает связность транспортных средств с мобильной сетью, облегчая взаимодействие между ними, а также с элементами дорожной инфраструктуры и окружающей обстановкой. Эта технология способствует повышению дорожной безопасности за счет предотвращения аварий и конфликтных ситуаций между автомобилями и пешеходами, а также оптимизирует управление транспортными потоками. C-V2X включает в себя связь между транспортными средствами и сетью, между транспортными средствами и дорожной инфраструктурой, а также непосредственную коммуникацию между транспортными средствами. Эти механизмы синергетически функционируют для повышения эффективности и безопасности движения [3].

В контексте подключенных автомобилей особое внимание уделяется роли технологии 5G в интеграции транспортного средства в экосистему через коммуникационный протокол «Транспортное средство во взаимодействии со всем» (C-V2X). Этот протокол, который также активно используется в сетях 4G, достигает наивысшей эффективности и функциональности благодаря возможностям 5G. Технология C-V2X расширяет потенциал подключенных автомобилей на базе 5G, включая их в более широкую сеть взаимодействия с дорожной инфраструктурой, другими транспортными сред-

ствами и даже пешеходами, что позволяет автомобилю активно реагировать на изменения в окружающей среде и обеспечивает более высокий уровень взаимодействия и безопасности [4].

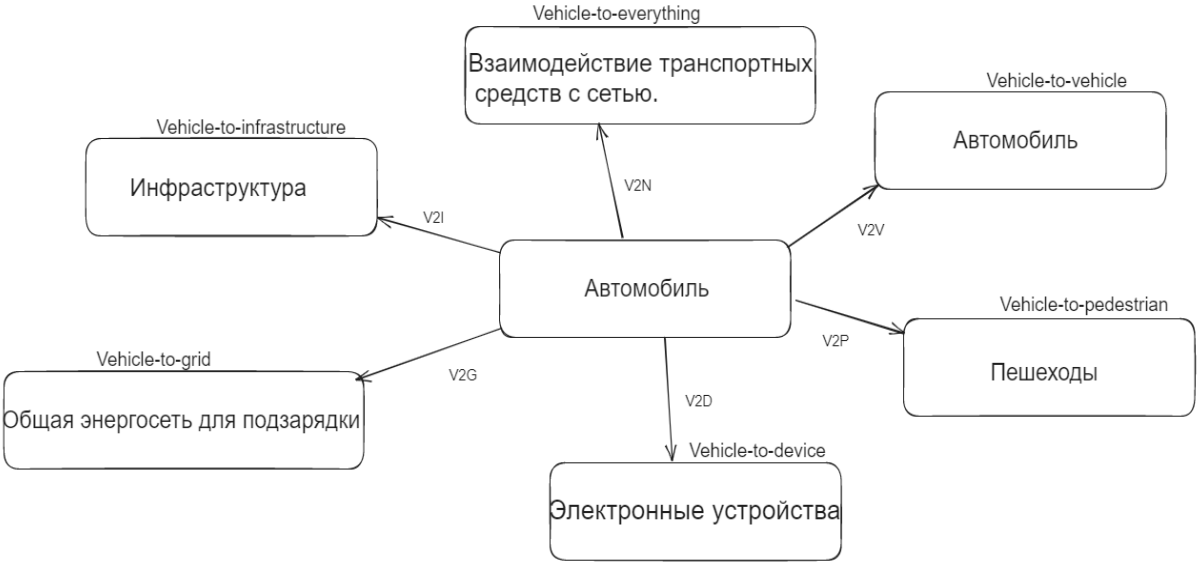


Рис. 1. Концепция V2X (Vehicle-to-Everything подключение автомобиля ко всему вокруг)

Вот как V2X технология соединяет автомобили с окружением:

Интеграция транспортных средств в систему V2X (Vehicle-to-Everything) последней генерации, версии 2N, расширяет возможности для обмена критически важной информацией между автомобилями и инфраструктурой

Эти уязвимости также открывают двери для разнообразных кибератак, включая атаки типа «отказ в обслуживании» (DoS), которые могут нарушить нормальные операции, или распространение малвари, подрывающего безопасность и функциональность системы.

Скомпрометированный канал управления может стать причиной других критических ситуаций на дороге, включая автомобильные столкновения и наезды на препятствия.

Для нейтрализации уязвимостей в канале управления, крайне важно применять продвинутые механизмы аутентификации и авторизации вместе с криптографическим обеспечением конфиденциальности передаваемой информации. К тому же, обязательно следует осуществлять регулярные пентесты и защищать сеть от DDoS-атак и других видов киберугроз.

Эксперты по кибербезопасности и инженеры, создающие беспилотные автомобили, должны сотрудничать для гарантии безопасности систем

управления и обеспечения защиты автономных транспортных средств от потенциальных киберугроз.

Список используемых источников

1. Tsolakis N., Zissis D., Papaefthimiou S. and Korfiatis N., Towards AI driven environmental sustainability: an application of automated logistics in container port terminals. International Journal of Production Research. 2022. Vol. 60 (14). PP. 4508-4528.

2. Sorooshian S., Khademi Sharifabad S., Parsaee M. and Afshari A.R.. Toward a modern last-mile delivery: Consequences and obstacles of intelligent technology // Applied System Innovation. 2022. Vol. 5 (4). P. 82.

3. Ryan M. The future of transportation: ethical, legal, social and economic impacts of self-driving vehicles in the year 2025 // Science and engineering ethics. 2020. Vol. 26(3). PP. 1185-1208.

4. Pham Q. V., Fang F., Ha V. N., Piran M. J., Le M., Le L. B., Hwang W. J. and Ding Z.. A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art // IEEE access. 2020. Vol. 8. PP. 116974-117017.

INVESTIGATION OF THE CONTROL SYSTEM AND IDENTIFICATION OF WEAKNESSES IN THE MANAGEMENT OF AN AUTONOMOUS VEHICLE

Bilan V., Perov R., Shevyakov V.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Modern cars are becoming not just vehicles, but full-fledged digital devices integrated into the ecosystem of the Internet of Things. The article examines key aspects of cybersecurity in the context of smart and connected vehicles, including vulnerabilities in mobile applications, firmware updates, and wireless communications. Special attention is paid to the C-V2X (Vehicle-to-Everything) technology, which ensures vehicle communication with other vehicles, road infrastructure and pedestrians, as well as the risk of cyber-attacks such as DoS, DDoS and malware injection. The article calls for a comprehensive approach to protecting connected cars to ensure not only convenience, but also user safety in the face of growing digital threats

Key words: *self-driving car, C-V2X, 5G, Bluetooth vulnerabilities, artificial intelligence, cybersecurity*

УДК 004.8
ГРНТИ 20.51.19

ИССЛЕДОВАНИЕ ТЕКУЩИХ СТРУКТУР И МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СФЕРЕ БЕСПИЛОТНОГО ТРАНСПОРТА

В. В. Билан, Р. А. Перов, В. Д. Шевяков

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

Статья посвящена анализу современных технологий беспилотных транспортных средств (БТС), их технической оснащенности, уровням автономности и вызовам, связанным с их внедрением. Рассмотрены ключевые компоненты систем автономного управления: лидары, радары, камеры, GPS и вычислительные блоки. Описаны этапы функционирования беспилотного автомобиля, начиная с восприятия окружающей среды и заканчивая управлением движением. Особое внимание уделено вопросам кибербезопасности и регуляторным барьерам, препятствующим массовому распространению автономных автомобилей. Также представлены уровни автономности от 0 до 5, с акцентом на достижения и прогнозы развития отрасли.

беспилотный автомобиль, искусственный интеллект, лидар, радар, системы машинного зрения, кибербезопасность, датчики

Беспилотные автомобили, функционирующие без непосредственного вмешательства человека, контролируются искусственным интеллектом. При внедрении одним из основополагающих в беспилотном автомобиле является сканеры, лидары, системы машинного зрения.

Кроме того, беспилотные транспортные средства обладают возможностью развивать высокую скорость и осуществлять операции, с исключительной точностью превосходя возможности человека за рулем, что является их достоинством, но иногда также представляет собой потенциальную опасность. Однако, как и другие технологические изделия, эти автомобили подвержены рискам кибернетических атак и хакерских взломов, что делает обеспечение их защиты от киберугроз абсолютно необходимым для их массового использования на ежедневной основе [1].

Автомобильная промышленность испытывает глубокие изменения: ведущие автопроизводители в сотрудничестве с разработчиками из сферы информационных технологий и телекоммуникаций стремятся к производству транспортных средств, способных к полной самоуправляемости. Переход к беспилотному транспорту уже неизбежен, и его массовое распространение

в ближайшем будущем кажется несомненным. Однако на пути к достижению эры полностью самоуправляемых автотранспортных средств еще множество технических и регуляторных препятствий необходимо преодолеть.

Необходимо изучить основополагающие понятия, связанные с беспилотными транспортными средствами (БТС), базирующимися на стандартных автомобилях, эксплуатируемых участниками дорожного движения. С технической стороны, превращение любого транспортного средства в автономное возможно. Основное отличие заключается в уровне автономности транспортного средства, что будет подробно разъяснено далее.

Все беспилотные аппараты следуют основополагающим принципам функционирования, во многом схожим друг с другом. Процесс работы типичного беспилотного транспортного средства охватывает следующие этапы. Начинается все с сенсорной системы восприятия, точнее, с набора датчиков, которые сканируют окружающее пространство, захватывая необходимую информацию о среде. Собранные данные передаются в блок планирования движения, который анализируя полученные сенсорные данные, картографическую информацию и позиционирование, разрабатывает маршрут и стратегию движения. Последний шаг – передача этих указаний блоку управления транспортным средством, отвечающему за непосредственное выполнение маневров в соответствии с разработанным планом перемещения [2].

Визуальное наблюдение через камеры дает возможность классификации объектов, будь то транспортные средства, пешеходы, указатели или светофоры. Радарные устройства, использующие радиоволны, способны обнаруживать объекты и измерять их скорости. Лидары же, оснащенные способностью лазерного сканирования, не только точно оценивают расстояние до объектов и их геометрические контуры, но и являются фундаментальным элементом всей системы.

– лидар, или лазерный измеритель расстояний, устанавливается на верхней части автомобиля и играет ключевую роль в системе вождения автономных транспортных средств. Он обеспечивает точное сканирование окружающей среды с помощью лазерных лучей, движущихся по горизонтали, для создания объемного образа пространства вокруг на расстоянии до 100 метров. Полученные данные объединяются с информацией с карт (например, Google Maps, Bing Maps, 2ГИС) для корректного соблюдения правил дорожного движения и определения оптимального маршрута передвижения;

– радиолокационные системы: в современных БПЛА обычно интегрируют не менее четырех радарных установок. Распределение по две единицы на передней и задней части аппарата обеспечивает всесторонний мониторинг окружающего пространства. Эти системы критичны для измерения расстояний до объектов, анализа их траекторий перемещения и скорости. Радары функционируют, посылая радиоволны, которые отскакивают от преград и возвращаются обратно к приемной антенне, тем самым выступая в роли оптических органов для дрона;
– датчик положения: GPS-ресивер, обеспечивающий технологии авто данные о географическом местоположении;
– видеокамера: ключевая для распознавания сигналов светофора и детектирования объектов, приближающихся на критическое расстояние. Типично монтируют минимум одну камеру возле зеркала заднего вида. В стандартной конфигурации автомобиля присутствует от одной до трех видеокамер.

Упомянутые ранее сенсоры собирают разнообразную информацию, требующую анализа. Обработка этих данных обычно осуществляется в автомобильных вычислительных системах, размещенных в основном в багажном отделении транспортного средства [3]. В них включены:
– основной вычислительный блок: отвечает за принятие ключевых решений касаемо движения автомобиля, основываясь на анализе информации, полученной от сенсоров;
– компьютер с визуальным интерфейсом и датчиками: управляет работой датчиков, установленных на машине;
– система управления рулевым управлением и приводом: активирует исполнение команд, связанных с маневрированием, остановкой и т.д.

В процессе движения по дороге автономный автомобиль использует лидар для создания трехмерной карты окружающего пространства, при этом он постоянно передает эти данные в бортовой компьютер для анализа. Бортовой компьютер синергетически работает с цифровыми картами, такими как Google Maps, чтобы интерпретировать получаемую информацию. В отличие от распространенного мнения, системы автономных транспортных средств часто предпочитают использование спутниковой связи, а не непосредственное подключение к интернету, для обеспечения более стабильного и надежного обмена данными. Компьютер анализирует информацию не только от лидара, но и от других датчиков, включая видеокамеры, радары и различные сенсоры, чтобы в реальном времени воссоздать детализирован-

ное представление о текущем дорожном положении. Это позволяет системе оценить поведение других участников движения и соответственно реагировать на изменения дорожной ситуации, например, ускоряться, тормозить перед светофором или поворачивать. Разработчики автономных транспортных средств стремятся обеспечить их способность к самостоятельной работе без необходимости специализированной инфраструктуры, делая беспилотники полноценными участниками общественного трафика. Существует несколько уровней автономности беспилотных автомобилей, каждый из которых характеризуется степенью самостоятельности и взаимодействия с окружающей средой [4].

В рамках классификации уровней автономии транспортных средств выделяются шесть уровней, от Уровня 0, при котором присутствует полное ручное управление автомобилем с элементарными предупреждающими системами о потенциальных угрозах на дороге, до Уровня 5, характеризующегося полной автономией транспортного средства без участия человека.

На Уровне 3 автоматизации транспортное средство обладает расширенными возможностями самостоятельного управления, тем самым предоставляя водителю дополнительное время для реагирования на сложные дорожные ситуации и перехвата управления при необходимости. В отличие от Уровня 2, который требует постоянного контроля за дорожной обстановкой и готовности оперативно вмешаться, на Уровне 3 водитель может выполнять роль наблюдателя, готового подключиться к управлению в экстренном случае.

В контексте автономного вождения, при достижении 4-го уровня автоматизации, управление транспортным средством полностью переходит к системе, давая возможность водителю полностью освободиться от задач управления, но такая автономность возможна лишь при наличии определенных предпосылок. К примеру, незаменимым условием являются объемные карты высокой разрешающей способности, обеспечивающие системе возможность точного позиционирования с прецизией до нескольких сантиметров. Большая часть исследователей и разработчиков в области автономного вождения стремится достигнуть именно этого уровня развития технологий.

Уровень 5 автономии означает полностью самоуправляемые транспортные средства, где управляющие элементы, такие как руль, отсутствуют, поскольку никакое человеческое вмешательство не требуется. Однако, согласно последним данным из отчета за 2020 год, посвященного развитию автономных транспортных средств, технологии, достигающие этого уровня,

на данный момент отсутствуют в реализации и не предвидятся в ближайшее время. Эксперты предсказывают, что до появления полностью автономных систем пройдет еще некоторое время, а на текущем этапе развития автоматизированные функции будут использоваться преимущественно для улучшения безопасности вождения, выступая в роли усовершенствованных ассистирующих систем для водителя.

Список используемых источников

1. Elallid B. B., Benamar N., Hafid A. S., Rachidi T., and Mrani N. A comprehensive survey on the application of deep and reinforcement learning approaches in autonomous driving // J. King Saud Univ. Comput. Inf. Sci. 2020. Vol. 34. № 9. PP. 7366–7390.

2. Rajabli N., Flammini F., Nardone R. and Vittorini V. Software verification and validation of safe autonomous cars: A systematic literature review // IEEE Access. 2020. Vol. 9. PP. 4797-4819.

3. Mohamed N., Al-Jaroodi J., Jawhar I., Idries A. and Mohammed F. Unmanned aerial vehicles applications in future smart cities // Technological forecasting and social change. 2020. Vol. 153. P. 119293.

4. James H. H., Pawel R. and Saduf G. Autonomous Vehicles and Robust Decision-Making in Dynamic Environments // Fusion of Multidisciplinary Research, An International Journal. 2020. Vol. 1(2). PP. 110-121.

RESEARCH OF CURRENT STRUCTURES AND METHODS OF INFORMATION SECURITY IN THE FIELD OF UNMANNED VEHICLES

Bilan V., Perov R., Shevyakov V.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article is devoted to the analysis of modern technologies of unmanned vehicles (UAVs), their technical equipment, levels of autonomy and the challenges associated with their implementation. The key components of autonomous control systems are considered: lidars, radars, cameras, GPS and computing units. The stages of the functioning of an unmanned vehicle are described, starting with the perception of the environment and ending with motion control. Particular attention is paid to cybersecurity issues and regulatory barriers that prevent the widespread adoption of autonomous cars. The levels of autonomy from 0 to 5 are also presented, with an emphasis on industry achievements and forecasts.

Key words: *self-driving car, artificial intelligence, lidar, radar, machine vision systems, cybersecurity, sensors*

УДК 004.8
ГРНТИ 20.51.19

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

Д. Д. Бучин, В. И. Лукашенок, П. А. Николаева

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

В статье рассматривается комплексный подход к обеспечению безопасности интернета вещей, охватывающий технические, криптографические и организационные аспекты. Подчеркивается важность принципа «безопасность по проектированию», включающего встраивание защитных механизмов на этапе разработки оборудования и программного обеспечения. Анализируются современные методы аутентификации, такие как цифровые сертификаты и двухфакторная аутентификация, а также применение сквозного шифрования с использованием алгоритмов AES-256, ChaCha20 и ECC. Рассматриваются перспективные технологии – блокчейн, машинное обучение и квантово-устойчивая криптография – как инструменты повышения защищенности IoT-инфраструктуры.

интернет вещей, кибербезопасность, криптография, аутентификация, шифрование, AES, блокчейн

Безопасность интернета вещей (IoT) требует комплексного подхода, сочетающего технические решения, стандартизированные протоколы и организационные меры. Основой защиты IoT-устройств является принцип «безопасность по проектированию», который предполагает встроенные механизмы защиты на этапе разработки оборудования и программного обеспечения.

Ключевую роль играет строгая аутентификация устройств в сети. Современные решения используют цифровые сертификаты и двухфакторную аутентификацию вместо уязвимых парольных систем. Для защиты передаваемых данных применяется сквозное шифрование с использованием проверенных алгоритмов, таких как AES-256, что предотвращает перехват информации даже при компрометации отдельных узлов сети [1].

Важным аспектом является регулярное обновление микропрограмм устройств через защищенные каналы. Многие производители внедряют механизмы автоматических обновлений с цифровой подписью, исключающей возможность установки модифицированного вредоносного ПО. Для крити-

чески важных систем применяется сегментация сетей, изолирующая IoT-устройства от других корпоративных ресурсов и интернета в целом.

Международные стандарты безопасности, такие как ISO/IEC 27001 и NIST IoT Cybersecurity Framework, устанавливают базовые требования к защите IoT-инфраструктуры. Они включают рекомендации по управлению доступом, мониторингу угроз и реагированию на инциденты. Для промышленного IoT особое значение имеет стандарт IEC 62443, регламентирующий защиту систем автоматизации и управления [2].

Перспективным направлением является использование технологий блокчейна для обеспечения неизменяемости данных с датчиков и создания децентрализованных систем аутентификации. Машинное обучение применяется для выявления аномального поведения устройств, что позволяет обнаруживать компрометацию на ранних этапах.

Организационные меры включают обязательный аудит безопасности на всех этапах жизненного цикла IoT-решений – от проектирования до утилизации оборудования. Особое внимание уделяется подготовке персонала, работающего с IoT-системами, и разработке четких регламентов реагирования на киберинциденты.

Эффективная защита IoT требует баланса между безопасностью, производительностью и стоимостью решений. Современные подходы предполагают многоуровневую систему защиты, где каждый элемент инфраструктуры – от отдельного датчика до облачной платформы – имеет соответствующие механизмы противодействия угрозам. Постоянное развитие стандартов и методов защиты позволяет минимизировать риски, связанные с растущим распространением интернета вещей [3].

Криптография играет незаменимую роль в обеспечении безопасности IoT-устройств. Благодаря ней данные остаются защищены на всех этапах их передачи и хранения. При ограниченных вычислительных ресурсах многих IoT-устройств применяются оптимизированные криптографические алгоритмы, обеспечивающие баланс между надежностью защиты и энергоэффективностью.

Симметричное шифрование широко используется для защиты передаваемых данных между IoT-устройствами и серверами. Алгоритм AES (Advanced Encryption Standard) с ключами длиной 128 или 256 бит является отраслевым стандартом благодаря своей надежности и относительно низким вычислительным требованиям. В системах реального времени, где важна минимальная задержка, могут применяться более легковесные алго-

ритмы, такие как ChaCha20, особенно эффективные для устройств с ограниченными ресурсами.

Асимметричная криптография, например, основанная на алгоритмах RSA или ECC (Elliptic Curve Cryptography) решает проблему безопасного обмена ключами. ECC приобретает особую популярность в IoT-средах благодаря тому, что обеспечивает сопоставимую с RSA безопасность при значительно меньшей длине ключей (256 бит ECC эквивалентен 3072 битам RSA). Это критически важно для устройств с ограниченной памятью и вычислительной мощностью [4].

Аутентификация устройств в IoT-сетях часто реализуется через механизм цифровых сертификатов X.509, которые могут быть предустановлены на устройстве еще на этапе производства. Для ресурсоограниченных устройств разработаны облегченные протоколы аутентификации, такие как OSCORE (Object Security for Constrained RESTful Environments), который является адаптацией стандарта COAP для защищенной коммуникации.

Защита целостности данных обеспечивается криптографическими хеш-функциями (SHA-256, SHA-3) и кодами аутентичности сообщений (HMAC). Эти методы позволяют обнаружить любые несанкционированные изменения данных при передаче или хранении. В системах, где важна не только целостность, но и подлинность источника данных, применяются алгоритмы цифровой подписи, которая основывается на алгоритме ECDSA (Elliptic Curve Digital Signature Algorithm).

Квантово-устойчивая криптография начинает рассматриваться как перспективное направление для долгосрочной защиты IoT-систем. Алгоритмы на основе решеток (Lattice-based cryptography) или хеш-подписей (SPHINCS+) хотя и требуют больше ресурсов, но обеспечивают защиту от потенциальных угроз со стороны квантовых компьютеров.

Особую сложность в IoT представляет управление ключами, так как многие устройства работают в автономном режиме и не могут регулярно обновлять криптографические материалы. Решения на основе технологии PKI (Public Key Infrastructure) адаптируются для IoT через использование облегченных протоколов и иерархических моделей распределения ключей. В некоторых промышленных IoT-системах применяется концепция «корня доверия» (Root of Trust), когда криптографические ключи встраиваются в аппаратное обеспечение на этапе производства чипов.

Современные тенденции включают разработку адаптивных криптографических систем, которые могут динамически изменять параметры шифро-

вания в зависимости от уровня угрозы и доступных ресурсов устройства. Это особенно важно для гетерогенных IoT-сетей, где одновременно работают устройства с разными вычислительными возможностями.

Криптографическая защита IoT продолжает развиваться, реагируя на новые вызовы, такие как появление более мощных атакующих методов и необходимость защиты данных на протяжении всего их жизненного цикла – от генерации на сенсорах до анализа в облачных системах.

Список используемых источников

1. Li B., Feng Y., Xiong Z., Yang W., Liu G. Research on AI security enhanced encryption algorithm of autonomous IoT systems // Information Sciences. 2021. Vol. 575. PP. 379–98. URL: https://www.sciencedirect.com/science/article/abs/pii/S0020025521006071 (дата обращения 10.06.2025).

2. Yaacoub J-pA., Noura H. N., Salman O., Chehab A. Ethical hacking for IoT: Security issues, challenges, Internet of things and cyber–physical systems // KeAi. 2023. URL: https://www.researchgate.net/publication/369857976_Ethical_Hacking_for_IoT_Security_Issues_Challenges_Solutions_and_Recommendation (дата обращения 10.06.2025).

3. Hamidi H. An approach to develop the smart health using Internet of Things and authentication based on biometric technology // Future Generation Computer Systems, 2019. Vol. 91. PP. 434–49. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18313517 (дата обращения 10.06.2025).

4. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy // Telecommunications Policy. 2017. Vol. 41(10). PP. 1027–38. URL: https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483 (дата обращения 10.06.2025).

Статья представлена научным руководителем, старшим научным сотрудником научно-исследовательского центра ВАС, кандидатом технических наук, доцентом Карповым М.А.

METHODS OF ENSURING SECURITY IN INTERNET OF THINGS SYSTEMS

Buchin D., Lukashenok V., Nikolaeva P.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article discusses an integrated approach to ensuring the security of the Internet of Things, covering technical, cryptographic and organizational aspects. The importance of the "design safety" principle is emphasized, which includes the embedding of protective mechanisms at the stage of hardware and software development. Modern authentication methods such as digital certificates and two-factor authentication, as well as the use of end-to-end encryption using AES-256, ChaCha20 and ECC algorithms are analyzed. Promising technologies such as blockchain, machine learning, and quantum–resistant cryptography is considered as tools to increase the security of the IoT infrastructure.

Key words: *Internet of things, cybersecurity, cryptography, authentication, encryption, AES, blockchain*

УДК 654.739
ГРНТИ 49.33.29

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ RAG ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ ИБ

В. О. Ветошев, М. Д. Горда

Санкт-Петербургский федеральный исследовательский центр Российской академии наук

Рост количества атак на российские организации сопровождается увеличением качества их реализации. В последнее время злоумышленники используют большие языковые модели, чтобы создавать вредоносное программное обеспечение, а также чтобы проводить сами атаки. Чем больше становится сложных инцидентов, там больше информации необходимо обработать специалисту по информационной безопасности. Современные подходы к расследованию инцидентов информационной безопасности требуют все большей автоматизации и интеллектуальной поддержки. Одним из перспективных решений в этой области является использование архитектуры Retrieval-Augmented Generation (RAG), сочетающей генеративные языковые модели с механизмами поиска по специализированным базам знаний. В докладе рассматриваются принципы построения и применения RAG в контексте анализа инцидентов: от обработки неструктурированных данных и формализации цифровых следов до генерации пояснительных выводов. Обсуждаются потенциальные преимущества данного подхода – возможное повышение полноты или оперативности расследований, а также возникающие при этом ограничения и требования к инфраструктуре.

искусственный интеллект расследования киберпреступлений, форензика

Про актуальность различных систем поддержки принятия решений специалистов по расследованию инцидентов информационной безопасности можно говорить на фоне возрастающей статистики успешных инцидентов в 2024-2025 годах. Причем важен не сам факт инцидента, а его последствия. Так, в 4 квартале 2024 года в ряде успешных кибератак на организации, завершившихся утечками конфиденциальной информации, основными объектами интереса злоумышленников выступали персональные данные (в 29 % случаев), учетные данные (26 %) и сведения, составляющие коммерческую тайну (20 %). В атаках, ориентированных на частных пользователей, преобладающими целями были учетные данные (47 %), персональные данные (22 %) и данные платежных карт (12 %).

Рост числа инцидентов, связанных с компрометацией учетных данных, в значительной степени обусловлен распространением сервисов формата

PHaaS (Phishing-as-a-Service), а также широким использованием вредоносного программного обеспечения класса инфостилеров. Так, в IV квартале 2024 года доля утечек учетных данных в организациях увеличилась на 4 процентных пункта по сравнению с предыдущим кварталом и на 16 процентных пунктов в сравнении с аналогичным периодом 2023 года. В сегменте атак на частных лиц доля компрометированных учетных данных достигла 47 %, что соответствует росту на 18 п. п. по сравнению с предыдущим кварталом и на 20 п. п. в годовом выражении [1].

Архитектура RAG состоит из 3 элементов:

1. Запрос вопроса или задачи, который формулирует человек (например, аналитик при расследовании инцидента). Примеры: «Какие подозрительные события были зафиксированы ночью?» или «Объясни возможный сценарий атаки по этим логам».

2. Поиск. Модель не просто «придумывает» ответ, а сначала ищет релевантную информацию в подготовленной базе знаний.

3. Генерация. Затем генеративная языковая модель берет найденную информацию как контекст и формирует связный, обоснованный ответ. То есть модель пишет текст, опираясь не на «собственные» знания, а на факты, найденные на предыдущем шаге.

Такая архитектура работы принципиально отличается от «чистой» LLM без RAG – где модель может отвечать только на основе своих встроенных знаний, которые могут быть устаревшими или неполными.

Среди преимуществ можно выделить следующие критерии:

– автоматизация сбора артефактов. RAG может самостоятельно формировать запросы к логам, SIEM или системам мониторинга, извлекая только релевантные фрагменты данных, что может ускорить процесс сбора доказательств и уменьшить нагрузку на специалистов по ИБ на первичных этапах;
– контекстный анализ журналов и логов. Модель искусственного интеллекта может более оперативно связать отдельные события в журналах безопасности в единую цепочку. Специалист может фокусироваться только на определенных элементах инцидента ИБ, сокращая трудозатраты на процесс расследования;
– распознавание шаблонов атак. Разработанная система может сопоставить ранее связанные в цепочку артефакты и их последовательность с известными техниками и тактиками популярных фреймворков (напр. MITRE

ATT&CK), что позволит оперативнее распознать тип атаки, потенциальное вредоносное воздействие и принять верное решение специалисту для нейтрализации потенциальных последствий;

– формирование гипотез и сценариев атаки. Разработанная система может предлагать специалисту различные цепочки и сценарии атаки для анализа. Специалист по ИБ быстро оценивает достоверность сценариев и выбирает наиболее вероятный;
– прогнозирование последствий. Модель может оценить, какие системы и данные могут оказаться под угрозой при текущем сценарии атаки, что может помочь быстрее определить приоритет реагирования и минимизировать ущерб. Система на базе RAG может подсказать уязвимые точки и возможные пути распространения атаки, помогая специалисту по ИБ планировать свои действия.

Имея определенные выше преимущества, система на базе RAG потенциально может иметь следующие ограничения и риски:

– необходимость актуальной и качественной базы знаний. Эффективность RAG напрямую зависит от полноты и актуальности базы знаний. Если база устарела или содержит неточности, система может выдавать неверные или неполные ответы. Требуется регулярное пополнение и поддержка базы данных знаний;
– риск генерации недостоверной информации (галлюцинации). Даже при наличии хорошей базы знаний языковая модель может дополнять ответ вымышленными деталями или некорректными связями. Это может быть особенно критично при подготовке официальных отчетов (например, в контролирующие органы). Поэтому специалист по ИБ всегда должен проверять результаты генерации;
– вычислительная нагрузка и затраты на инфраструктуру. Для качественной работы RAG требуется мощное оборудование: производительные серверы или облачные ресурсы для хранения базы знаний и для работы языковой модели. Как и любая другая система, система на базе моделей ИИ требует определенных ресурсов и определенных подходов, и их минимизации.

Так как эффективность и качество работы системы и ответов от RAG напрямую зависит от корректности данных в базе знаний, авторами были предложены 2 категории источников знаний – технические и научные.

С точки зрения технических могут быть интегрированы как международные стандарты, базы данных угроз и уязвимостей, так и внутренние материалы, накопленные компанией или разработчиками системы. В качестве источников знаний, обеспечивающих содержательную основу для генерации и анализа, целесообразно использовать таксономии атак, таких как MITRE ATT&CK, включающие в себя верифицированные экспертами тактики, техники и процедуры.

Важным компонентом также являются базы зарегистрированных уязвимостей, включая CVE, NVD и БДУ, содержащие формализованные описания известных уязвимостей и соответствующие им идентификаторы. Существенную роль играют отчеты по киберугрозам (Threat Intelligence Reports), представляющие собой аналитические сводки о текущем состоянии угроз, их векторах и методах реализации.

Наряду с внешними источниками важное значение приобретают внутренние кейсы, отчеты расследований и иные документы, отражающие накопленный опыт организации в расследовании инцидентов. Дополнительную ценность представляют руководства и стандарты, регламентирующие порядок реагирования на инциденты информационной безопасности и методы сбора цифровых доказательств.

В рамках алгоритмической составляющей RAG могут использоваться различные методики обработки, анализа и интерпретации информации. Базовый уровень включает алгоритмы поиска, по ключевым словам, и индикаторам компрометации, позволяющие осуществлять первичную фильтрацию релевантных данных. Последовательности реагирования, представленные в виде алгоритмов, обеспечивают системную реализацию шагов при инциденте и могут быть использованы как шаблоны в процессе генерации ответов. Важной составляющей также выступают методики анализа цифровых артефактов, включая построение временных диаграмм и реконструкцию последовательностей событий.

Используя корректные источники с технической и научной точки зрения, предполагается достигнуть лучших результатов использования технологии RAG в качестве поддержки принятия решений специалистов по информационной безопасности [2, 3].

Проводилось сравнение различных подходов к расследованию, результаты которого представлены в таблице 1.

ТАБЛИЦА 1. Сравнение с аналогичными решениями

Параметр	Только специалист	Традиционная автоматизация	LLM (чистая генерация)	RAG
Требования к квалификации	Очень высокие	Высокие	Средние	Средние-низкие
Скорость расследования	Низкая	Средняя	Высокая	Высокая
Точность и полнота анализа	Высокая (зависит от опыта)	Средняя	Низкая без базы	Высокая
Вероятность ошибки или галлюцинации	Низкая	Низкая (ошибки сценариев)	Высокая	Низкая (контролируется фактами)
Объяснимость выводов	Высокая	Средняя	Низкая	Высокая
Гибкость и масштабируемость	Низкая	Средняя	Высокая	Высокая

На основе результатов сравнения можно сделать вывод, что на данном этапе, с теоретической точки зрения, система, которая будет использовать RAG в качестве основы формирования гипотез, должна быть самой эффективной. Использование только специалистов сопровождается высокими требованиями к квалификации, а также точность и полнота анализа зависит напрямую от квалификации и, часто, от человеческого фактора. Проблематика использования квалифицированных специалистов заключается в их потенциальной стоимости. Ведь, чтобы получить квалифицированного специалиста, необходимо его сначала обучить и продолжать обучать периодически.

Традиционные средства автоматизации действительно превосходят человека по скорости выполнения рутинных задач, однако их эффективность ограничена рамками заранее определенных сценариев. Такие системы плохо адаптируются к нестандартным ситуациям, демонстрируют ограниченную точность анализа, а в условиях динамично меняющейся обстановки могут давать ошибки вследствие устаревших правил или некорректных шаблонов. При этом требования к квалификации оператора, управляющего автоматизированной системой, остаются высокими, особенно, если речь

идет о необходимости интерпретации результатов или корректировки логики обработки.

Использование больших языковых моделей в режиме чистой генерации обеспечивает высокую скорость и масштабируемость, но сопровождается рисками появления галлюцинаций – ложных или недостоверных выводов, не подкрепленных исходными данными. Такие ошибки зачастую трудно выявить без привлечения эксперта. Кроме того, объяснимость результатов LLM остается на низком уровне, а сама модель не способна обосновывать свои гипотезы ссылками на исходные источники или данные.

Интеграция RAG позволяет нивелировать указанные ограничения за счет совмещения генеративных возможностей с доступом к проверенным источникам знаний. Это обеспечивает не только высокую точность и релевантность гипотез, но и их верифицируемость, что критически важно в задачах расследования инцидентов информационной безопасности. Благодаря гибкости и масштабируемости такие системы адаптируются к различным уровням пользовательской квалификации и сложности инцидентов, что делает архитектуру RAG наиболее сбалансированным и перспективным решением.

Работа выполнена при финансовой поддержке РНФ (проект 25-11-20028).

Список используемых источников

1. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года // URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id19 (дата обращения 10.05.2025).

2. Горда М. Д. Концепт ассистента для расследования инцидентов информационной безопасности на основе искусственного интеллекта / М. Д. Горда // Информатизация и связь. 2025. № 1. С. 123-128. DOI 10.34219/2078-8320-2025-16-1-123-128.

2. Gorda M. On the Use of Artificial Intelligence in Cybersecurity Incident Investigations // 2025 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation. 2025. PP. 747-752. DOI: 10.1109/SmartIndustryCon65166.2025.10986177.

Статья представлена научным руководителем, доцентом кафедры Защищенных систем связи СПбГУТ, кандидатом технических наук, доцентом А. А. Чечулиным.

ON THE USE OF RAG IN CYBERSECURITY INCIDENT INVESTIGATION

Vetoshev V. Gorda M.
St. Petersburg Federal Research Center of the Russian Academy of Sciences

The increasing number of attacks on Russian organizations is accompanied by a rise in the sophistication of their execution. Recently, malicious actors have begun to leverage large language models (LLMs) not only to generate malicious software but also to orchestrate the attacks themselves. As complex incidents become more frequent, cybersecurity specialists are required to process ever-larger volumes of information. Modern approaches to cybersecurity incident investigation thus demand greater automation and intelligent decision support.

One of the promising solutions in this domain is the use of the Retrieval-Augmented Generation (RAG) architecture, which combines generative language models with retrieval mechanisms based on specialized knowledge bases. This presentation explores the principles of designing and applying RAG in the context of incident analysis – from processing unstructured data and formalizing digital traces to generating explanatory conclusions. The potential advantages of this approach are discussed, including improved completeness and timeliness of investigations, along with the associated limitations and infrastructure requirements.

Key words: *artificial intelligence, cybercrime investigation, digital forensics*

УДК 004.492.3
ГРНТИ 81.93.29

ОБНАРУЖЕНИЕ АНОМАЛИЙ В ВЕБ-ТРАФИКЕ С ПОМОЩЬЮ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Л. А. Виткова[1,2], И. П. Колинко[1]

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В условиях стремительной цифровизации количество веб-трафика значительно возрастает из-за широкого распространения удаленной работы, развития облачной инфраструктуры, повсеместного использования веб-приложений и роста количества устройства «интернета вещей». Вместе с этим растет число киберпреступлений: в 2024 году в России зафиксировано 765,4 тыс. инцидентов, что на 13,1 % больше, чем в 2023 году, а их доля достигла 40 % от всех преступлений [1]. С 2006 года кибератаки смещаются на конечных пользователей, при этом актуальным типом атак остаются SQL-инъекции и ботнеты. К 2024 году 90 % трафика зашифровано, что затрудняет обнаружение угроз. В 2023–2025 годах хакеры активно используют облачные хранилища и легитимные инструменты, ускоряя атаки и применяя методы «living off the land». Фишинг остается основным способом проникновения, а уязвимости вроде Log4Shell широко эксплуатируются. Для всех типов вышеописанных угроз одними из самых опасных атак являются атаки нулевого дня, неуловимые для традиционных методов. Это подчеркивает актуальность внедрения систем защиты на основе ИИ. Обученные на нормальном трафике, эти системы выявляют аномалии, предотвращая вторжение хакеров. Далее рассматриваются подходы машинного обучения к детекции веб-атак, а также формулируются последние тенденции развития этой области.

веб-трафик, искусственный интеллект, обнаружение аномалий, IDS /IPS

Современные исследования IDS (Intrusion Detection System, системы обнаружения вторжений), основанные на использовании искусственного интеллекта, выделяют несколько ключевых направлений:

– гибридные модели – совместное использование CNN, LSTM и автоэнкодеров для комплексного анализа трафика;
– payload-анализ – использование векторных представлений для глубокого анализа содержимого;
– оптимизация признаков – применение эвристик и гибридных методов;
– интерпретируемость – развитие объяснимого ИИ для повышения доверия к системам.

Эти тенденции направлены на создание универсальных, эффективных и прозрачных IDS, способных противостоять различным типам угроз и атакам нулевого дня.

Современные системы обнаружения вторжений все чаще используют комбинации архитектур нейросетей глубокого обучения, таких как сверточные нейронные сети (Convolutional Neural Networks, CNN), особые архитектуры рекуррентных сетей с использованием технологии короткой долгосрочной памяти (Long Short-Term Memory, LSTM), рекуррентные блоки с управлением (Gated Recurrent Units, GRU) и автоэнкодеры. Эти модели позволяют эффективно анализировать сложные структуры сетевого трафика, выявляя как пространственные, так и временные закономерности.

Одним из примеров является модель CNN+LSTM, предложенная в исследовании [2]. Эта архитектура сочетает в себе возможности CNN для извлечения локальных признаков из данных и LSTM для анализа последовательностей во времени. Модель была протестирована на наборе данных UNSW-NB15, который включает трафик с различными типами атак, такими как DoS и эксплойты. Результаты показали, что точность классификации достигает 98,85 %. Такой результат показывает, что эта модель одна из самых эффективных в своем классе. Важным преимуществом является ее применимость к устройствам с ограниченными вычислительными ресурсами.

Другой подход представлен в работе [3], где используется мультимодальный автоэнкодер (Multimodal Deep Autoencoder, MDAE) в сочетании с GRU. Эта модель была обучена на датасете CICIDS2017, содержащем современные типы атак, включая DDoS, SQL-инъекции и ботнеты. MDAE позволяет извлечь компактное представление данных из мультимодальных источников (например, заголовков пакетов и их содержимого), а GRU, как и LSTM в работе [2], эффективно моделирует временные зависимости. Итоговая точность составила 99,1 %, а уровень ложных срабатываний (False Positive Rate, FPR) остался минимальным.

Автоэнкодеры также применяются для снижения размерности данных и обнаружения аномалий. В статье [4] описана модель, где автоэнкодер сначала сжимает признаки сетевого трафика в компактное пространство, а затем метод поиска аномалий OCSVM (One-Class SVM) и гауссовы смеси (Gaussian Mixture Models, GMM) используются для выявления отклонений. Тестирование на наборе данных NSL-KDD показало точность 98,73 % при

низком уровне ложных срабатываний. Однако стоит отметить, что датасет NSL-KDD содержит записи трафика 2009 года, а это значит, что он устарел.

Комбинированные архитектуры, такие как CNN+LSTM, MDAE+GRU и автоэнкодеры с OCSVM, демонстрируют высокую адаптивность к различным типам трафика и атакам. Они позволяют учитывать как пространственные, так и временные характеристики данных, что делает их перспективными для разработки IDS следующего поколения.

Традиционные IDS часто ограничиваются анализом заголовков пакетов, однако современные атаки, такие как HTTP-инъекции или замаскированные вредоносные нагрузки, требуют более глубокого подхода. Payload-based анализ фокусируется на содержимом пакетов, что значительно повышает способность систем выявлять сложные угрозы.

В исследовании [5] предложен метод, использующий модифицированную версию алгоритма Word2Vec для преобразования байтовых последовательностей из payload в векторные представления. Этот подход заимствует идеи из обработки естественного языка, рассматривая байты как "слова", а пакеты как "предложения". После получения векторов применяется алгоритм k-ближайших соседей (k-Nearest Neighbors, kNN) для классификации трафика. Модель была протестирована на датасетах CICIDS2017 и CTU-13 и достигла точности 99 %. Такой высокий результат объясняется способностью метода улавливать семантические закономерности в данных, что особенно полезно для обнаружения атак на прикладном уровне.

Payload-based анализ позволяет выявлять угрозы, которые остаются незаметными для традиционных систем, например, замаскированные эксплойты в зашифрованном трафике. Однако он сталкивается с проблемами масштабируемости и обработки больших объемов данных в реальном времени. Для решения этих задач предлагается интеграция с гибридными архитектурами глубокого обучения, такими как CNN, которые могут ускорить анализ.

Сетевые данные характеризуются высокой размерностью, что усложняет работу IDS. Оптимизация признакового пространства позволяет повысить точность классификации и снизить вычислительные затраты.

Метод TSO (Tuna Swarm Optimization), предложенный в [3], вдохновлен поведением косяков тунца и использует эвристический алгоритм оптимизации для выбора наиболее релевантных признаков. Алгоритм способен адаптироваться к различным типам трафика, и это делает его универсаль-

ным инструментом для IDS. В сочетании с блоками MDAE и GRU, TSO достиг точности 99,1 % на датасете CICIDS2017, притом он смог выделить минимально возможное количество признаков, что позволило повысить производительность системы.

Альтернативой TSO является подход «гибридного выбора признаков» (HFS, Hybrid Feature Selection) [6], интегрирующий несколько методик: отбор признаков, основанный на их корреляции (CFS, Correlation-based Feature Selection) для устранения проблемы мультиколлинеарности, рекурсивное уменьшение количества признаков (RFE, Recursive Feature Elimination) для итеративного отбора признаков и алгоритм случайного леса (RF, Random Forest) в качестве базового классификатора. Практическая реализация HFS в комбинации с LightGBM для систем обнаружения вторжений в программно-конфигурируемых сетях (SDN-IDS) показала его превосходство над традиционными методами отбора признаков. В частности, на тестовом наборе данных NSL-KDD была достигнута точность классификации 98,72 %, а также отмечено значительное улучшение производительности при обработке потокового трафика.

Методы TSO и HFS обеспечивают баланс между точностью и производительностью, что критически важно для реальных систем. Они позволяют сократить объем данных, сохраняя информативность, и делают IDS более устойчивыми к шуму.

Сравнение различных моделей демонстрирует их сильные и слабые стороны:

– CNN + LSTM: Точность 98,85 % на UNSW-NB15 [2]. Подходит для устройств с ограниченными ресурсами;
– TSO + MDAE + GRU: Точность 99,1 % на CICIDS2017 [3]. Высокая адаптивность к сложным атакам, однако вызывает вопросы скорость работы системы в «реальном времени»;
– AE + OCSVM + GMM: Точность 98,73 % на NSL-KDD [4]. Эффективен для обнаружения аномалий. Стоит заметить, что был использован устаревший датасет, а также нет данных о возможности использования в «реальном времени»;
– Payload Embedding + kNN: Точность 99 % на CICIDS2017 и CTU-13 [5]. Отлично справляется с атаками на уровне приложений. Так же как и в предыдущей архитектуре, скорость потоковой обработки данных в статье не была освещена;

– HFS + LightGBM: Точность 98,72 % на NSL-KDD [6]. Устаревший датасет, но бустинговые алгоритмы обычно отличаются высоким быстродействием.

Гибридные модели показывают наилучшие результаты благодаря сочетанию различных подходов, что позволяет им адаптироваться к реальным условиям.

Рассмотренные в статье подходы машинного обучения, включая системы ИИ, обученные на нормальном трафике, эффективно выявляют аномалии и атаки нулевого дня, преодолевая ограничения традиционных методов. Однако масштабирование этих решений для реального времени остается проблемой. Также одной из основных препятствий для повсеместного внедрения IDS на базе ИИ является низкая интерпретируемость выводов моделей. Специалисты ИБ хотят знать, каким образом «умная» IDS приняла решение, что событие было аномальным. Это критично для ускорения будущего расследования или для принятия решения о, например, блокировки пользователя. Будущие исследования должны сосредоточиться на повышении вычислительной эффективности и интерпретируемости моделей. Развитие ИИ-систем детекции аномалий в веб-трафике играет ключевую роль в защите от все более изощренных угроз, обеспечивая устойчивость цифровой экосистемы.

Список используемых источников

1. Происшествия. ТАСС: Информационное агентство России. URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 06.06.2025).

2. Altaie R. H., Hoomod H. K. An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm // Engineering, Technology & Applied Science Research. 2024. № 5. PP. 16740–16743.

3. Gowthami G., Silvia Priscila S. Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach // International Journal of Computational Complexity and Biomedical Systems. 2023. № 4. PP. 355–374.

4. Wang C., Sun Y., Lv S., Wang C., Liu H., Wang B. Intrusion Detection System Based on One-Class Support Vector Machine and Gaussian Mixture Model // Electronics. 2023. № 94. P. 930.

5. Mehedi Hassan, Md Enamul Haque, Mehmet Engin Tozal, et al. Intrusion Detection Using Payload Embeddings // IEEE Access. 2021. № 10. PP. 4015-4030.

6. Logeswari G., Bose S., Thangasamy Anitha. An Intrusion Detection System for SDN Using Machine Learning // Intelligent Automation & Soft Computing. 2023. № 1. PP. 867–880.

DETECTING ANOMALIES IN WEB TRAFFIC USING ARTIFICIAL INTELLIGENCE MODELS

Kolinko I., Vitkova L.
[1, 2]St. Petersburg Federal Research Center of the Russian Academy of Sciences
[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In the context of rapid digitalization, web traffic volume is increasing significantly due to the widespread adoption of distance work, the development of cloud infrastructure, the ubiquitous use of web applications, and the growing number of Internet of Things (IoT) devices. Concurrently, the number of cybercrimes is rising: in 2024, 765.4 thousand incidents were recorded in Russia, representing a 13.1 % increase compared to 2023, and accounting for 40 % of all crimes [1]. Since 2006, cyberattacks have increasingly targeted end-users, with SQL injections and botnets remaining prevalent attack types. By 2024, 90 % of traffic is encrypted, complicating threat detection. During 2023–2025, hackers have actively exploited cloud storage and legitimate tools, accelerating attacks and employing "living off the land" techniques. Phishing remains the primary infiltration method, and vulnerabilities such as Log4Shell are widely exploited. For all the aforementioned threat types, zero-day attacks represent some of the most dangerous, evading traditional detection methods. This underscores the relevance of implementing AI-based security systems. Trained on normal traffic, these systems identify anomalies, thereby preventing hacker intrusions. The following sections examine machine learning approaches to web attack detection and outline the latest development trends in this field.

Key words: *web traffic, artificial intelligence, anomaly detection, zero-day attacks*

УДК 004.056
ГРНТИ 49.33.35

СТЕГОСИСТЕМА ДЛЯ ВИДЕО С УЛУЧШЕННОЙ СКРЫТНОСТЬЮ, ИСПОЛЬЗУЮЩАЯ КВАНТОВЫЙ КОМПЬЮТЕР С ЦЕЛЬЮ УСКОРЕНИЯ ПРОЦЕДУРЫ ВЛОЖЕНИЯ

Е. Ю. Герлинг, В. И. Коржик

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

В работе рассматривается возможность использование квантового компьютера для стегосистемы с минимизацией внесения изменений в заданном «покрывающем объекте», представленном в виде видеофайла. Использование квантового компьютера позволит ускорить процесс вложения скрываемой информации в файл, что, в свою очередь, приведет к увеличению объема передаваемой информации.

стеганография, видеофайл, вложение, покрывающий объект, стеганограммы, хеширование, квантовый компьютер, алгоритм Гровера

Введение

Как известно, стегосистемы (СГ) предназначены для скрытой передачи (или хранения) конфиденциальной информации, присутствующей в различных покрывающих объектах (ПО). В качестве таких ПО могут использоваться неподвижные изображения, цифровые данные, видеофайлы, текстовые файлы, аудиофайлы, машинные коды и другая информация.

В отличие от криптографии (КГ), где скрытность содержания секретной информации (СИ) обеспечивается ее шифрованием, от СГ требуется скрыть в ПО и сам факт присутствия такой СИ, что было бы невозможно при использовании только КГ. Монография [1] представляет собой наиболее полный набор сведений по традиционной СГ, где описываются методы оценки ее секретности, алгоритмы вложения и извлечения СИ в различное ПО, методы стегоанализа (СГА) и оценки эффективности СГА. Аналогичные сведения по системам СГ можно найти и в учебнике [2].

В [1], а также в [2] показано, что идеально секретную СГ, т.е. такую, для которой даже при использования наилучшего метода СГА справедливо равенство $P_{\text{fa}} = P_{\text{m}} = 0{,}5$, где P_{fa} – вероятность ложного обнаружения СГ, а P_{m} – вероятность пропуска обнаружения СГ, можно получить лишь для не-

которых искусственных моделей ПО, которые практически не встречаются на практике.

Однако в последнее время в теории построения СГ появились новые направления, связанные с использованием искусственного интеллекта на базе технологии нейронных сетей. Это СГ, построенные на основе технологии GAN (Generative Adversarial Network) [3].

Еще более радикальное направление последних систем СГ получило название «СГ без вложения» (embeddingless SG) [4]. Общая идея такой технологии довольно проста и для неподвижных изображений в качестве ПО она может быть кратко описана следующим образом.

Пусть имеется большая база цифровых изображений. Также как и для СГ-GAN, первоначально зашифровывается все конфиденциальное сообщение и делится на порции длиной m бит. Затем от случайно выбранного изображения вычисляется хеш-функция с длиной хеша m бит и полученный хеш сравнивается с первой порцией криптограммы. При совпадении данные изображения включаются в первую часть СГ. В противоположном случае данное изображение из базы игнорируется, мы переходим к следующему случайно выбранному изображению и повторяем еще раз всю процедуру. Так формируется набор изображений, хеши от которых совпадают со всеми порциями криптограммы. Этот набор изображений сохраняется (или передается по каналам связи), как полная СГ.

Ясно, что в этом случае ни одно из сохраненных изображений не подвергалась изменениям и поэтому такой вид СГ полноправно можно считать «СГ без вложения». Однако данный подход имеет два существенных недостатка.

Первый заключается в том, что СГ, состоящая из случайно выбранных из базы изображений, выглядит подозрительно, как некоторая стеганограмма. Второй же недостаток состоит в том, что ПО оказывается случайно выбранной для обычных пользователей.

В литературе, правда, предлагается использовать алгоритм Дирихле [5], который с использованием специально обученных нейронных сетей может отобразить близкие по семантике изображения и подвергнуть анализу на совпадение хешей только их. Однако такая «близость» может оказаться недостаточно обоснованной.

В следующем разделе настоящей работы описывается алгоритм вложения максимального количества информации в произвольно выбранный за-

ранее видеофайл, что полностью снимает оба перечисленных выше недостатка, но, конечно, не может претендовать на название СГ без вложения.

1. Алгоритм построения СГ повышенной секретности с изменением одного бита в каждом кадре видеофайла

Схема алгоритма вложения показана на рис. 1, а извлечения – на рис. 2.

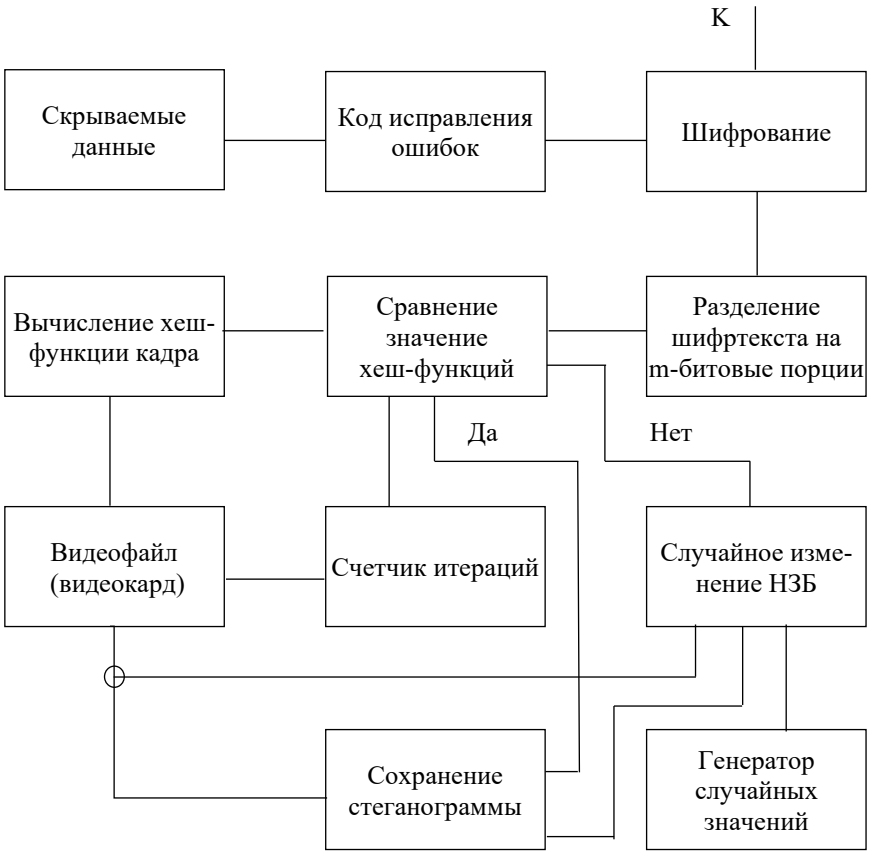


Рис. 1. Алгоритм вложения скрываемой информации в заданный видеофайл

Как видно из рис. 1, заданный двоичный видеофайл подвергается стойкому потоковому (для отсутствия размножения ошибок) шифрованию, полученная криптограмма делится на «порции» длиной m бит каждая. Кадр видеофайла хешируется при помощи бесключевых хеш-функций, имеющих на выходе двоичную последовательность длиной m бит, которая последовательно сравнивается с порциями криптограммы.

При их полном совпадении текущий кадр сохраняется и осуществляется переход к обработке следующего кадра видеоизображения.

Если же эти две m-битовые последовательности не совпадают, хотя бы в одном из этим m бит, то случайно и взаимно независимо выбирается байт

из описания видеопотока кадра и его наименее значащий бит (НЗБ) изменяется на противоположный. Затем вновь вычисляется хеш-функция измененного кадра. Описанная выше процедура повторяется до тех пор, пока не наступит совпадение. Если же при заданном значении, и при количестве повторений $\leq l_0$, совпадения не наступает, то для данного кадра будет использовать код исправления ошибок. Очевидно, что чем больше выбрана длина порции l, тем больше время требуется для преобразования видеофайла в стеганограмму. С другой стороны, чем больше l, тем меньше будет вероятность ошибки в порции из m символов после дешифрования стеганограммы, то есть выбором параметра l_0 можно производить обмен между этими двумя величинами, которые определяют эффективность предлагаемой стегосистемы.

Можно сравнивать предлагаемый метод с тривиальным методом вложения путем инверсии одного бита НЗБ в каждом кадре. Однако в последнем случае пришлось бы указать, какой из пикселей каждого кадра подвергся вложению, что, безусловно, позволило бы реализовать тривиальный метод стегоанализа.

На рис. 2 представлена блок-схема алгоритма извлечения конфиденциальной информации легитимным пользователем.

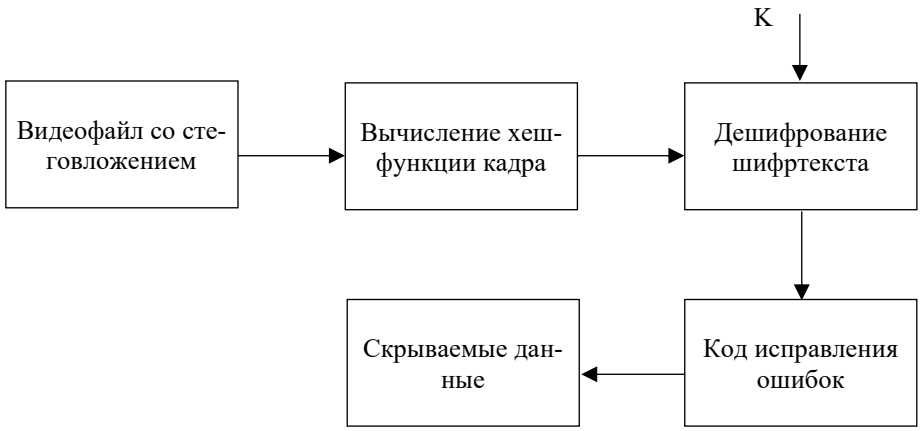


Рис. 2. Блок-схема алгоритмы извлечения конфиденциальной информации легитимным пользователем

Данная схема достаточно проста и не требует дополнительных пояснений. Можно лишь заметить, что если при помощи совпадения хешей кадров и блоков криптограммы длиной m количество попыток случайного выбора изменяемых битов превысит заданный порог l, то на данном m-блоке возникают ошибки, которые (при не слишком большой их вероятности) могут быть исправлены корректирующим m-ичным кодом, исправляющим

ошибки, например, кодом Рида-Соломона (РС) с символами из конечного поля Галуа GF(q), где $q = 2^m$. (Задача в выборе параметров РС-кода и алгоритма исправления ошибок выходит за рамки настоящей статьи, но авторы собираеются решать ее в ближайшем будущем).

2. Оценка вероятностей совпадения порций криптограммы с хешами кадров, в которых в случайно выбранном байте инвертирован НЗБ, для при заданном числе попыток

Рассмотрим сначала идеализированный (наилучший для разрабатываемой стегосистемы) случай, когда мы предположим, что после каждого преобразования кадра с инвертированным НЗБ случайно выбранного байта вероятность получения хеша с любой порцией криптограммы длиной m будет одинакова и равна 2^{-m}. Легко видеть, что также вероятности как функции числа попыток l и длины хеша m имеют следующий вид:

$$P_c(m, l) = 1 - \left(\frac{2^m - 1}{2^m}\right)^l \quad (1)$$

В таблице 1 представлены значения вероятностей, вычисленных по (1) для $m = 5$ и $m = 10$, l от10 до 10^4.

ТАБЛИЦА 1. Вероятности успешных попыток преобразования видеофайла для предложенного метода построения стегосистемы для параметров $m = 5$ и $m = 10$, $l < 10000$

l	10	50	100	150	200	500	1000	10000
$P_c(m, l)$ при $m = 5$	0,272	0,796	0,958	0,992	0,998	1	1	1
$P_c(m, l)$ при $m = 10$	0,010	0,048	0,093	0,136	0,177	0,387	0,624	1

Поскольку реально должны использоваться не случайные бесключевые хеш-функции, а одна из стандартных, то было произведено моделирование алгоритма вложения в файл с кадром формата 1920x1080 (примерно 2 миллиона пикселей) для стандартной хеш-функции. Результат экспериментов показан в таблице 2.

ТАБЛИЦА 2. Экспериментальная вероятности успешных попыток преобразования видеофайла для предложенного метода построения стегосистемы и стандартной хеш-функции CRC32 для параметров $m = 5$ и $m = 10$, $l < 10000$

l	10	50	100	150	200	500	1000	10000
$P_c(m, l)$ при $m = 5$	0,250	0,781	0,969	1	1	1	1	1
$P_c(m, l)$ при $m = 10$	0,010	0,045	0,090	0,133	0,173	0,380	0,603	1

Из результатов таблицы 2 видно, что сложности «вложения» скрытой информации является вполне достижимой при создании видеофайла.

Также из таблиц 1-2 видно, что теоретические расчеты требуемых попыток вложения близки к экспериментальным данным.

3. Использование алгоритма Гровера

В таблицах 1-2 рассмотрено вложение 5 и 10 бит, при этом по теоретическим расчетам в кадр формата 1920x1080 можно вложить максимум 17 бит, поскольку количество пикселей примерно 2 миллиона, что в итоге позволит повысить скорость передачи. Основанная проблема вложения большого объема информации – время поиска необходимого для изменения НЗБ может занять довольно много времени. Так, поиск нужной комбинации для вложения 17 бит может занять более 6 лет, что, конечно, неприемлемо. Для решения этой проблемы подойдет квантовый компьютер и алгоритм Гровера, которые позволит уменьшить количество необходимых итераций в $\sqrt{l}$ при поиске нужного значения хеш-функции. Сравнение времени и количества итерации для вложения методом прямого перебора и алгоритмом Гровера приведено в таблице 3.

ТАБЛИЦА 3. Сравнение времени и количества итерации для вложения методом прямого перебора и алгоритмом Гровера

Длина хеша (количество вкладываемых бит)	Количество итераций для прямого перебора	Оценка времени прямого перебора, сек	Количество итераций для алгоритма Гровера	Оценка времени перебора для алгоритма Гровера, сек
4	200	10	15	0,5
5	400	20	20	1

Длина хеша (количество вкладываемых бит)	Количество итераций для прямого перебора	Оценка времени прямого перебора, сек	Количество итераций для алгоритма Гровера	Оценка времени перебора для алгоритма Гровера, сек
6	800	60	29	2
7	1 600	180	40	5
8	3 200	718	57	13
9	6 300	$3x10^3$	80	36
10	12 500	$11x10^3$	112	100
11	25 000	$45x10^3$	159	285
12	50 000	$180x10^3$	224	804
13	100 000	$718x10^3$	317	$2x10^3$
14	200 000	$3x10^6$	448	$6x10^3$
15	400 000	$11,5x10^6$	633	$18x10^3$
16	800 000	$46x10^6$	895	$51x10^3$
17	1 600 000	$184x10^6$	1265	$145x10^3$

Как видно из таблицы 3, квартовый компьютер и алгоритм Гровера позволит значительно сократить количество итераций при поиске нужного значений хеш-функции кадра, что также приведет к увеличению скорости передачи данных.

Заключение

Как видно из результатов расчетов, приведенных в таблице 3, использование алгоритма Гровера позволяет не только уменьшить количество итераций, но и сократить время вложения. Так, вложение 17 бит при прямом переборе займет почти 6 лет, а при использовании алгоритма Гровера – 1,5 дня. Следовательно, использование алгоритма Гровера позволит существенно сократить время вложение, а значит, и повысить скорость передачи информации.

Список используемых источников

1. Fridrich J., Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010. 437 с.

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

3. Zhang K. A., Cuesta-Infante A., Xu L., Veeramachaneni K.. SteganoGAN: High Capacity Image Steganography with GANS, arXiv: 1901.03892v2 [cs.CV], 2019.

4. Li B., He J. H., Huang J. W., and Shi Y. Q. A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing 2011. Vol. 2. № 2. PP. 142-172.

5. Blei D. M., Ng A. Y., Jordan M. I. Latent Dirichlet Allocation // Journal of Machine Learning Research. 2003. № 3. PP. 993-1022.

VIDEO STEGOSYSTEM WITH IMPROVED SECURITY USING A QUANTUM COMPUTER TO ACCELERATE THE EMBEDDING PROCESS

Gerling E., Korzhik V.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The paper examines the possibility of using a quantum computer for a stegosystem with minimization of changes in a given "cover object" represented as a video file. The use of a quantum computer will accelerate the process of embedding hidden information into the file, which, in turn, will lead to an increase in the volume of transmitted information.

Key words: *steganography, video file, embedding, cover object, steganograms, hashing, quantum computer, Grover's algorithm*

УДК 004.51
ГРНТИ 81.93.29

ВИЗУАЛИЗАЦИЯ ДАННЫХ БЕЗОПАСНОСТИ НА ГЕОГРАФИЧЕСКИХ КАРТАХ СРЕДСТВАМИ ЯЗЫКА PYTHON

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

Со временем разнообразие киберугроз неуклонно растет, и некоторые атаки имеют специфические шаблоны поведения, связанные с географическим местоположением. Поэтому для выявления отдельных видов кибератак важную роль играет геолокация инцидента безопасности. Также отображение данных безопасности на географических картах может оказать неоценимую помощь для цифровой криминалистики. В докладе представлен подход к отображению данных безопасности на географических картах с помощью языка программирования Python.

визуализация данных, визуальный анализ, геоданные, информационная безопасность

Введение

Существует ряд киберугроз, которые можно распознавать с помощью изучения геолокации всплывающих событий информационной безопасности. Например, для DDoS-атак характерным паттерном является отправка пакетов со множества разных IP-адресов на один и тот же хост. Также некоторые исследователи предлагают использовать данные о геолокации и языковых предпочтениях в целях выявления вредоносных сайтов [1].

Кроме того, географические карты могут использоваться в приложениях информационной безопасности в составе средств обнаружения и предотвращения вторжений [2].

Таким образом, геолокация может оказаться полезной оператору для анализа паттернов событий безопасности. Поэтому возникает необходимость разработать эффективный подход к отображению данных безопасности на географических картах.

Краткий обзор средств к визуализации географических карт

Географические карты могут отображаться как с помощью специализированных приложений, таких как QGIS, Google Earth Engine, Carto и др. [3], так и посредством соответствующих библиотек различных языков программирования, например, JavaScript и Python.

Обе эти группы обладают как преимуществами, так и слабыми местами. Так, готовые приложения обладают широким функционалом, однако имеют сложности в процессе интеграции с кастомными приложениями. Кроме того, могут возникать трудности с отображением дополнительных данных из сторонних датасетов с целью решения специфических задач информационной безопасности.

Географические карты, созданные с помощью языков программирования, обладают высокой совместимостью с кастомными приложениями, а также могут отображать все необходимые исследователю данные, однако при этом обладают ограниченным функционалом.

При подборе средств визуализации геоданных следует учитывать данные ограничения, чтобы найти необходимый компромисс между возможностью встраивания, функциональностью и кастомизацией.

Подход

Для отображения инцидентов безопасности были опробованы три библиотеки Python для рисования географических карт: cartopy, plotly и folium.

На рис. 1 показана карта, нарисованная с помощью библиотеки cartopy. На визуализации отображено количество пострадавших от фишинговых атак в разных странах. Количественные метрики можно отображать с помощью таких примитивов как цвет, оттенок, размер [4]. На данном графике количество отображается с помощью оттенка цветовой шкалы.

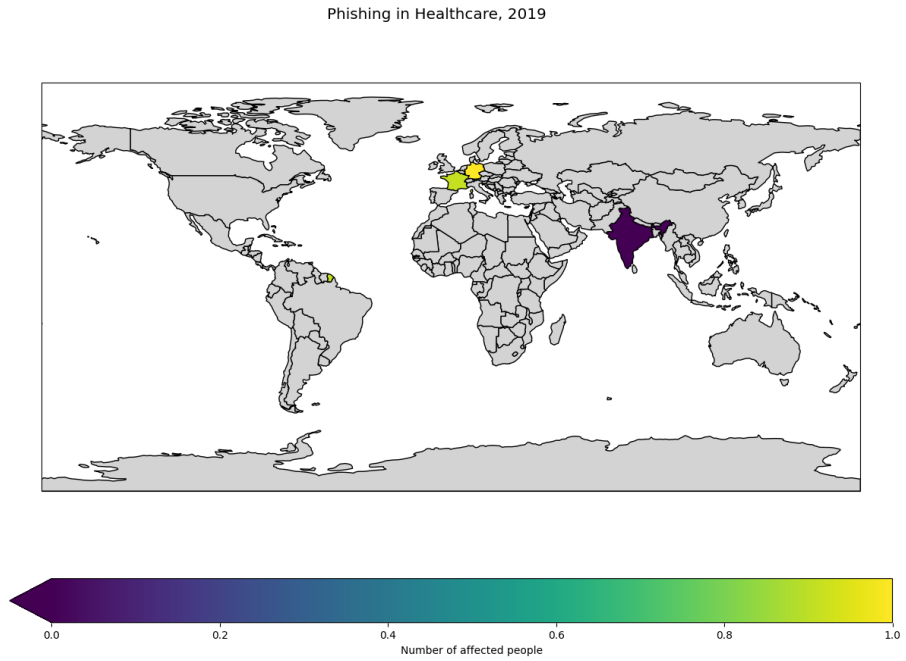


Рис. 1. График количества пострадавших от фишинга в разных странах на основе cartopy

Карта на рисунке выше была улучшена (рис. 2, слева). Территории разных стран были раскрашены в соответствии с количеством проживающих в них людей. При этом, как показано на верхней цветовой шкале, чем темнее оттенок, тем больше население в стране.

Библиотека cartopy предоставляет возможность накладывать дополнительные визуальные объекты поверх географической карты. Это позволило обозначить локации инцидентов безопасности с помощью точек с заданным радиусом. Также была добавлена еще одна цветовая шкала, чтобы оттенками красного показать количество пострадавших от кибератаки.

Однако некоторые точки сливались с раскрашенной картой, поэтому было принято решение сделать карту полупрозрачной (рис. 2, справа). Кроме того, полупрозрачные контуры границ между странами позволили добавить названия населенных пунктов так, чтобы они были хорошо различимы.

Также cartopy позволяет группировать объекты с помощью цвета. На рис. 2 справа цвета точек зависят от группы атаки, а их размер – от количества пострадавших людей.

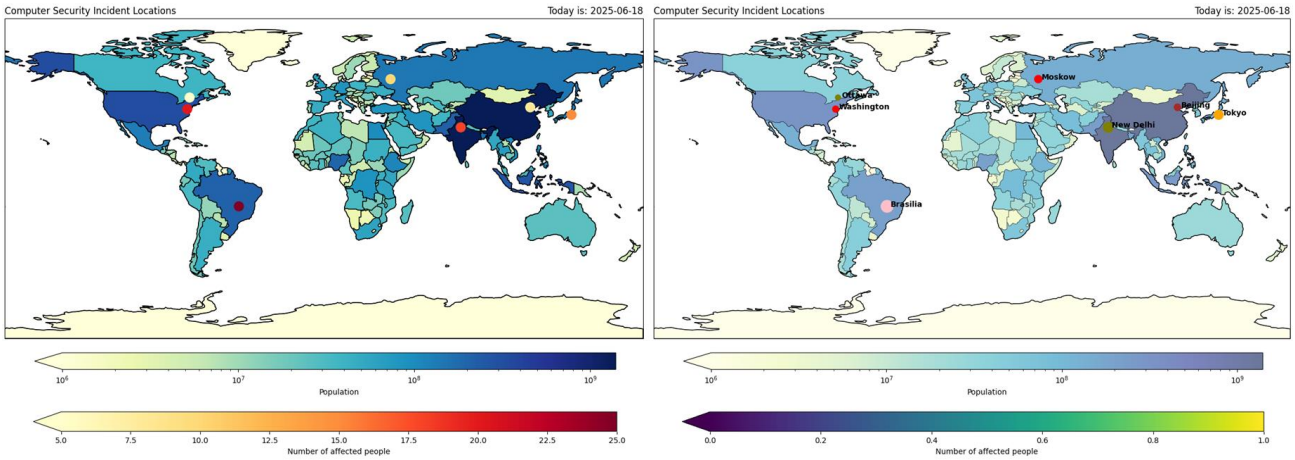


Рис. 2. Отображение геолокации инцидентов безопасности, с прозрачностью и без

На рис. 3 изображена карта, нарисованная с помощью библиотеки plotly.

Рис. 3. Отображение количества пострадавших от разных групп кибератак с помощью библиотеки plotly

При использовании этой библиотеки дополнительная информация также может быть отображена в виде геометрических фигур, размера, цвета, оттенка и прозрачности. Уровень критичности атаки можно показать, используя палитры, доступные для графиков plotly. Уровень критичности атаки показан посредством площади фигуры, при этом фигуры расположены в соответствии с геолокациями инцидентов.

Отличительной особенностью данной визуализации являются интерактивные элементы, такие как вызов дополнительной информации при наведении указателя мыши. На рисунке ниже можно видеть данные о населенном пункте, типе атаки и уровне критичности.

Способ группировки по типу атаки представлен на рис. 4. Данная карта также включает в себя легенду справа, позволяющую оператору сразу увидеть все типы инцидентов, отображенных на карте. Метриками на данной визуализации являются тип атаки, обозначенный цветом, и расположение точек в зависимости от геолокации инцидента.

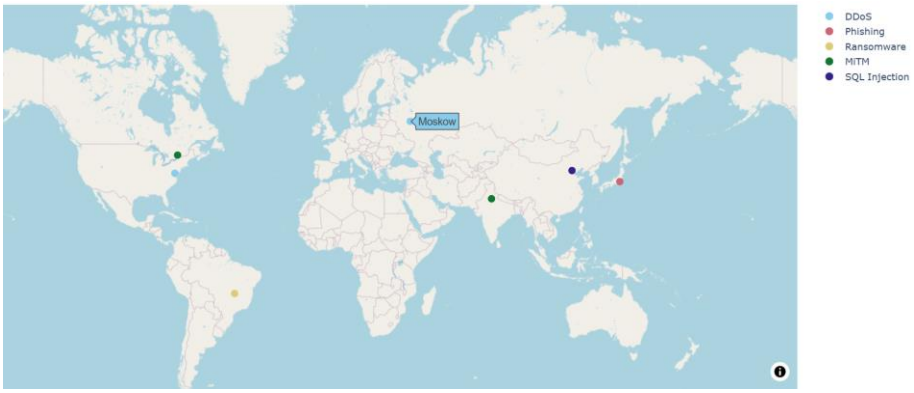


Рис. 4. Группировка инцидентов в зависимости от типа с помощью цвета

Возможный способ отображения геолокации инцидентов безопасности и степени их критичности с помощью тепловых карт представлен на рис. 5.

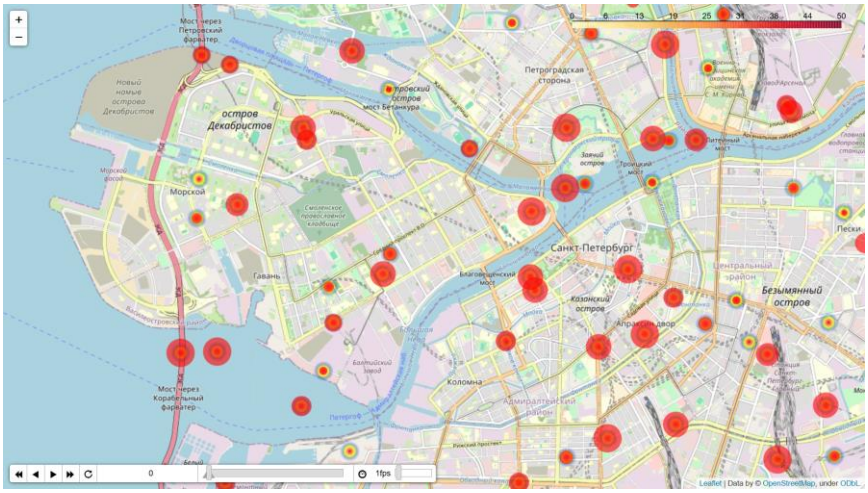


Рис. 5. Пример тепловой карты инцидентов безопасности на основе folium

На визуализации показаны метрики расположения и уровня критичности атаки. Точки на тепловой карте располагаются, исходя из локации, в то время как размер зависит от уровня критичности инцидента. Также добавлены оттенки красного, чтобы обозначить временную метку.

Заключение

В работе представлен обзор программных средств языка Python для создания визуализации данных безопасности на геокартах. Рассмотрены библиотеки folium, cartopy и plotly. Они предоставляют множество средств для отображения данных, связанных с геолокацией, и позволяют добавлять различные графические примитивы, увеличивая количество информации, которую можно отобразить на графике. Полученные результаты позволят более эффективно анализировать данные об инцидентах безопасности, для которых важна геолокация.

В дальнейшем планируется разработка прототипа системы визуализации данных безопасности на геокартах и оценка его эффективности.

Работа выполнена при совместной финансовой поддержке РНФ и СПб НФ (проект 24-21-20058).

Список используемых источников

1. Mansoori M., Welch I. Geolocation tracking and cloaking of malicious web sites //2019 IEEE 44th Conference on Local Computer Networks (LCN) // IEEE, 2019. PP. 274-281.
2. LevelBlue. Viewing Asset Details in LevelBlue USM Appliance. URL: https://cybersecurity.att.com/documentation/usm-appliance/asset-management/viewing-asset-details.htm (дата обращения: 10.06.2025).
3. Carto Documentation. Google Earth Engine. URL: https://docs.carto.com/carto-user-manual/workflows/components/google-earth-engine (дата обращения: 10.06.2025).
4. Котенко И. В., Коломеец М. В., Жернова К. Н., Чечулин А. А. Визуальная аналитика для информационной безопасности: области применения, задачи и модели визуализации //Вопросы кибербезопасности. 2021. № 4 (44). С. 2-15.

VISUALIZATION OF SECURITY DATA ON GEOGRAPHICAL MAPS USING PYTHON PROGRAMMING LANGUAGE

Zhernova K.
St. Petersburg Federal Research Center of the Russian Academy of Sciences

Over time, the variety of cyber threats has been steadily increasing, and some attacks have specific patterns of behavior related to geographical location. Therefore, geolocation of a security incident plays an important role in detecting certain types of cyber attacks. Also, displaying security data on geographical maps can be of invaluable help for digital forensics. The report presents an approach to displaying security data on geographical maps using the Python programming language.

Key words: *data visualization, visual analysis, geodata, information security*

УДК 004.032.26
ГРНТИ 81.93.29

ПОДХОДЫ К ОТБОРУ ПРИЗНАКОВ ДЛЯ ВИЗУАЛИЗАЦИИ ДАННЫХ БЕЗОПАСНОСТИ

К. Н. Жернова

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

По сети постоянно передаются колоссальные объемы информации. Поэтому данные сетевой безопасности могут содержать большое количество метрик. По этой причине для повышения ситуационной осведомленности немаловажно правильно отбирать признаки, необходимые для наиболее эффективного анализа этих данных. Одним из методов анализа данных по-прежнему является визуализация. В докладе представлен комбинированный подход к отбору признаков в данных безопасности для последующей визуализации, чтобы сделать ее более эффективной. Также приведены примеры возможного применения данного подхода.

машинное обучение, нейронные сети, информационная безопасность.

Введение

Нейронные сети способны достаточно быстро обрабатывать большие массивы данных, поэтому часто применяются для задач безопасности, в которых нужно анализировать множество разнообразных метрик. Однако правильный отбор анализируемых метрик может не только сократить обрабатываемое количество информации, но и повысить точность анализа данных нейросетевыми моделями [1, 2].

Визуализация данных безопасности позволяет снизить размерность данных, однако из-за уменьшения метрик данных, содержащихся на визуализации, правильный отбор признаков становится критичным. По этой причине требуется создать комбинированный подход к отбору признаков в данных безопасности, чтобы впоследствии визуализировать именно эти признаки.

Краткий обзор подходов к отбору признаков

Под отбором признаков чаще всего подразумеваются методы на основе машинного обучения. Они подразделяются на две основные категории: (1) встроенные методы и (2) методы-обертки. Примерами встроенных методов может служить применение моделей-классификаторов, таких как логисти-

ческая регрессия (random forest, RF) или случайный лес (logistic regression, LR). Одним из методов-оберток является, например, метод последовательного выбора признаков (sequential forward selection, SFS).

Среди методов, не основанных на машинном обучении, часто применяется расчет линейной корреляции. Ее можно отнести к группе фильтрующих методов.

Подход

На основании предположения о том, что совмещение этих методов может повысить эффективность обучения модели на отобранных признаках, был проведен эксперимент.

Для этого были задействованы следующие библиотеки программного языка Python: sklearn, matplotlib и numpy. Выбор языка Python обоснован его преимуществами, которые состоят в частоте использования, высокой степени интеграции с новыми разрабатываемыми приложениями, а также постоянно разрабатывающимися и улучшающимися библиотеками.

Набор данных представлял собой файл csv с содержащимися в нем размеченными статистическими данными об уязвимости кода, написанного на языке JavaScript [3]. Авторы данного набора исследовали возможность предсказывать наличие уязвимостей в JavaScript-функциях с помощью машинного обучения [4]. В качестве целевого признака выступала бинарная метрика Vuln, говорящая о том, присутствуют ли уязвимости в коде или нет. Вначале был проведен отбор с помощью машинного обучения, с использованием моделей RF и LR. Отобранные признаки и степени их важности для предсказания представлены на рисунке ниже (рис. 1).

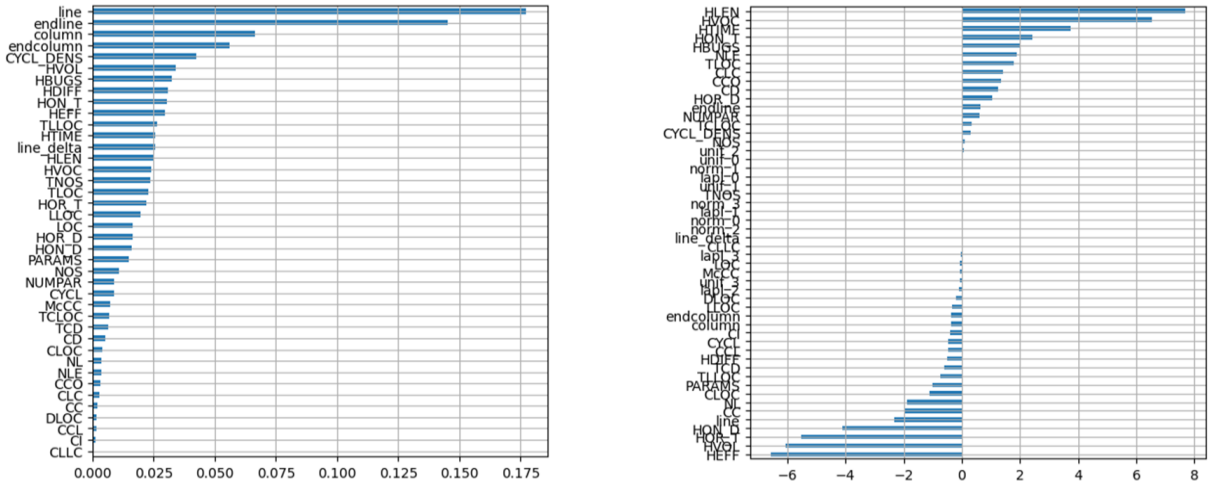


Рис. 1. Результаты отбора признаков с помощью RF (слева) и LR (справа)

Далее к данным применялся метод последовательного выбора признаков на основе алгоритма k ближайших соседей (KNN). Недостатком этого метода является то, что KNN не позволяет рассчитывать коэффициенты важности признаков, однако самой значимой метрикой с точки зрения KNN оказалась HDIFF.

Последним методом для отбора в рамках данного эксперимента служил расчет линейной корреляции с помощью корреляционной матрицы. Визуализация данной матрицы представлена на рис. 2. Как можно видеть, наиболее коррелирующими с наличием уязвимостей признаками оказались endcolumn, column, а также line и endline с наиболее сильной отрицательной корреляцией.

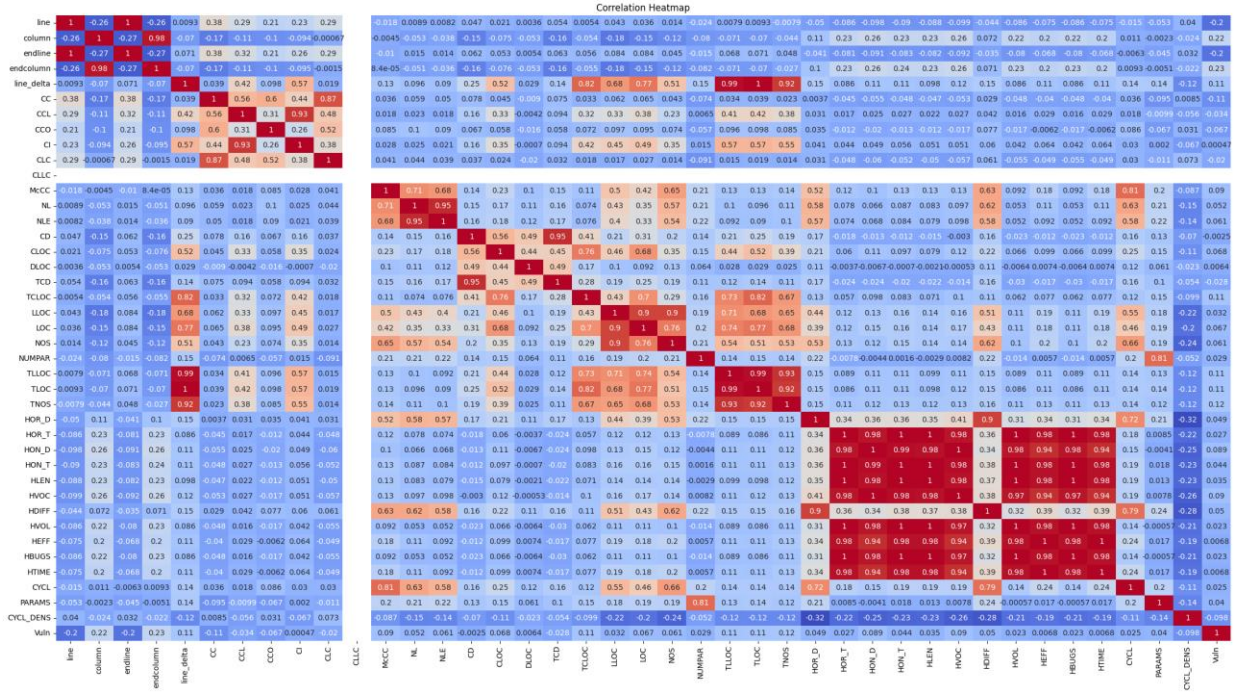


Рис. 2. Результаты отбора признаков с помощью матрицы корреляции

На основе результатов отбора для визуализации и последующего обучения нейросетевой модели были выбраны следующие признаки:

– line (по результатам RF и корреляционной матрицы);
– HDIFF (по результатам KNN);
– HLEN (по результатам LR).

Также рассматривался признак HTIME, который получил поддержку и от LR, и от RF, но был далеко не первым в списке. При этом важно понимать, что признак line так или иначе поддерживали все алгоритмы, так как при проверке с помощью KNN он оказался в первой десятке признаков.

Результаты

Отобранные признаки (line, HDIFF, HLEN и HTIME) были визуализированы на графиках рассеяния. На рис. 3 представлен пример из нескольких случайных графиков для признака line.

Затем сгенерированные изображения были поданы на вход модели сверточной нейронной сети (CNN) для обучения. Графики, основанные на признаках line и HDIFF, показали высокие значения метрик эффективности модели при валидации, в то время как значения для признака HLEN, отобранного алгоритмом LR как наиболее значимого, оказались существенно ниже. Это может объясняться тем, что логистическая регрессия не подходит для случаев, когда зависимость между признаками нелинейная.

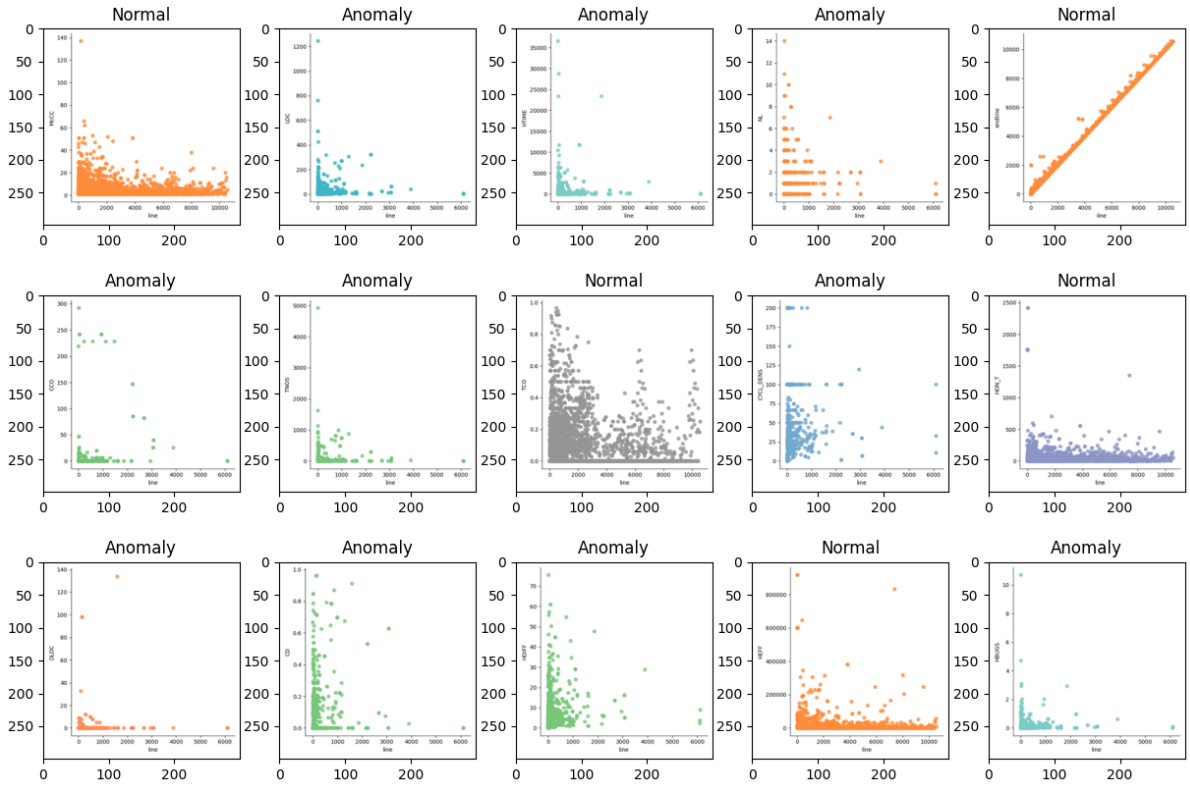


Рис. 3. Графики рассеяния на основе признака line

В то же время обучение на основе признака HTIME дало неожиданно высокий результат, превосходящий все остальные. Это позволяет сделать вывод о том, что комбинированный подход требует более детального рассмотрения, несмотря на эффективность.

Числовые значения показаны в таблице 1.

ТАБЛИЦА 1. Значения показателей эффективности модели в зависимости от признака

Отобранный признак	Аккуратность, %	Точность, %	Полнота, %	F1-мера, %
line	99,4444	100,0	100,0	100,0
HDIFF	96,4444	100,0	100,0	100,0
HLEN	62,6389	84,0909	75,0	74,2063
HTIME	100,0	100,0	100,0	100,0

Заключение

В работе представлен краткий обзор методов отбора признаков для создания визуализации данных безопасности на основе этих признаков. Полученные визуализации могут быть проанализированы с помощью нейронных сетей (например, CNN). Рассмотрены алгоритмы LR, RF, KNN и расчет линейной корреляции. Полученные результаты позволят более эффективно подбирать признаки для визуализации с целью обучения нейронных сетей.

В дальнейшем планируется более детальное изучение эффективности методов отбора признаков.

Работа выполнена при совместной финансовой поддержке РНФ и СПб НФ (проект 24-21-20058).

Список используемых источников

1. Deore M. et al. GRASE: Granulometry Analysis with Semi Eager Classifier to Detect Malware //International Journal of Interactive Multimedia and Artificial Intelligence. 2024. Vol. 8. №. 6. PP. 120-134.

2. Funde S., Swain G. Big data privacy and security using abundant data recovery techniques and data obliviousness methodologies //IEEE Access. 2022. Vol. 10. PP. 105458-105484.

3. Ferenc R., Hegedűs P., Gyimesi P., Antal G., Bán D., Gyimóthy T. Challenging machine learning algorithms in predicting vulnerable javascript functions //2019 IEEE/ACM 7th International workshop on realizing artificial intelligence synergies in software engineering (RAISE). IEEE, 2019. PP. 8-14.

4. Ferenc R., Hegedűs P., Gyimesi P., Antal G., Bán D., Gyimóthy T. JavaScript Vulnerability DataSet. URL: http://www.inf.u-szeged.hu/~ferenc/papers/JSVulnerabilityDataSet/ (дата обращения 07.03.2025).

APPROACHES TO FEATURE SELECTION FOR SECURITY DATA VISUALIZATION

Zhernova K.
St. Petersburg Federal Research Center of the Russian Academy of Sciences

Huge amounts of information are constantly being transmitted over the network. Therefore, network security data may contain a large number of metrics. For this reason, in order to increase situational awareness, it is important to correctly select the features necessary for the most effective analysis of this data. Visualization is still one of the methods of data analysis. The report presents a combined approach to selecting features in security data for subsequent visualization to make it more effective. Examples of possible applications of this approach are also given.

Key words: *machine learning, neural networks, information security*

УДК 004.056.5
ГРНТИ 81.93.2

ОПРЕДЕЛЕНИЕ КЛАССА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА ОСНОВЕ КРИТЕРИЯ МИНИМУМА СРЕДНЕГО РИСКА

И. А. Зикратов

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

Предложен метод к определению класса защищенности ресурсов автоматизированных систем управления технологическими процессами, основанный на вероятностной оценке степени возможного ущерба и уровня значимости (критичности) обрабатываемой в ней информации. В качестве метода решения задачи использован критерий минимума среднего риска, известный в статистической теории принятия решений. Метод может быть использован специалистами по кибербезопасности организаций при проектировании системы защиты информации в автоматизированных системах управления.

информационная безопасность, автоматизированные системы управления технологическими процессами, оценка угроз, степень возможного ущерба, критерий минимума среднего риска

Проблема обеспечения информационной безопасности (ИБ) стоит в ряду первостепенных задач при проектировании автоматизированных систем управления технологическими процессами (АСУ ТП).

В настоящее время существуют различные системы защиты информации (СЗИ) для АСУ ТП, разработка и применение которых реализовывается в рамках существующей нормативно-правовой базы. Одной из задач, решаемых разработчиками СЗИ на этапе аудита АСУ ТП, является задача определения класса защищенности автоматизированной системы управления [1]. Далее, на основе требований, предъявляемых СЗИ для АСУ ТП данного класса, анализа модели угроз, оценки уязвимостей, модели нарушителя, определяются требования к СЗИ, обеспечивающей требуемый уровень защищенности информации. Для решения этой задачи имеются различные подходы и методы [2-5].

Устанавливаются три класса защищенности автоматизированной системы управления. Самый низкий класс (К3) – третий, самый высокий – первый (К1). Класс защищенности автоматизированной системы управления

определяется в зависимости от уровня значимости (УЗ) (критичности) обрабатываемой в ней информации, значение которой, однозначно определяется степенью возможного ущерба (ВУ) от нарушения ее целостности, доступности или конфиденциальности. Степень возможного ущерба определяется заказчиком или оператором экспертным или иным методом и может быть высокой, средней или низкой [1]. Таким образом, класс защищенности имеет строгую зависимость от УЗ, которая в свою очередь определяется степенью ВУ. Степень ВУ можно представить как функцию $F(x)$ от свойств безопасности x. Тогда соответствие классов защищенности уровням УЗ и ВУ можно записать в виде таблицы:

ТАБЛИЦА 1. Соответствие класса защищенности от атрибутов

Класс защищенности	Уровень значимости	Степень ущерба $F(x)$	Свойство безопасности
К1	Высокий	f_1 – высокая	$\exists x,$ при котором $F(x) \to f_1$
К2	Средний	f_2 – средняя	$\exists x,$ при котором $F(x) \to f_2$
К2	Низкий	f_3 – низкая	$\forall x,\ F(x) \to f_3$

Очевидно, что недостаточно обоснованная оценка степени ВУ может привести либо к ущербу, возникшему в результате преодоления недостаточной СЗИ, либо к излишним затратам, возникающим при построении избыточной СЗИ.

Таким образом, задача состоит в том, чтобы на основе имеющихся в распоряжении сведений о факторах, влияющих на величину возможного ущерба, обоснованно определить его уровень, и, соответственно, класс защищенности АСУ ТП.

Решение поставленной задачи может быть основано на интеллектуальных методах анализа данных, одним из распространенных является байесовский подход, который предоставляет ряд преимуществ:

– возможность получения апостериорной оценки вероятности инцидента;
– возможность отслеживания поступления новых данных;
– выявление зависимость между факторами, влияющими на ИБ;

– логическое объяснение своих выводов, физическая интерпретация и изменение структуры отношений между значениями задачи.

Привлекательность байесовского подхода состоит в том, что имеющаяся в распоряжении экспертов информация может не отвечать требованиям представительности статистической выборки, что делает использование многих традиционных частотных подходов неправомерным. Более того, ситуация, в которой принимается решение, может быть вообще новой и никогда ранее не анализируемой. Эти особенности усложняют процесс принятия решений и могут поставить под сомнение какие-либо выводы и заключения. В этом случае байесовский подход, и основанный на нем критерий минимума среднего риска, могут оказаться весьма полезными и эффективным для количественной оценки степени ВУ.

Согласно этому критерию, задачу можно описать следующим образом [6]:

1. Если классификатор причисляет объект *r* к классу C_j, ($j = \overline{1,T}$, где T – количество классов), когда на самом деле он принадлежит классу C_i, то классификатор несет потери L_{ij}.

2. Если для объекта вычислить математические ожидания таких потерь (условные средние риски):

$$f_j = \sum_{i=1}^{T} L_{ij} P(H_i) p(r/H_i), \quad (1)$$

где H_i – гипотезы о принадлежности объекта к классу C_i, $P(H_i)$ – вероятность класса, $p(r/H_i)$ – условная вероятность принадлежности атрибутов объекта *r* к классу C_i, тогда объект будет причислен к тому классу, средний риск для которого минимальный. Очевидно, что вероятности классов должны образовывать полную группу событий.

Рассмотрим реализацию предложенного критерия применительно к нашей задаче на тривиальном примере.

Пусть необходимо определить класс АСУ ТП некоторого предприятия. При этом из общей статистики организаций, занимающейся аналогичной деятельностью, известно, что 50 % АСУ относятся к классу К3, 30 % к классу К2 и 20 % – К3. Тогда $P(H_1) = 0{,}2$, $P(H_2) = 0{,}3$, $P(H_3) = 0{,}5$. Известно, что реализация некоторой угрозы *Y* может привести к нарушению конфиденциальности и целостности информации, обрабатываемой в АСУ ТП. При этом нарушение конфиденциальности приводило в 45 % случаев к низкой степени ущерба, в 23 % случаев к средней степени, и в 15 % – к высокой. Нарушение целостности, имевшее место при реализации угрозы *Y*,

приводило к низкой, средней и высокой степени ущерба соответственно в 25 %, 24 % и 28 % случаев. На основе этих данных составим таблицу:

ТАБЛИЦА 2. Исходные данные

	i	1	2	3
Вероятность класса	$P(H_i)$	0,2	0,3	0,5
Нарушение конфиденциальности	$P(r_1/H_i)$	0,15	0,23	0,45
Нарушение целостности	$P(r_2/H_i)$	0,25	0,24	0,28

Очевидно, что ошибочное определение класса защищенности приводит к ущербу. При этом возможны следующие варианты потерь:

1. В случае, если класс защищенности занижен, и, следовательно, СЗИ не соответствует уровню угроз, организация может понести потери, связанные с реализацией угрозы нарушения информационной безопасности.

2. В противном случае, при завышенном классе защищенности АСУ ТП, организация несет потери, связанные с построением избыточно дорогой СЗИ.

Исходя из этих соображений, зададимся уровнем потерь в формуле (1).

Если классификатор верно определил класс защищенности, то потери отсутствуют, т.е. $L_{11} = L_{22} = L_{33} = 0$.

Если класс защищенности ошибочно определен, как менее высокий (вариант 1), то величину потерь зададим: $L_{12} = L_{23} = 50, L_{13} = 100$.

Если класс защищенности ошибочно определен, как более высокий (вариант 2), то $L_{21} = L_{32} = 5, L_{31} = 10$.

В процессе сбора фактов вероятности гипотез будут повышаться, если факты поддерживают их, и понижаться в противном случае. Предположим, мы получили одно свидетельство – в результате реализации угрозы *Y* произошло нарушение конфиденциальности информации. Тогда, согласно выражению (1), средний риск отнесения объекта *r* к классу 1 будет равен:

$$f_1 = L_{11}P(H_1)p(r_1/H_1) + L_{21}P(H_2)p(r_1/H_2) + L_{31}P(H_3)p(r_1/H_3) = 2{,}595.$$

Аналогично средний риск отнесения объекта к классу 2:

$$f_2 = L_{12}P(H_1)p(r_1/H_1) + L_{22}P(H_2)p(r_1/H_2) + L_{32}P(H_3)p(r_1/H_3) = 2{,}625,$$

и, соответственно, к классу 3:

$$f_3 = L_{13}P(H_1)p(r_1/H_1) + L_{23}P(H_2)p(r_1/H_2) + L_{33}P(H_3)p(r_1/H_3) = 6{,}45.$$

Анализ вычислений показал, что при заданных исходных средний риск принимает минимальное значение для гипотезы H_1. Т.е. с наибольшей вероятностью степень возможного ущерба оценивается как высокая. В таком случае, согласно методике ФСТЭК [1], АСУ ТП должна иметь класс защищенности К1.

Предположим, что через какое-то время получено еще одно свидетельство по факту нарушения целостности информации. Тогда для гипотезы H_1:

$$f_1 = L_{11}P(H_1)p(r_1/H_1)p(r_2/H_1) + L_{21}P(H_2)p(r_1/H_2)p(r_2/H_2) + L_{31}P(H_3)p(r_1/H_3)p(r_2/H_3) = 0{,}69.$$

Аналогично средний риск отнесения объекта к классу 2:

$$f_2 = L_{12}P(H_1)p(r_1/H_1)p(r_2/H_1) + L_{22}P(H_2)p(r_1/H_2)p(r_2/H_2) + L_{32}P(H_3)p(r_1/H_3)p(r_2/H_3) = 0{,}678,$$

и, соответственно, к классу 3:

$$f_3 = L_{13}P(H_1)p(r_1/H_1)p(r_2/H_1) + L_{23}P(H_2)p(r_1/H_2)p(r_2/H_2) + L_{33}P(H_3)p(r_1/H_3)p(r_2/H_3) = 1{,}58.$$

Из расчетов видно, что величины средних рисков изменились. Теперь минимальный средний риск соответствует гипотезе H_2.

Заключение

Таким образом, задаваясь величиной потерь L_{ij}, априорными вероятностями гипотез и наблюдая значения атрибутов классифицируемого объекта, и используя для этого критерий минимума среднего риска, можно обоснованно определять степень возможного ущерба для АСУ ТП. Дальнейшие действия при выборе класса защищенности однозначно определены таблицей 1 в соответствии с методикой ФСТЭК [1].

Список используемых источников

1. Приказ ФСТЭК РФ от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах».

2. Гвоздев А. В., Зикратов И. А., Лебедев И. С., Лапшин С. В., Соловьев И. Н. Прогнозная оценка защищенности архитектур программного обеспечения // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 4 (80). С. 126-130.

3. Зикратов И. А., Одегов С. В. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. 2012. № 4 (80). С. 121-126.

4. Сухопаров М. Е., Соловьев И. Н., Лебедев И. С., Комаров И. И. Методика анализа архитектуры систем защиты информации на основе типовых элементов // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 3 (85). С. 151-154.

5. Клишин Д. В., Чечулин А. А. Анализ методов оценки правильности реализации информационной безопасности // В книге: Региональная информатика (РИ-2024). Материалы XIX Санкт-Петербургской международной конференции. Санкт-Петербург, 2024. С. 114-115

6. Зикратова Т. В. Метод группового управления в мультиагентных робототехнических системах в условиях воздействия дестабилизирующих факторов // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 92-100. DOI:10.31854/1813-324X-2021-7-3-92-100

DETERMINING THE SECURITY CLASS OF AN AUTOMATED PROCESS CONTROL SYSTEM BASED ON THE MINIMUM AVERAGE RISK CRITERION

Zikratov I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

A method for determining the security class of resources in automated process control systems is proposed, based on a probabilistic assessment of the degree of possible damage and the level of significance (criticality) of the information processed in it. The criterion of minimum average risk, known in the statistical theory of decision making, is used as a method for solving the problem. The method can be used by cybersecurity specialists in organizations when designing an information security system in automated control systems.

Key words: *information security, automated process control systems, threat assessment, degree of possible damage, minimum average risk criterion*

УДК 004.8
ГРНТИ 20.51.19

АНАЛИЗ ВЗАИМОДЕЙСТВИЯ МЕЖДУ БЛОКАМИ В КОНТЕКСТЕ ОПРЕДЕЛЕНИЯ УГРОЗ ДЛЯ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

И. В. Ковальский, В. Б. Сычужников, М. А. Уралов

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

В статье рассматриваются современные угрозы кибербезопасности в контексте автономных и подключенных транспортных средств. Особое внимание уделено архитектуре взаимодействия между функциональными блоками беспилотного автомобиля, включая сенсоры, центральный блок управления, системы управления двигателем, питания, защиты и информационно-развлекательные комплексы. Проанализированы методы кибератак на ключевые компоненты транспортного средства, такие как радар FMCW, лидар, ультразвуковые датчики, камеры, GPS, TPMS, а также коммуникационные шины (CAN, LIN, FlexRay, Ethernet) и протоколы V2X. Выделены типы атак – от DoS и подмены данных до физического доступа через OBD и удаленных атак через FOTA.

автономные транспортные средства, кибербезопасность, кибератаки, сенсорные системы, CAN-шина, DoS-атака, подмена данных

Взаимодействие между блоками в бесплотном автомобиле может быть организовано с помощью специального программного обеспечения, которое обеспечивает обмен данными между различными компонентами [1]. Цепочка взаимодействия (рис. 1) может выглядеть следующим образом:

1. Сенсоры обнаруживают окружающую среду и отправляют данные в центральный блок управления.

2. Центральный блок управления обрабатывает данные и принимает решения о дальнейших действиях.

3. Если требуется, центральный блок управления отправляет команды другим блокам, чтобы они выполнили необходимые действия, например, увеличили или уменьшили скорость, повернули налево или направо.

4. Блок управления двигателем получает команды от центрального блока управления и заставляет двигатель работать соответственно этим командам.

5. Блок питания следит за зарядом батарей и отправляет данные в центральный блок управления, чтобы он мог принимать решения о необходимости замены или перезарядки батарей.

6. Блок защиты обеспечивает защиту от угроз безопасности, таких как взлом, вирусы, атаки злоумышленников и т.д.

7. Блок информационно-развлекательной системы (ИРС) обеспечивает взаимодействие с пассажирами и предоставляет им информацию о поездке, возможностях развлечений и т.д.

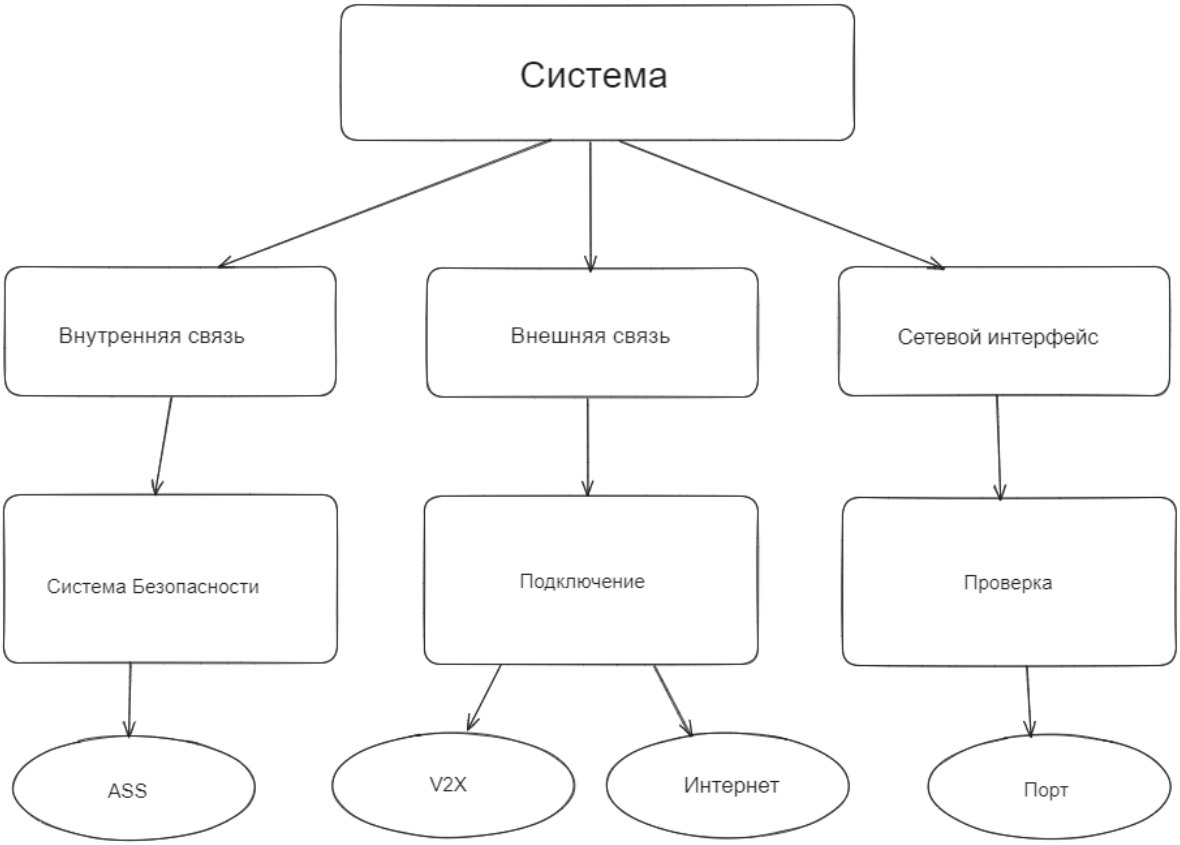


Рис. 1. Таксономия методов атак на автономные транспортные средства

ASS предназначены для предотвращения аварий путем оказания поддержки водителю.

Радар FMCW представляет собой особый тип радиолокационных датчиков, который излучает непрерывные частотно модулированные волны – Spoofing of radar.

Датчик скорости вращения колеса ABS – злоумышленники могут отключить магнитное поле ABS, поместив электромагнитный привод между датчиком скорости вращения колеса ABS (WSS), который прерывает вывод

датчика скорости колеса, что может привести к неправильному поведению всей ABS.

TPMS – это электронная система, предназначенная для контроля давления воздуха внутри пневматических шин – эта атака позволяет злоумышленнику узнать местоположение транспортного средства, и они могут подделать показания давления, после чего водитель может остановить транспортное средство для проверки давления, что может привести к физическим атакам или ограблению [2].

GPS – манипулирование координатами – такая подмена позволяет злоумышленнику манипулировать маршрутом пользователя, подставляя ложное местоположение в навигационной системе. Множество функций в автомобиле подключены к глобальной системе позиционирования (GPS). Как только доступ к GPS скомпрометирован, для злоумышленников становится проще осуществить атаку на прочие системы, зависящие от GPS в транспортном средстве.

Лидар – атака, инициируемая злоумышленниками, заключается в излучении света с длиной волны, идентичной длине волн лидарных импульсов. Это вызывает дисфункцию лидарных систем, влияя на их способность достоверно передавать сигналы для транспортного средства.

Ультразвуковой датчик, инструмент парковочной системы, подвергается уязвимостям при атаках через ее слепые зоны. Не способен детектировать узкие объекты, что позволяет преступникам использовать эти промежутки для проведения незаметных действий при маневрах с задним ходом. В контексте атак с использованием интерференций, агрессоры могут внедрять внешние ультразвуковые датчики, направленные на нарушение функционала оригинального ультразвукового датчика транспортного средства.

Камера – преступники применяют интенсивные осветительные устройства для выведения из строя камер, при постоянном воздействии, это может вызвать внезапную остановку системы.

Коммуникационный канал – Distributed Denial of Service (DDoS) атаки на интернет-подключенные машины. Этот сценарий разворачивается, когда злоумышленник перегружает канал передачи данных, создавая шум или интерференцию. Злоумышленник целенаправленно транслирует большой объем беспорядочных данных в сеть, вызывая таким образом перегрузку, что влечет за собой задержки в передаче данных, удлинение времени ответа системы и, в некоторых случаях, неспособность доставки сообщений их получателям [3].

На уровне сети или транспорта происходит передача водителю недостоверных данных и безопасностных предупреждений, способных вызвать потенциально опасные сценарии.

Протоколы маршрутизации подвержены угрозам, вызванным недостатками в их безопасности. Атака типа "серая дыра" позволяет агрессорам манипулировать трафиком, пропуская или блокируя данные по своему усмотрению, что затрудняет ее выявление.

Сеть контроллера области сети (CAN) предоставляет потенциал для двух основных категорий взлома автомобиля: физического доступа и удаленной атаки. К элементам авто, особо подверженным риску при физическом доступе, относятся интерфейсы для подключения к бортовой диагностике (OBD), тогда как удаленные атаки чаще всего направлены на системы бесключевого доступа и телематические устройства. Осуществление таких атак возможно через использование стандартов передачи данных в автомобиле, включая CAN, Ethernet и FlexRay, в силу их недостатка в механизмах аутентификации данных и шифровании информации [4].

Ethernet-атаки CAM нацелены на компрометацию таблицы MAC-адресов в автомобильных системах доступа к мультимедиа. Атакующие генерируют и отправляют в сеть множество пакетов с различными MAC-адресами, чтобы исчерпать возможности целевого устройства по регистрации новых адресов.

LIN (Local Interconnect Network) – это последовательная коммуникационная система, предназначенная для взаимодействия между элементами автомобильных систем. Атакующие могут подделывать фреймы данных в этом протоколе, нарушая функционирование зависимых устройств, что вызывает их некорректную работу.

FlexRay представляет собой протокол высокоскоростной связи, предназначенный для автотранспортных средств. Атакующий может создавать серии доминирующих сигналов на этой коммуникационной линии, вызывая тем самым обрыв связи в ходе атаки типа «отказ в обслуживании» (DoS). Для осуществления подобного нарушения, преступник должен корректировать значение PIN-кода на передающем устройстве в меньшую сторону. В стратегии, нацеленной DoS-атаки, осуществляется либо блокировка узла для отправки информации к заданной цели, либо сделать данные недоступными для ее выполнения.

Схемы воздействия на систему управления автономного транспортного средства представлены в таблице 1.

ТАБЛИЦА 1. Схемы воздействия на систему управления автономного транспортного средства

Классификация	Подсистемы	Системы	Атаки
Система безопасности	ASS	Радар FMCW	Имитация сигналов радара, Маскировка под сигналы радара
		Датчик скорости вращения колеса в системе антиблокировки (ABS).	Атака, нарушающая работу, и атака на подделку идентичности
		TPMS	Sniffing attack Атака с перехватом данных
		GPS	Маскировка геолокации
		Лидар	DoS attack
		Ультразвуковой датчик	Sensor interference attacks, Атаки на сенсорные помехи
		Камера	Атака слепоты, также известная как фантомная атака, является методом нарушения безопасности.
Подключение	V2X	Канал связи	DoS attack, sybil attack
		Протоколы сетевого или транспортного слоя	data falsification attack
		Протоколы маршрутизации	grey hole attack
	Интернет	CAN bus	frame falsifying attack
		Ethernet	CAM attack
		LIN bus	False frame attack
		FlexRay	Full and target DoS attack
Проверка	Порт OBD	CAN bus	packet capture, packet insertion
	FOTA	Внедренное ПО	Control override attacks , Spoofing attack

Для защиты от атак на канал управления, одним из важных мер предосторожности является использование надежных криптографических алгоритмов, сильных паролей, многоуровневой аутентификации, проверки це-

лостности и аутентичности данных, а также обновления программного обеспечения. Также необходимо проводить регулярные тестирования на безопасность и обеспечить обучение персонала и пользователей правильному использованию автомобилей.

Однако встроенные электронные компоненты несут в себе риски безопасности, что делает их целью для хакеров, желающих проникнуть в автомобильные системы. В данной статье рассматриваются различные методы кибератак на современные автомобили, включая те, что обладают автономностью и подключены к сети. Анализ угроз выделяет четыре основные области атак в автомобиле: сетевые интерфейсы, внутренние сети, внешние связи и электронные управляющие системы. Данное исследование помогает выявить текущие уязвимости и атаки, что, в свою очередь, способствует разработке всесторонних мер защиты от подобных угроз.

Список используемых источников

1. Wang D., Wang C., Wang Y., Wang H., and Pei F. An autonomous driving approach based on trajectory learning using deep neural networks // Int. J. Automot. Technol. 2021. Vol. 22. № 6. PP. 1517–1528.

2. Wang T., Guan Z., Peng T., Li D., and Zhao R. Human-like decision making for autonomous lane changing using deep learning // in Proc. IEEE 2nd Int. Conf. Inf. Technol., Big Data Artif. Intell. (ICIBA) 2021. Vol. 2. PP. 950–955.

3. Zhang W. and Wang W. Learning V2V interactive driving patterns at signalized intersections // Transp. Res. C, Emerg. Technol. 2019. Vol. 108. PP. 151–166.

4. Ye F., Zhang S., Wang P., and Chan C.-Y. A survey of deep reinforcement learning algorithms for motion planning and control of autonomous vehicles // in Proc. IEEE Intell. Vehicles Symp. (IV), Nagoya, Japan, Jul. 2021. PP. 1073–1080. DOI: 10.1109/IV48863.2021.9575880.

ANALYZING THE INTERACTION BETWEEN BLOCKS IN THE CONTEXT OF IDENTIFYING THREATS TO AUTONOMOUS VEHICLES

Kovalsky I., Sychuzhnikov V., Uralov M.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article examines modern cybersecurity threats in the context of autonomous and connected vehicles. Special attention is paid to the architecture of interaction between the functional units of an unmanned vehicle, including sensors, a central control unit, engine control systems, power supply, protection and infotainment complexes. Methods of cyber-attacks on key vehicle components such as FMCW radar, lidar, ultrasonic sensors, cameras, GPS, TPMS, as well as communication buses (CAN, LIN, FlexRay, Ethernet) and V2X protocols are analyzed. The types of attacks are highlighted, from DoS and data substitution to physical access via OBD and remote attacks via FOTA.

Key words: *autonomous vehicles, cybersecurity, cyber-attacks, sensor systems, CAN bus, DoS attack, data substitution.*

УДК 004.8
ГРНТИ 20.51.19

АНАЛИЗ ПОДХОДОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ БЕСПИЛОТНОГО ТРАНСПОРТА

И. В. Ковальский, В. Б. Сычужников, М. А. Уралов

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

В условиях стремительного развития автономных транспортных средств и их интеграции с облачными вычислительными ресурсами обеспечение защиты информации становится критически важной задачей. Данные, генерируемые и хранимые в таких системах – от телеметрии и сигналов датчиков до системных логов – представляют собой ценные активы, требующие надежной защиты от несанкционированного доступа, утечек и потерь. В данной работе рассматриваются ключевые аспекты информационной безопасности, включая шифрование данных с использованием современных криптографических методов, таких как AES, управление криптографическими ключами, контроль доступа на основе аутентификации и авторизации, а также стратегии резервного копирования и восстановления данных. Особое внимание уделяется применению аппаратных модулей безопасности (HSM) и доверенных исполнительных сред (TEE) для защиты ключей, а также использованию ролевой модели доступа (RBAC) для эффективного управления правами.

защита информации, автономные транспортные средства, шифрование данных, AES, управление ключами, контроль доступа, аутентификация

Защита информации, сохраняемой в системах хранения данных автономных транспортных средств и облачных вычислительных ресурсах, играет ключевую роль в обеспечении информационной безопасности. Всякие данные, собранные или созданные автономным транспортным средством, могут быть представлены как ценный актив. Без адекватных мер защиты эта информация может легко стать объектом несанкционированного доступа со стороны киберпреступников. Для обеспечения конфиденциальности, целостности и доступности этой информации используются разнообразные технологии шифрования данных, являющиеся основой для обеспечения ее безопасности [1].

Криптография преобразует информацию в код, делая ее нечитаемой без соответствующего дешифровки ключа. AES, или Расширенный Стандарт Шифрования, является одним из самых эффективных методов защиты данных, сравнимый с высокозащищенным сейфом, разгадать который без уни-

кального ключа крайне сложно. Возможность применения AES в различных конфигурациях позволяет повысить уровень безопасности. При этом важно учитывать контекст использования шифрования. В автомобилях информация может шифроваться на различных устройствах хранения данных, таких как жесткие диски, SSD или USB-накопители, включая данные о передвижениях, сигналы с датчиков и системные логи. При обмене данными с облачными сервисами для целей аналитики или хранения, шифрование необходимо как на этапе передачи данных, так и при их хранении в облаке, обеспечивая их защиту на всех этапах работы с информацией [2].

Шифрование, хотя и критично важно, представляет собой только часть целой системы безопасности. Охрана ключей, необходимых для кодирования и раскодирования информации, становится вторым неотъемлемым элементом. Управление ключами по своей сути аналогично обеспечению безопасности ключей от всех ваших сейфов. Мало иметь защищенные сейфы; критически важно также обеспечивать безопасное хранение самих ключей и четко определять круг лиц, имеющих к ним доступ [3]. При этом ключи следует генерировать в случайном порядке и обеспечивать их хранение в надежных устройствах, таких как аппаратные модули безопасности (HSM) или доверенные исполнительные среды (TEE), что гарантирует высочайший уровень защиты чувствительных данных благодаря использованию специализированных защитных чипов. Эффективность системы безопасности также предполагает регулярное обновление ключей, аналогично изменению паролей, для минимизации рисков их возможной компрометации [4].

Контроль доступа стоит на втором месте по значимости в системе защиты информации при ее сохранении. Он критичен даже при использовании шифрования, так как централизованно управляет персональными правами на взаимодействие с данными. Эта система безопасности удостоверяется в подлинности каждого запроса на вход, аналогично проверке допуска в хранилище ценностей, и предоставляет доступ только проверенным пользователям. Для функционирования контроля доступа применяются разнообразные техники и методологии. Механизм аутентификации подтверждает идентичность субъекта, стремящегося получить доступ, применяя, к примеру, парольные системы, обработку биометрических данных или использование специальных ключей. После идентификации, процесс авторизации определяет определенный набор допустимых операций для пользователя

или процесса. В частности, использование ролевой модели доступа (RBAC) позволяет эффективно распределять права на основе занимаемых ролей, облегчая управление правами доступа и снижая риск ошибочного предоставления прав. В контексте разработки беспилотных авто, контроль доступа имеет особое значение для ограничения взаимодействия с критически важной информацией на бортовых системах транспортного средства, например, контроль над управлением, а также для защиты данных телеметрии и другой информации, сохраняемой на удаленных серверах.

При всех мерах безопасности, включая качественное шифрование и эффективное управление доступом, риск утраты или нарушения целостности информации остается актуальным. В таком контексте стратегии резервного копирования и восстановления данных играют ключевую роль, выступая в качестве надежного «спасательного круга» при потере ценных данных. Процесс резервирования информации предполагает создание ее дубликатов, которые могут быть использованы для восстановления первоначального состояния данных после их потери или повреждения. Существуют различные методики резервирования, в частности, полное, при котором копируется вся информация, инкрементное, охватывающее только новые изменения по сравнению с последней копией, и дифференциальное, включающее все изменения с момента последнего полного резервирования. Для сохранности данных и удобства их восстановления они могут быть скопированы как на локальные устройства хранения данных, такие как внешние жесткие диски, так и в облачные сервисы для гарантии защиты от физических повреждений носителей и обеспечения непрерывного доступа к данным.

Список используемых источников

1. Dokania S., Hafez A. H. A., Subramanian A., Chandraker M., and C. Jawahar V., IDD-3D: Indian driving dataset for 3D unstructured road scenes // in Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV), India, Jan. 2023. PP. 4471–4480.

2. Chang M.-F., Lambert J., Sangkloy P., Singh J., Bak S., Hartnett A., Wang D., Carr P., Lucey S., Ramanan D., and Hays J. Argoverse: 3D tracking and forecasting with rich maps // in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2019. PP. 8740–8749.

3. Zhou H., Laval J., Zhou A., Wang Y., Wu W., Qing Z., and Peeta S. Review of learning-based longitudinal motion planning for autonomous vehicles: Research gaps between self-driving and traffic congestion // Transp. Res. Rec., J. Transp. Res. Board. 2022. Vol. 2676. № 1. PP. 324–341.

4. Hu X., Chen L., Tang B., Cao D., and He H. Dynamic path planning for autonomous driving on various roads with avoidance of static and moving obstacles // Mech. Syst. Signal Process. 2018. Vol. 100. PP. 482–500.

ANALYSIS OF INFORMATION SECURITY APPROACHES IN THE FIELD OF UNMANNED VEHICLES

Kovalsky I., Sychuzhnikov V., Uralov M.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

With the rapid development of autonomous vehicles and their integration with cloud computing resources, ensuring information security is becoming a critical task. The data generated and stored in such systems, from telemetry and sensor signals to system logs, are valuable assets that require reliable protection against unauthorized access, leaks and losses. This paper examines key aspects of information security, including data encryption using modern cryptographic techniques such as AES, cryptographic key management, authentication and authorization-based access control, and data backup and recovery strategies. Particular attention is paid to the use of hardware security modules (HSM) and trusted execution environments (TEE) to protect keys, as well as the use of a role-based access model (RBAC) for effective rights management.

Key words: *information security, autonomous vehicles, data encryption, AES, key management, access control, authentication*

УДК 654.739
ГРНТИ 49.33.29

ИСПЫТАТЕЛЬНАЯ ЛАБОРАТОРИЯ ВУЗА КАК ПРИМЕР ОТРАСЛЕВОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТУКТУРЫ, ФУНКЦИОНИРУЮЩИЕГО В СФЕРЕ НАУКИ

А. В. Красов

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

В феврале 2025 года были утверждены методические рекомендации по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере науки. Данный документ конкретизировал вопросы категорирования организаций, занимающихся наукой, в том числе вузов. Несмотря на то, что основной вид деятельности вузов – образовательная, отсутствует в перечне 187 ФЗ, но каждый из вузов проводит научно-исследовательские и опытно-констукторские работы. Научные лаборатории, в которых выполняются эти работы, могут являться объектами критической инфраструктуры. Это подтверждаются все большим числом вузов, которые прошли процесс категорирования. В качестве примера возможного объекта была выбрана научная лаборатория по изучению промышленной водородной энергетики.

безопасность критической информационной инфраструктуры, значимый объект критической информационной инфраструктуры, типовые отраслевые объекты критической инфраструктуры, функционирующие в сфере науки

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [1] (далее – 187-ФЗ) регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. В 187-ФЗ определены 12 сфер народного хозяйства, сфера образования в их число не входит, однако наука является неотъемлемой частью системы высшего образования. Если рассматривать параметры ежегодного мониторинга эффективности вузов, то из более 150 отчетных параметров, 16 относятся к показателю по научно-исследовательской деятельности, который является одним из шести основных показателей деятельности вуза. Значительную роль показателей по научной работе играют и показатели конкурса Контрольных цифр приема, особенно для определения числа бюджетных мест аспирантов и магистров организации. Ведущие университеты, рассчитывающие на основное число бюджетных мест, показывают более одного

миллиона рублей на каждого научно-педагогического работника, а это не только сотрудники научных лабораторий, но и весь профессорско-преподавательский состав. Таким образом, объем средств, получаемый от научной деятельности для ведущих вузов, в несколько раз больше, чем субсидия на выполнение государственного задания по основному виду деятельности и оплаты от студентов контрактной формы обучения.

Представляется, что большинство наиболее финансово значимых научных разработок связанны с новыми перспективными направлениями развития науки. Для иллюстрации процесса категорирования научной лаборатории в качестве значимого объекта критической инфраструктуры, был выбрана научная лаборатория по исследованию установки водородной энергетики. Статья не предполагает описание какой-то конкретной лаборатории, выбор специфики деятельности данного гипотетического объекта обусловлен исключительно возможностью показать на примере оценки масштаба последствий реализации угроз информационной безопасности по всем 5-и возможным категориям.

Допустим, что данная гипотетическая лаборатория оснащена экспериментальным стендом, в котором используется мембранная технология, позволяющая получить ограниченный объем чистого водорода, достаточный для оценки эффективности технологии, возможно оценить до 10 литров в час. Сама установка является самостоятельно созданным из подручных материалов не сертифицированным оборудованием, созданным более 10 лет назад, которое имеет компьютеризированную систему управления и обработки экспериментальных данных, но созданную примерно в это же время на основе устаревшей западной компьютерной техники и программного обеспечения. При этом можно допустить, что лаборатория является активным участником крупных НИР и ОКР с государственным финансированием.

До 2025 г. отсутствие четких подзаконных актов для организаций в сфере науки приводило к тому, что подавляющее большинство организаций, несмотря на наличие требований 187-ФЗ, не подавали документы на категорирование, не выполняли требования по обеспечению информационной безопасности значимых объектов. В феврале 2025 г. Министерством науки и высшего образования по согласованию с ФСТЭК России были утверждены «Методические указания по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере науки» [2], данный документ утвердил типовые перечни отраслевых про-

цессов, методики оценки показателей значимости, отраслевой порядок процедуры категорирования и рекомендации по заполнению форм документов.

Как отмечалось выше, вуз должен быть отнесен к субъекту КИИ как минимум в связи с выполнением НИР и ОКР, подтверждением которых есть в регулярной отечности вуза в данных мониторинга результативности научных организаций, мониторинге эффективности вузов. Также в уставных видах деятельности вуза могут быть использованы коды ОКВЭД, относящие организацию к субъектам КИИ. Например: 72.1 – Научные исследования и разработки в области естественных и технических наук, к тематике которого без сомнения относится выбранная для примера гипотетическая лаборатория. Всего в списке приложения № 1 к металлическим указаниям [2] приведено 12 кодов ОКВЭД, к которым можно отнести темы НИР и ОКР вузов большинства, и не только технических вузов [4].

В связи с этим нужно серьезно задуматься о необходимости прохождения процедуры категорирования необходимо всем вузам. В силу краткости статьи, формальные вопросы организации процесса категорирования в ней не рассмотрены, они подробно описаны в [2]. Основное внимание в статье уделено процессу категорирования, оценки возможно ущерба мерам по обеспечению информационной безопасности в соответствии с выбранной категорией.

С учетом этого, первая задача – это рассмотрение возможных действий нарушителей, среди которых могут быть как внешние, так и внутренние нарушители. С учетом того, что выбранный в качестве примера объект подключен общеуниверситетской сети с доступа в интернет без собственных средств межсетевого экранирования и предотвращения вторжений, можно говорить об атаках со стороны внешних нарушителей, среди которых могут быть нарушители с высоким потенциалом, отрыто из научных публикаций сотрудников данной лаборатории, в том числе в зарубежных научных изданиях, имеющих информацию о значимости процессов, структуре лабораторной установки, кадровом обеспечении и др., что позволяет организовать высокоэффективную таргетированную (целевую) атаку, направленную на приучение максимального ущерба, тем более в условиях тотального отсутствия средств информационного противодействия. Способствовать этому без сомнения будут и внутренние нарушители, как правило, работающие на неполных ставках, совмещающих возможности дополнительных заработках преподаванием, отвлекающихся на вопросы оформления статей и публика-

ций, работу с дипломниками, т.е. значительную часть времени оборудование работает бесконтрольно.

Вторая задача – анализ угроз информационной безопасности, который необходимо проводить на основании БДУ ФСТЭК, но основе возможных действий нарушителя. С учетом предложенного выше, гипотетического объекта, возможные угрозы информационной безопасности, которые могут привести к возникновению компьютерных инцидентов, можно представить так:

– компьютерная разведка – получение нарушителем информации о структуре установки, режимах работы, полученным результатам;
– фальсификация результатов изменений, что может спровоцировать неправильные действия оператора;
– формирование команды на работу установки, приводящей к сбою, выбросам в данном случае взрывоопасных веществ в помещение, выходу из строя оборудования.

Следующей задачей является оценка масштаба возможных последствий в результате возникновения компьютерных инцидентов и соотношение их с показателями значимости для каждого показателя. Применительно для организаций науки в приложении № 6, 7 методических указаний [2] приведены отраслевые рекомендации по методам оценки. Применительно к выбранному примеру, можно констатировать (указаны только пункты, для которых последствия применимы):

Социальная значимость:

1. Причинение ущерба жизни и здоровью людей. Однозначно, если инцидент приведет к взрыву выработанного чистого водорода будет иметь серьезные последствия не только для сотрудников данной лаборатории, но и для соседних помещений, в которых проводится плановый учебный процесс. По данным Института комплексной безопасности в строительстве НИУ МГСУ и Центра компетенций НТИ при ИПХФ РАН, взрыв водорода детонирует со скоростью 2820 м/с (это в 7 раз выше, чем у дымного пороха), что может вызвать разрушение перекрытий и стен. Подробное исследование взрывоопасности водорода приведено в [3]. Ущерб может измеряться в десятках человек. Объектом в данном случае будет является системы, обеспечивающие выполнение процессов в лаборатории, работоспособность испытательных стендов.

Политическая значимость:

7. Нарушения условий международного договора …. (далее по тексту) – в том случае, если в данной лаборатории выполняется НИР в рамках международного договора, что с высокой долей вероятности может быть, особенно с учетом высокой вероятности таргетированной (целевой) атаки внешних нарушителей. По данному показателю к объектам будет относиться все перечисленные в [2] отраслевые объекты КИИ.

Экономическая значимость:

8. Возникновения ущерба субъекту КИИ … (далее по тексту) – возможно применимы, в зависимости от объема НИР лаборатории. Объекты аналогично п. 7.

Экологическая значимость:

11. Вредные воздействия на окружающую среду – применимы, так как водород относится к взрывоопасным веществам. Учитываются системы, обеспечивающие выполнение процессов в лаборатории.

Значимость для обеспечения обороны страны, безопасности государства и правопорядка:

13. Снижение показателей государственного оборонного заказа – с высокой вероятностью применимо, в связи со спецификой водородной энергетики. Объекты аналогично п. 7.

Таким образом, категория значимости для подобного объекта будет определяться по всем 5 возможным параметрам, скорее всего она будет не ниже 2-й, что потребует соответствующих требований к системе обеспечения этого значимого объекта.

В соответствии с приказом ФСТЭК РФ от 20.02.2020 №35:

– в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;
– в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;
– в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

Подробно вопросы категорирования рассмотрены в учебно-методическом пособии, выпущенном в СПбГУТ в соавторстве с руководителями управления ФСТЭК России [5].

Список используемых источников

1. Федеральный закон 187 «О безопасности критической информационной инфраструктуры Российской Федерации» утвержден 26 июня 2017 г.
2. Методические указания по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере науки» утвержден 21 февраля 2025 г.
3. Мильман О. О., Федоров В. А., Карпушин А. Г., Лошкарева Е. А. Взрывоопасность водорода при низких давлениях в конденсаторах энергоустановок // Международный научный журнал Альтернативная энергетика и экология. 2013. № 6-1(127). С. 17-22. EDN:QIPUCN
4. Красов А. В., Лансере Н. Н., Фадеев И. И. и др. Типовые офтальмологические информационные системы, являющиеся объектами критической информационной инфраструктуры // Офтальмохирургия. 2022. № S4. С. 85-91. DOI:10.25276/0235-4160-2022-4S-85-91. EDN%CBKURN
5. Шакин Д. Н., Красов А. В., Лансере Н. Н., Фадеев И. И. Категорирование объектов критической информационной инфраструктуры: учебное пособие. СПб., СПбГУТ. 2022. 60 с.

TESTING LABORATORY OF THE UNIVERSITY AS AN EXAMPLE OF AN INDUSTRIAL OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE FUNCTIONING IN THE FIELD OF SCIENCE

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

In February 2025, guidelines were approved for categorizing critical information infrastructure facilities operating in the field of science. This document specified the issues of categorizing organizations engaged in science, including universities. Despite the fact that the main activity of universities is educational, it is not in the list of 187 FZ, but each of the universities conducts research and experimental work. Scientific laboratories in which these works are performed can be objects of critical infrastructure. This is confirmed by an increasing number of universities that have gone through the categorization process. As an example of a possible object, a scientific laboratory for the study of industrial hydrogen energy was chosen.

Key words: *security of critical information infrastructure, significant object of critical information infrastructure, typical industry objects of critical infrastructure operating in the field of science*

УДК 004.056.57
ГРНТИ 81.93.29

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ И СИСТЕМА КОНТРОЛЯ ДОСТУПА В СФЕРЕ УСЛУГ ТЕЛЕПРИСУТСТВИЯ

А. В. Красов, А. В. Панков, И. А. Ушаков

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

В статье рассматриваются теоретические и практические аспекты применения биометрической аутентификации в системах контроля доступа для услуг телеприсутствия. Представлен комплексный анализ существующих методов, их преимуществ и недостатков, а также предложены инновационные решения для повышения эффективности и безопасности систем.

биометрическая аутентификация, телеприсутствие, системы контроля доступа, информационная безопасность, биометрические данные, мультимодальные системы

Телеприсутствие представляет собой передовую технологию, обеспечивающую максимально реалистичное взаимодействие пользователей с удаленными объектами и субъектами через цифровые каналы связи. В условиях растущей цифровизации общества особую актуальность приобретает вопрос обеспечения информационной безопасности таких систем [1].

Теоретические основы биометрической аутентификации.

Биометрическая аутентификация базируется на использовании уникальных биологических характеристик человека. Основные категории биометрических признаков:

1. Статические характеристики, такие, как дактилоскопические данные, геометрия ладони, радужная оболочка, черты лица.

2. Динамические характеристики, такие, как голос, почерк, манера набора текста, особенности походки [2].

Типовая архитектура системы телеприсутствия включает следующие компоненты [3]:

1. Модуль сбора данных:
– сенсорные устройства;
– препроцессоры.

2. База данных эталонов:
– хранилище шаблонов;
– индексы.

3. Подсистема сравнения:
– алгоритмы сопоставления;
– метрики оценки.

4. Модуль принятия решений
– правила верификации;
– протоколы.

Процесс обработки данных происходит последовательно и включает следующие этапы [3]:
– сбор исходных данных;
– предварительная обработка;
– извлечение признаков;
– формирование шаблона;
– сохранение в базе данных;
– верификация/идентификация.

Как метрики качества биометрической системы используются следующие параметры: FAR (False Acceptance Rate) – вероятность ложного допуска, FRR (False Rejection Rate) – вероятность ложного отказа, а также EER (Equal Error Rate) – равная ошибка.

Варианты практической реализации рассматриваемой в данной статье системы телеприсутствия многочисленны, и включают в себя, но не ограничиваются, следующими сценариями [4]:
– удаленные медицинские консультации;
– дистанционное образование;
– виртуальные бизнес-встречи;
– финансовый сектор;
– государственная служба.

Кроме того, необходимо упомянуть механизмы безопасности и защиты данных от кибератак и злоумышленников [5]:
– криптографическое шифрование;
– биометрический фьюзинг;
– многофакторная аутентификация;
– защита от атак;
– аудит доступа.

Современные технологии стремительно трансформируют подходы к безопасности и взаимодействию в цифровой среде. Среди наиболее перспективных направлений выделяются мультимодальные системы, объединяющие несколько способов аутентификации (например, голос, лицо и от-

печаток пальца), что значительно повышает надежность. Поведенческая биометрия анализирует уникальные паттерны поведения пользователя – от манеры печати на клавиатуре до походки, создавая динамический профиль безопасности.

Особую роль играет искусственный интеллект, который не только оптимизирует процессы, но и предугадывает угрозы благодаря предиктивной аналитике. Для защиты данных на принципиально новом уровне внедряется квантовая криптография, устойчивая к взлому даже квантовыми компьютерами. Завершает картину переход к облачным решениям, обеспечивающим масштабируемость и доступность без потери производительности [6].

Экономический аспект внедрения

Реализация таких технологий требует тщательного анализа затрат. Основные статьи расходов включают [7]:

– оборудование (например, биометрические сканеры или квантовые ключевые распределители);
– программное обеспечение с поддержкой алгоритмов ИИ и мультимодальной интеграции;
– обслуживание инфраструктуры, включая регулярные обновления и аудит безопасности;
– обучение персонала, так как работа с инновационными системами требует новых компетенций;
– техническая поддержка для оперативного устранения сбоев и адаптации под меняющиеся требования.

Инвестиции в эти направления окупаются за счет снижения рисков кибератак и повышения эффективности бизнес-процессов.

Экспериментальное исследование и методика тестирования

Для комплексной оценки эффективности предложенных решений был проведен многоэтапный цикл испытаний. На первом этапе осуществлялся сбор тестовых данных, включающий формирование обширной базы поведенческих и биометрических показателей, полученных от более чем тысячи пользователей в различных сценариях взаимодействия. После сбора данных проводилась тщательная калибровка системы, в ходе которой специалисты настраивали алгоритмы искусственного интеллекта для оптимальной работы в условиях, максимально приближенных к реальной эксплуатации.

Результаты исследования и выводы

Проведенные испытания продемонстрировали значительное улучшение ключевых показателей системы безопасности. Благодаря реализации мультимодального подхода, удалось достичь высокой точности аутентификации, что существенно снижает риски несанкционированного доступа. Особого внимания заслуживает достигнутое сокращение времени реакции системы, что делает процесс идентификации практически незаметным для пользователей.

Заключение

Развитие биометрической аутентификации в сфере телеприсутствия открывает новые перспективы для повышения безопасности и удобства использования цифровых сервисов. Интеграция передовых технологий и инновационных решений способствует созданию надежных систем контроля доступа. Для решения задач сохранения безопасности, целостности и доступности информации в системе предлагается следующая общая схема системы телеприсутствия с биометрической аутентификацией:

1. Телеприсутственная платформа:
– биометрический модуль;
– сенсорный блок;
– процессор;
– хранилище.

2. Система управления:
– сервер приложений;
– база данных.

3. Каналы связи:
– сеть передачи;
– протоколы;

4. Пользовательский интерфейс:
– клиентское ПО;
– веб-интерфейс.

Список используемых источников

1. Optimized Data Transmission and Signal Processing for Telepresence Suits in Multiverse Interactions / A. Volkov, A. Muthanna, A. Paramonov [et al.] // Journal of Sensor and Actuator Networks. 2024. Vol. 13. № 6. P. 82. DOI 10.3390/jsan13060082. EDN:VBEMLB

2. Проничев В. Д., Ушаков И. А. Автоматизированный анализ изменений в сетевых конфигурациях устройств на основе нейронных сетей // Подготовка профессиональных

кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024). Сб. лучших докладов в 2-х т., СПб.: СПбГУТ. 2025. С. 443-448. EDN:DDZZOT

3. Тамбовский А. Н., Ушаков И. А. Архитектура сервиса сбора данных для обнаружения инсайдерских угроз в файловых системах Linux // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024). Сб. лучших докладов в 2-х т., СПб.: СПбГУТ. 2025. С. 273-276. EDN:AZDKWU

4. Свидетельство о государственной регистрации программы для ЭВМ № 2025617273 Российская Федерация. Программа взаимодействия с библиотекой AutoML для тестирования нейронных сетей на уязвимости: заявл. 10.03.2025: опубл. 25.03.2025 / С. И. Штеренберг; заявитель Санкт-Петербургский государственный университет промышленных технологий и дизайна. EDN:MQFVFR

5. Крутиков А. Н., Страйстар В. А., Ушаков И. А. Методы обнаружения инсайдеров в компьютерных сетях с использованием больших данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании: XIII Международная научно-техническяа и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 507-510. EDN:OHMPGB

6. Свидетельство о государственной регистрации программы для ЭВМ № 2025619491 Российская Федерация. Программа мониторинга загруженности процессора и оперативной памяти вычислительного узла облачной платформы OpenStack: заявл. 07.04.2025: опубл. 16.04.2025 / С. И. Штеренберг, А. В. Поляничева, Р. В. Алехин, П. Е. Шелкоплясова; заявитель Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. EDN:AQPEUP

7. Штеренберг С. И. Моделирование защиты ассимиляционной памяти в среде обработки Больших данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 1. С. 48-54. DOI 10.46418/2079-8199_2024_1_8. EDN:WTOYUB

Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2025-005, "Прикладные научные исследования в области создания сервисов и приложений в перспективных сетях связи" (регистрационный номер ПТНИ: 1024032900317-4).

BIOMETRIC AUTHENTICATION AND ACCESS CONTROL SYSTEM IN TELEPRESENCE SERVICES

Krasov A., Pankov A., Ushakov I.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article examines theoretical and practical aspects of biometric authentication implementation in access control systems for telepresence services. It provides a comprehensive analysis of existing methods, their advantages and limitations, along with innovative solutions to enhance system efficiency and security.

Key words: *biometric authentication, telepresence, access control systems, information security, biometric data, multimodal systems*

УДК 004.056
ГРНТИ 81.93.29

АНАЛИЗ АТАК ТИПА ОТРАВЛЕНИЯ ДАННЫХ В СФЕРЕ УСЛУГ ТЕЛЕПРИСУТСТВИЯ

А. В. Красов, И. А. Ушаков, С. И. Штеренберг

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

В последние годы нейросетевые алгоритмы широко используются в различных приложениях – от распознавания изображений до систем рекомендаций. Вместе с этим возрастает и риск атак, направленных на подрыв их функциональности. Одной из наиболее опасных видов атак является Data Poisoning. В этой статье будет рассмотрен механизм Data Poisoning, его влияние на нейросетевые модели, а также методы защиты и предотвращения подобных атак в сфере услуг телеприсутствия.

Data Poisoning, нейронные сети, искусственный интеллект, телеприсутствие, информационная безопасность

Data Poisoning (отравление данных) в нейронных сетях представляет собой серьезную угрозу, поскольку злоумышленник может внедрить искаженные или специально подготовленные данные в один или несколько пакетов данных, которые затем будут использованы для обучения модели. Это может быть сделано путем компрометации узла в распределенной системе или путем манипулирования данными на этапе их сбора или передачи. Например, может изменить некоторые изображения в наборе данных для обучения модели компьютерного зрения, добавив специфические метки или признаки, которые приведут к неправильной классификации определенных объектов.

Также вредоносные данные могут привести к тому, что модель будет обучаться неправильно, что может проявляться в виде снижения точности, предвзятости или даже выполнения определенных действий в пользу злоумышленника. Например, модель может начать классифицировать определенные типы данных неправильно или выдавать предвзятые результаты. Например, в системе, которая анализирует кредитные заявки, злоумышленник может внести изменения в данные таким образом, чтобы модель начала одобрять заявки с определенными признаками, которые обычно указывают на высокий риск невозврата кредита.

Что касается распределенных систем, где данные обрабатываются параллельно на разных узлах, влияние отравленных данных может быстро распространиться на всю систему. Это особенно опасно, если модель используется для принятия важных решений, таких как финансовые транзакции, медицинская диагностика или безопасность. Например, в распределенной системе, анализирующей данные о здоровье пациентов, отравленные данные могут привести к неправильной диагностике или лечению, что может иметь серьезные последствия для здоровья пациента.

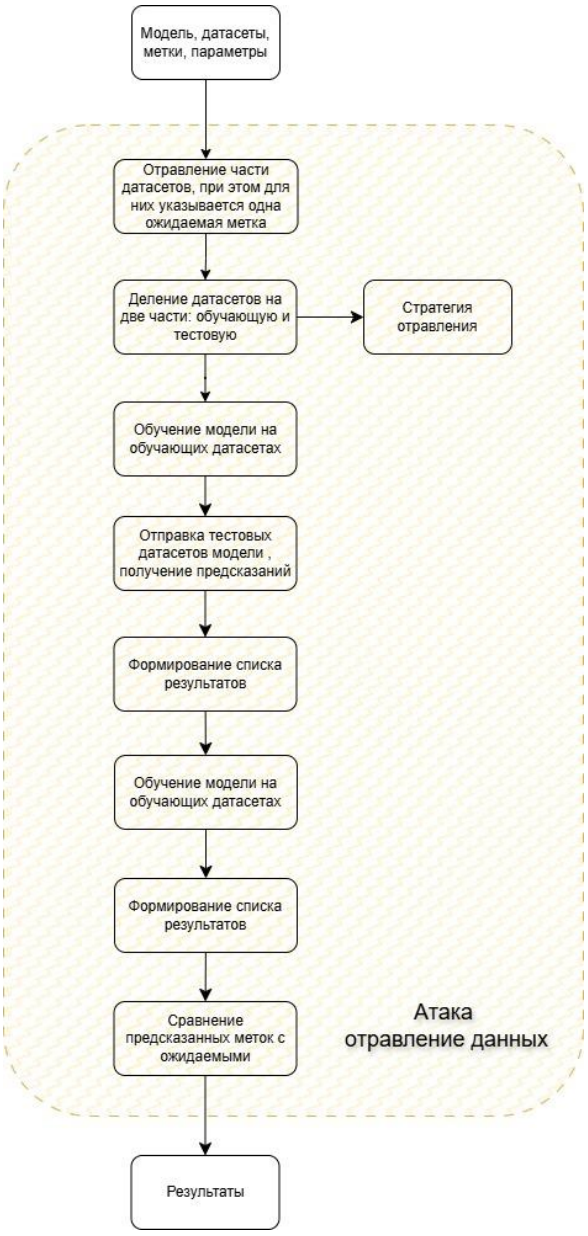


Рис. 1. Схема работы библиотеки при атаке отравление данных

Методы защиты от Data Poisoning включают в себя подготовку и проверку обучающих датасетов на наличие аномалий, выбросов и признаков манипулирования. Например, использование статистических методов для выявления выбросов и аномалий в данных, а также применение алгоритмов машинного обучения для обнаружения подозрительных паттернов (рис. 1). Разработка и использование алгоритмов, устойчивых к отравленным данным, может помочь минимизировать их влияние на обучение модели. Например, алгоритмы, которые могут идентифицировать и игнорировать аномальные данные, могут повысить устойчивость модели. Например, применение методов разделения датасетов, где несколько моделей обучаются на разных подмножествах данных, и их предсказания объединяются для повышения устойчивости к отравленным данным. Мониторинг и анализ поведения модели в процессе обучения и после развертывания могут помочь выявить признаки отравления данных.

Например, резкое снижение точности или необычные паттерны в предсказаниях модели могут указывать на проблему. А именно, использование метрик качества модели и сравнение их с базовыми значениями для выявления аномалий в поведении модели.

Так же необходимо использовать данные для обучения модели из различных источников для снижения риска отравления данных, так как злоумышленнику будет сложнее манипулировать всеми источниками одновременно. Например, сбор данных из различных географических регионов или из разных типов источников (например, социальные сети, датчики, базы данных) для уменьшения зависимости от одного источника данных.

Регулярное обновление и аудит модели на предмет уязвимостей помогает своевременно выявить и устранить проблемы, связанные с отравлением данных [1, 2, 3].

Структура работы системы безопасности, которая использует алгоритмы искусственного интеллекта и машинного обучения для обнаружения подозрительной активности и потенциальных угроз в распределенной сети показана на рис. 2.

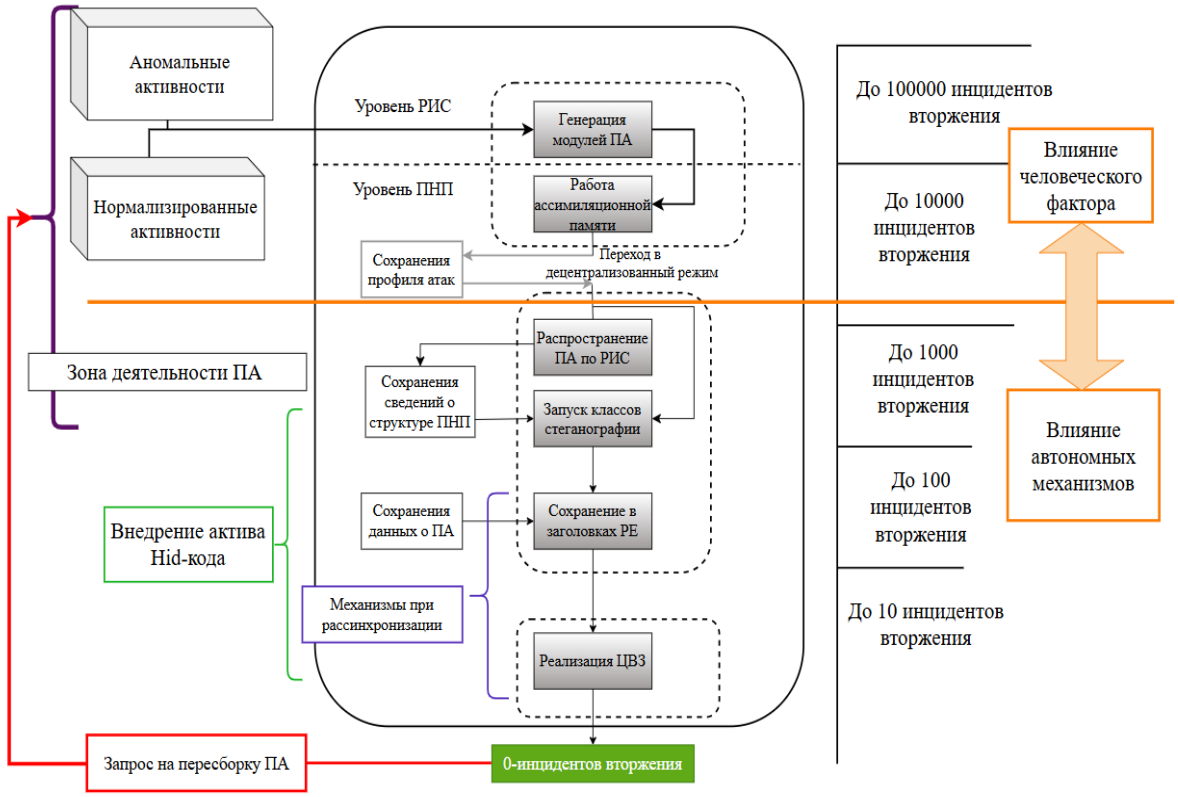


Рис. 2. Структурная схема (модель) устройства пакетно-нейросетевой программы для защиты в сфере телеприсутствия

В отличие от традиционных систем [4, 5, 6], которые опираются на заранее определенные правила и сигнатуры известных атак, новая модель способна анализировать большие объемы данных, выявлять сложные и скрытые угрозы, а также адаптироваться к новым видам атак. Для повышения устойчивости системы возможна также реализация обфусцированных элементов в исполняемых файлах [7, 8, 9].

Сейчас на рынке есть много обфускаторов с открытым кодом. Один из основных способов защититься от реверс-инжиниринга – это вставка мертвого кода и данных так, чтобы не было видно, что они ни на что не влияют. Это довольно простой метод обфускации, и многие проекты используют разные инструменты для его реализации, согласно недавним исследованиям.

В методике, предложенной на кафедре Защищенных систем связи СПбГУТ, наблюдается снижение вероятности «ложного» переобучения нейросети, модель ИИ в целом становится недоступной для атакующего. За счет обфускации как раз возрастает затруднение при обратном проектировании модели ИИ.

Исследование выполнено при финансовой поддержке Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, соглашение № 071-03-2025-005, "Прикладные научные исследования в области создания сервисов и приложений в перспективных сетях связи" (регистрационный номер ПТНИ: 1024032900317-4).

Список используемых источников

1. Штеренберг С. И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии // Офтальмохирургия. 2022. № S4. С. 51-57.

2. Штеренберг С. И. Анализ работы алгоритмов защиты информации на основе самомодифицирующегося кода с применением стеговложения // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 2. С. 86-90.

3. Штеренберг С. И. Методика применения в адаптивной системе локальных вычислительных сетей стеговложения в исполнимые файлы на основе самомодифицирующегося кода // Системы управления и информационные технологии. 2016. № 1(63). С. 51-54. EDN:VOOKUZ

4. Волков А. Н., Кучерявый А. Е. Туманные вычисления в сетях IMT-2030 для услуг телеприсутствия // XIV Всероссийское совещание по проблемам управления: сборник научных трудов, Москва, 17–20 июня 2024 года. Москва: Институт проблем управления им. В. А. Трапезникова РАН, 2024. С. 2295-2297. EDN:JXYICQ

5. Кучерявый А. Е., Маколкина М. А., Парамонов А. И. и др. Модельная сеть для исследований и обучения в области услуг телеприсутствия // Электросвязь. 2022. № 1. С. 14-20. DOI 10.34832/ELSV.2022.26.1.001. EDN:GBQWCV

6. Фокин Г. А., Кучерявый А. Е. Размещение устройств сверхплотной сети в пространстве. Часть 1. модели и методы геометрического фактора // Информационные технологии и телекоммуникации. 2022. Т. 10. № 3. С. 32-59.

7. Штеренберг С. И., Красов А. В. Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 1. исследование // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 14-20.

8. Штеренберг С. И., Красов А. В. Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 2. тестирование и оценка эффективности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 3. С. 3-8.

9. Штеренберг С. И., Красов А. В. Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 3. принцип действия программного агента и проверка его работоспособности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 34-40.

ANALYSIS OF DATA POISONING ATTACKS IN THE FIELD OF TELEPRESENCE SERVICES

Krasov A., Ushakov I., Shterenberg S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In recent years, neural network algorithms have been widely used in various applications, from image recognition to recommendation systems. At the same time, the risk of attacks aimed at undermining their functionality increases. One of the most dangerous types of attacks is Data Poisoning. This article will discuss the Data Poisoning mechanism, its impact on neural network models, as well as methods to protect and prevent such attacks in the field of telepresence services.

Key words: *Data Poisoning, neural networks, artificial intelligence, telepresence, information security*

УДК 004.056.55
ГРНТИ 81.93.29

О ПОИСКЕ НЕВЫЧЕТОВ

Д. И. Кушнир, С. Н. Шемякин

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

Необходимость поиска невычета в простом поле возникает в ряде несимметричных систем шифрования, в частности при построении шифров на эллиптических кривых. Кроме того, определение невычетов может быть полезно при определении примитивных корней, задачах разложения на множители и других задачах теории чисел. В работе представлен алгоритм, позволяющий значительно ускорить выяснение наличия свойства «данное число является невычетом».

несимметричные шифры, квадратичный невычет, определение корня в простом поле

В ряде прикладных задач, связанных, например, с построением криптографических систем, возникает задача вычисления корня из некоторого числа в простом поле $GF(p)$.

Сложность вычисления корня определенным образом зависит от вида модуля, которым определено поле. Кроме того, в любом случае может потребоваться быстрая оценка, имеет ли решение квадратичное сравнение $x^2 = a \bmod p$, и, если число a является квадратичным невычетом, то решений у соответствующего сравнения нет. В случае $p = 4 \cdot k + 3$ и $p = 8 \cdot k + 3$ корень извлекается относительно несложно, но в случае $p = 8 \cdot k + 1$ задача оказывается несколько сложнее. Пусть задано простое поле $GF(p)$ и большое простое число p имеет вид $p = 8 \cdot k + 1$, тогда при поиске корня из числа $n \in GF(p)$ приходится пользоваться алгоритмом Тонелли [1]. В данном алгоритме в процессе вычисления квадратного корня производится поиск какого-либо невычета a в поле $GF(p)$.

Напомним некоторые сведения из теории чисел [2, 3]. Число a называют невычетом (или квадратичным невычетом) по простому модулю p, если значение символа Лежандра для него равно «-1»,

$$\left(\frac{a}{p}\right) = -1.$$

Это значит, что для числа a не существует квадратного корня в поле $GF(p)$. Для вычисления значения символа Лежандра можно воспользоваться критерием Эйлера:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (mod\ p).$$

Однако при расчете предпочтительнее применять квадратичный закон взаимности и воспользоваться существующими таблицами индексов для малых модулей:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Результаты численного моделирования показали, для простых чисел p заданного вида в диапазоне до 10 000 000, одно из чисел 3, 5, 7, 11 оказывается первым найденным невычетом (при переборе начиная с наименьшего); рассмотрение начинаем с числа 3, так как 2 для чисел $8 \cdot k + 1$ всегда вычет. Доля таких событий оказалась приблизительно равной 0.87. В частности, число 3 оказалось первым невычетом в половине проверок, число 5 в 0.25, а число 7 в 0.12 проверок. Кроме того, числа 3, 5, 7, 11, 13, 17, 19 покрывают долю более 0.97 из общего количества невычетов, встретившихся первыми при переборе от меньших к большим. Для любого другого простого числа вероятность оказаться первым невычетом достаточно мала и не превышает 0.01. Можно предположить, что значения этих долей сохранятся и при работе с действительно большими числами. Более вероятно, что эти доли будут уменьшаться с ростом модуля p, хотя и достаточно медленно.

Таким образом, для поиска невычета оптимальным будет производить такой поиск последовательно, проверяя каждое простое число в порядке возрастания в качестве кандидата на квадратичный невычет по простому модулю.

Как уже было отмечено ранее, одним из наиболее эффективных методов проверки того, является ли число квадратичным вычетом, считается вычисление символа Лежандра, применяя квадратичный закон взаимности. Однако для больших простых p выполнение указанных преобразований может оказаться затратной операцией, особенно при большом количестве таких операций.

Для потенциального сокращения времени проверок составим таблицу предвычисленных значений квадратичных невычетов и дополнительных параметров.

При построении такой таблицы воспользуемся гипотезой Эйлера [4, 5]. В ныне доказанной гипотезе Эйлера утверждается, что число a является квадратичным вычетом или невычетом по модулю p одновременно для всех

простых p из арифметической прогрессии $q + (4 \cdot a) \cdot t$. Иначе говоря, если $q = p \pmod{4a}$ – нечетные простые числа, то

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

Таким образом, если нам дан большой простой модуль p, и для него необходимо проверить, является ли некоторое число a квадратичным невычетом, то достаточно это сделать для числа a по модулю небольшого простого числа q. Так как, уже среди нескольких первых небольших простых чисел a с большой вероятностью содержится невычет, то составим таблицу небольших простых чисел, потенциальных кандидатов на квадратичные невычеты, и набора тех чисел q, которые можно получить из исходного большого простого с помощью соотношения $q = p \pmod{4a}$.

Так как в работе уделялось внимание нахождению квадратичных невычетов для последующей операции извлечения корня, то наиболее актуальным является рассмотрения случая, когда $p = 8 \cdot k + 1$. Для данного случая для всех чисел p в диапазоне от 3 до 10 000 000 составим списки невычетов a, и какие значения q формируются, если a оказалось квадратичным невычетом. При обработке всех указанных чисел в подавляющем большинстве случаев, как было указано ранее, квадратичным невычетом оказывалось уже одно из первых простых чисел (3, 5, 7, 11, 13, 19). Кроме того, в рассматриваемом диапазоне самым большим значением минимального квадратичного невычета оказалось число 163, тридцать восьмое простое число. Полученные данные были оформлены в структуру данных словарь, для эффективного определения в дальнейшем наличия или отсутствия необходимых значений в указанной структуре. Таким образом была сформирована следующая предвычисленная структура (см. рис 1):

```
{3: {5},
5: {17, 13},
7: {17, 5, 13},
11: {41, 13, 29, 17},
13: {41, 5, 37},
17: {5, 37, 41, 61, 29},
19: {37, 41, 13, 53, 29},
23: {5, 37, 17, 53, 89, 61},
29: {97, 101, 37, 41, 73, 17, 113, 89, 61},
31: {37, 73, 13, 17, 29, 53, 89, 61},
37: {97, 5, 13, 109, 113, 17, 61, 89, 29},
41: {97, 101, 137, 13, 109, 17, 29, 149, 53, 89, 157},
43: {5, 37, 73, 137, 113, 29, 149, 157, 89, 61},
47: {5, 73, 41, 137, 13, 109, 113, 181, 29}, ...}
```

Рис. 1. Словарь соответствий: {невычет (a): {набор возможных простых остатков при делении на $4 \cdot a$ чисел вида $8 \cdot k + 1$}}.

В данной структуре число перед двоеточием – потенциальный невычет, набор чисел после двоеточия – возможные остатки, получаемые при делении числа p на квадратичный невычет a (такие остатки могут быть получены, только если a квадратичный невычет по модулю p и по модулю q).

Можно ограничить эту структуру значением невычета 19, однако, структура не занимает много памяти и поиск по ней может производиться весьма эффективно, что позволяет оставить максимальный набор ранее полученных элементов.

Дальнейшее применение такой таблицы в поиске невычета предполагает выбор очередного простого числа a из ряда 3, 5, 7, 11, … для проверки того, является ли оно квадратичным невычетом по некоторому модулю p. Далее производится вычисление значения $q = p \pmod{4a}$ и проверка, присутствует ли в предвычисленной таблице нужная комбинация невычета a и остатка q.

Например, необходимо проверить, является ли число 7 квадратичным невычетом по модулю 241. Находим $q = 241 \pmod{4 \cdot 7} = 17$. Проверяем, есть ли в таблице запись 7: …, 17 …, или, другими словами, присутствует ли элемент 17 у ключа 7. Убеждаемся, что присутствует, значит число 7 – это квадратичный невычет по модулю 241.

Так как таблица имеет конечный размер, то она не может покрыть все случаи. Данный факт означает, что если в таблице не нашлось соответствие, то проверяемое число все равно может быть квадратичным невычетом. Это особенно актуально для позиций со значением a, попавшим в конец вычисленной структуры, так как в этом случае не все потенциальные значения q были выявлены). Для малых a, отсутствие соответствия означает, что данное a квадратичный вычет.

Например, необходимо проверить, является ли число 5 квадратичным невычетом по модулю 241. Находим $q = 241 \pmod{4 \cdot 5} = 1$. Такой записи в таблице нет, следовательно, невозможно утверждать, что число a является невычетом, кроме того, так как $q = 1$, то это гарантирует, что a является квадратичным вычетом по модулю 241.

Составленная описанным образом структура позволяет ускорить нахождение квадратичного невычета по простому модулю, так, например, при вычислениях на устройствах с одинаковыми вычислительными ресурсами проверка того не является ли число $a = 7$ невычетом по модулю $p = 11636921$ заняло примерно 8 секунд на основе применения свойства квадратичной взаимности и менее 2 секунд по составленной структуре (проверка

повторялась 10 млн. раз для набора статистики). Проверка же того, не является ли число $a = 7$ невычетом по модулю 5673 битного простого числа, заняло порядка 120 секунд на основе закона квадратичной взаимности и порядка тех же 2 секунд по предвычисленной структуре (проверка выполнялась 10 млн. раз).

Предложенный способ поиска квадратичных невычетов или проверки данного числа, является ли оно квадратичным невычетом, позволяет на порядок ускорить получение результата. Наибольшее преимущество может быть получено при поиске невычетов для больших простых модулей размером несколько сотен бит. В задачах поиска невычета, если данные о невычете и соответствующем простом остатке от деления простого модуля на $4a$ не попали в таблицу, можно произвести проверку данного числа вычислением на основе свойства взаимности, или перейти к другому потенциальному невычету и выполнить проверку для него, но вероятность того, что придется прибегнуть к этой процедуре, пренебрежимо мала.

Список используемых источников

1. Menezes A. J., Van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 2018. 810 p.

2. Бухштаб А. А. Теория чисел. М.: Просвещение, 1965. 383 с.

3. Виноградов И. М. Основы теории чисел. М.-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. 176 с.

4. Бибиков П. В., Козеренко К. В., Малахов А. И. Теория чисел во Второй школе. – М.: МЦНМО, 2021. 200 с.

5. Акимов Д. В., Беляев Д. А., Бибиков П. В. и др. Вокруг квадратичного закона взаимности. М.: МЦНМО, 2024. 80 с.

ABOUT SEARCHING FOR NONRESIDUE

Kushnir D., Shemyakin S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The necessity of finding a nonresidue in a simple field arises in a number of asymmetric encryption systems, in particular when constructing ciphers on elliptic curves. In addition, the determination of nonresidue can be useful in determining primitive roots, multiplier decomposition problems and other number theory problems. In this paper we present an algorithm that allows us to significantly speed up the elucidation of the existence of the property «a given number is a nonresidue».

Key words: *asymmetric ciphers, quadratic nonresidue, root detection in a simple field*

УДК 004.056.5
ГРНТИ 81.93.29

АКТИВНЫЕ МЕТОДЫ СБОРА ИНФОРМАЦИИ О МОШЕННИКАХ

А. П. Кюнер, А. А. Чечулин

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

В данной статье рассматриваются методы совершенствования системы защиты информации предприятия, а также обеспечения безопасности частных лиц путем применения активных методов противодействия нарушителю. Предпринимаемые меры защиты направлены на применение навыков специалистов в области информационной безопасности, приемов социальной инженерии для поиска, накопления и анализа данных об атакующем. В статье подчеркивается необходимость квалификации специалистов по информационной безопасности, сопоставимой с методами и навыками нарушителя информационной безопасности. В связи с тем, что значительная часть информационных ресурсов и научных работ, описывающих методы защиты от социальной инженерии, фокусирует основное внимание на развитии защитных механизмов потенциальной жертвы, описанный в настоящей работе подход позволяет расширить возможности по предотвращению атаки на ранних стадиях.

социальная инженерия, сбор информации, деанонимизация нарушителя, мошенничество

Угроза нарушения информационной безопасности (ИБ), исходящая от применения злоумышленниками методов социальной инженерии (СИ), наиболее чувствительна для финансового сектора. Утечки персональных данных, разнообразие каналов доставки вредоносного контента, несоблюдение сотрудниками компаний элементарных мер ИБ позволяют злоумышленникам обходить средства защиты информации (ЗИ), используя человеческий фактор, при этом эффективность атаки напрямую зависит от объема и актуальности сведений о жертве. В целях противодействия социо-инженерным атакам (СИ-атакам) на различных стадиях крупным компаниям необходима узкоспециализированная команда специалистов различных областей ИБ [1].

Разработка методов защиты от угрозы совершения кибератак с использованием приемов СИ остается одной из важнейших задач государства. Информационные источники акцентируют основное внимание на повышении осведомленности и внедрении технических мер, позволяющих выявить факт мошенничества. Согласно статистике [2], специалисты в области ЗИ также вступают в диалог с мошенниками. Одной из причин успеха таких

атак является отсутствие настроек приватности в системах передачи данных. Данный факт свидетельствует о том, что пользователи, не имеющие опыта работы в области ИБ, еще больше подвержены риску успешной реализации СИ-атаки (рис. 1).

Рис. 1. Должности сотрудников, вступивших в переписку [2]

В работе [3] автор подчеркивает, что обучение пользователей является последней линией защиты и не гарантирует их безопасность. Эту проблему может частично устранить массовое оповещение о реальных атаках. Также автор упоминает о том, что несоблюдение «цифровой гигиены» способствует накоплению знаний нарушителем. Необходимость противодействовать атакам на различных стадиях [4] требует наличия у подразделений по ИБ знаний о потенциальном нарушителе, которых будет достаточно для оценки его возможностей, методов атаки, объема данных.

Немаловажным аспектом системы ЗИ организации является подготовка сотрудников отдела ИБ, которые являются менее уязвимыми к СИ-атакам, при этом нужно уделять внимание повышению знаний специалистов о новых атаках [5]. Автор научной работы [6] подчеркивает, что для эффективного обнаружения и противодействия различным типами нарушителей ИБ, подразделение должно быть укомплектовано специалистами различного профиля и иметь разнообразные технические средства. Возможности отдела ИБ крупной компании сопоставимы с уровнем Н2-Н3 возможностей нарушителя, согласно приложению 8 к Методике оценки угроз

безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК) [7].

В целях разработки технических, организационных и физических мер ЗИ, в особенности субъектов критической информационной инфраструктуры [8], требуется учитывать возможность совершения атак с применением методов СИ, при этом необходимо не допустить вступления неподготовленных работников в диалог с мошенниками [9], иметь возможность оперативной передачи сведений об инциденте специалисту по ИБ (или ответственному за ЗИ в подразделении). Следует учесть тот факт, что принципиально новых атак не существует (при условии непрерывного отслеживания угроз и инцидентов), но сложнее распознать атаки через скомпрометированные учетные записи.

Деанонимизация злоумышленника позволяет в ряде случаев предотвратить атаку. Вопросами сбора сведений о киберпреступнике занимается подразделение «К» Министерства внутренних дел [10], применяя различные методы деанонимизации. Этот метод не находит массового применения и сосредоточен на раскрытии преступлений, совершаемых дистанционно. При использовании данного подхода учитывается тот факт, что мошенник не обладает техническими и организационными мерами ЗИ, следовательно, уязвим перед СИ-атаками. Также, информация о новых видах угроз может быть получена путем разведки открытых источников, однако данный подход является недостаточно оперативным [11]. Сложной задачей остается поиск утечек данных из-за запрета соответствующих инструментов законодательством.

Путем опроса экспертов в области ИБ определены следующие параметры злоумышленника, интересующие специалиста отдела ИБ:

– цели атаки;
– методы анонимизации;
– используемые технические средства;
– источники и объем знаний об объектах атаки;
– квалификация;
– психологический портрет;
– численность и состав;
– местонахождение;
– сценарий атаки;
– параметры объектов атаки.

В целях усовершенствования существующих мер защиты сотрудников от СИ-атак и повышения знания о методах их проведения, модель угроз (МУ) ИБ должна разрабатываться с учетом сведений об атакующем (рисунок 2). При разработке МУ необходимо учитывать ключевые моменты в прошедших инцидентах.

Рис. 2. Схема уточнения параметров нарушителя

Существуют различные способы сбора сведений о нарушителе ИБ, среди которых можно выделить 2 группы: активные и пассивные. К пассивным относятся: разведка открытых источников, разведка угроз, просмотр информационных порталов по ИБ или других источников (например, компаний-партнеров или жертв). Активные методы, в свою очередь, подразумевают непосредственные воздействия на нарушителя со стороны специалиста по ИБ, осуществляемые вербально или техническими средствами (рисунок 3). Данный способ сбора может быть реализован при выполнении условия, что уровень возможностей подразделения по ИБ не меньше, чем уровень возможностей нарушителя [7].

Рис. 3. Методы сбора информации о мошенниках

Пассивные методы сбора сведений о мошенниках, такие как разведка открытых источников и отслеживание угроз, позволяют установить места проведения атак, предпосылки, например, опубликованные утечки персональных данных или новости о компании. Анализ атак позволяет создать шаблон жертвы, сделать предположение о сроках появления сведений у зло-

умышленника, объем сведений, определить других подверженных атакам сотрудников. В анализ также входит изучение учетных записей (телефонных номеров) злоумышленников, заголовком электронных писем, арендованных для кибератак серверов.

Активные методы сбора сведений о нарушителе ИБ применяются правоохранительными органами и подразделениями по информационному противоборству. Вербальное взаимодействие может быть, осуществляется, когда злоумышленник считает, что ведет диалог со своей жертвой, на месте которой находится специалист по ИБ. В ходе диалога представляется возможным установить цели атаки, технические средства, сценарий, психологический портрет злоумышленника.

Технические методы нацелены на деанонимизацию, изучение технических средств, источники знаний, местонахождение, состав. Ниже представлены технические средства достижения этих целей, следует добавить, что указанные средства схожи с инструментами мошенника.

– sandbox для анализа подозрительных писем и вложений;
– средства связи и оперативного оповещения;
– средства проверки доступности адресата: корпоративный телефонный номер, обезличенная электронная почта, учетная запись в средствах мгновенного обмена сообщениями с приватными настройками;
– canary token в сочетании с психологическими приемами позволяет определить IP-адрес злоумышленника, при высоком правдоподобии документа он может быть доставлен другим мошенникам;
– средства удаленного доступа и другие утилиты для киберразведки в сочетании с арендованным сервером;
– honeypot в виде информационного ресурса или учетной записи;
– инструменты для тестирования информационных ресурсов злоумышленника в сочетании со средствами анонимизации.

Заключение

В данной статье проведен обзор причин успеха СИ-атак и методов защиты, отражены интересующие специалиста по ИБ параметры нарушителя. Представлены методы сбора информации о мошенниках путем использования специалистами подразделений по ЗИ технических средств и различных приемов. Одним из недостатков в системе обеспечения ИБ являются слабые знания о нарушителе. При проектировании системы ЗИ и разработке руководящих документов, таких, как МУ, политикой ИБ учитываются общепри-

нятые принципы моделирования возможностей потенциального нарушителя, которые, как правило, не уточняются и с учетом опыта противодействия совершенным атакам. Применение подразделениями по ЗИ активных методов получения информации о нарушителе ИБ путем прямого контакта с ним позволяет получить ряд полезных для разработки мер защиты сведений.

Список используемых источников

1. Атаки на финансовый сектор глазами PT SWARM: социальная инженерия 2025. URL: https://ptresearch.media/articles/ataki-na-finansovyj-sektor-glazami-pt-swarm-soczialnaya-inzheneriya-2025 (дата обращения: 22.06.2025).

2. Иванов А. В. Особенности защиты от угроз социальной инженерии / А.В. Иванов // Вестник Московского университета МВД России. 2023. № 7. С. 237-241. DOI:10.24412/2073-0454-2023-7-237-241

3. Родивилин И. П. Социальная инженерия как угроза информационной безопасности: тенденции и защита // Информационные технологии и математическое моделирование в управлении сложными системами. 2023. № 3(19). С. 30-38.

4. Кюнер А. П. Особенности противодействия методам социальной инженерии специалистами по информационной безопасности в рамках центров мониторинга и реагирования // Информатизация и связь. 2025. № 2. С. 97-101. DOI:10.34219/2078-8320-2025-16-2-97-101

5. Останина Е. А. Подготовка специалистов различных направлений по информационной безопасности в современных условиях // Человеческий капитал. 2023. № 7(175). С. 120-129. DOI:10.25629/HC.2023.07.15

6. Кочин В. П., Шанцов А. В. Методика создания и структура корпоративного подразделения информационной безопасности. Цифровая трансформация. 2022. № 28(3). С. 65-72.

7. Методика оценки угроз безопасности информации. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 24.06.2025).

8. Новикова Е. Ф. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии / Е. Ф. Новикова, В. Н. Хализев // Прикаспийский журнал: управление и высокие технологии. 2019. № 4(48). С. 127-135. DOI:10.21672/2074-1707.2019.48.4.127-135

9. Шастина А. Р. Социальная инженерия в структуре киберпреступности: к вопросу о противодействии телефонному мошенничеству // Аграрное и земельное право. 2024. № 9(237). С. 300-302. DOI:10.47643/1815-1329_2024_9_300

10. Фарахиев Д. М. Способы и методы деанонимизации лиц, совершающих преступления в информационном пространстве // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 4. С. 249–254. DOI:10.36511/2078-5356-2022-4-249-254

11. Янгаева М. О. Получение криминалистически значимой информации о личности преступника путем поиска по открытым источникам (OSINT) // Алтайский юридический вестник. 2023. № 4(44). С. 181-190.

SOCIAL ENGINEERING. ACTIVE METHODS OF COLLECTING DATA ABOUT SCAMMERS

Kyuner A., Chechulin A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

This article describes methods for the enterprise cybersecurity improvement, as well as upgrading the safety of individuals by using active methods against the violator. The countermeasures are focused on using the qualification of information security officers, social engineering tactics to search storage and analyze information about the violator. The article takes into account the need of cybersecurity officers' skills, which are comparable to the intruder and his methods. Due to the fact that a significant amount of online resources and articles describing protective methods against social engineering as developing security tools of potential victim, this approach allows to expand the possibilities for preventing an attack at first stage.

Key words: *social engineering, data gathering, intruder deanonymization, scamming*

УДК 004.056.53
ГРНТИ 81.93.29

МЕХАНИЗМ МОДЕЛИРОВАНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОБЪЕКТ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

В. А. Липатников[1], Д. В. Макаренко[1], А. А. Шевченко[2]

[1] Военная академия связи им. Маршала Советского Союза С. М. Буденного
[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

Цифровизация общества дала толчок к созданию значительного количества объектов критической информационной инфраструктуры государственного управления, экономики и социальной сферы. Обеспечение кибербезопасности данных объектов является одной из приоритетных задач. В связи с этим необходима разработка проактивных систем обеспечения кибербезопасности, в основе которых будут лежать такие механизмы моделирования атак, которые позволят в режиме реального времени прогнозировать развитие конфликтной ситуации для формирования предупреждающих и сдерживающих мер.

моделирование, компьютерная атака, кибербезопасность, прогнозирование.

В настоящее время в целях повышения уровня цифрового развития государственного и муниципального управления, ключевых отраслей экономики и социальной сферы уже сформировано и функционируют значительное количество цифровых платформ. Они, согласно Федеральному закону «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ, являются объектами критической информационной инфраструктуры (КИИ), к защите которых предъявляются определенные требования, регламентируемые тем же Федеральным законом.

На фоне значительного роста количества объектов КИИ и с учетом современных условий сложившейся геополитической обстановки в мире, в 2024 году объекты КИИ являлись первоочередными целями для политически мотивированных злоумышленников, что подтверждается данными аналитических отчетов различных компаний, предоставляющих услуги в сфере кибербезопасности (КБ). Так, за год совокупное число компьютерных атак (КА) выросло в 2,5 раза по сравнению с 2023 годом и почти достигло 130 тысяч, причем в 64 % от общего числа КА целями являлись объекты КИИ.

Данная тенденция обусловлена тем, что злоумышленники используют технологии искусственного интеллекта (ИИ) на различных этапах реализации КА, а именно – для сбора и анализа информации о жертве на этапе разведки, для генерации скриптов, создания вредоносного программного обеспечения и фишинговых сообщений и эксплуатации уязвимостей на этапе внедрения в IT-инфраструктуру, для автоматизации работы мошеннических аккаунтов и управления ботнетом на этапе выполнения команд КА.

Ввиду вышесказанного, вновь разрабатываемые системы обеспечения КБ объектов КИИ в нынешних условиях должны в режиме времени, близком к реальному, выявлять, прогнозировать и предотвращать КА, опережая высокотехнологичного злоумышленника в его решениях путем моделирования его действий.

В связи с тем, что моделирование КА является одним из важных подпроцессов обеспечения КБ, разработкой методов и способов его реализации занимаются как отечественные, так и зарубежные ученые. Так в [1, 2] авторы развивают идею автоматизации тестирования на проникновение за счет применения технологий ИИ. В [3, 4] предлагается сценарное моделирование КА на основе проведения Red Team / Blue Team учений. Наряду с вышеперечисленными методами, активно исследуются возможности применения имитационного моделирования для решения данной задачи, описанные в [5, 6]. Также в современных условиях развития технологий, учеными [7, 8] предлагается для моделирования КА применять технологии ИИ для анализа возможных угроз, уязвимостей и векторов атак с использованием моделей угроз. Близким к данному направлению является моделирование сценариев атак с помощью базы знаний MITRE ATT&CK о тактиках, техниках и процедурах, которые применяют злоумышленники, развитие которого получило отражение в работах [9, 10]. Авторы в [11] предлагают оценивать КБ за счет автоматизации симуляции КА на основе использования технологии ИИ. И, наконец, в [12, 13] описываются способы моделирования КА на уровне бизнес-процессов. Отмечая их значительный вклад в развитие теории и практики моделирования КА, следует сказать, что предлагаемые ими методы и способы позволяют через призму различных факторов анализировать воздействия злоумышленника, но недостаточны для решения задачи заблаговременного предупреждения и пресечения атакующих воздействий. В связи с этим необходимо обратить внимание на разработку такого подхода моделирования КА, который позволил бы создавать проактивные информационно-управляющие системы обеспечения КБ объектов КИИ,

позволяющие в режиме реального времени выявлять КА, формировать и реализовывать предупреждающие и сдерживающие меры.

В связи с этим, целью данной работы является повышение КБ объектов КИИ за счет раннего предупреждения КА злоумышленника, а задачей – разработать механизм моделирования КА, позволяющий прогнозировать их вектор.

Решение. Согласно [14], моделирование – это метод исследования объектов познания на их моделях, заключающийся в построении и изучении моделей реально существующих предметов, явлений, разнообразных процессов и конструируемых объектов для определения либо улучшения их характеристик, рационализации способов их построения, управления ими.

Ввиду этого, моделирование, как процесс, состоит из определенных этапов. Глобально можно выделить два этапа: построение модели и ее изучение. С учетом анализа литературы в области моделирования [15, 16] процесс моделирования протекает, как показано на рис. 1.

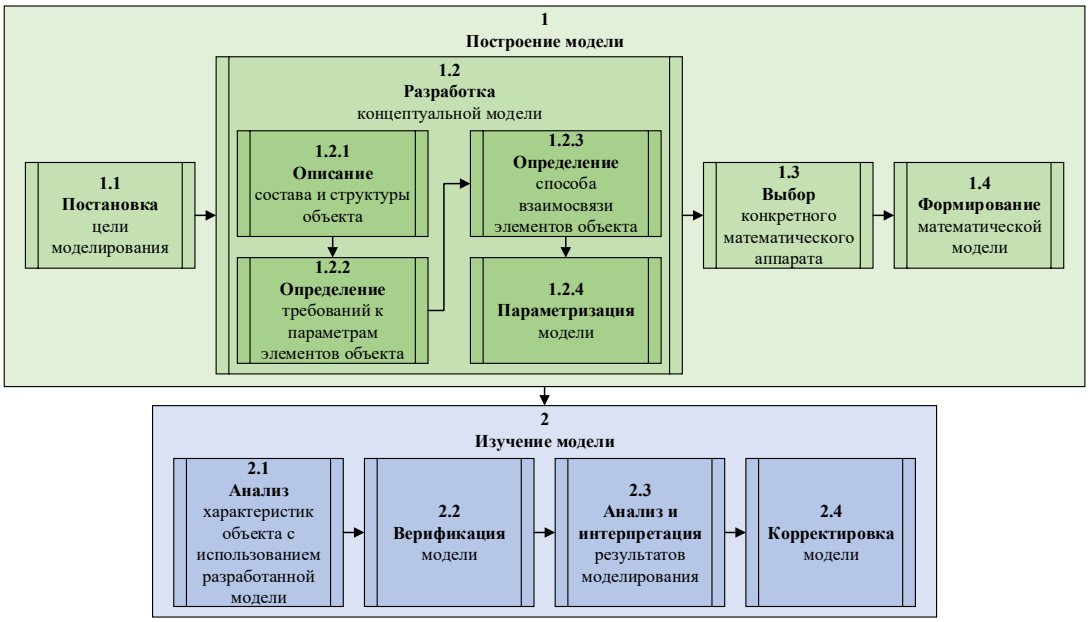


Рис. 1. Блок-схема процесса моделирования

С точки зрения обеспечения КБ, целью моделирования КА является идентификация, прогнозирование и смягчение потенциальных угроз для объекта КИИ.

Для достижения цели моделирования, необходимо разработать концептуальную модель КА, которая будет включать в себя описание параметров и характеристик атаки. Например, в качестве параметров можно выделить следующие множества: множество целей КА (системы или данные, которые

могут представлять наибольшую ценность для злоумышленников) $A = \{a_i, \{ER\}_i, \{IR\}_i, \{DER\}_i, \{DIR\}_i\}$, $i = 1, \ldots, n$, где n – количество целей КА, a_i – i-ая цель КА, $\{ER\}_i$ – множество внешних рисков (политических, экономических, технологических, информационных и социальных, экологических) при атаке на i-ую цель, $\{IR\}_i$ – множество внутренних рисков (технических, технологических, финансовых и др.) при атаке на i-ую цель, $\{DER\}_i$ – множество видов ущерба при идентификации внешних рисков из множества $\{ER\}_i$, $\{DIR\}_i$ – множество видов ущерба при идентификации внутренних рисков из множества $\{IR\}_i$; множество векторов КА (фишинг, вредоносное программное обеспечение, DDos-атаки и др.) $VCA = \{vca_j, \{SA_l, t_l\}_j\}$, $j = 1, \ldots, m$, $l = 1, \ldots, k$ где m – количество векторов КА, vca_j – j-ый вектор КА, $\{SA_l, t_l\}_j$ – множество последовательных действий злоумышленника j-ого вектора КА, k – количество последовательных действий злоумышленника j-ого вектора КА, SA_l – l-ое действие злоумышленника j-ого вектора КА, t_l – время реализации l-ого действия злоумышленника j-ого вектора КА; и др. Параметры могут меняться вследствие изменения или конкретизации цели моделирования.

С учетом поставленной цели моделирования, КА характеристиками могут быть вероятность реализации злоумышленником j-ого вектора КА (P_{vca_j}); вероятность реализации l-ого действия злоумышленника j-ого вектора КА ($P_{SA_{lj}}$); множество внутренних рисков при реализации злоумышленником j-ого вектора КА на i-ую цель $RER = \{rer_{SA_{lij}}\}$, где $rer_{SA_{lij}}$ – внутренний риск при реализации l-ого действия злоумышленника j-ого вектора КА на i-ую цель; множество внешних рисков при реализации злоумышленником j-ого вектора КА на i-ую цель $RIR = \{rir_{SA_{lij}}\}$, где $rir_{SA_{lij}}$ – внешний риск при реализации l-ого действия злоумышленника j-ого вектора КА на i-ую цель; и др. Характеристики также могут меняться в следствии изменения или конкретизации цели моделирования.

Учитывая приведенные выше параметры и характеристики для достижения поставленной цели необходимо найти следящие зависимости: P_{vca_j} и $P_{SA_{lj}}$ от времени и $rer_{SA_{lij}}$ и $rir_{SA_{lij}}$ от P_{vca_j} и $P_{SA_{lj}}$.

В виду того, что процесс реализации КА для объекта КИИ носит случайный характер, и ему присущ скачкообразный переход от подпроцесса к подпроцессу, а вероятностные закономерности меняются во времени, то имеет место следующее определение КА: «компьютерная атака – это дискретный стохастический нестационарный процесс целенаправленного воз-

действия злоумышленника на объекты КИИ с помощью программных и (или) программно-аппаратных средств в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации». Исходя из определения для моделирования КА выбран математический аппарат марковских случайных процессов, что позволяет составить и исследовать зависимости P_{vca_j} и $P_{SA_{lj}}$ от времени, описанные в [17-19], и как следствие составить и исследовать зависимости $rer_{SA_{lij}}$ и $rir_{SA_{lij}}$ от P_{vca_j} и $P_{SA_{lj}}$.

Таким образом, предложен механизм моделирования КА, позволяющий проводить идентификацию, прогнозирование и смягчение потенциальных угроз для объекта КИИ за счет исследования зависимостей вероятностей реализации КА, действий злоумышленника, внутренних и внешних рисков вследствие успешного воздействия от времени.

Список используемых источников

1. Vendhan, D., Veera Balagan, K., Saravana Kumar, P., Siva Muthu Narayanan Sabari Ganesh A. Development of an Automated Penetration Testing for Cybersecurity // International Research Journal on Advanced Engineering Hub (IRJAEH). 2025. Vol. 3. № 3. PP. 915-920.

2. Ныркov А.П., Юмашева Е.С., Кириков А. В. Оптимизация процесса тестирования на проникновение в АСУ технологическими процессами с использованием алгоритмов машинного обучения // Вестник государственного университета морского и речного флота им. адмирала С. О. Макарова. 2024. Т. 16. № 3. С. 456-466.

3. Chindruș C., Caruntu C. F. Enhancing cybersecurity readiness through the red and blue team competition // Bulletin of the Polytechnic Institute of Iași, Electrical Engineering, Power Engineering, Electronics Section. 2024. Vol. 69. № 2. PP. 35-56.

4. Москалева Е. А., Шеншин А. И., Каданцев И. А. Полигонные киберучения на примере моделирования компьютерных эпидемий сетей // Информация и безопасность. 2023. Т. 26. № 3. С. 439-446.

5. Scherb C., Heitz L. B., Grimberg F., Grieder H., Maurer M. A Cyber Attack Simulation for Teaching Cybersecurity // Proceedings of Society 5.0 Conference 2023 (EPiC Series in Computing). Vol. 93. PP. 129-140.

6. Шишов Н. В., Ломазов В. А., Ломазова В. И. Имитационное моделирование реализации компьютерной атаки с повышением привилегий пользователя системы электронного документооборота // Инженерный вестник Дона. 2023. № 2(98). С. 92-100.

7. Kim S., Heo G., Zio E., Shin J., Song J. Cyber attack taxonomy for digital environment in nuclear power plants // ELSEVIER Nuclear Engineering and Technology. 2020. № 50. PP. 995-1001.

8. Саенко И. Б., Лаута О. С., Карпов М.А., Крибель А. М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. 2021. № 1. С. 36-44.

9. Xiong W., Legrand E., Åberg O.,·Lagerström R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix // Software and Systems Modeling. 2022. Vol. 21. PP. 157-177.

10. Касимова А. Р., Золотарев В. В., Сафиуллина Л. Х., Сабирова Д. И. Моделирование вектора сетевых атак на локальную сеть с применением базы MITRE ATT&CK // Прикаспийский журнал: управление и высокие технологии. 2023. № 4(64). С. 88-96.

11. Mallick Md A. I., Nath R. Simulating Cyber Threats: A Review of AI-powered Attack Simulators for Enhanced Cybersecurity // World Scientific News. 2024. № 197. PP. 13-54.

12. Zare H., Wang P., Zare M.J., Azadi M., Olsen P. Business Continuity Plan and Risk Assessment Analysis in Case of a Cyber Attack Disaster in Healthcare Organizations // In: Latifi, S. (eds) 17th International Conference on Information Technology–New Generations (ITNG 2020). Advances in Intelligent Systems and Computing. 2020. Vol. 1134. PP.137-144.

13. Бердюгин А. А., Ревенков П. В. Оценка риска воздействия кибератак в технологиях электронного банкинга (пример программной реализации) // Финансы: теория и практика. 2020. Т. 24. № 6. С. 51-60.

14. Моделирование // Большая российская энциклопедия. Том 20. Москва. 2012. С. 576.

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

16. Голубева Н. В. Математическое моделирование систем и процессов: Учебное пособие. 2-е изд., стер. СПб.: Издательство «Лань», 2016. 192 с.

17. Липатников В. А., Косолапов В. С., Шевченко А. А., Сокол Д. С. Модель оценки процесса подготовки и реализации вторжений в сетях IP-телефонии // Информация и космос. 2021. № 4. С. 55-69.

18. Липатников В. А., Шевченко А. А. Математическая модель процесса управления информационной безопасностью распределенной информационной системы в условиях несанкционированного воздействия злоумышленника // Информационные системы и технологии. 2022. № 3(131). С. 121-130.

19. Шевченко А. А. Математическая модель информационного противоборства двух систем в информационно-телекоммуникационном пространстве // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции, Санкт-Петербург, 14–15 октября 2020 года. СПб: ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С.М. Буденного» МО РФ, 2020. С. 237-241.

CYBER ATTACK SIMULATION MECHANISM FOR CRITICAL INFRASTRUCTURE PROTECTION

Lipatnikov V.[1], Makarenko D.[1], Shevchenko A.[2]
[1] Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
[2] The Bonch-Bruevich Saint Petersburg State University of Telecommunications

Societal digitalization has significantly increased the number of critical information infrastructure assets in governmental, economic, and social domains. Cybersecurity assurance for such assets remains a top priority. To address emerging threats effectively, proactive cybersecurity systems must be developed, leveraging advanced attack modeling techniques capable of simulating and forecasting adversarial behavior in real time. These models should support the generation of early warnings and countermeasures to mitigate potential cyber threats.

Key words: *modeling, computer attack, cybersecurity, forecasting*

УДК 004.8
ГРНТИ 20.51.19

БЕЗОПАСНОСТЬ ВСТРОЕННЫХ СЕТЕЙ В АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВАХ С ПОМОЩЬЮ ПРОТОКОЛА TOUCAN

В. И. Лукашенок, П. А. Николаева, А. П. Таранущенко

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

В статье рассматривается архитектура сетевой инфраструктуры современных автономных транспортных средств, включая внутренние и внешние коммуникационные системы, основанные на протоколе CAN. Проведен анализ ключевых компонентов системы: сетевого интерфейса, локальной и глобальной сетей, а также программно-аппаратной платформы. Особое внимание уделено киберугрозам, классифицированным по уровням архитектуры – от сетевого интерфейса до внутренней и внешней инфраструктуры. Представлены типологии атак, включая DoS, MITM, SQL-инъекции, брутфорс и эксплуатацию уязвимостей ПО, а также физические и природные угрозы.

автономные транспортные средства, CAN-шина, кибербезопасность, TOUCAN, сетевая архитектура, кибератаки, атаки типа MITM, DoS/DDoS, SQL-инъекции

Авто последнего поколения оснащаются комплексной внутренней сетью, отличающейся многообразием (рис. 1.), аналогичным разнообразию моделей машин. Эти системы обеспечивают взаимодействие компонентов через унифицированные коммуникационные протоколы [1].

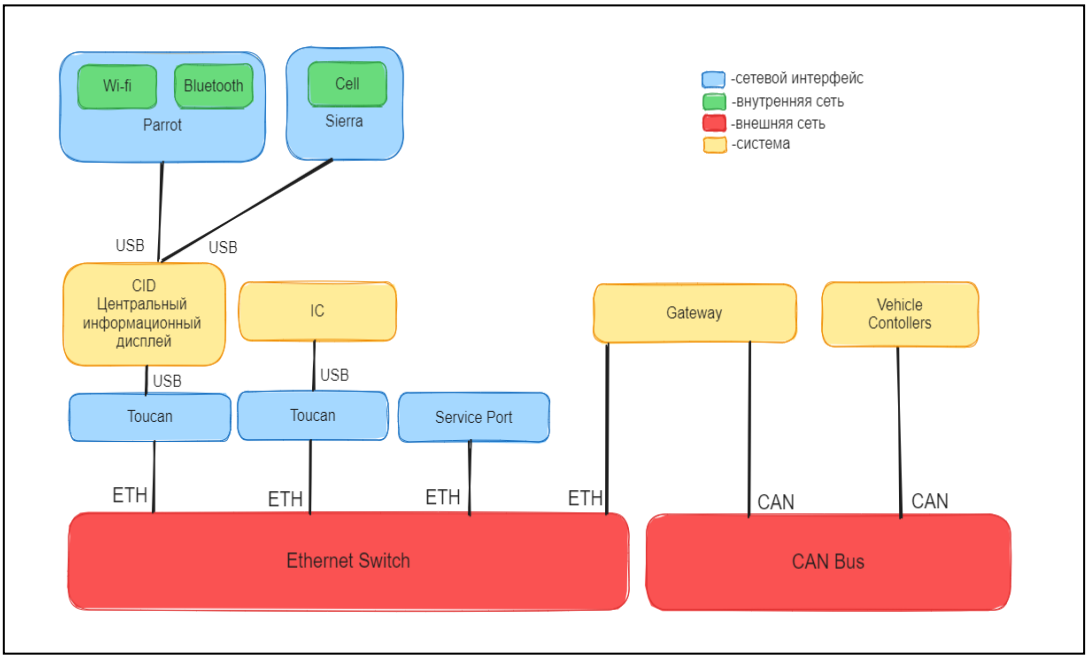


Рис. 1. Структура сетевого устройства Tesla

В рамках исследования угроз беспилотным автомобилям, первым шагом стало создание модели этих транспортных средств.

TOUCAN – это новый протокол безопасности, предназначенный для обеспечения безопасности и в то же время совместимый как с CAN. Он обеспечивает безопасность с точки зрения подлинности, целостности и конфиденциальности, но при этом не требует обновления (аппаратного обеспечения) существующих ЭБУ или обогащения сети новыми компонентами.

Контроллер локальной сети (Controller Area Network, CAN bus) представляет собой автомобильный стандарт интерфейса, созданный для обеспечения обмена данными между различными микроконтроллерами и устройствами внутри транспортного средства без необходимости централизованного управляющего компьютера. Проектировался как система мультиплексирования сигналов через один-два провода для уменьшения количества необходимой проводки и, таким образом, уменьшения веса и стоимости автомобилей, но его применение выходит за пределы автомобильной индустрии, распространяясь на любую область, где требуется надежный обмен сообщениями [2].

Сетевой шлюз переформатирует данные из одного протокольного стандарта в другой для обеспечения коммуникации между различными сетевыми средами.

Controller Area Network (CAN) является ключевым стандартом для создания промышленных сетевых систем, предназначенных для интеграции устройств и датчиков в автомобиле. Этот интерфейс обеспечивает подключение к CAN-шине автономных систем управления, включая системы руления, торможения и ускорения, а также различные датчики. Благодаря этому автомобиль получает возможность самостоятельного передвижения без участия водителя. Включение в конструкцию автомобиля систем помощи водителю (ADAS) позволяет расширить функционал автоматизации, например, путем добавления способностей адаптивного реагирования на изменяющиеся дорожные условия, как, например, на скользком дорожном покрытии.

Коммуникация между модулями в автомобиле с бесплатной архитектурой может реализовываться через определенные программные решения, гарантирующие трансфер информации между отдельными элементами. Представим, как обрабатывается информация:

Датчики фиксируют параметры окружающего мира и передают информацию в главный контроллер, после чего центр управления, проанализировав скорость передачи данных, сам двигатель и устройство информационно-развлекательной системы, которое служит для коммуникации с пассажирами, предлагает им данные о маршруте, развлекательных функциях и т.д. [3].

Следовательно, каждый из компонентов системы находится в постоянной координации с другими, гарантируя безопасность и удобство перемещения пользователей.

Исследование структуры (таблицы 1-6) выявило, что ключевыми компонентами модели служат: интерфейс связи, локальная сеть, глобальная сеть и общая архитектура системы.

ТАБЛИЦА 1. Ключевые компоненты автономного транспортного средства

Элемент	Описание
Сетевой интерфейс	устройство, обеспечивающее подключение автономного транспортного средства к внешней сетевой инфраструктуре
Внутренняя сеть	блок охватывает все компоненты, соединенные в рамках сетевой инфраструктуры, включая ПК, системы децентрализованного хранения данных и прочее
Внешняя сеть	блок содержит все компоненты, подсоединенные к сетевой архитектуре, включая внешние элементы, такие как различные устройства Интернета вещей или серверы, расположенные вдали
Система	блок содержит программы, аппаратные средства и ОС, функционирующие на аппарате [4]

ТАБЛИЦА 2. Атаки на сетевые интерфейсы

Атака	Описание
Сетевое сканирование и использование уязвимостей	включает нападения через открытые порты, слабые пароли, уязвимые сервисы и прочее. Преступники эксплуатируют эти слабости для взлома системы и перехвата управления
Атаки «отказа в обслуживании» (DoS) и распределенные атаки «отказа в обслуживании» (DDoS)	могут вызвать отказ в обслуживании системы, делая ее неконтролируемой
Man-in-the-middle (MITM) атаки	могут предоставить злоумышленникам возможность перехватывать и модифицировать информацию, передаваемую между беспилотным транспортным средством и сервером, влекущее за собой риск некорректного изменения направления движения или прочих неблагоприятных исходов

ТАБЛИЦА 3. Группы атак на внутреннюю сеть

Атака	Описание
Брутфорс паролей	Преступники способны применять техники перебора для взлома учетных записей, интегрированных с системой
Агрессивные действия против материальной основы инфраструктуры	Злоумышленники способны применять техники смены MAC-адресов для проникновения в систему
Инъекции SQL	Атакующие могут эксплуатировать слабости в системах баз данных, стремясь проникнуть и получить контроль над всей информацией, хранящейся в устройстве

ТАБЛИЦА 4. Группы атак на внешнюю сеть

Атака	Описание
Межсетевые атаки	Злодеи могут применять методы атаки "человек посередине" для перехвата и изменения в процессе передачи информации
Атаки на удаленный доступ	При отсутствии надежной защиты удаленного доступа к устройству, атакующие могут эксплуатировать эту уязвимость для взятия под свой контроль устройства
Атаки на панель администратора	Атакующие способны эксплуатировать пробелы в защите веб-приложений для взлома административного интерфейса, что позволяет им модифицировать настройки оборудования

ТАБЛИЦА 5. Группы атак на систему

Атака	Описание
Вредоносные программы	Преступники могут создать и интегрировать зловред в систему, с целью обеспечения дистанционного контроля над устройством
Физические атаки	Атакующие способны применять физические способы атаки для нанесения вреда компьютерному оборудованию и ОС, что в конечном итоге может вызвать утрату управления над устройством
Атаки на уязвимости	Преступники могут эксплуатировать недостатки в ОС или ПО, для вторжения в систему и ее контроля

ТАБЛИЦА 6. Типология угроз для автономных транспортных средств

Угроза	Описание
Кибератаки и взлом	Автономные транспортные средства, оснащенные сложными электронными управляющими системами, представляют собой потенциальные цели для хакерских атак. Злоумышленники способны проникать в системы этих транспортных средств, получая доступ к чувствительной информации, вмешиваться в работу систем жизнеобеспечения или даже осуществлять контроль над управлением автомобилем
Проблемы в ПО	Автономные транспортные средства функционируют на основе сложных алгоритмов и программного кода, подверженного потенциальным дефектам, способным вызвать некорректную работу системы управления и, как следствие, дорожно-транспортные происшествия
Механические неисправности	Как и в случае с любым механизмом, беспилотные транспортные средства подвержены сбоям, способным вызвать дорожно-транспортные происшествия
Несоблюдение правил дорожного движения	Многие автономные транспортные средства иногда могут нарушать правила дорожного движения без весомых оснований и демонстрировать неправильное поведение при встрече с различными дорожными условиями
Различные природные условия	Атмосферные явления вида гололед, выпадение снега, ливневые осадки представляют серьезный вызов для автономных транспортных средств, создавая потенциал для разнообразных рисков
Технические сбои	Автономные транспортные средства оснащены множеством детекторов и измерительных устройств, подверженными потенциальным неисправностям, влекущим за собой риск нарушения функционирования систем безопасности
Вмешательство людей	Интервенции человека могут нарушать функционирование автономного транспорта, порождая хаотические дорожные условия, включая неожиданные пересечения дорожного полотна из-за равнодушия или сознательного отказа предоставить преимущество беспилотному транспортному средству

Список используемых источников

1. Guan Y., Ren Y., Li S. E., Sun Q., Luo L., and Li K. Centralized cooperation for connected and automated vehicles at intersections by proximal policy optimization // IEEE Trans. Veh. Technol.. 2020. Vol. 69. № 11. PP. 12597–12608.

2. Tran V. P., Garratt M. A., Kasmarik K., and Anavatti S. G. Dynamic frontier-led swarming: Multi-robot repeated coverage in dynamic environments // IEEE/CAA J. Autom. Sinica. 2023. Vol. 10. № 3. PP. 646–661.

3 Shah S., Dey D., Lovett C., and Kapoor A. AirSim: High-fidelity visual and physical simulation for autonomous vehicles // in Proc. Field Service Robot., Berlin, Germay, 2018. PP. 621–635

4. Yang Z., Zhang Y., Yu J., Cai J., and Luo J. End-to-end multi-modal multi-task vehicle control for self-driving cars with visual perceptions // in Proc. 24th Int. Conf. Pattern Recognit. (ICPR), Aug. 2018. PP. 2289–2294.

Статья представлена научным руководителем, старшим научным сотрудником научно-исследовательского центра ВАС, кандидатом технических наук, доцентом Карповым М. А.

SECURITY OF EMBEDDED NETWORKS IN AUTONOMOUS VEHICLES USING THE TOUCAN PROTOCOL

Lukashenok V., Nikolaeva P., Taranushchenko A.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

The article examines the architecture of the network infrastructure of modern autonomous vehicles, including internal and external communication systems based on the CAN protocol. The analysis of the key components of the system is carried out: the network interface, local and global networks, as well as the software and hardware platform. Special attention is paid to cyber threats, classified by architecture levels – from the network interface to the internal and external infrastructure. Typologies of attacks are presented, including DoS, MITM, SQL injection, brute force and exploitation of software vulnerabilities, as well as physical and natural threats.

Key words: *autonomous vehicles, CAN bus, cybersecurity, TOUCAN, network architecture, cyber-attacks, MITM attacks, DoS/DDoS, SQL injections.*

УДК 004.8
ГРНТИ 20.51.19

ПРОИСХОЖДЕНИЕ УЯЗВИМОСТЕЙ И НАПРАВЛЕНИЯ АТАК В ОБЛАСТИ АВТОНОМНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

В. И. Лукашенок, П. А. Николаева, А. П. Таранущенко

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

В данной работе представлен анализ кибербезопасностных угроз, угрожающих автономным транспортным средствам (АТС) на различных уровнях – от программного обеспечения и аппаратных компонентов до процессов разработки и логистики. Особое внимание уделено уязвимостям, связанным с использованием сторонних программных библиотек, недостаточной защитой внутренних и внешних коммуникационных каналов, рискам физического доступа к бортовому оборудованию, инсайдерским угрозам и атакам на цепочку поставок. Рассмотрены конкретные сценарии эксплуатации уязвимостей, включая внедрение вредоносного кода через компоненты обработки сенсорных данных, манипуляции через CAN-шину, атаки типа man-in-the-middle в беспроводных сетях и подмену комплектующих на этапе производства. Подчеркивается, что высокая структурная сложность АТС и глубокая интеграция разнородных систем значительно увеличивают поверхность атаки. Выявленные риски требуют комплексного подхода к обеспечению безопасности на всех этапах жизненного цикла транспортного средства, включая строгий контроль внешних зависимостей, усиление протоколов аутентификации и шифрования, физическую защиту интерфейсов и повышение осведомленности персонала.

автономные транспортные средства, кибербезопасность, уязвимости ПО, сторонние библиотеки, CAN-шина, атаки man-in-the-middle, инсайдерские угрозы, безопасность коммуникаций

Эта статья охватывает анализ потенциальных угроз, которые могут быть эксплуатированы агрессорами для проведения атак на механизмы обеспечения цифровой безопасности автономных транспортных средств.

Помимо этого, дополнительные уязвимости могут появиться из-за внедрения сторонних компонентов и библиотек, допускающих ускоренную разработку ПО, но в то же время влекущих за собой риски безопасности из-за внешних зависимостей. Ошибки в этих внешних ресурсах могут стать причиной проникновения вредоносного кода в систему, как, например, через библиотеку обработки изображений. Структурная сложность автономных автомобилей, объединяющая системы как управления двигателем, так и навигации и идентификации объектов, усиливает потенциал уязвимостей. Некорректная интеграция среди разнородных компонентов может стать

причиной критических сбоев. Например, недостаток синхронизации между системой навигации и управлением может предоставить атакующему возможность перенаправления транспортного средства [1].

Автономные транспортные средства активно внедряют экстернальные программные библиотеки и платформы, что способствует более быстрому прогрессу в создании, улучшению производительности и расширению возможностей, однако это влечет за собой риски безопасности. Часто такой софт создается сторонними разработчиками, и выявленные в нем недостатки могут подвергнуть рискам всю систему. Примером может служить программа обработки визуальных данных от камер, где уязвимость может позволить вредоносным субъектам внедрить код через манипулирование входящими изображениями. Аналогичным образом, устаревшие версии компонентов, содержащие изъяны, упрощают атаки посредством известных эксплойтов. Проблематика интеграции стороннего кода может привести к ошибкам, делая поведение систем нестабильным и подверженным атакам. Например, неправильная настройка компонента обработки радарных данных может исказить определение препятствий, подвергая опасности безопасность вождения [2].

Автономные транспортные средства осуществляют коммуникацию по обширной сети, куда входят Wi-Fi, Bluetooth, 5G, протоколы V2X, Controller Area Network (CAN), Ethernet и др. Ненадежная защита этих каналов, вместе с протоколами и конфигурациями безопасности, повышает риск несанкционированного доступа, манипуляции или блокировки информации. Рассмотрим, например, CAN-шины, способствующие взаимодействию между устройствами внутри автомобиля. Их основной недостаток – отсутствие аутентификации и шифрования, что дает возможность атакующему, проникнув в систему через порт OBD-II, вносить ложные команды и контролировать основные функции, такие как торможение, управление или работу двигателя. В случае Wi-Fi, эксплуатируемого для обмена данными с облачными хранилищами или обновлениями программного обеспечения, злоумышленники могут перехватывать данные или осуществлять атаки "man-in-the-middle", целящиеся на кражу данных или подмену ПО. При использовании 5G, хоть и предлагающего улучшенную безопасность по сравнению с предшественниками, угрозы могут крыться в настройках безопасности, а также в эксплуатации протокольных или инфраструктурных уязвимостей провайдеров. Атаки на физическом уровне, такие как применение глушилок

сигнала GPS или создание помех, способны существенно мешать работе сенсоров и навигационных систем [3].

Неавторизованный физический доступ к элементам авто является значимой опасностью. Доступ к устройствам управления, датчикам и модулям связи может дать злоумышленникам возможность проникновения в системы, модификации параметров или внедрения зловредных программ. Подключившись к разъему OBD-II для диагностики авто, атакующий может изменить конфигурации, внедрить вирусы или извлечь сведения о работе машины. Манипуляции с составляющими, например, подмена оригинальных датчиков или управляющих блоков на зараженные версии, могут повлечь негативные последствия. Так, замена датчика линий дорожной разметки способна искажать информацию о маршруте или выключать защитные функции. Также, эксплуатация уязвимостей в портах, вроде USB, может служить для распространения вирусов или хищения данных. Например, через зараженный USB-накопитель злоумышленник может инфицировать автомобильную систему [4].

Инсайдерские угрозы, исходящие от персонала, ответственного за техническое обслуживание транспортных средств или обработку информации, зачастую недостаточно воспринимаются всерьез, в то время как их потенциал для нанесения урона весьма значителен. Сотрудники, обладающие правами доступа к корпоративным данным или критическим IT-инфраструктурам, могут злоупотреблять этим доступом для осуществления киберпреступлений, таких как хищение конфиденциальной информации, проведение акций саботажа или предоставление путей входа для внешних атакующих. В качестве примера, работник, имеющий доступ к информации о движении и состоянии транспортного средства, может передать эти данные как конкурентам, так и киберпреступникам. Технические ошибки, допущенные персоналом из-за неправильной конфигурации защитных систем или несоблюдения установленных процедур, могут создавать уязвимые точки в защите. Случаи недостаточной обученности персонала по вопросам кибербезопасности могут вызвать нарушения в применении защитных мер и открыть лазейки для атак. Например, работник, неосведомленный о тактике фишинговых атак, может активировать малварь, открыв компрометированный электронный документ, что делает систему уязвимой к заражению. Инсайдерские угрозы представляют более сложную задачу для выявления и нейтрализации по сравнению с внешними нападениями.

Атаки на цепочку поставок являются многоуровневой и зачастую незаметной опасностью, которая начинается задолго до момента отправки автомобиля с завода. Уязвимости могут возникнуть на любой стадии – начиная с производства комплектующих, и заканчивая логистикой и доставкой. В качестве примера, производители могут включать уязвимости в программное или аппаратное обеспечение автомобилей. Преступные группировки могут атаковать, перехватывая и подменяя оригинальные комплектующие на контрафактные или инфицированные. Одним из примеров является подмена микрочипов на производстве. Кроме того, использование логистических сетей для внедрения малвари в системы управления позволяет киберпреступникам перехватывать важные данные о доставках и использовать их во вредоносных целях. Обнаружение атак на цепочку поставок обычно усложнено использованием легитимных путей и ресурсов, что делает их особенно эффективными и затрудняет защиту от них.

Список используемых источников

1. Smith A., Dickinson J. E., Marsden G., Cherrett T., Oakey A., Grote M. Public acceptance of the use of drones for logistics: The state of play and moving towards more informed debate // Technology in Society. 2022. Vol. 68. PP. 101883. URL: https://www.sciencedirect.com/science/article/pii/S0160791X22000240 (дата обращения 10.06.2025).

2. Pham Q. V., Fang F., Ha V. N., Piran M. J., Le M., Le L. B., Hwang W. J., Ding Z. A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art // IEEE access. 2020. Vol. 8. PP. 116974-117017. URL: https://www.researchgate.net/publication/342085839_A_Survey_of_Multi-Access_Edge_Computing_in_5G_and_Beyond_Fundamentals_Technology_Integration_and_State-of-the-Art (дата обращения 10.06.2025).

3. Lee D., Hess D. J., Heldeweg M. A. Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis // Technology in Society. 2022. Vol. 71. PP. 102079. URL: https://www.sciencedirect.com/science/article/pii/S0160791X22002202 (дата обращения 10.06.2025).

4. Di X., Shi R. A survey on autonomous vehicle control in the era of mixed-autonomy: From physics-based to AI-guided driving policy learning // Transportation research part C: emerging technologies. 2020. Vol. 125. PP. 103008. URL: https://www.researchgate.net/publication/342886877_A_Survey_on_Autonomous_Vehicle_Control_in_the_Era_of_Mixed-Autonomy_From_Physics-Based_to_AI-Guided_Driving_Policy_Learning (дата обращения 10.06.2025).

Статья представлена научным руководителем, старшим научным сотрудником научно-исследовательского центра ВАС, кандидатом технических наук, доцентом Карповым М. А.

THE ORIGIN OF VULNERABILITIES AND THE DIRECTION OF ATTACKS IN THE FIELD OF AUTONOMOUS VEHICLES

Lukashenok V., Nikolaeva P., Taranushchenko A.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

This paper presents an analysis of cybersecurity threats that threaten autonomous vehicles (ATS) at various levels, from software and hardware components to development and logistics processes. Particular attention is paid to vulnerabilities related to the use of third-party software libraries, insufficient protection of internal and external communication channels, risks of physical access to on-board equipment, insider threats and supply chain attacks. Specific vulnerability exploitation scenarios are considered, including the introduction of malicious code through sensor data processing components, manipulation via the CAN bus, man-in-the-middle attacks in wireless networks and replacement of components at the production stage. It is emphasized that the high structural complexity of PBX and the deep integration of heterogeneous systems significantly increase the attack surface. The identified risks require a comprehensive approach to ensuring security at all stages of the vehicle's lifecycle, including strict control of external dependencies, enhanced authentication and encryption protocols, physical interface protection, and increased staff awareness.

Key words: *autonomous vehicles, cybersecurity, software vulnerabilities, third-party libraries, CAN bus, man-in-the-middle attacks, insider threats, communications security*

УДК 654.739
ГРНТИ 49.33.29

МОДЕЛЬ ПРЕДСТАВЛЕНЯ ДАННЫХ О КОМПЬЮТЕРНЫХ ИНЦИНДЕНТАХ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

А. В. Майоров

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

Для обнаружения угроз на основе анализа поведения пользователей и выявления анатомией необходима высококонтрастная и масштабируемая система управления базами данных. В настоящее время наболее эффективными является NoSQL (Not only SQL). Решения на основе NoSQL в целом предоставляют масштабируемый и гибкий способ решения задач, которые ранее управлялись реляционными базами данных. В статье представлено формальное описание аномалий, приведены оценки требуемого объема хранилища данных для сохранения информации на примере анализа реальных инцидентов.

угрозы информационной безопасности, аномалии поведения пользователя, NoSQL, большие данные

С ростом сложности информационных систем и изменением ландшафта угроз традиционные методы аудита [1] информационной безопасности могут оказаться недостаточными. Для построения модели представления данных об инсайдерских атаках [2] в целях обнаружения инсайдеров в компьютерных сетях рассмотрим источники собираемых данных. В качестве источников данных для аналитики поведения пользователей могут быть все клиентские устройства, подключенные как к беспроводным, так и к проводным компонентам компьютерной сети [3].

На рис. 1 приводится пример источников для сбора сведений, которыми могут выступать данные [4], передаваемые по сети, различные приложения, а также используемые устройства.

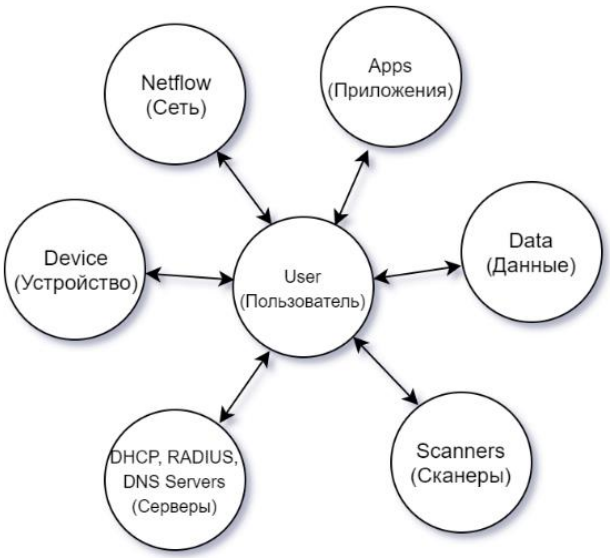


Рис. 1. Источники для сбора данных, описывающих поведение пользователя в государственных информационных системах

Формальный вид модели представления данных о компьютерных атаках [5] имеет следующий вид:

$$M = \langle A, I \rangle,$$

где: A – атрибуты поведения пользователя:

$$A = \langle DataSorce, Users, Data, Parser \rangle,$$

$DataSorce$ – источники данных:

$$Users = \langle IPFIX, Application, File, PC, Device \rangle,$$

$IPFIX$ – сетевой поток;
$Application$ – приложение;
$File$ – файл операционной системы;
PS – сканер компьютеров сети;
$Device$ – серверы и другие устройства компьютерной сети.

$Users$ – пользователи:

$$Users = U_{i=1}^{P} Users_i,$$
$$Users_i = \langle UsersID_i, Attr_i, Sessions_i \rangle,$$

$UsersID_i$ – идентификатор пользователя;
$Attr_i$ – атрибуты пользователя;
$Sessions_i$ – сессия пользователя.

Data – бинарные битовые цепочки, хранящиеся на источниках данных:

$$Data = \{0,1\}^{+}$$

$Parser$ – отображение, формирующие сессию из исходных данных в зависимости от типа источника этих данных и времени, которое можно описать как:

$$Parser: Data \times DataSource \times Time \rightarrow Sessions.$$

Модель инсайдера I описывается в виде:

$$I = \langle R, L, Q, G \rangle$$

где: R – набор признаков, по которым принимается решение об отнесении пользователя к множеству инсайдеров (регламентированный график работы, допустимая нагрузка на сеть, оценка работы с информационными ресурсами и т.п.);

L – уровни доступа, определяющие права пользователей в компьютерной сети, нарушение которых означает потенциальную инсайдерскую деятельность;

Q – квалификация инсайдера, определяющая необходимый уровень подготовки для проведения атаки (например: нарушитель с базовым (низким) потенциалом – согласно БДУ ФСТЭК – В.1**,** возможность использовать ресурсы для неправомерного доступа к информации только из общедоступных источников; нарушители с базовым повышенным уровнем (В.2) – могут использовать и модернизировать имеющиеся в свободном доступе средства реализации угроз, могут самостоятельно планировать сценарии реализации угроз; нарушитель со средними возможностями (В.3) использует профессиональные (коммерческие) для реализации угроз, приобретает информацию об уязвимостях, имеет возможности и опыт анализа программного кода; нарушитель с высоким потенциалом (В.4) – имеет доступ к исходному коду системного программного обеспечения, средства получения информации об уязвимостях нулевого дня, возможности создания и использования специальных технических средств несанкционированного получения информации;

G – вектор инсайдерской деятельности, связанный с соответствующими угрозами нарушения конфиденциальности, целостности и доступности информации.

Для хранения информации о компьютерных инцидентах [6] необходима система управления базами данных (СУБД), способная легко масшта-

бироваться и обладающая высокой скоростью обработки запросов. Для этой цели в настоящее время используются СУБД NoSQL (Not only SQL). Решения на основе NoSQL в целом предоставляют масштабируемый и гибкий способ решения задач, которые ранее управлялись реляционными базами данных.

По требованиям ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации» срок хранения данных о компьютерном инциденте установлен в три года, по требованиям к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак [7] и реагирования на компьютерные инциденты (утвержден приказом ФСБ России от 06.05.2019 N 196) предусматривают срок хранение не менее шести месяцев, международные документы, в частности Payment Card Industry Data Security Standard, предусматривают хранение данных в течении не менее одного года, из которых не менее трех месяцев должны находится в оперативном доступе.

Для государственных информационных систем в методическом документе ФСТЭК определяется срок хранения событий информационной безопасности так же определяется не менее трех месяцев.

С учетом предложенной в статье модели представления данных о компьютерных атаках [8], объем записи о компьютерном инциденте составляет 500-1000 байт. Общий объем данных о компьютерном инциденте может превышать 1 Тбайт, эффективная обработка таких объемов информации требует адекватно эффективных методов хранения информации на основе NoSQL технологий баз данных, например таких как OrientDB, которая объединяет в себе возможности документо-ориентированной и графо-ориентированной баз данных.

Список используемых источников

1. Котенко И. В., Ушаков И. А. Модели NoSQL баз данных для мониторинга кибербезопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 498-501. EDN:XSUGHB

2. Андрианов В. И., Красов А. В., Липатников В. А. Инновационное управление рисками информационной безопасности: учебное пособие. СПб.: СПбГУТ, 2012. 396 с. ISBN 978-5-91891-092-4. EDN:QSMDNH

3. Ушаков И. А., Котенко И. В., Овраменко А. Ю. и др. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 4. С. 66-71. DOI 10.46418/2079-8199_2020_4_10. EDN:HSQQIJ

4. Миняев, А. А., Красов А. В., Сахаров Д. В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29-33. DOI 10.46418/2079-8199_2020_1_5. EDN:ULHTJK

5. Kotenko I., Izrailov K., Krasov A., Ushakov I. An approach for stego-insider detection based on a hybrid nosql database // Journal of Sensor and Actuator Networks. 2021. Vol. 10. № 2. DOI 10.3390/jsan10020025. EDN:IKOMVS

6. Майоров А. В. Архитектура и программная реализация системы обнаружения компьютерных атак в корпоративных и государственных информационных системах на основе методов интеллектуального анализа // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 40-46. DOI 10.46418/2079-8199_2023_2_8. EDN:HEPDFF

7. Котенко И. В., Ушаков И. А., Пелевин Д. В., Овраменко А. Ю. Гибридная модель базы данных NoSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1(85). С. 46-54. EDN:VVQAKH

8. Майоров А. В., Красов А. В., Ушаков И. А. Модель представления Больших данных о компьютерных атаках в формате nosql // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 2. С. 47-54. DOI 10.46418/2079-8199_2023_2_9. EDN:GDZKWM

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

MODEL OF PRESENTATION OF DATA ON COMPUTER INCIDENTS OF STATE INFORMATION SYSTEMS

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

To detect threats based on user behavior analysis and anatomy detection, a highly contrasting and scalable database management system is needed. Currently, NoSQL (Not only SQL) is the most effective. NoSQL-based solutions generally provide a scalable and flexible way to solve problems that were previously managed by relational databases. The article presents a formal description of anomalies, estimates the required volume of data storage for storing information using the example of analyzing real incidents.

Key words: *Information security threats, user behavior anomalies, NoSQL, big data*

УДК 681.3
ГРНТИ 50.43.19

ТЕСТИРОВАНИЕ ИСТОЧНИКА ЭНТРОПИИ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА СВЕТОДИОДЕ

С. Ю. Михневич[1], А. Ю. Семенович[1], Тэт Н.[2]

[1] Белорусская государственная академия связи
[2] Белорусский государственный университет информатики и радиоэлектроники

Физические генераторы случайных чисел приобретают все большую популярность в связи с зависимостью случайных последовательностей, снятых с псевдослучайных генераторов от входного значения. В статье показано, что физический генератор случайных чисел на светодиоде не относится к IID источникам. Для него проведен расчет минимальной энтропии.

генератор случайных чисел, энтропия, источник случайности, тестирование

Генераторы случайных чисел (далее – ГСЧ) играют критически важную роль в современном цифровом мире. Их использование охватывает широкий спектр приложений: от криптографической защиты и аутентификации до статистического моделирования, научных симуляций и генерации тестов. В рекомендациях Национального института стандартов и технологий утверждается, что надежная генерация случайных битов является основой для построения стойких криптографических систем, особенно в условиях активного противостояния с потенциальным злоумышленником, способным воспользоваться предсказуемостью генератора для компрометации ключей и протоколов [1].

Одной из ключевых причин необходимости совершенствования ГСЧ является то, что во многих системах применяются псевдослучайные ГСЧ (далее – ПГСЧ), основанные на компьютерных алгоритмах. Они не обладают истинной энтропией, а лишь имитируют случайность. Поскольку ПГСЧ функционируют на базе детерминированных вычислений, даже при внешне равномерном распределении их выходных значений, знание начального параметра позволяет с высокой точностью воспроизводить и предсказывать всю последовательность. Это делает такие ПГСЧ уязвимыми для криптоанализа, особенно в случае плохой инициализации или предсказуемого начального состояния [2].

Кроме криптографии, где последствия уязвимостей катастрофичны, подобные недостатки отражаются и на точности численного моделирования. Даже надежные ПГСЧ могут обладать скрытыми долговременными корреляциями. В частности, хорошо известен феномен «Random numbers fall mainly in the planes», выявленный Марсальей (1968), согласно которому выходы линейных конгруэнтных генераторов могут демонстрировать кластеризацию и паттерны, что искажает статистику в многомерных симуляциях [2]. Поэтому в последнее время идет активная разработка физических генераторов случайных чисел, основанных на источниках шумов.

Как отмечается в NIST SP 800-90B, источники шума, используемые в физических ГСЧ, часто обладают способностью реагировать на внешние изменения, например, изменения температуры, напряжения или электромагнитных наводок, что может как усилить, так и ухудшить генерацию энтропии. Поэтому такие ГСЧ проектируются с учетом таких воздействий и дополняются адаптивными тестами работоспособности [1].

Надежная генерация случайных чисел предполагает не только наличие подходящего источника энтропии, но и проверку корректности, устойчивости и качества работы генератора. Методы тестирования существенно отличаются для псевдослучайных и физических ГСЧ, поскольку они различаются по природе источника случайности и характеру потенциальных отказов [2].

Физические ГСЧ зависят от непредсказуемых физических процессов (например, теплового шума, квантовых флуктуаций). Следовательно, их тестирование должно проверять не только выходные данные, но и сам физический процесс генерации [2]. В документе *NIST SP 800-90B* этому посвящен целый раздел 4, где описаны «тесты на работоспособность» (health tests), разделенные на три категории:

1. Start-up tests – выполняются при включении или перезагрузке устройства;

2. Continuous tests – постоянно отслеживают состояние источника во время работы;

3. On-demand tests – запускаются по запросу пользователя или системы.

Основная цель health tests – быстрое обнаружение сбоев или отклонений от ожидаемого поведения источника шума, таких как:

– резкое снижение энтропии;
– появление периодичности в сигнале;
– физическая неисправность схемы генерации [1].

Проверка физического процесса (или источника шума) на энтропию реализуется разными тестами в зависимости от того, можно ли отнести последовательности, сгенерированные данным источником энтропии к IID (независимым и одинаково распределенным) или нет. Это критично, так как в реальных физических источниках шум может быть зависим от температурных или электромагнитных колебаний. Тестирование на IID позволяет выявить скрытые паттерны или корреляции, которые могут искажать результат генерации. Предположение IID лежит в основе многих методов оценки энтропии, упрощая анализ случайности в последовательностях, создаваемых ГСЧ, включая те, которые используются в криптографических приложениях NIST SP 800-90B.

NIST SP 800-90B рекомендует следующий процесс для определения того, можно ли рассматривать источник энтропии как IID. Это включает:

1. Сбор данных. Собирается большая выборка необработанных выходных данных из источника энтропии – обычно не менее 1000000 бит – для обеспечения достаточного объема данных для надежного статистического анализа.

2. Тестирование. NIST определяет ряд тестов, предназначенных для обнаружения не-IID поведения, которые можно объединить в пять групп, включающие:

– Chi-square test проверяет, значительно ли отклоняется наблюдаемое распределение частот от ожидаемых вероятностей.
– Compression test оценивает, можно ли сжать последовательность. Высокая сжимаемость подразумевает избыточность и отсутствие независимости.
– Collision test измеряет, насколько часто повторяющиеся значения появляются раньше, чем статистически ожидается.
– Markov test изучает зависимости между последовательными значениями.
– Runs test обнаруживает необычно длинные последовательности одинаковых значений.

Каждый набор тестов нацелен на соответствующий аспект предположения IID. Источник, который не проходит несколько из этих тестов, скорее всего, не является IID [1].

В работе проведено тестирование последовательностей, выданных генератором случайных чисел на светодиоде [3, 4], на соответствие IID (таблица 1).

ТАБЛИЦА 1. Результаты тестирования на соответствие IID последовательностей случайных чисел

Тест	Пройден или не пройден (да/нет)
Тестирование перестановок	Да
Длина направленных пробегов	Да
Количество направленных пробегов	Да
Количество пробегов на основе медианы	Да
Длины пробегов на основе медианы	Да
Средняя статистика теста на столкновение	Да
Максимальная статистика теста на столкновение	Да
Статистика теста на периодичность	Да
Статистика теста на ковариацию	Да
Статистика теста на сжатие	Да
Проверка независимости для двоичных данных	Нет
Тестирование соответствия для двоичных данных	Да
Длина самого длинного повторяющегося подстрочного теста	Да
Количество увеличений и уменьшений	Да

Один тест исследуемые последовательности не проходят, в соответствии с рекомендациями NIST источник относится к IID, следовательно, для оценки энтропии к нему применяются тесты для IID источников. Таким образом, источник энтропии исследуемого ГСЧ является IID источником.

Оценка минимальной энтропии (min-entropy) – это оценка наименьшей возможной энтропии среди всех возможных значений, которую можно использовать в криптографии как нижнюю границу для оценки безопасности. NIST описывает более 10 методов оценки энтропии, включая:

1. The Most Common Value Estimate;
2. Collision Estimate;
3. Markov и Compression Estimate;
4. Longest Repeated Substring и MultiMMC Estimates.

Для исследуемого источника IID типа применен тест столкновений (2) для оценки его энтропии. В результате расчетов получено значение 6, 4. Идеальное значение для 8-битной системы рассчитывается по формуле 1

$$H = -log_2 2^{-8}. \quad (1)$$

Полученное значение энтропии близко к идеальному. Таким образом, источник энтропии генератора случайных чисел на светодиоде, с которого снимали последовательности, является достаточно надежным.

Список используемых источников

1. Национальный институт стандартов и технологий (NIST). Рекомендации по источникам энтропии, используемым для генерации случайных битов (SP 800-90B). Гайтерсбург: NIST, 2018. 78 с.

2. Quantum Random Number Generators / M. Herrero–Collantes, J. C. Garcia–Escartin // Reviews of Modern Physics. 2017. Vol.89. № 1. PP. 1–54.

3. Барановский О. К., Горбадей О. Ю., Зеневич А. О. Исследование возможности использования лавинных фотодиодов в режиме одноквантовой регистрации для создания квантовых генераторов случайных чисел // Приборы и техника эксперимента. 2018. № 1. С. 34–38. DOI:10.7868/S0032816218010147.

4. Асаенок М. А., Зеневич А. О., Новиков Е. В. Исследование возможности использования кремниевых фотоэлектронных умножителей для создания генераторов случайных числовых последовательностей // Известия вузов. Электроника. 2020. Т. 25, № 2. С. 114–122. DOI: 10.24151/1561-5405-2020-25-2-114-122.

TESTING THE ENTROPY SOURCE OF A LED RANDOM NUMBER GENERATOR

Mikhnevich S.,[1] Semenovich A.[1], Tet Naung[2]
[1] Belarusian State Academy of Telecommunications
[2] Belarusian State University of Informatics and Radioelectronics

Physical random number generators are becoming increasingly popular due to the dependence of random sequences taken from pseudorandom generators on the input value. The article shows that a physical LED random number generator does not belong to IID sources. The minimum entropy was calculated for it.

Key words: *Random number generator, entropy, randomness source, testing*

УДК 004.056.57
ГРНТИ 81.93.29

РАЗРАБОТКА МОДЕЛИ ДАННЫХ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ЗАШИФРОВАННОМ ТРАФИКЕ

А. В. Панков

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

Данная статья ставит своей целью рассмотреть разработку модели данных, позволяющей построить алгоритм выявления аномалий в зашифрованном трафике. Не производится расшифровка данных, то есть проверка трафика происходит в режиме реального времени. Зашифрованный трафик представляет собой особый тип задачи, так как он скрывает содержание передаваемых данных, делая традиционные методы анализа менее эффективными. В работе рассматривается способ обнаружения и борьбы с кибератаками нескольких различных типов.

локальные сети, уровень сигналов, радиочастотный спектр, абонент

Программный комплекс (рис. 1) состоит из двух частей: первой части, которая обучает модели на основе предоставленных датасетов, и второй части, которая реализует детектирование вредоносного трафика с помощью обученных первой частью моделей [1]. Такая структура ПК удобна по той причине, что она позволяет обучать, тестировать и использовать несколько вариантов моделей. Также при каждой сборке и при каждом запуске второй части ПК не обязательно каждый раз переобучать модели, достаточно предоставить ей обученную заранее модель [2].

Код внутри основного блокнота (который реализует обучение бинарной и мультиклассовой моделей) работает по следующему алгоритму:

– чтение и предобработка (удаление лишних столбцов, приведение значений к числовому виду и т.д.) основного датасета;
– если присутствуют датасеты со сгенерированными атаками, то они тоже читаются, предобрабатываются и объединяются в отдельный датасет;
– каждый тип трафика в основном датасете разделяется обучающую и тестовую выборки;
– все Web-атаки в обучающей выборке балансируются с остальными типами трафика по методу Random over sampling;

– на основе данных из основного датасета формируются объекты классов MinMaxScaler и SelectKBest – эти объекты используются для нормализации данных в выборках и для отбора наиболее важных параметров;
– обучение бинарной модели, данные размечаются по методу, который был описан в п. 3.5 для бинарной модели;
– обучение мультиклассовой модели, из обучающей выборки убираются данные о нормальном трафике, а метки изменяются по методу, который был описан в п.3. 5 для мультиклассовой модели;
– тестирование бинарной модели, данные размечаются по методу, который был описан в п. 3.5 для бинарной модели;
– тестирование мультиклассовой модели, из обучающей выборки убираются данные о нормальном трафике, а метки изменяются.

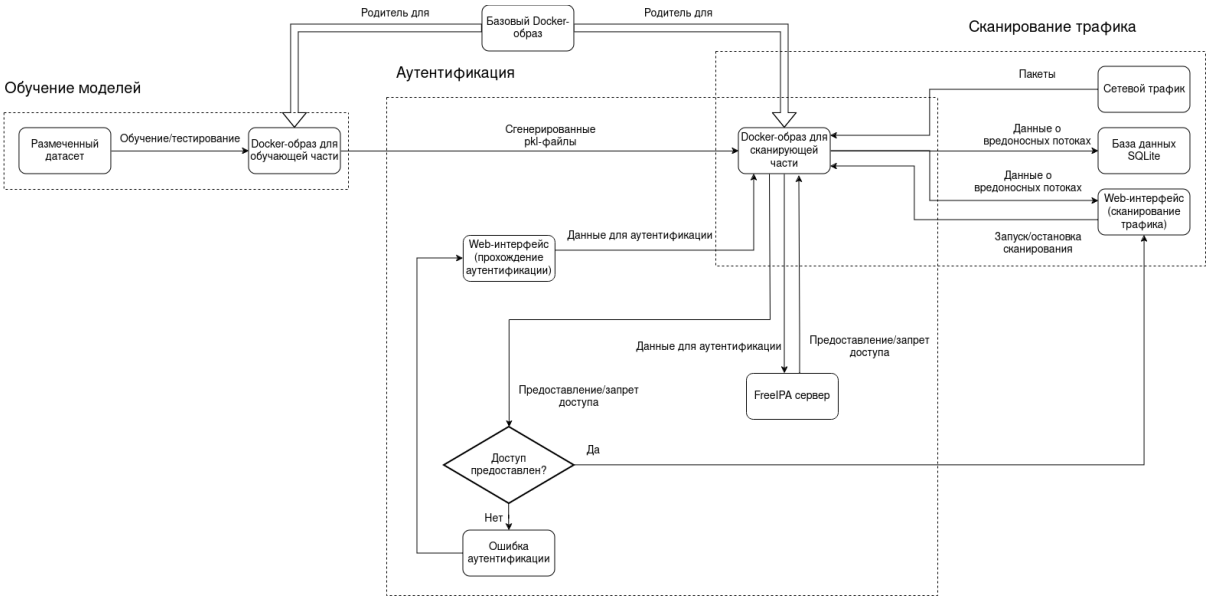


Рис. 1. Общая структура программного комплекса

Код во второй части ПК работает по следующему алгоритму:

1) запускается web-север nicegui, в котором подготавливается форма для аутентификации пользователя;

2) после того, как пользователь введет нужные данные и нажмет кнопку «Войти», содержимое страницы будет изменено на интерфейс для детектирования трафика;

3) после того, как пользователь выберет интерфейс для перехвата трафика, а также нажмет кнопку «Начать сканирование», будет запущен CICFlowMeter, который будет перехватывать и обрабатывать трафик;

4) данные о каждом потоке, которые возвращаются CICFlowMeter, в первую очередь подготавливаются к обработке бинарной моделью, т.е. идет нормализация и отбор необходимых параметров;

5) данные о потоке обрабатываются бинарной моделью, если бинарная модель распознала поток как нормальный, то его обработка продолжается дальше, в противном случае, его обработка прекращается;

6) данные о потоке передаются мультиклассовой модели, которая присваивает потоку метку – эта метка добавляется к данным о потоке;

7) данные о потоке добавляются в начало таблицы, которая выводится пользователю в веб-интерфейсе;

8) данные о потоке записываются в базу данных.

В университетской сети на базе кафедры защищенных систем связи был собран стенд из двух машин. Трафик в университетской сети состоит из нормального трафика, однако для проверки работы моделей на стенде было реализовано несколько Web-атак. На первой машине, которая была атакующей, была установлена операционная система Kali Linux. На второй машине, исполнявшей роль жертвы, была установлена операционная система Debian.

В роли атакуемого веб-приложения выступало DVWA (Damn Vulnerable Web Application). В качестве инструментов для проведения атак были выбраны следующие программы:

– OWASP ZAP – инструмент для сканирования веб-сайтов;
– jsql-injection – инструмент для поиска и эксплуатации sql-инъекций;
– xsser - инструмент для поиска и эксплуатации межсайтового скриптинга.

С помощью OWASP ZAP были проведены следующие атаки:

– Active scanning – атака с целью нахождения известных уязвимостей;
– Forced browse – брут-форс атака, предназначенная для выявления файлов, которые присутствуют на сервере и относятся к веб-приложению.

Результаты тестирования моделей представлены в таблицах. В таблице 1 представлены результаты для бинарной модели, а в таблице 2 – для мультиклассовой.

ТАБЛИЦА 1. Результаты тестирования бинарной модели

Тип трафика	Как модель распознала атаки		Как модель распознала атаки (в процентном соотношении)	
	Benign	Attack	Benign, %	Attack, %
Active scanning	96	3214	3	97
Forced browse	15	1329	1	99
SQL-инъекция	32	389	8	92
XSS	21	2530	1	99
Нормальный трафик	1193329	139889	90	10

ТАБЛИЦА 2. Результаты тестирования мультиклассовой модели

Тип трафика	Как модель распознала атаки			Как модель распознали атаки (в процентном соотношении)		
	DoS	Bot	Web	DoS, %	Bot, %	Web, %
Active scanning	1	0	3213	1	0	99
Forced browse	0	0	1329	0	0	100
SQL-инъекция	0	0	389	0	0	100
XSS	2	40	2488	0,08	1,58	98,4
Нормальный трафик, который был признан бинарной моделью как атака	9120	21704	109065	6,5	15,5	78

ПК был протестирован в реальной сетевой среде университета. В сети присутствовали обычные компьютеры, злоумышленник и жертва, Обычные компьютеры генерировали нормальный сетевой трафик, в то время как злоумышленник генерировал вредоносный трафик, проводя атаки на жертву. Злоумышленник проводил атаки, которые были перечислены в предыдущем пункте. ПК был запущен на отдельном хосте с 64 Гб ОЗУ и 16 ядрами процессора. Чтобы ПК мог получать доступ ко всем пакетам, был использован метод зеркалирования трафика с коммутатора.

При работе программного комплекса задержек не возникало. В исходный код ПК был встроен код, позволяющий замерять время, прошедшее от момента получения от CICFlowMeter данных о потоке, до момента окончания определения типа трафика. Это позволило вычислить среднее время обработки одного потока для нормального трафика – 0.0068 с и вредоносного трафика – 0.0163 с.

Время запуска программного комплекса составляет от 5 до 10 секунд. При аутентификации, выборе интерфейса для перехвата и запуске сканирования существенные задержки отсутствуют.

Заключение

1. Был разработан программный комплекс, который состоит из двух частей: первой части, которая предназначена для обучения моделей, необходимых для обнаружения и классификации вредоносного трафика, и второй части, которая реализует детектирование вредоносного трафика с помощью моделей, которые были обучены в первой части.

2. Модели протестированы в сети университета. Они показывают недостаточное качество обнаружения, если их не обучать на данных о смоделированных атаках (новых техниках).

3. В случае, если модели обучить на данных о смоделированных атаках, то они могут выдавать более хорошие результаты, чем без дообучения, даже если объем обучающих выборок был очень маленьким, однако при этом ложные срабатывания все равно будут присутствовать.

4. Проведено тестирование программного комплекса в режиме реального времени. Исследованы нефункциональные характеристики программного комплекса.

Список используемых источников

1. Mell Peter. Understanding intrusion detection systems, IS Management Handbook, 2003;409–418.

2. Liao H-J, Lin C-HR, Lin Y-C, Tung K-Y. Intrusion Detection System: A Comprehensive Review. J Netw Comput Appl. 2013; 36(1): 16–24.

Статья представлена научным руководителем, доцентом кафедры ИКС, и. о. заведующего кафедрой ИБКС СПбГУТ, кандидатом технических наук, доцентом Ушаковым И. А.

DEVELOPMENT OF A DATA MODEL FOR ANOMALY DETECTION IN ENCRYPTED TRAFFIC

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

This report aims to present the development of a data model enabling the creation of an algorithm for detecting anomalies in encrypted traffic. The approach does not involve data decryption, meaning traffic analysis occurs in real-time without compromising confidentiality. Encrypted traffic presents a unique challenge as it conceals payload content, rendering traditional analysis methods less effective. The report examines a novel methodology for detecting and mitigating various types of cyberattacks within encrypted data streams.

Key words: *cybersecurity, attack detection, machine learning, encrypted traffic.*

УДК 004.054
ГРНТИ 50.41.25

ИСПОЛЬЗОВАНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЭФФЕКТИВНОГО АНАЛИЗА СХОЖЕСТИ ТРЕЙСЕРОВ СТЕКА

А. А. Попов

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

Трассировки стека необходимы для выявления ошибок в программном обеспечении, однако ручной анализ их сходства может отнимать много времени и приводить к ошибкам. Традиционные подходы часто не обладают эффективностью, необходимой для масштабного использования, что требует автоматизированного решения.

машинное обучение, трассировка стека

Трассировки стека необходимы для выявления ошибок в программном обеспечении, однако ручной анализ их сходства может отнимать много времени и приводить к ошибкам [1]. Традиционные подходы часто не обладают эффективностью, необходимой для масштабного использования, что требует автоматизированного решения [2]. В статье предлагается подход, использующий машинное обучение, который использует как данные трассировки стека, так и показатели производительности системы для улучшения точности анализа ошибок. Предлагаемый подход не только упрощает обнаружение ошибок, но и способствует сокращению циклов разработки, предоставляя ценный инструмент для разработчиков программного обеспечения.

Методы машинного обучения стали мощными инструментами для анализа и прогнозирования поведения систем. Среди них – сиамские сети, позволяющие определять сходство между точками данных, что делает их идеальными для сравнения показателей производительности и трассировки стека. Создавая векторные представления, эти сети позволяют проводить точные сравнения, улучшая обнаружение аномалий и первопричин.

Сиамские CNN особенно хорошо подходят для анализа показателей производительности, которые часто представлены в виде временных рядов данных. Преобразуя эти данные в структуры, похожие на изображения, с помощью таких методов, как угловые поля Грамиана или рекуррентные диаграммы, CNN могут эффективно отражать пространственные иерархии. Та-

кой подход позволяет сети узнавать отличительные особенности данных, что облегчает точное измерение сходства.

Для реализации использования сиамских CNN для оценки схожести показателей производительности потребуются следующие шаги:

1. Сбор данных: сбор полного набора данных показателей производительности из различных запусков системы или экспериментов. Этот набор данных должен включать несколько экземпляров одного и того же приложения или системы в разных конфигурациях или условиях.

2. Предварительная обработка: очистка и предварительная обработка данных показателей производительности, чтобы обеспечить согласованность и удаление ненужной или избыточной информации.

3. Извлечение признаков: преобразование предварительно обработанных показателей производительности в подходящий формат для ввода в сиамскую сверточную нейронную сеть. Это может включать преобразование данных в изображения или матрицы, поскольку сиамские нейронные сети хорошо справляются с захватом пространственных шаблонов.

4. Архитектура сиамской сверточной нейронной сети: проектирование архитектуры сиамской сверточной нейронной сети с двумя идентичными подсетями. Каждая подсеть должна состоять из сверточных слоев для извлечения соответствующих признаков из данных показателей производительности. Последний слой сети должен выводить оценку сходства или метрику расстояния.

5. Обучение: обучение сиамской сверточной нейронной сети с использованием функции сравнительных потерь, которая побуждает сеть минимизировать расстояние между схожими показателями производительности и максимизировать расстояние между разнородными показателями. Использование пар показателей производительности в качестве обучающих данных с соответствующими метками, указывающими на их сходство или различие.

6. Оценка: Проверка обученной сиамской сверточной нейронной сети на отдельном наборе данных проверки, чтобы оценить ее производительность при измерении сходства между показателями производительности. Расчет оценочных показателей, такие как точность, достоверность и отзыв, для оценки эффективность модели.

Используя сиамские CNN, разработчики могут автоматически выявлять закономерности и корреляции между показателями производительности, что позволяет им принимать обоснованные решения.

Трассировки стека, представляющие последовательности вызовов функций, являются последовательными по своей природе и имеют переменную длину. Сиамские RNN, особенно те, которые используют слои LSTM или GRU, отлично справляются с обработкой таких последовательностей [3]. Поддерживая скрытое состояние, которое фиксирует контекст с течением времени, RNN могут генерировать осмысленные векторные представления, что позволяет эффективно сравнивать различные трассировки стека.

Для реализации использования сиамских RNN для оценки схожести трассировок стека потребуются следующие шаги:

1. Сбор трассировки стека: сбор набора данных трассировок стека из разных запусков выполнения или журналов ошибок.

2. Предварительная обработка: очистка и предварительная обработка трассировки стека, для удаления ненужных деталей. Стандартизация формата и размещение имен функций, чтобы создать согласованное представление.

3. Кодирование последовательности: преобразование предварительно обработанных трассировок стека в последовательности, подходящие для ввода в сиамскую RNN.

4. Архитектура сиамской RNN: проектирование архитектуры сиамской RNN с двумя идентичными подсетями, каждая из которых содержит рекуррентные слои, такие как долговременная краткосрочная память (LSTM) или управляемые рекуррентные единицы (GRU). Рекуррентные слои фиксируют последовательные зависимости в трассировках стека.

5. Обучение: обучение сиамской RNN с использованием подходящей функции потерь, такой как контрастная потеря или потеря триплета, которая побуждает сеть изучать сходство между трассировками стека.

6. Оценка: Оценка обученной сиамской RNN на отдельном наборе данных проверки, чтобы оценить ее производительность при измерении сходства трассировки стека.

Используя сиамские RNN, разработчики могут автоматически выявлять похожие трассировки стека, что позволяет ускорить отладку и анализ первопричин [1, 4].

Интеграция сиамских CNN и RNN дает несколько преимуществ. К ним относятся улучшенное обнаружение аномалий, причинный анализ, связывающий проблемы производительности с определенными путями кода. Кроме того, эти модели предоставляют масштабируемое решение, адаптируясь к растущей сложности систем и автоматизируя рутинные задачи монито-

ринга. Предлагаемая модель, оценивающая совокупность результатов схожести, полученных от сиамских CNN и сиамских RNN представлена на рисунке 1.

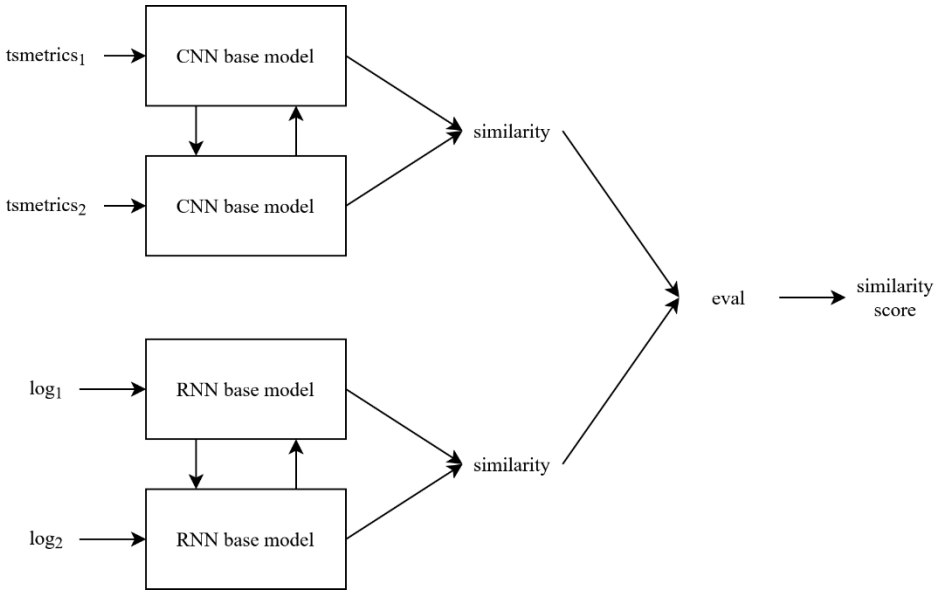


Рис. 1. Предлагаемая модель машинного обучения для определения схожести совокупности показателей производительности и трассировок стека

Анализ схожести трассировок стека при помощи машинного обучения является сложной задачей, требующей большого объема данных для анализа. Для определения эффективности данного метода требуется наличие сформированного набора данных, необходимого для проверки работы модели.

Список используемых источников

1. Yang H., Xu Y., Li Y. and Choi H.-D. K-Detector: Identifying Duplicate Crash Failures in Large-Scale Software Delivery // 2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). 2020. С. 1–6.

2. Vasiliev R., Koznov D., Chernishev G., Khvorov A., Luciv D., Povarov N. TraceSim: An Alignment Method for Computing Stack Trace Similarity // MaLTeSQuE 2020: Proceedings of the 4th ACM SIGSOFT International Workshop on Machine-Learning Techniques for Software-Quality Evaluation. 2020. С. 25–30.

3. Khvorov A., Vasiliev R., Chernishev G., Rodrigues I. M., Koznov D. and Povarov N. S3M: Siamese Stack (Trace) Similarity Measure // 2021 IEEE/ACM 18th International Conference on Mining Software Repositories (MSR). 2021. С. 266–270.

4. Rodrigues M., Aloise D. and Fernandes E. R. FaST: A linear time stack trace alignment heuristic for crash report deduplication // 2022 IEEE/ACM 19th International Conference on Mining Software Repositories (MSR). 2022. С. 549–560.

Статья представлена научным руководителем, доцентом кафедры кибербезопасности СПбГУТ, кандидатом технических наук Пестовым И. Е.

USING MACHINE LEARNING TO EFFICIENTLY ANALYZE STACK TRACER SIMILARITIES

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

Stack traces are essential for identifying and diagnosing software errors, yet manually analyzing their similarities can be time-consuming and error-prone. Traditional approaches often lack the efficiency needed for large-scale applications, necessitating a more automated solution. This article introduces a novel machine learning approach that leverages both stack trace data and system performance metrics to enhance error analysis. By integrating these inputs, the method addresses the challenge of comparing stack traces by converting them into numerical representations, such as embeddings, and incorporating performance metrics like CPU usage and response time.

Key words: *machine learning, stack trace analysis*

УДК 004.8
ГРНТИ 20.51.19

АНАЛИЗ ЭФФЕКТИВНОСТИ ШУМОВЫХ ИСКАЖЕНИЙ В ЗАЩИТЕ СВЕРТОЧНЫХНЕЙРОННЫХ СЕТЕЙ ОТ ИТЕРАТИВНОЙ СОСТЯЗАТЕЛЬНОЙ АТАКИ IGSM

В. Е. Садовников, И. Б. Саенко

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

Современные системы компьютерного зрения, основанные на сверточных нейронных сетях (CNN), демонстрируют высокую точность распознавания образов, однако остаются уязвимыми к состязательным атакам, таким как итеративный метод знака градиента (IGSM). В данной работе исследуется эффективность различных методов защиты от IGSM-атак, включая наложение гауссовского шума, JPEG-сжатие и использование автоэнкодеров (DAE, CAE, VAE). Эксперименты проводились на наборе данных STL-10 с применением CNN-модели. Результаты показали, что атака IGSM снижает точность распознавания с 90 % до 4–6 % при отсутствии защиты. Наибольшую эффективность продемонстрировали гибридные подходы, особенно комбинация сверточного автоэнкодера (CAE) и JPEG-сжатия.

состязательные атаки, IGSM, сверточные нейронные сети, устойчивость моделей, автоэнкодеры, JPEG-сжатие, методы защиты

Современные системы распознавания изображений на основе технологий машинного обучения и искусственного интеллекта находят широкое применение в различных сферах – от видеонаблюдения и автономного транспорта до медицинской диагностики и биометрической идентификации. Высокая точность распознавания, достигаемая с помощью глубоких нейронных сетей, особенно сверточных архитектур (CNN), делает их ключевым элементом интеллектуальных систем. Однако, несмотря на высокую эффективность, такие системы уязвимы к специфическим видам атак – так называемым состязательным атакам (adversarial attacks), которые представляют собой целенаправленное внесение малозаметных, но стратегически подобранных возмущений во входные данные, приводящих к ошибочной классификации [1]. Эти возмущения, как правило, незаметны для человеческого глаза, но способны кардинально изменить поведение модели. В условиях использования незащищенных каналов передачи данных, особенно в реальном времени (например, при видеосвязи), проблема уязвимости к состязательным атакам становится критически важной.

Целью данного исследования является разработка и анализ эффективности методов защиты сверточных нейронных сетей от одной из наиболее опасных итеративных атак – IGSM (Iterative Gradient Sign Method). Основная задача заключается не только в выявлении признаков атак, но и в минимизации их влияния на точность распознавания, что напрямую повышает надежность и безопасность систем компьютерного зрения.

Одной из наиболее распространенных и эффективных атак является IGSM, представляющая собой итеративное развитие метода FGSM (Fast Gradient Sign Method) [2]. В отличие от одношагового FGSM, IGSM применяет малые возмущения к изображению многократно, постепенно сдвигая его в сторону границы принятия решений модели, что делает атаку более точной и менее заметной. Математически процесс генерации состязательного примера описывается следующей формулой:

$$x_{t+1} = Clip_{x.\varepsilon}(x_t + \varepsilon * sign(\nabla_x J(\theta, x_t, y)))$$

где x_t – изображение на итерации t, ε – малый шаг изменения пикселей, $J(\theta,x_t,y)$ – функция потерь, $\nabla_x J$ – ее градиент по входным данным, а $\mathrm{Clip}_{x,\varepsilon}$ – операция ограничения, гарантирующая, что итоговое изображение остается в пределах ε окрестности исходного. Благодаря итеративному подходу, IGSM демонстрирует более высокую эффективность по сравнению с FGSM, но требует значительно больших вычислительных ресурсов [3].

В ответ на растущую угрозу состязательных атак разрабатываются различные методы защиты. В представленном исследовании рассматривается гибридный подход, объединяющий три ключевых стратегии: наложение шумов, JPEG-сжатие и нейронная очистка с использованием автоэнкодеров. Такой комбинированный подход позволяет не только подавлять атакующие возмущения, но и сохранять высокую точность распознавания.

Идея защиты с помощью шума основана на том, что состязательные возмущения имеют малую амплитуду и высокочастотную природу [4]. Наложение более интенсивного случайного шума (например, гауссовского) может «затушевать» или подавить атакующее возмущение, снижая вероятность ошибочной классификации. В исследовании использовалось наложение гауссовского шума с различными значениями стандартного отклонения σ: 0.2, 0.3 и 0.4.

Однако этот метод имеет существенный недостаток: чрезмерное усиление шума может повредить семантически значимую информацию в изображении, что приводит к снижению общей точности модели даже на чистых

данных. Эксперименты показали, что при σ = 0.4 эффективность защиты падает, так как шум начинает доминировать над полезным сигналом. Таким образом, выбор оптимального уровня шума является критически важным.

JPEG-сжатие, традиционно используемое для уменьшения размера изображений, оказалось эффективным средством защиты от состязательных атак. Дело в том, что процесс сжатия включает квантование коэффициентов дискретного косинусного преобразования (DCT), что приводит к подавлению высокочастотных компонентов – именно тех, которые чаще всего используются в состязательных возмущениях. В результате структура атаки разрушается, а визуальное качество изображения остается приемлемым.

В эксперименте исследовалось сжатие с различными уровнями качества: q = 5, q = 10 и q = 15. Результаты показали, что даже при низком качестве (q = 5) метод обеспечивает значительное повышение устойчивости модели. Наилучшие результаты были достигнуты при q=10, где баланс между подавлением шума и сохранением деталей оказался оптимальным.

Наиболее перспективным направлением защиты является использование нейронных сетей для предварительной очистки входных данных. В рамках исследования применялись три типа автоэнкодеров:

– Denoising Autoencoder (DAE) – обучен восстанавливать исходное изображение из зашумленной версии, что делает его эффективным против различных типов искажений, включая состязательные.
– Convolutional Autoencoder (CAE) – использует сверточные слои для извлечения пространственных признаков и более точно восстанавливает структуру изображения.
– Variational Autoencoder (VAE) – генеративная модель, способная восстанавливать изображения на основе вероятностного распределения, но менее точная в задачах очистки.

В качестве тестового набора данных использовался STL-10 – набор цветных изображений размером 96×96 пикселей, содержащий 10 классов объектов (автомобили, птицы, кошки и др.). Обучающая выборка включала 5000 изображений, тестовая – 8000. Для распознавания применялась сверточная нейронная сеть, обученная на чистых данных. Атака IGSM применялась к тестовой выборке, после чего оценивалась точность распознавания с применением различных методов защиты.

Точность оценивалась по формуле:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

где TP – истинно положительные, TN – истинно отрицательные, FP и FN – ошибки первого и второго рода соответственно.

Результаты экспериментов

Без защиты точность распознавания после атаки IGSM падала с ~90 % до всего 4–6 %, что подтверждает высокую эффективность атаки. Применение методов защиты в отдельности дало следующие результаты:

– DAE: точность повысилась до 39–34 %;
– CAE: до 40–36 %;
– JPEG (q=10): до 41–36 %;
– Гауссов шум (σ=0.2): до 19–18 %.

Наиболее эффективными оказались CAE и JPEG-сжатие, тогда как шум дал лишь умеренное улучшение.

При комбинации двух методов наблюдался значительный прирост эффективности. Наилучший результат показала комбинация CAE + JPEG (q = 10) – точность достигла 48–44 %. Это свидетельствует о синергетическом эффекте: автоэнкодер восстанавливает общую структуру изображения, а JPEG-сжатие удаляет остаточные высокочастотные искажения.

Однако при комбинации всех трех методов (например, DAE + JPEG + Гаусс) точность снижалась по сравнению с парными комбинациями. Это объясняется тем, что наложение шума, будучи полезным в умеренных дозах, при последовательном применении с другими методами начинает искажать уже очищенное изображение, что приводит к деградации качества. Таким образом, избыточная обработка может быть вредной.

Подводя итоги, можно сделать следующие выводы:

1. IGSM-атака чрезвычайно эффективна против незащищенных сверточных сетей, снижая точность распознавания до критически низких значений.

2. Эксперименты показали, что CAE продемонстрировал наилучшую эффективность среди автоэнкодеров, обеспечивая более высокую точность распознавания после атаки IGSM.

3. Гибридные методы защиты – наиболее перспективный путь повышения устойчивости. Комбинирование различных подходов позволяет компенсировать недостатки каждого из них.

4. Наиболее эффективной комбинацией оказалось использование нейронной очистки (CAE) в паре с JPEG-сжатием (q = 10). Такой подход

обеспечивает максимальное подавление состязательных возмущений при минимальной потере информации.

5. Наложение шума может быть полезным, но требует тонкой настройки параметров. Его применение в составе комплексной защиты может оказаться контрпродуктивным из-за накопления искажений.

6. Оптимальные параметры защиты должны определяться экспериментально для каждой задачи и архитектуры модели.

В дальнейшем перспективным направлением исследования является исследование других типов атак (например, ZOO, PGD), а также применение ансамблевых моделей, что позволит системе переключаться в режим повышенной безопасности.

Список используемых источников

1. A. Du, B. Chen, T.-J. Chin, Y. W. Law, M. Sasdelli, R. Rajasegaran, and D. Campbell, “Physical adversarial attacks on an aerial imagery object detector,” in WACV, 2022. PP. 1796–1806.

2. R. Duan, X. Ma, Y. Wang, J. Bailey, A. K. Qin, and Y. Yang, “Adversarial camouflage: Hiding physical-world attacks with natural styles,” in CVPR, 2020. PP. 1000–1008.

3. F. Nesti, G. Rossolini, S. Nair, A. Biondi, and G. Buttazzo, “Evaluating the robustness of semantic segmentation for autonomous driving against real-world adversarial patch attacks,” in WACV, 2022. PP. 2280–2289.

4. S. Casper, M. Nadeau, D. Hadfield-Menell, and G. Kreiman, “Robust feature-level adversaries are interpretability tools,” NIPS,vol. 35. PP. 33 093–33 106, 2022.

ANALYSIS OF THE EFFECTIVENESS OF NOISE DISTORTION IN PROTECTING CONVOLUTIONAL NEURAL NETWORKS FROM ITERATIVE ADVERSARIAL IGSM ATTACKS

Sadovnikov V., Saenko I.
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

Modern computer vision systems based on convolutional neural networks (CNNs) demonstrate high pattern recognition accuracy, but remain vulnerable to adversarial attacks such as the iterative Gradient Sign Method (IGSM). This paper examines the effectiveness of various methods of protection against IGSM attacks, including the imposition of Gaussian noise, JPEG compression and the use of autoencoders (DAE, CAE, VAE). The experiments were performed on the STL-10 dataset using the CNN model. The results showed that the IGSM attack reduces recognition accuracy from 90 % to 4-6 % in the absence of protection. Hybrid approaches have demonstrated the greatest effectiveness, especially the combination of convolutional autoencoder (CAE) and JPEG compression.

Key words: *adversarial attacks, IGSM, convolutional neural networks, model stability, autoencoders, JPEG compression, protection methods*

УДК 004.056
ГРНТИ 81.93.29

ВВЕДЕНИЕ НОВОГО ТЕРМИНА – «ИНТЕЛЛЕКТУАЛЬНЫЙ IDS» В ОТРАСЛИ ЗАЩИЩЕННЫХ СИСТЕМ СВЯЗИ

С. И. Штеренберг

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

В настоящей работе особое внимание придается звучащему все также по-старому, но для исследования в области «самозащиты» для систем искусственного интеллекта, по-новому термину – «Интеллектуальный IDS». Здесь стоит сразу отметить, что это не совсем должна быть система обнаружения вторжений в прямом смысле этого слова. Задача обнаруживать вторжения дается для сохранения целостности прежде всего специализированных пакетно-нейросетевых программ.

технологическая сингулярность, интеллектуальные IDS, цифровой ДНК, Индустрия 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, 2]. В живой природе основу нервной системы составляют биологические нейроны (рис. 1) – это удивительные клетки, которые можно назвать строительными блоками нашего мышления. Эти клетки работают как сложная система коммуникаций, где каждый элемент способен принимать, обрабатывать и передавать особые сигналы, используя для этого как химические, так и электрические импульсы.

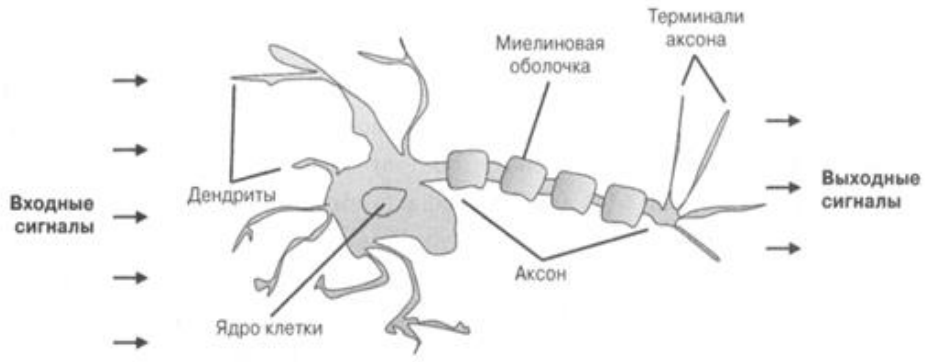


Рис. 1. Упрощенная схема биологического нейрона

Благодаря такому механизму природа создала невероятно эффективную систему обработки информации, которую ученые ежедневно пытаются воспроизвести и создать действительно мыслящий искусственный интеллект (далее – ИИ). Именно наблюдение за работой биологических нейронов вдохновило разработчиков на создание искусственных нейронных сетей – виртуальных систем, способных к обучению и адаптации. Только в искусственных моделях нейросетей в качестве нейронов выступают простейшие процессоры, а нейронные связи между ними передают данные в виде числовых значений от нейрона к нейрону (рис. 2).

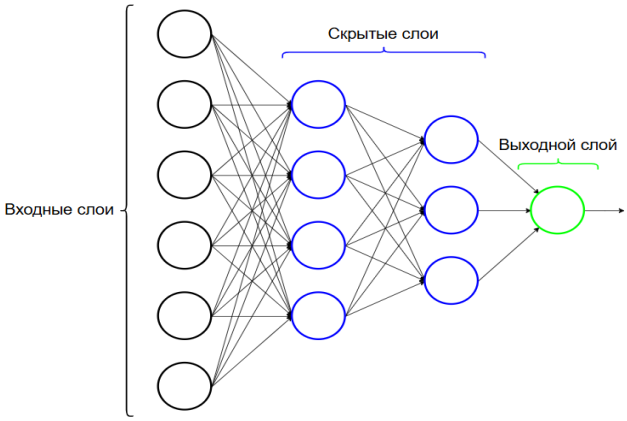


Рис. 2. Многослойная нейронная сеть

Для повышения эффективности ИИ требуется перехода к децентрализованной архитектуре на всех уровнях: от сбора данных до оптимизации разработки. Распределенная архитектура – это система, которая состоит из нескольких узлов, которые могут быть физически разделены, но соединены сетью.

Все больший отказ от использования централизованных систем обусловлен тем, что пакетно-нейросетевая программа (далее – ПНП) имеет существенные ограничения, обусловленные уязвимостью к отказам в критических узлах. Полная зависимость от центрального сервера создает риск полного выхода системы из строя при любом сбое или взломе. Это особенно опасно для критически важных систем, где требуется непрерывная работа. Для решения этих проблем требуется переход на использование систем обнаружения вторжений, где:

– данные собираются и обрабатываются распределено;
– вычисления распределяются между множеством узлов;
– оптимизация происходит на основе коллективного интеллекта;

– отказоустойчивость обеспечивается за счет дублирования функций и запараллеливания задач.

Такой подход не только повышает надежность систем искусственного интеллекта, но и улучшает их производительность за счет параллельной обработки данных и снижения рисков моментального выхода из строя.

В условиях постоянно растущих требований к ИИ, становится очевидно, что централизованная модель достигла пределов своих возможностей и использование ее в ПНП очень ограничено. Подобно тому, как городская транспортная система эволюционировала от единственной магистрали к разветвленной сети маршрутов, ИИ нуждается в переходе к более гибкой и масштабируемой архитектуре.

Основная уязвимость кроется в самой архитектуре централизованных систем: непрерывный поток информации, направляющийся к центральному узлу для обработки, создает многочисленные точки потенциального риска. Данные подвергаются возможной атаки со стороны злоумышленника как при передаче, так и в процессе хранения. Такой подход к развитию ПНП открывает множество существенных преимуществ. В первую очередь, он значительно усиливает прозрачность и конфиденциальность данных, поскольку исключает единую точку контроля и распределяет информацию по множеству узлов, что делает систему более устойчивой к взлому.

Безопасность также выходит на новый уровень благодаря интеллектуальной IDS, минимизируются риски несанкционированного доступа в систему. Особое значение приобретает стимулирование инноваций в интеллектуальный IDS. Различные компании могут эффективно сотрудничать, используя коллективный интеллектуальный потенциал и создавая адаптивные системы ИИ.

Процесс функционирования пакетных нейросетевых программ начинается с предварительной подготовки обучающих данных, которая включает в себя очистку, нормализацию и преобразование данных в формат, подходящий для обучения модели. Затем данные разделяются на небольшие группы одинакового размера – пакеты. Это позволяет каждому узлу системы обрабатывать свой пакет данных независимо от других, что способствует параллельной обработке и ускоряет обучение.

В новой методике построения новой самоорганизующейся карты интеллектуальной IDS участвует также многомерное нормальное распределение [3, 4, 5]. В нашем случае для получение общей картины выражения гауссовской смесовой схемы, используем формулу:

$$P_{(x_i,y_i)} = \sum_{j=1}^{K} z_{ij}\tau_j \frac{1}{(2\tau)^{d/2}\sqrt{|\varepsilon_j|}} exp(-\frac{1}{2}(x_i - \mu_i)^{\tau} \sum_{j}^{-1}(x_j - \mu_j)) \quad (1)$$

Потенциал развития самоорганизующейся карты раскрывается в вычислении значения:

$$Q_{(x_i,y_i)} = z\left|\sum_{i=1}^{n} ln \sum_{j=1}^{K} z_{ij}\tau_j \frac{1}{(2\tau)^{d/2}\sqrt{|\varepsilon_j|}} exp(-\frac{1}{2}(x_i - \mu_i)^{\tau} \sum_{j}^{-1}(x_j - \mu_j))|H, \Theta^t\right| \quad (2)$$

Этот процесс повторяется для всех эпох обучения, пока модель не достигнет требуемого уровня точности или не будет достигнута другая заданная цель. Количество эпох, размер пакетов и другие гиперпараметры могут настраиваться для оптимизации процесса обучения и достижения наилучших результатов [6]. Распределенная обработка дает возможность работы с большими объемами данных, поскольку разделение данных на пакеты и их распределение по узлам позволяет обрабатывать терабайты данных. Улучшение масштабируемости системы, так как при необходимости можно добавить дополнительные узлы для обработки данных. Однако функционирование ПНП в интеллектуальной IDS также сопряжено с определенными сложностями:

– необходимость синхронизации данных и моделей между узлами, что может вызвать задержки и потребовать дополнительных ресурсов;
– управление задержками и несоответствиями в сетевых соединениях, которые могут повлиять на скорость и надежность передачи данных между узлами;
– выбор оптимального размера пакета для обеспечения стабильности и эффективности обучения, так как слишком маленькие или слишком большие пакеты могут снизить производительность системы;
– обеспечение безопасности и конфиденциальности данных при передаче между узлами и хранении на них.

Чтобы интеллектуальная IDS хорошо работала с новыми данными, важно применять технику регуляризации. Это своего рода защита от переобучения – когда модель просто запоминает тренировочные примеры, и не может реагировать на них, для последующего обучения на новых данных. В общем смысле переобучение – это явление, при котором модель хорошо работает на обучающих данных, но плохо справляется с новыми, ранее не

встречавшимися примерами. Благодаря технике регуляции, модель ИИ остается гибкой и может справляться с новыми, ранее невиданными входными данными. Более широкое представление об устройстве новых типов интеллектуальных IDS, и характеристики данного термина упоминается и раскрывается в работах [7, 8, 9, 10].

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. Шумилов А. В. Анализ существующих и разработка новых программных комплексов обработки и интерпретации информации о геофизических исследованиях скважин // Вестник Пермского национального исследовательского политехнического университета. Геология. Нефтегазовое и горное дело. 2019. Т. 19. № 2. С. 162-174.

3. Самоорганизующиеся карты: [нейронное моделирование, варианты самоорганизующихся карт, физиологическая интерпретация SOM, обучающееся векторное квантование, применение самоорганизующихся карт, средства программного обеспечения для SOM] / Т. Кохонен; пер. 3-го англ. изд. В. Н. Агеева под ред. Ю. В. Тюменцева. М.: Бином. Лаб. знаний, 2008. 655 с.

4. Штеренберг С. И. Установление вектора развития интеллектуальной системы обнаружения вторжений для задач защиты искусственного интеллекта // Технологии информационного общества: Сборник трудов XVII Международной отраслевой научно-технической конференции, Москва, 02–03 марта 2023 года. М.: ООО "Издательский дом Медиа паблишер", 2023. С. 113-115. EDN:OVJIJG

5. Штеренберг С. И. Архитектура защищенной интеллектуальной системы обнаружения вторжений и инцидентов в распределенных информационных системах // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25–27 октября 2023 года. СПб.: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 321-326. EDN:IIZFPV

6. Березкин А. А. Динамическое распределение ресурсов с использованием искусственного интеллекта в спутниковых каналах связи / А. А. Березкин, Р. В. Киричек, Х. Д. Фук // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2023): Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов: в 2-х томах, Санкт-Петербург, 05–07 декабря 2023 года. СПб.: СПбГУТ, 2024. С. 234-239.

7. Свидетельство о государственной регистрации программы для ЭВМ № 2025617273 Российская Федерация. Программа взаимодействия с библиотекой AutoML для тестирования нейронных сетей на уязвимости: заявл. 10.03.2025: опубл. 25.03.2025 / С. И. Штеренберг; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна». EDN:MQFVFR

8. Свидетельство о государственной регистрации программы для ЭВМ № 2024662343 Российская Федерация. Программа автоматического машинного обучения оценки уровня безопасности моделей IDS для классификации данных: № 2024619702:

заявл. 02.05.2024: опубл. 27.05.2024 / С. И. Штеренберг; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна». EDN:CERKWP

9. Свидетельство о государственной регистрации программы для ЭВМ № 2024667615 Российская Федерация. Программа автоматического машинного обучения обнаружения атак на нейросети и определения других видов сетевых атак: № 2024666144: заявл. 15.07.2024: опубл. 26.07.2024 / С. И. Штеренберг, М. И. Муравьев; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна». EDN:BOGOJF

10. Штеренберг С. И. Метод построения архитектуры интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы / С. И. Штеренберг // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 1. С. 82-90. DOI 10.46418/2079-8199_2024_1_15. EDN:HOCHCV

INTRODUCTION OF A NEW TERM - "INTELLIGENT IDS" IN THE INDUSTRY OF SECURE COMMUNICATION SYSTEMS

Shterenberg S.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

In this paper, special attention is paid to the new term "Intelligent IDS", which still sounds the same in the old way, but for research in the field of "self-defense" for artificial intelligence systems. It should be noted right away that this is not exactly supposed to be an intrusion detection system in the literal sense of the word. The task of detecting intrusions is given to preserve the integrity of primarily specialized package neural network programs.

Key words: *Technological singularity, intelligent IDS, digital DNA, Industry 5.0, quasi-biological paradigm*

СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

УДК 004.056.5
ГРНТИ 81.93.29

О ВЫБОРЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В. А. Волостных[1], В. А. Задбоев[1], А. А. Шевченко[2]

[1]Военная академия связи имени Маршала Советского Союза С. М. Буденного
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

В статье рассматриваются вопросы выбора средств криптографической защиты информации при создании защищенных информационных систем. Актуальность темы определяется возросшим уровнем угроз безопасности информации, передаваемой по сетям общего пользования и новыми требованиями законодательства в области информационной безопасности. В силу сложности применения средств криптографической защиты для обеспечения безопасности информации конфиденциального характера, данные средства в коммерческих структурах применяются относительно редко, в силу чего опыта их применения недостаточно, чем и вызван интерес к данной теме. На основе проведенного анализа нормативной базы по организации защиты информации криптографическими средствами и опыта авторов определены основные подходы к выбору шифровальных (криптографических) средств защиты информации.

государственные информационные системы, информация конфиденциального характера, организация защиты информации, средства криптографической защиты информации, шифровальные средства, электронная подпись, эффективность работ

С развитием информационных систем и широким их применением для управления государством, коммерческими предприятиями, расширился спектр угроз безопасности информации. В настоящее время спектр и интенсивность применения угроз существенно возросла и возникла необходимость обеспечения защиты информации, передаваемой по сетям связи. Очевидно, что наиболее эффективными средствами защиты информации, передаваемой по сетям связи, являются средства криптографической защиты информации (СКЗИ). Вопросы создания СКЗИ предприятий рассмотрены в [1, 2], однако вопросы выбора СКЗИ остались за рамками данных работ, и

исходя из этого, предлагается следующий подход к их приобретению и эксплуатации.

Известно, что рынок СКЗИ в Российской Федерации весьма значителен, а учитывая, что стоимость таких средств весьма различна в зависимости от предназначения, класса защиты, варианта исполнения и других параметров, то выбор средств защиты представляет значительную сложность. Далее предлагается последовательность выбора СКЗИ для организации защиты информации, не содержащей сведений, составляющих государственную тайну.

Как известно, при приобретении любой продукции, получении услуг принято учитывать их стоимость. Поэтому предлагается исходить из эффективности приобретения и эксплуатации средств защиты информации [3]. Под эффективностью приобретения и эксплуатации средств защиты информации будем понимать соотношение их способности выполнять те функции, для которых они приобретаются к затратам на их приобретение и эксплуатацию.

На основе анализа опыта ряда государственных и коммерческих структур, создававших СКЗИ, и в соответствии с требованиями [4-6], предлагается следующее обобщенное выражение оценки эффективности (1).

$$Э_{ПР+ЭКС} = \frac{W_{СИС}+W_{ХИП}+W_{УБИ}+W_{ЗИП}}{S_{ПР}+S_{УСТ}+S_{ЭКС}+S_{ВЫВ}}, \quad (1)$$

где $Э_{ПР+ЭКС}$ – эффективность приобретения и эксплуатации СКЗИ, $W_{СИС}$ – степень соответствия возможностей СКЗИ структуре информационной системы, $W_{ХИП}$ – степень соответствия возможностей СКЗИ характеру информационных потоков, $W_{УБИ}$ – степень соответствия класса защиты информации СКЗИ актуальным угрозам безопасности информации, $W_{ЗИП}$ – соответствие уровня сложности эксплуатации СКЗИ потенциальному уровню квалификации персонала подразделения криптографической защиты информации предприятия, $S_{ПР}$ – стоимость приобретения СКЗИ, $S_{УСТ}$ – стоимость установки (монтажа, настройки и ввода в эксплуатацию) СКЗИ, $S_{ЭКС}$ – стоимость эксплуатации СКЗИ, $S_{ВЫВ}$ – стоимость вывода из эксплуатации СКЗИ.

Рассмотрим основные слагаемые эффективности приобретения и эксплуатации СКЗИ.

При оценке $W_{СИС}$ необходимо соотнести максимальное количество обслуживаемых объектов информатизации (ОИ) рассматриваемого СКЗИ к количеству ОИ и структуре предприятия, с учетом перспектив его развития.

При оценке $W_{\text{ХИП}}$ необходимо сравнить возможности СКЗИ по скорости обработки информации с информационными потоками на самом критическом направлении информационной системы предприятия.

При определении $W_{\text{УБИ}}$ необходимо:

Во-первых, определить максимальный требуемый уровень ограничения доступа к информации. Если информационная система предназначена для обработки информации, являющейся государственной тайной, то необходимо рассматривать только СКЗИ, имеющих сертификат ФСБ России, в котором указано, что данное средство предназначено для обработки сведений, составляющих государственную тайну с определенным грифом, и этот гриф должен быть не ниже грифа секретности, информации предполагаемой к обработке в информационной системе предприятия [7].

Во-вторых, необходимо определить нормативный документ, в соответствии с которым необходимо установить класс защищенности СКЗИ. Для государственной информационной системы (ГИС) необходимо руководствоваться приказом ФСБ России от 18 марта 2025 г. N 117, для иных ИС необходимо руководствоваться приказом ФСБ России от 10 июля 2014 г. N 378 [8].

Информация, содержащаяся в ГИС государственных унитарных предприятий и государственных учреждений, подлежит защите с использованием СКЗИ, если:

– законодательными и (или) иными нормативными правовыми актами Российской Федерации предусмотрена обязанность по защите информации, содержащейся в ИС, с использованием СКЗИ;
– в ИС осуществляется передача информации по каналам связи, проходящим за периметром охраняемой территории предприятия (учреждения), ограждающих конструкций охраняемого здания, охраняемой части здания, выделенного помещения;
– необходимо признание электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью;
– в ИС осуществляется хранение данных на носителях информации, предназначенных для записи, хранения и воспроизведения информации, обрабатываемой с использованием средств вычислительной техники, несанкционированный доступ к которым со стороны третьих лиц не может быть исключен с помощью некриптографических методов и способов.

Для обеспечения защиты информации, содержащейся в ИС, должны использоваться СКЗИ соответствующего класса от уровня значимости, обрабатываемой в ИС в соответствии с Требованиями [4-6], и сертифицированные ФСБ России с последующим обоснованием в модели угроз безопасности информации, техническом проекте и техническом задании на создание (развитие) ИС.

В документах определяется состав и содержание организационных и технических мер по обеспечению безопасности персональных данных (ПДн) при их обработке в ИС ПДн с использованием СКЗИ, необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности.

При создании СКЗИ формируется совокупность предположений о возможностях, которые могут использоваться источником угроз при создании способов, подготовки и проведении атак.

Таким образом, на основе вышесказанного, определяется класс СКЗИ, который может быть от КС1 до КА.

Следующим этапом оценки варианта приобретения СКЗИ являются экономические оценки. Очевидно, что стоимость приобретения СКЗИ, как правило, зависит от региона, политики дилеров и объема закупок, что проблем расчетов не вызывает.

Стоимость установки (монтажа, настройки и ввода в эксплуатацию) СКЗИ $S_{\text{УСТ}}$ определяется способом установки:

а) с привлечением специалистов сторонних организаций (самый оптимальный вариант привлечение специалистов предприятия-изготовителя);

б) установка СКЗИ персоналом предприятия. Кроме того, необходимо учитывать стоимость аттестации ИС, после оснащения ее СКЗИ [9].

Очевидно, что, как и вариант а) так и вариант б) имеют свои плюсы и минусы.

Стоимость эксплуатации СКЗИ $S_{\text{ЭКС}}$ включает:

а) изготовление ключей и их смену;

б) оплату труда персонала подразделения криптографической защиты;

в) расходы на послегарантийный ремонт.

Стоимость вывода из эксплуатации СКЗИ $S_{\text{ВЫВ}}$ включает расходы на утилизацию шифратора (если он подлежит уничтожению в соответствии с документацией на СКЗИ), стоимость архивирования документированной информации, если она зашифрована СКЗИ, стоимость накладных расходов на оформление процедуры вывода из эксплуатации СКЗИ.

Кроме того, иногда при приобретении средств защиты учитывают предполагаемый срок эксплуатации средств защиты, что определяется как техническими параметрами, так и сроком действия сертификатов и перспективами их продления.

Таким образом при оценке эффективности работ по созданию подсистемы криптографической защиты необходимо выбирать СКЗИ с минимально необходимыми параметрами, чтобы они соответствовали требованиям нормативных документов, но чрезмерно не увеличивали их стоимость. Целесообразно сформировать ряд вариантов работ, оценить их эффективность и на основании таких оценок принимать решение о создании подсистемы криптографической защиты ИС организации, учреждения, предприятия.

Данные материалы распространяются на основные типы СКЗИ, включая средства электронной подписи, которые также относятся к криптографическим средствам [10].

Список используемых источников

1. Викулова А. Ю., Волостных В. А., Кононов П. А., Парфиров В. А. Защита персональных данных территориально-распределенных предприятий // 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. 155-160.

2. Волостных В. А., Воробьев П. А., Задбоев В. А. Организация защиты конфиденциальной информации на предприятии средствами криптографической защиты // Перспективы безопасности-2024. Сб. материалов II научно-технической конференции, посвященной информационной безопасности. СПб., 2024. С. 9-13.

3. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

4. Волостных В. А., Парфиров В. А., Петров А. В. Оценка эффективности электронного документооборота организации // Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сб. статей II Всероссийской научно-технической конференции. Федеральное государственное автономное учреждение «Военный инновационный технополис «ЭРА». Анапа, 2020. С. 414-421.

5. Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

6. Приказ ФСБ России от 18 марта 2025 г. N 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

7. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие

требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

8. Волостных В. А. Глава 3. Нормативная правовая база Российской Федерации обеспечения информационной безопасности. В книге: Технологии защиты информации в условиях кибернетического противоборства. Костарев С. В., Карганов В. В., Липатников В. А. Санкт-Петербург, 2020, С. 94-158.

9. Липатников В. А., Шевченко А. А., Мелехов К. В., Ткачев Д. Ф. Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках // Информационно-управляющие системы. 2024. № 1(128). С. 44-55.

10. Шевченко А. А. Модель процесса несанкционированного воздействия нарушителем на информационно-телекоммуникационную сеть // Инновационная деятельность в Вооруженных Силах Российской Федерации: тр. всеарм. науч.-практ. конф. СПб.: Военная академия связи им. Маршала Советского Союза С. М. Буденного, 2019. С. 158-166.

ON THE CHOICE OF MEANS OF CRYPTOGRAPHIC PROTECTION OF INFORMATION

Volostnykh V., Zadboev V., Shevchenko A.
[1]Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article considers the issues of choosing means of cryptographic protection of information when creating secure information systems. The relevance of the topic is determined by the increased level of threats to the security of information transmitted over public networks and new requirements of legislation in the field of information security. Due to the complexity of using cryptographic protection tools to ensure the security of confidential information, these tools are used relatively rarely in commercial structures, due to which there is insufficient experience in their use, which is what caused the interest in this topic. Based on the analysis of the regulatory framework for organizing information protection by cryptographic tools and the experience of the authors, the main approaches to the selection of encryption (cryptographic) means of information protection are determined.

Key words: *government information systems, confidential information, information security organization, cryptographic information security tools, encryption tools, electronic signature, work efficiency*

УДК 355.233.23
ГРНТИ 78.25.33

ПРЕЛАГАЕМЫЕ ДОПОЛНЕНИЯ К ПРОГРАММЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО СПЕЦИАЛЬНОЙ СВЯЗИ В ВОЕННОМ УЧЕБНОМ ЦЕНТРЕ С УЧЕТОМ ОПЫТА ПРОВЕДЕНИЯ СВО

В. А. Гриднев, А. К. Сагдеев

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

В статье предлагается курс дополнительной подготовки к существующей программе обучения специалистов по специальной связи в военном учебном центре, в котором учтен опыт применения средств связи в ходе проведения специальной военной операции. Появление новой техники и средств связи в войсках привело к необходимости подготовки специалистов с требуемыми компетенциями, обеспечивающими уверенную эксплуатацию новых средств и техники связи в войсках. Целью дополнительного курса подготовки выпускников является формирования и закрепление у студентов компетенций по применению новых средств связи в условиях боевых действий. Предлагаемый дополнительный курс к программе подготовки специалистов по специальной связи в военном учебном центре с учетом опыта проведения специальной военной операции может быть полезен педагогическому и руководящему составу ВУЦ.

предлагаемые дополнения к программе подготовки специалистов в области телекоммуникационных технологий, формирование расширенных компетенций у выпускников военного учебного центра с учетом опыта специальной военной операции

Проблема подготовки специалистов по специальной связи в современных условиях является крайне актуальной в связи с проведением специальной военной операции (СВО).

В настоящее время 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].

Проведение СВО позволило вскрыть недостатки в существующей организации и обеспечении связи в боевых условиях и на практике понять, что необходим пересмотр и доработка отдельных положений по применению средств связи в новых условиях. Разработанные и внедренные накануне проведения СВО средства и техника связи оказались не совсем пригодными к использованию из-за громоздкости и явной заметности для средств разведки

и поражения противника. Большие размеры антенно-мачтовых устройств и транспортных средств демаскируют узлы связи, а соответственно и пункты управления, снижают мобильность войск связи и надежность управления войсками и оружием. Под них сложнее выкопать капониры, чтобы полностью защитить и замаскировать аппаратные от средств разведки и огня. Средства радиосвязи легко обнаруживаются средствами радиоэлектронной борьбы противника, что ведет к уничтожению узлов связи и нарушению управления. Все эти проблемы поставили вопрос по пересмотру подходов в организации связи и применении техники связи.

Учитывая новую практику организации связи и применения средств (техники) связи в условиях боевых действий, необходимо обеспечить внесение изменений в программы подготовки специалистов по специальной связи.

Для решения выявленных проблем необходимо на основе имеющихся программ подготовки специалистов по специальной связи сформировать курс дополнительных занятий для студентов выпускного курса военного учебного центра (ВУЦ). Целью этого курса должна быть дополнительная подготовка выпускников по организации и обеспечению связи с учетом опыта проведения СВО. Такой дополнительный курс подготовки расширит компетенции у студентов выпускных курсов и позволит сформировать навыки необходимые для обеспечения связи в боевых условиях [2].

В ходе дополнительного курса подготовки занятия с выпускниками планируется проводить в часы самостоятельной работы и дополнительное время, которое должно формироваться и указываться в отдельном плане по дополнительной подготовке выпускников.

Такой курс дополнительной подготовки со студентами выпускных групп в ВУЦ уже проводится на кафедре проводной электросвязи. Занятия позволяют изучить порядок применения новых средств связи, которые ранее не изучались в рамках программы подготовки выпускников по причине их отсутствия на кафедре и сформировать необходимые компетенции по применению этих средств связи. Новые средства связи зарекомендовали себя в основном хорошо и имеют много достоинств [3].

Достоинством новых средств связи являются:

– малые габариты и вес (позволяют легко маскировать и размещать их в защитных сооружениях, что обеспечивает живучесть средств связи от воздействия средств поражения);

– узкая диаграмма направленности антенн (оказывает влияние на повышение дальности связи, снижает потребляемую мощность и радио заметность их для средств пеленгации противника);
– низкая потребляемая мощность;
– мобильность применения новых средств связи (оперативность развертывания и перемещения их в случае необходимости);
– быстрое вхождение в связь с корреспондентом (быстрый набор связей, настроек и обеспечение большого количества каналов);
– маскированные и закрытые режимы работы (незаметность или полная защита переговоров от доступа к информации противника);
– возможностей построения обходных путей прохождения информации (настройка адресов корреспондента и запасных путей обхода информации в случае выхода из строя основных транзитных пунктов передачи информации);
– обмен большими потоками данных между разными узлами связи.

Однако на ряду с достоинствами новых средств связи имеются и недостатки:

– малая емкость аккумуляторных батарей, что требует их замены один раз в сутки (что демаскирует размещенные на местности замаскированные средства связи);
– заметность для средств пеленгации противника источников сигналов от работающих средств связи (что может привести к их уничтожению);

Все перечисленные достоинства новых средств связи в комплексе обеспечивают устойчивую, надежную и бесперебойную связь, снижают их заметность для средств разведки противника (снижают возможность перехвата информации и обнаружения). Что в целом повышает живучесть системы управления войсками и оружием.

Использование различных средств связи, как радио, так и инфокоммуникационных, позволяют создать дополнительные каналы связи и обеспечить разветвленность сети связи и ее многоканальность, что в свою очередь повышает возможности и надежность системы связи.

Поэтому, дополнительная подготовка со специалистами разных специальностей (радио, радиорелейных, спутниковых средств связи и средств инфокоммуникаций) обеспечивает расширение их компетенций, так как все подразделения связи в войсках используют вышеуказанные средства связи комплексно и соответственно каждый выпускник должен ими владеть в полной мере уверенно и без затруднений осваивать новые образцы.

Контроль за эффективностью и качеством дополнительной подготовки выпускников с точки зрения системности обеспечивают отзывы из войск от самих же выпускников, которые служат в войсках и от их командиров. Эти отзывы являются обратной связью, которая позволяет оперативно решать проблемы в режиме личного общения.

Обратная связь с войсками позволяет подтвердить необходимость и эффективность курса дополнительной подготовки. По времени освоения выпускниками первичных должностей (вхождения в курс дел на местах службы) можно судить о правильности выбранного дополнительного курса занятий. Обратная связь осуществляется через личные контакты в социальных сетях. Благодаря такому общению выпускники рассказывают о проблемах на местах службы и одновременно получают необходимую им информационную поддержку от преподавателей кафедры проводной электросвязи. В свою очередь, у преподавателей появляется информация о том, на что необходимо обратить внимание в первую очередь при подготовке очередных выпускников ВУЦ и какие изменения внести в программы подготовки студентов специалитета. Информационная поддержка кафедры, которую используют выпускники, проходящие службу в войсках и на СВО, помогает им расширить их возможности по организации и обеспечению связи, что в целом положительно влияет и на имидж ВУЦ в войсках [4].

Таким образом, дополнительная подготовка выпускников в ВУЦ помогает не только формировать и развивать профессионально важные качества у студентов в ходе процесса их обучения и воспитания в ВУЦ, но и расширяет их профессиональные компетенции, что оказывает эффективное влияние на качество подготовки специалистов по специальной связи. А обратная связь с выпускниками ВУЦ через личные контакты и отзывы командиров частей позволяет оценить уровень подготовки выпускников и эффективность программы обучения, внести необходимые корректировки в тематические планы и обеспечить информационную поддержку студентам в войсках, что положительно влияет качество подготовки студентов специалитета и имидж ВУЦ в войсках.

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 т. СПб.: СПбГУТ, 2023. С. 527–532.

2. Тишков В. В., Лукьянчик В. Г., Лукьянчик В. Н. Обоснование облика построения перспективных комплексов и средств связи на основе опыта организации связи при проведении специальной военной операции // Военная мысль. 2023. № 9.

3. Груздев Д. А., Музыкантов А. Н., Сагдеев А. К. Организация воспитательного процесса в ходе обучения в ВУЦ // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XI Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. Т. 4. С. 259-263.

4. Кощеев А. В., Лашин Ю. Ф., Сагдеев А. К., Халепа С. Л. Предложения по оптимизации системы связи специального назначения и организационно-штатной структуры подразделений связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. X Юбилейная Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2021. Т. 4. 551 с. С. 96-101.

PROPOSED ADDITIONS TO THE PROGRAM OF SPECIAL COMMUNICATION SPECIALISTS TRAINING AT THE MILITARY EDUCATIONAL CENTER, TAKING INTO ACCOUNT THE EXPERIENCE OF CONDUCTING

Gridnev V., Sagdeev A.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article offers a course of additional training to the existing training program for special communications specialists at the military training center, which takes into account the experience of using communications equipment during a special military operation. The emergence of new equipment and communications equipment in the military has led to the need to train specialists with the required competencies to ensure the safe operation of new communications equipment in the military. The purpose of the additional graduate training course is to form and consolidate students' competencies in the use of new means of communication in combat conditions. The proposed additional course to the training program for special communications specialists at the military training center, taking into account the experience of conducting a special military operation, may be useful to the teaching and management staff of the University.

Key words: *The proposed additions to the training program for specialists in the field of telecommunications technologies, the formation of expanded competencies for graduates of the military training center, taking into account the experience of a special military operation*

УДК 378.4.
ГРНТИ 14.35.07

ВЛИЯНИЕ КАЧЕСТВА УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ НА МОТИВАЦИЮ К ЗАНЯТИЯМ ФИЗИЧЕСКОЙ КУЛЬТУРОЙ У СТУДЕНТОВ ВОЕННОГО УЧЕБНОГО ЦЕНТРА ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА

Т. А. Иваненко

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

Статья посвящена актуализации проблемы повышения мотивации к занятиям физической культурой у студентов военного учебного центра. Проведен сравнительный анализ по формированию мотивов к занятиям физической культурой у категории обучающихся СПбГУТ и военного учебного центра технического университета. Определено, что качество учебно-методического обеспечения процесса обучения студентов влияет на формирование мотивов к занятиям физической культурой.

качество, учебно-методическое обеспечение, мотивы, мотивация, физическая культура, студенты ВУЦ

Главной задачей современного высшего профессионального образования является качество подготовки специалиста, реализация которого напрямую зависит от учебно-методического обеспечения (УМО) образовательного процесса, регламентируется требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) и Федеральным законом от 29.12.2012 г. № 273-ФЗ [1].

Определяющим фактором реализации данной задачи является соответствие качества образования потребностям личности, общества и государства [2].

Образовательная программа во всех учебных заведениях направлена на развитие как умственных способностей обучающихся, так и совершенствование физических качеств, способствующих улучшению физического здоровья студентов [3].

На сегодняшний день наблюдается снижение мотивации заниматься физической культурой и спортом (ФКиС) среди молодежи [4].

В связи с этим, проблема исследования мотивов и факторов их формирования, направленных на повышение мотивации студентов к занятиям ФКиС, по-прежнему является актуальной.

Цель исследования: поиск путей и перспективных направлений повышения мотивации студентов военного учебного центра (ВУЦ) к занятиям физической культурой (ФК).

Объект исследования – образовательный процесс студентов технического университета.

Предмет исследования – формирование мотивов у студентов ВУЦ к занятиям ФК.

Гипотеза исследования. Процесс формирования мотивов к занятиям ФК у студентов ВУЦ будет эффективным, если: в процессе обучения будут выявлены факторы, ориентированные на овладение системой знаний и умений в области физкультурной деятельности, повышение мотивации к занятиям ФК в техническом университете.

Исходя из цели и гипотезы, ставились задачи:

1. Дать характеристику понятий «мотивация», «мотив».

2. Выявить факторы и мотивы, способствующие повышению мотивации к занятиям ФКиС у студентов технического университета.

3. Исследовать характер влияния качества УМО процесса обучения на формирование мотивов к занятиям ФК у студентов ВУЦ.

Методы исследования: анкетирование, анализ сформированности мотивов к занятиям ФК в процессе обучения студентов в техническом университете.

База исследования. Выборку составили обучающиеся 1–5 курсов, в количестве 78 человек, из них: студенты СПбГУТ – 47 чел.; студенты ВУЦ – 31 чел.

В научных исследованиях учеными нередко поднимался вопрос мотивации и мотивов к занятиям физической культурой, их положительного влияния на здоровье студентов, поиска факторов и методов, направленных на повышение интереса к ним в процессе обучения в вузе [3, 4, 5].

В научных трудах сущность понятия «мотивация» раскрывается исследователями, как побуждение человека к действию, представляющих собой комплекс мер для достижения поставленной цели, как процесс, в результате которого приобретается личностный смысл, создается устойчивый интерес в потребности личности к занятиям ФК [4, 6, 7, 8].

«Мотив» побуждает человека осуществлять осознанные активные действия в достижение цели, приводит к желаемому результату, под воздействием условий, факторов, интересов и потребностей личности [9].

Рассматривая мотивы, как осознанную активность человека, их подразделяют на: процессуальные, реализуемые в процессе занятий и результативные, направленные на результат деятельности, достигнуть которые возможно систематизацией занятий ФК, под воздействием определенных факторов [10].

Как отмечают ученые (Герасимов И. В., Кельдасов Т. Д., 2020; Бабичев А. М., Ивченко Н. В., Шарухин А. П., 2025) на мотивацию к занятиям влияют множество факторов, таких как [11, 12]:

– постановка реально достижимой цели, способствующей улучшению личных показателей, ориентированной на конечный результат;
– подбор регулярного графика занятий, приносящий положительный результат;
– мотивы, способствующие выработки устойчивой привычки и др.

Таким образом, активация физической деятельности обучающихся и мотивация к занятиям ФК, в процессе обучения в вузе, направлены на достижение их работоспособности, формирование оптимального уровня физической подготовленности и устойчивого интереса к занятиям ФК, достижение поставленной цели в совокупности личных потребностей.

Изучив понятия «мотивация», «мотивы», побуждающие к физической активности студентов в процессе обучения в вузе, повышения заинтересованности, можно предположить изменение уровня их активности и мотивации к занятиям ФК. Учитывая исходные мотивы, можно корректировать временные мотивы получения результата и формировать устойчивые мотивы к занятиям ФК.

Определяя потребности студентов к занятиям ФК в вузе, следует создавать соответствующие условия и определять факторы, способствующие формированию нравственного поведения, ценностной ориентации, мотивации обучающихся к занятиям ФК, росту личных достижений.

Таким образом, поиск путей формирования учебно-познавательных мотивов и мотивации к занятиям ФК, решается через изменение качества УМО процесса обучения студентов.

С целью определения влияния УМО процесса обучения физической культурой на формирование мотивации студентов к занятиям ФК, было проведено исследование, в ходе которого решались задачи:

– определить факторы влияния на формирование мотивов;
– выявить сформированность мотивов к занятиям ФК у студентов вуза;
– определить мотивацию студентов к занятиям ФК.

Учебные занятия физической культурой ведутся с первых дней обучения студентов в вузе, в связи с чем встает вопрос приобщения студентов к системным занятиям на начальном этапе обучения и мотивации их к занятиям ФК в процессе дальнейшего обучения в вузе.

Уже на первых этапах обучения у обучающихся появляется возможность улучшить показатели оценки уровня физической подготовленности. Получив необходимые теоретические знания, после лекционного курса по дисциплине «Физическая культура и спорт» («ФКиС»), студентам следует сконцентрировать внимание на выполнении заданий для самостоятельной практической подготовки, которые способны компенсировать недостаточность отводимого количества часов практических занятий ФК в сетке расписания, что позволит постепенно наращивать тренировочные нагрузки, влиять на повышения уровня физической подготовленности.

Таким образом, формирование мотивов и мотивации студентов к систематическим самостоятельным занятиям, позволит повлиять на изменение их образовательного потенциала, приобрести достаточный уровень физической подготовленности, обогатиться необходимыми знаниями, умениями и навыками и приобрести необходимые компетенции.

Реализация качества УМО процесса обучения в удовлетворении потребностей студентов может способствовать формированию мотивов и устойчивой мотивации к системным занятиям ФК, в процессе всего периода их обучения.

С целью изучения потребностей обучающихся, повышения мотивации к занятиям ФК, был проведен социологический опрос. В качестве основного метода использовалось анкетирование методом случайного отбора.

В анкетирование приняли участие 78 респондентов, из которых были выделены студенты СПбГУТ (47 чел.), из них: 16 чел. – 1 курса, 31 чел. – 2 курса; студенты ВУЦ СПбГУТ (31 чел.), из них: 2 чел. – 2 курса, 8 чел. – 4 курса, 21 чел. – 5 курса.

На мотивацию студентов к занятиям физической культурой повлияло множество факторов и мотивов, из которых хочется отметить несколько основных, ее повышающих.

Влияние полученных знаний на мотивацию обучающихся к занятиям ФК, выявлялось с помощью вопроса: «Является ли полезным, прослушанный курс лекций по теоретическому разделу дисциплины «ФКиС» при занятиях ФК?» (рис. 1).

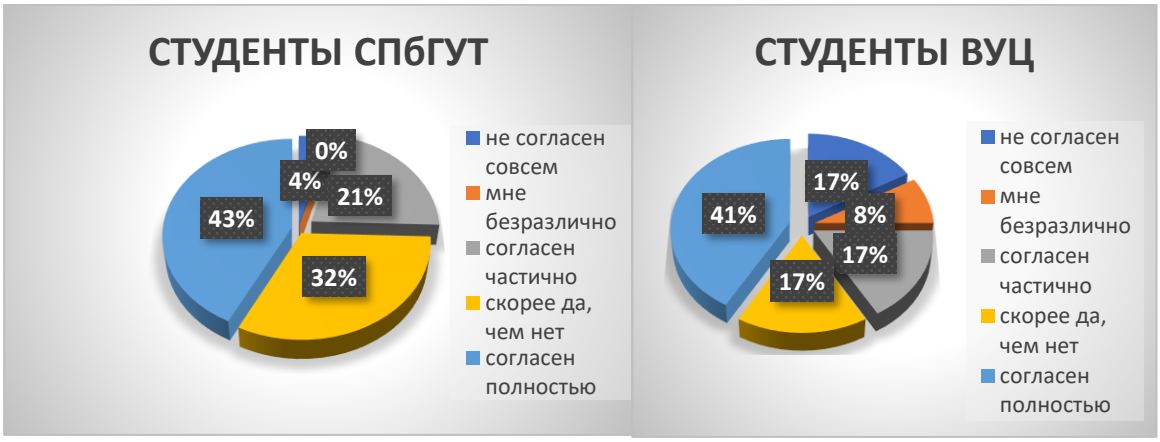


Рис. 1. Сравнительный анализ фактора влияния по освоению теоретического раздела дисциплины «ФКиС», на формирование мотива готовности студентов к занятиям ФК

Анализ результатов тестирования по категории данного вопроса показал адекватное оценивание студентами полезности пройденного курса теоретического раздела дисциплины «ФКиС», как у обучающихся СПбГУТ (43 % респондентов ответили «согласен полностью» и 32 % – «скорее да, чем нет»), так и у студентов ВУЦ (41 % и 17 %) соответственно (рис.1), что свидетельствует о допустимом уровне ее сформированности (более 50 %, положительных ответов), а так же указывает на необходимость привлечения дополнительных ресурсов, с использованием современных технологий, преподавателями кафедры ФК и контроля за проведением занятий лекционного цикла по дисциплине «ФКиС», в целях улучшения качества проведения занятий и повышения интереса обучающихся к занятиям ФК.

Сформированность мотивов у студентов вуза, к посещению практических занятий ФК, выявлялась с помощью вопроса: «Удовлетворяют ли Вас практические занятия ФК в вузе?» (рис. 2).

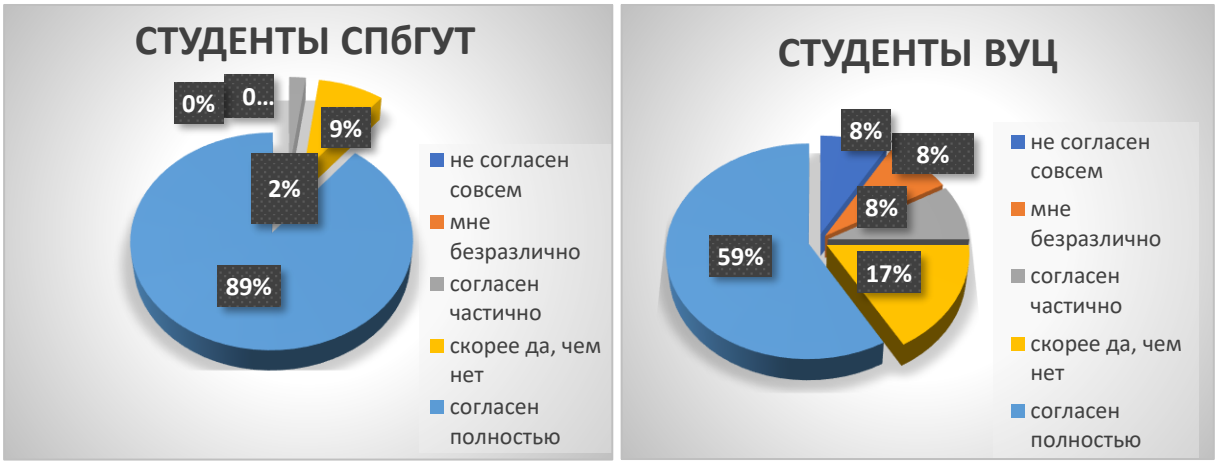


Рис. 2. Сравнительный анализ формирования мотивации у студентов к занятиям ФК

Проведенный анализ данных результатов тестирования, указывающего на степень удовлетворенности занятиями ФК в вузе, и сформированность мотивов у обучающихся в процессе реализации практической деятельности, выявили следующее: у обучающихся СПбГУТ – 89 % респондентов ответили «согласен полностью» и 9 % – «скорее да, чем нет», у студентов ВУЦ – 59 % и 17 %, соответственно (рис. 2), что свидетельствует об их ценностных ориентирах и стойкой мотивации обучающихся к занятиям ФК.

Разница в показателях по данной категории вопроса указывает на осуществляемые подходы в расстановке приоритетов у студентов ВУЦ, направленные на самосовершенствование и ориентированного на решение профессиональных задач, поставленных перед выпускниками – системной физической подготовленности в дальнейшей профессиональной деятельности.

Влияние фактора влияния качества УМО процесса обучения на мотивацию студентов к занятиям ФК выявлялось с помощью вопроса: «Готовы ли Вы использовать свое свободное время для самостоятельных занятий ФКиС?» (рис. 3).

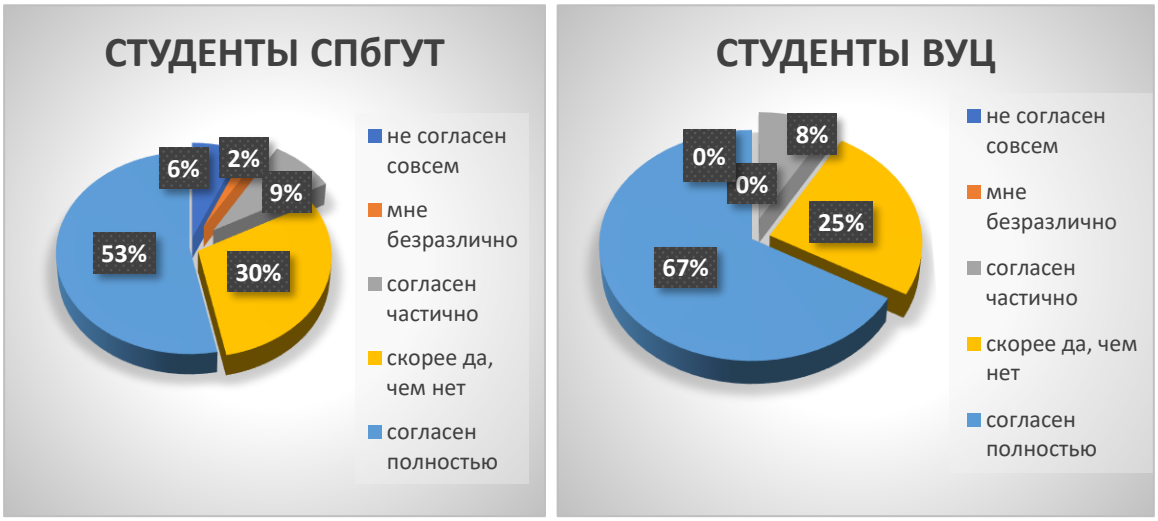


Рис. 3. Сравнительный анализ влияния качества УМО на повышение мотивации к занятиям ФК студентов СПбГУТ и ВУЦ

Анализ результатов опроса по выявлению влияния УМО процесса обучения на мотивацию к занятиям ФК показал, что 67 % респондентов из числа студентов ВУЦ СПбГУТ проявили готовность использовать свое свободное время для занятий ФКиС, против 53 % – у обучающихся СПбГУТ (рис. 3), что свидетельствует о допустимом качестве УМО процесса обучения, его проявлении на сформированность мотивов.

Показатели к готовности использования личного свободного времени обучающимися для занятий ФК следующие: 6 % «не согласен совсем», 2 %

«мне безразлично» – ответили обучающихся СПбГУТ и полная готовность – у студентов ВУЦ, что указывает на их стойкую мотивацию к дальнейшей систематизации самостоятельных занятий ФК в процессе всего обучения в вузе и приоритетах к достижению физической готовности по роду дальнейшей профессиональной деятельности.

Таким образом, можно сделать вывод, что качество УМО процесса обучения влияет на формирование мотивов, повышение мотивации у студентов к занятиям физической культурой, способствует самостоятельной деятельности, самосовершенствованию и их самореализации в области ФКиС.

Список используемых источников

1. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 г. № 273-ФЗ (ред. от 29.07.2017).

2. Королев Е. В., Беспалов А. Е., Агафонова В. В. Учебно-методическое обеспечение образовательных программ // Строительство: наука и образование. 2018. Т. 8. № 3 (29). С. 67–78.

3. Кирсанова А. А., Яткин И. В. Формирование мотивации к занятиям физической культурой у студентов. // Молодой ученый. 2025. № 16 (567). С. 326–328. URL: https://moluch.ru/archive/567/124196/ (дата обращения: 28.06.2025).

4. Кашина А. В., Патрикеев Г. В. Формирование мотивации к занятиям физической культурой и спортом у школьников // Материалы X Международной студенческой научной конференции «Студенческий научный форум», Москва, 15–20 февраля 2018. М.: Издательство: ООО «Научно-издательский центр «Академия Естествознания», 2018. URL: https://scienceforum.ru/2018/article/2018005524 (дата обращения: 28.06.2025).

5. Иваненко А. В. Развитие физической культуры студентов на современном этапе // Современная наука: актуальные проблемы теории и практики. Серия: Гуманитарные науки. 2017. № 2. С. 33–35.

6. Славинский Н. В., Кузнецова З. В. Исследование влияния физической культуры на мотивацию в обычной жизнедеятельности // Ученые записки университета им. П. Ф. Лесгафта. 2022. № 6 (208). С. 348–350.

7. Дуркин П. К. Формирование у школьников интереса к физической культуре: учеб. пособие. Архангельск. гос. техн. ун-т, 2006. 128 с. ISBN 5-26100274-5

8. Макаренко В. К. Формирование мотивации к занятиям физической культурой и спортом // Известия Пензенского государственного педагогического университета им. В. Г. Белинского. 2008. № 10. С. 140–144. URL: https://cyberleninka.ru/article/ n/formirovanie-motivatsii-k-zanyatiyam-fizicheskoy-kulturoy-i-sportom (дата обращения: 28.06.2025)

9. Шарухин А. П., Сапожников А. С. Учебная деятельность курсантов военных образовательных организаций высшего образования войск национальной гвардии РФ: критерии оценки качества // Актуальные проблемы гуманитарных и социально-экономических наук. 2017. Т. 10, № 11 (11). С. 53–54.

10. Бахарева Е. В., Иванова Л. В., Коваленко Е. А. Формирование мотивации к занятиям физической культурой у школьников // Евразийский Научный Журнал. 2015. № 7. С. 31–34. URL: https://journalpro.ru/articles/formirovanie-motivatsii-k-zanyatiyam-fizicheskoy-kulturoy-u-shkolnikov/ (дата обращения: 29.06.2025)

11. Бабичев А. М., Ивченко Н. В., Шарухин А. П. Воспитание ответственности курсантов центров подготовки личного состава войск национальной гвардии Российской

Федерации за выполнение служебно-боевых задач / Под научной редакцией А. П. Шарухина: учебное пособие. Санкт-Петербург: ЛЕМА, 2025. 87 с. ISBN 978-5-00105-993-6

12. Герасимов И. В., Кельдасов Т. Д. Ценностно-мотивационные установки индивидуальных занятий физическими упражнениями // Наука 2020: Инновационные технологии оздоровительной физической культуры. 2020. № 3 (39). С. 127–131.

Статья представлена заведующим кафедрой ФК СПбГУТ, кандидатом педагогических наук, доцентом Иваненко А. В.

THE IMPACT OF THE QUALITY OF EDUCATIONAL AND METHODOLOGICAL SUPPORT ON THE MOTIVATION OF STUDENTS OF THE MILITARY TRAINING CENTER OF A TECHNICAL UNIVERSITY TO ENGAGE IN PHYSICAL EDUCATION

Ivanenko T.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The article is devoted to the actualization of the problem of increasing the motivation to engage in physical culture among students of the military training center. A comparative analysis was conducted to determine the formation of motives for physical culture among students of St. Petersburg State University of Telecommunications and the military training center of the technical university. It was determined that the quality of the educational and methodological support for the learning process of students affects the formation of motives for physical culture.

Key words: *Quality, educational and methodological support, motives, motivation, physical culture, university students*

УДК 378.4. 37.048.45
ГРНТИ 14.35.07

ФОРМИРОВАНИЕ КОМПЕТЕНТНОСТИ ПРЕПОДАВАТЕЛЯ-МЕТОДИСТА КАК ФАКТОР СОВЕРШЕНСТВОВАНИЯ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОЦЕССА ОБУЧЕНИЯ СТУДЕНТОВ ВОЕННОГО УЧЕБНОГО ЦЕНТРА

Т. А. Иваненко

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

Цель исследования – поиск подходов, способствующих совершенствованию учебно-методического обеспечения (УМО) процесса обучения студентов военного учебного центра (ВУЦ). Проведен анализ особенностей УМО процесса обучения студентов ВУЦ. Выявлены проблемы, актуализированы подходы к формированию высокого уровня компетентности преподавателя-методиста. Представлен механизм оценки уровня формирования компетентности преподавателя-методиста, посредством проведения смотра-конкурса «Лучший преподаватель-методист». Показана результативность управленческой и методической деятельности преподавателей-методистов, направленной на совершенствование УМО процесса обучения студентов ВУЦ.

компетентность, преподаватель-методист, учебно-методическое обеспечение, студенты ВУЦ

Введение

Одной из задач высшего профессионального образования является обеспечение качества подготовки специалистов в новых условиях.

Необходимым условием решения данной задачи является выявление механизмов обновления содержания профессионального образования, способов и факторов формирования высокого уровня профессиональной компетентности преподавателей.

Преподаватель, сталкиваясь с проблемами методического характера в процессе обучения студентов решает их через сложный нормативный комплекс документации.

Профессорско-преподавательский состав (ППС) должен обладать необходимыми знаниями основ научной и учебно-методической работы, умениями в области решения методических и технологических проблем учебного процесса для формирования организационно-нормативного комплекса

документации, разработки рабочих программ дисциплин и методических материалов, издания учебных материалов, поиска инноваций и методик обучения, системного повышения квалификации и др. [1, 2].

Методическое сопровождение образовательного процесса создает необходимые условия для качественной реализации образовательных программ, активации учебной деятельности и управления ею.

Актуальность данной работы обусловлена необходимостью формирования высокого уровня компетентности преподавателя-методиста, направленной на совершенствование УМО процесса обучения студентов ВУЦ.

Цель исследования – поиск подходов и механизмов, способствующих формированию высокого уровня профессиональной компетентности преподавателя-методиста, направленной на совершенствование УМО образовательного процесса.

Материалы и методы

Использовались методы: теоретические (анализ и обобщение), статистические (обработка полученных данных).

Результаты и обсуждения

Методическая деятельность является важным аспектом деятельности преподавателя в образовательном процессе, направленная, прежде всего на совершенствование педагогического мастерства ППС, методик повышения качества и эффективности проведения всех видов учебных занятий.

Мастерство преподавателя развивается и реализуется в его педагогической деятельности, являясь качественным ориентиром, к которому нужно стремиться.

Педагогическое мастерство ППС проявляется в уровне овладения педагогической деятельностью, в эффективном осуществлении профессиональной деятельности, направленной на всестороннее развитие обучающихся.

Развитие педагогического мастерства профессионала – это процесс становления преподавателя-методиста в образовательной среде вуза.

Понятие «Лучший преподаватель-методист» ассоциируется с высоким уровнем педагогического мастерства, культуры, такта, компетентности преподавателя, обладающего и способного сформировать у обучающихся соответствующие профессиональные и нравственные качества [3, 4].

Термин «компетенции» определяется, как способность преподавателя применять знания, умения и личностные качества для успешной деятельности в определенной области [5].

Понятие компетенции содержит не только профессиональные знания и умения, но и внепрофессиональные навыки, социальные компетенции, или ключевые квалификации преподавателя, что дополняет их как «методические компетенции» [6].

Профессиональная деятельность преподавателя тесно взаимосвязана с методической деятельностью, в связи с чем проектирование и реализация смотра-конкурса «Лучший преподаватель-методист» приобретает особую направленность, ориентированную на повышение уровня компетентности ППС, качества УМО процесса обучения студентов ВУЦ.

Таким образом, содержание категории «Лучший преподаватель-методист», является основой при определении критериев и показателей, позволяющих количественно измерять методическую деятельность преподавателя.

С целью проверки эффективности использования механизма управления методической деятельностью, формирования компетентности преподавателей-методистов ВУЦ, было организовано исследование по проектированию и реализации смотра-конкурса «Лучший преподаватель-методист».

Проектирование конкурса, направленное на повышение методической и профессиональной компетентности ППС, реализовывалось в таких видах деятельности, как:

– системное повышение квалификации;
– изучение современных педагогических методик;
– участие и выступление с докладами на научно-практических, учебно-методических конференциях;
– изучение и использование педагогической, учебно-методической литературы;
– демонстрация педагогического опыта, посредством проведения показных занятий.

В смотре-конкурсе приняли участие: 29 чел., из числа ППС кафедр, циклов ВУЦ СПбГУТ.

Реализация конкурса осуществлялась с учетом качества УМО процесса обучения студентов ВУЦ, готовности ППС к методической деятельности. Для оценивания его реализации, разрабатывался диагностический инстру-

ментарий, назначались эксперты из числа специалистов учебно-методического отдела, начальников, заместителей начальников кафедр, циклов ВУЦ.

Принимая во внимание, планирование индивидуальных планов ППС, определялись критерии формирования профессиональной компетентности преподавателей-методистов, проводился количественный подсчет данных, показателей критериев, компонентов методической деятельности.

Общая оценка методической деятельности кафедр, циклов ВУЦ определялась, как средняя арифметическая величина, по всем критериям компонентов компетенции преподавателей-методистов (рис. 1).

Показатель оценки сформированности компетенции определялся путем деления полученной суммы баллов на общее количество критериев компонентов, отображает уровень выраженности профессиональной компетенции ППС [7].

Интерпретация результатов:

– от «0» до «3» баллов, соответствует низкому уровню – компетенция не сформирована;
– от «3» до «7» баллов, достаточный уровень – компетенция сформирована, присутствуют резервы для повышения уровня методической компетентности;
– от «7» до «10» баллов, высокий уровень – компетенция полностью сформирована.

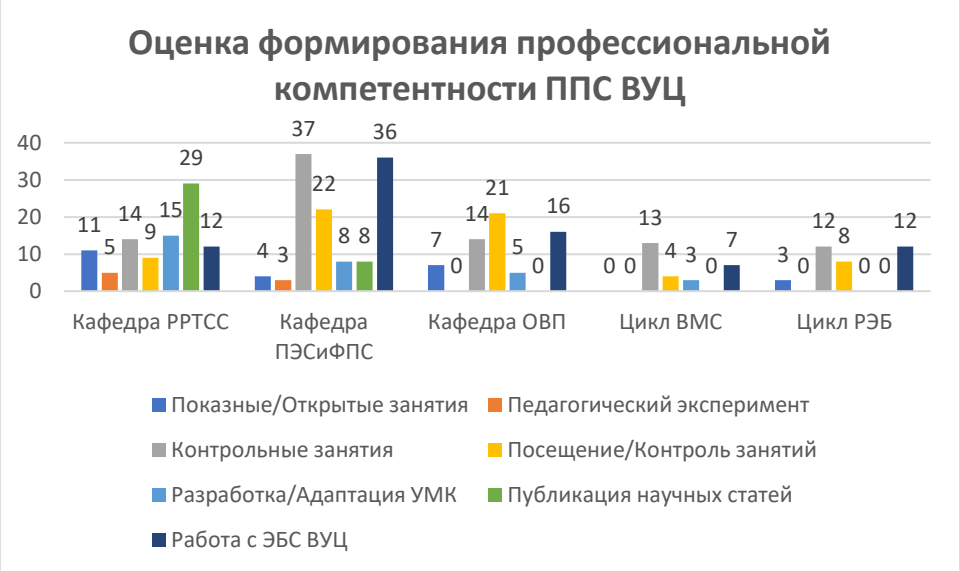


Рис. 1. Показатели критериев формирования уровня профессиональной компетентности преподавателей-методистов кафедр, циклов ВУЦ, за 2024/25 учебный год

Суммируя значения данных показателей компетентности, выявлялись лучшие преподаватели-методисты ВУЦ.

Исходя из итогов, смотра-конкурса «Лучший преподаватель-методист», определено: лучшим преподавателем-методистом, с результатом 7,63 балла, стал представитель из числа ППС кафедры РРТСС; вторую позицию, с одинаковым результатом 3,75 балла, разделили преподаватели-методисты кафедры ПЭСиФПС и ОВП; на третьей позиции, с результатом 3,5 балла – преподаватель-методист кафедры РРТСС, что позволило кафедрам РРТСС, ПЭСиФПС и ОВП занять лидирующие позиции в рейтинге кафедр, циклов ВУЦ, за 2024/25 учебный год.

Результаты исследования представлены с точки зрения эффективности реализации управленческой деятельности учебно-методического отдела ВУЦ, направленной на формирование и развитие профессиональной компетентности преподавателей-методистов.

Таким образом, проектирование и реализация смотра-конкурса «Лучший преподаватель-методист» служит, одним из факторов, активации методической деятельности, концептуальной основой которой является совершенствование УМО образовательного процесса, что подтверждается уровнем сформированности профессиональной компетентности ППС ВУЦ СПбГУТ.

Список используемых источников

1.Селуянов А. А., Фархиев М. В. Анализ внедрения в обучение студентов программы «Основы военной подготовки» // Теория и практика военного образования в гражданских вузах: педагогический поиск: сборник материалов VI Всероссийской научно-практической конференции с международным участием. Екатеринбург, 16-17 ноября 2023 г.: в 2 частях: Часть 1. Екатеринбург: Издательство УМЦ УПИ, 2023. С. 29-40.

2. Шпаков Г. Г. Требования к профессорско-преподавательскому составу военных кафедр в вузах // Гуманитарный вестник. 2014. № 2 (29). С. 131-133.

3. Положение о лучшем преподавателе-методисте. Военная академия радиационной, химической и биологической защиты имени Маршала Советского Союза С. К. Тимошенко URL: https://varhbz.mil.ru/upload/site38/document_file/Polozhenie_o_luchshem_prepodavatele-metodiste.pdf?ysclid=mcutmdjzdb498609251 (дата обращения 08.07.2025).

4. Зимняя И. А. Ключевые компетенции – новая парадигма результата образования // Высшее образование сегодня. 2003. № 5. С. 34-44.

5. Федеральные государственные образовательные стандарты высшего профессионального образования: законодательно-нормативная база проектирования и реализации: Учебно-информационное издание. М.: Исследовательский центр проблем качества подготовки специалистов, Координационный совет учебно-методических объединений и научно-методических советов высшей школы, 2009. 100 с. URL: https://www.miigaik.ru/

education/umo/documents/methodical-materials/20101129193958-7679.pdf?ysclid=mdbknmhqb466595207 (20.07.2025)

6. Байденко, В. И. Компетентностный подход к проектированию государственных образовательных стандартов высшего профессионального образования (методологические и методические вопросы). Методическое пособие. М.: Исследовательский центр проблем качества подготовки специалистов, 2005. 114 с.

7. Логинова С. Л. Диагностика уровня сформированности методической компетентности преподавателя высшей школы // Современные наукоемкие технологии. 2017. № 11. С. 134-139; URL: https://top-technologies.ru/ru/article/view?id=36858 (дата обращения: 29.07.2025).

Статья представлена заведующим кафедрой ФК СПбГУТ, кандидатом педагогических наук, доцентом Иваненко А. В.

FORMATION OF THE TEACHER-METHODOLOGIST'S COMPETENCE AS A FACTOR IN IMPROVING THE EDUCATIONAL AND METHODOLOGICAL SUPPORT OF THE MILITARY TRAINING CENTER'S STUDENT LEARNING PROCESS

Ivanenko T.
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

The purpose of the study is to search for approaches that contribute to improving the educational and methodological support for the learning process of students at the Military Training Center (VUC). The analysis of the features of the UME of the University students' learning process is carried out. Problems have been identified, approaches to the formation of a high level of competence of a teacher-methodologist have been updated, and a mechanism for assessing the level of competence formation of a teacher-methodologist has been presented through a review competition "The best teacher-methodologist". The effectiveness of the methodological activities of teachers-methodologists aimed at improving the educational process of students of the Higher School of Economics is shown.

Key words: *Competence, teacher-methodologist, educational and methodological support, students of the Higher Education Center*

ИННОВАЦИИ ДЛЯ АРКТИКИ

УДК 004.421
ГРНТИ 47.14.17

О МЕТОДАХ АНАЛИЗА СИГНАЛОВ НА ОСНОВЕ ДЕКОМПОЗИЦИИ НА ЭМПИРИЧЕСКИЕ МОДЫ

А. В. Запайщиков

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

Данная работа посвящена обзору основных методов анализа сигналов с использованием алгоритма декомпозиции на эмпирические моды. Приводятся и рассматриваются: само понятие эмпирической моды, а также рассматриваются основные достоинства и недостатки данного метода по сравнению с анализом, использующим механизм преобразования Фурье или вейвлет-анализом. Обращается особое внимание на сам алгоритм декомпозиции сигнала. Оценивается возможность применения алгоритма к конкретным сигналам для очистки последних от шумовых составляющих, а также выявления трендовых составляющих.

математические методы анализа сигналов, эмпирические моды, преобразование Фурье, вейвлет-анализ, фильтрация сигналов, электроэнцефалограмма, электрокардиограмма

Целью данной работы является обзор основных методов анализа сигналов с использованием алгоритма декомпозиции на эмпирические моды.

В классической теории обработки сигналов достаточно широко распространены временные методы анализа, спектральные методы анализа (основанные на преобразовании Фурье), а также частотно-временные (например, вейвлет-анализ [1-3]). Однако существуют и иные методы анализа. В данной статье предлагается рассмотреть анализ сигналов на основе декомпозиции на эмпирические моды.

Эмпирической модой обычно называется функция, заданная непрерывно на интервале существования сигнала или дискретно в виде вектора отсчетов, которая имеет, в общем случае, произвольную форму и произвольную аналитическую запись (если таковая существует), но при этом непременно удовлетворяющая двум необходимым условиям [4-8]:

1. Общее число максимумов и минимумов такой функции (т. е. общее число экстремумов) должно быть строго равно числу нулей функции либо отличаться от числа нулей по модулю не более чем на единицу:

$$N_{\text{МАКС}} + N_{\text{МИН}} = N_0 \text{ или } N_{\text{МАКС}} + N_{\text{МИН}} = N_0 \pm 1$$

где $N_{\text{МАКС}}, N_{\text{МИН}}, N_0$ – число максимумов, минимумов и нулей функции соответственно.

2. Локальное (мгновенное) среднее значение функции, определенное в виде полусуммы двух огибающих, должно быть меньше или равно заранее определенному пороговому значению η, зависящему от машинной точности ε и погрешностей, связанных с получением, преобразованием и передачей сигнальной информации:

$$\frac{U(k) + L(k)}{2} \leq \eta,\ k = \overline{1,\ N}$$

где $U(k)$ и $L(k)$ – значения верхней и нижней огибающих сигнала в -й момент времени. N – общее количество сигнальных отсчетов. η – некоторый порог, устанавливаемый обработчиком-экспертом и обычно принимающий близкие к нулю значения.

В случае разложения по Фурье-базису или вейвлет-базису используется следующая формула [4]:

$$s(k) = \sum_i c_i f_{i_{\text{ДЕТ}}}(k)$$

где $s(k)$ – исходный сигнал, c_i – коэффициенты разложения, $f_{i_{\text{ДЕТ}}}(k)$ – детерминированные (априорно известные) базисные функции.

В случае с разложением по вейвлет-базису требуется выбрать конкретный необходимый вейвлет-базис (материнский вейвлет) под заданную форму исходного сигнала. Зачастую, это весьма непростая задача.

В случае декомпозиции на эмпирические моды используется следующая формула [4]:

$$s(k) = \sum_i c_i f_i(k)$$

где $s(k)$ – исходный сигнал, c_i – коэффициенты разложения, $f_i(k)$ – априорно неизвестные (но апостериорно известные) «базисные» функции, которые извлекаются из самого исходного сигнала.

При декомпозиции на эмпирические моды, сами базисные функции формируются апостериорно и являются уникальными для каждого исходного сигнала, что, с одной стороны, является несомненным преимуществом по сравнению с первыми двумя случаями, но с другой стороны – недостатком (из-за невозможности их применения к другим сигналам) [4].

На рисунке 1 представлен алгоритм декомпозиции сигнала на эмпирические моды.

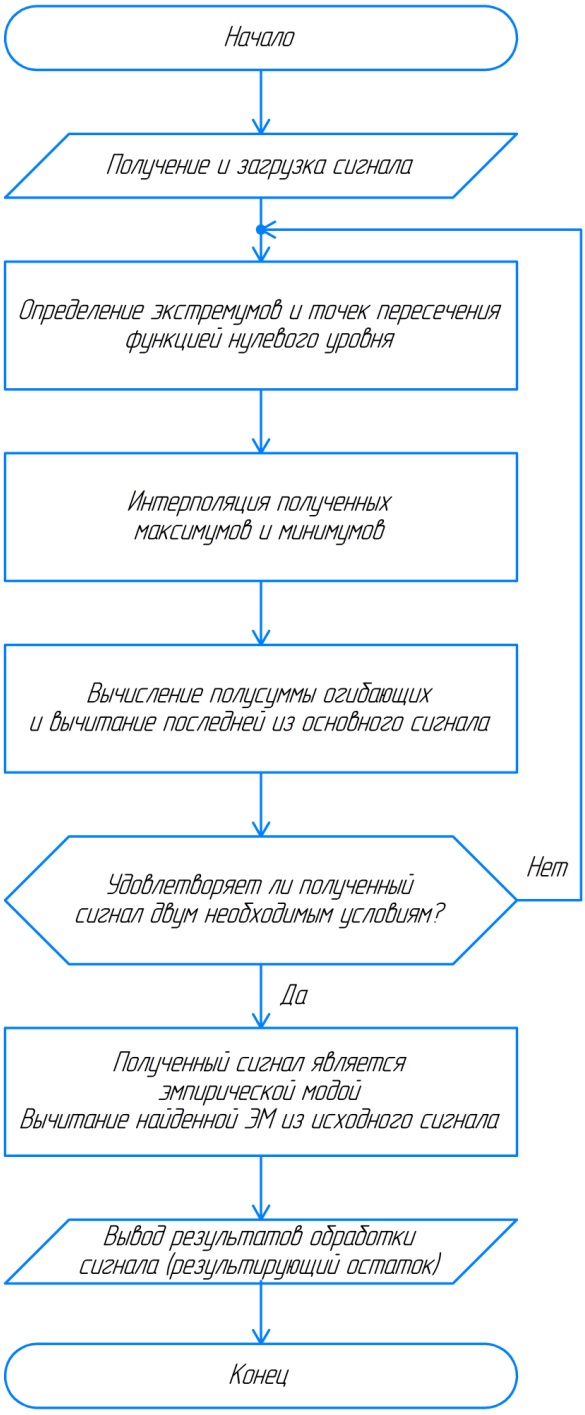


Рис. 1. Алгоритм декомпозиции сигнала на эмпирические моды

Рассмотрим сам процесс декомпозиции на эмпирические моды для конкретных сигналов электроэнцефалограммы и кардиограммы.

Электроэнцефалограммой (ЭЭГ) называется сигнал, который может быть зарегистрирован на поверхности головы человека и является результатом суммации и фильтрации электрической активности отдельных групп нейронов [9]. Используя полученные данные электроэнцефалограммы, при использовании того или иного математического метода анализа ЭЭГ, можно проводить функциональную диагностику головного мозга человека [10].

На рисунке 2 представлен пример декомпозиции на эмпирические моды сигнала электроэнцефалограммы с извлечением трех эмпирических мод и результирующего остатка.

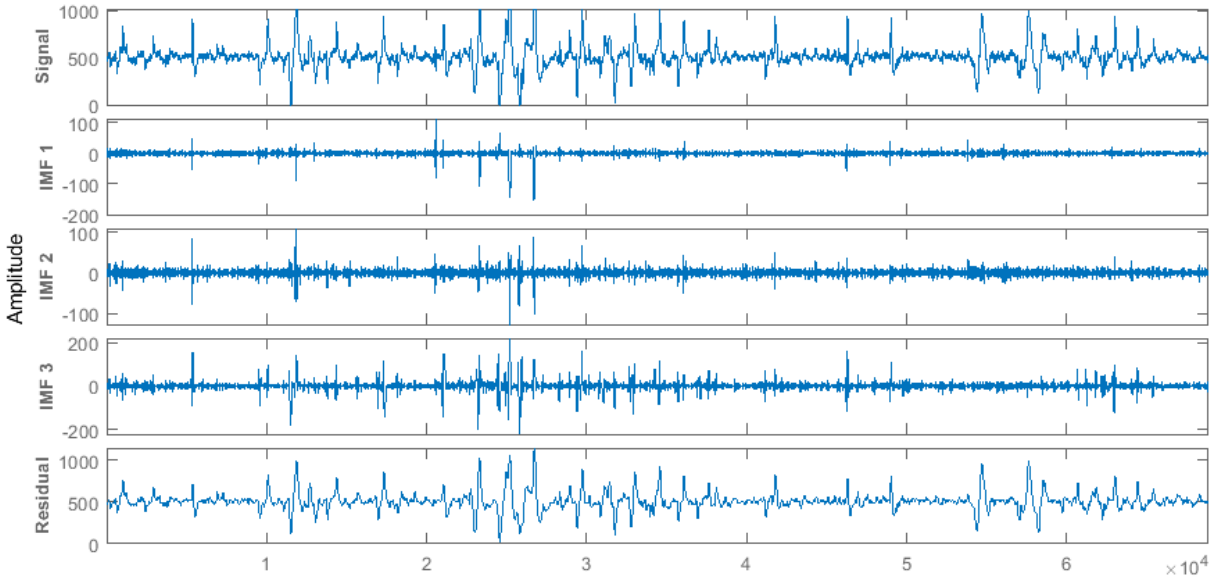


Рис. 2. Пример декомпозиции на эмпирические моды сигнала электроэнцефалограммы с извлечением трех эмпирических мод и результирующего остатка

Стоит заметить, что результирующий сигнал, в отличие от исходного, является более «чистым». Таким образом можно заявить, что над сигналом с помощью математического аппарата декомпозиции на эмпирические моды была произведена операция фильтрации и очистки от шумовых составляющих.

Электрокардиограммой (ЭКГ) называется сигнал, который может быть зарегистрирован с поверхности кожи человека и является результатом электрической активности его сердца [9].

На рисунке 3 представлен пример декомпозиции на эмпирические моды сигнала электрокардиограммы с извлечением трех эмпирических мод и результирующего остатка.

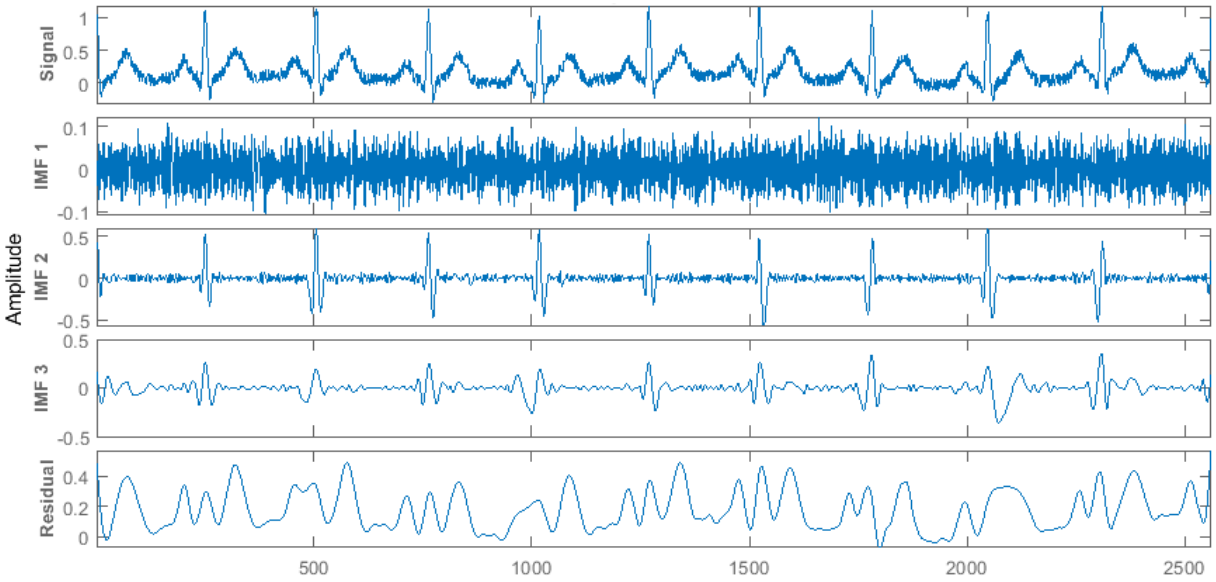


Рис. 3. Пример декомпозиции на эмпирические моды сигнала электрокардиограммы с извлечением трех эмпирических мод и результирующего остатка

В отличие от предыдущего случая, здесь результирующим остатком является некий тренд, изначально присутствующий в исходном сигнале и полученный в явном виде с помощью математического аппарата декомпозиции на эмпирические моды.

Статья представлена научным руководителем: заместителем директора ИМ СПбГУТ по учебной работе, доцентом кафедры РТ, кандидатом технических наук, доцентом Степановым А. Б.

Список используемых источников

1. Степанов А. Б., Козлов Д. В., Запайщиков А. В. Автономный портативный электроэнцефалограф на базе одноплатного компьютера Nvidia Jetson // Вестник Воронежского государственного технического университета 2022. Т. 18. № 2. С. 77-85.

2. Запайщиков А. В., Козлов Д. В., Степанов А. Б. Разработка портативного электроэнцефалографа на базе графического процессора. // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): Всерос. науч.-метод. конф. магистрантов и их руководителей. СПб.: СПбГУТ, 2022. С. 73-76.

3. Stark H.-G. Wavelets and Signal Processing. Berlin: Springer, 2005. 158 p.

4. Клионский Д. М., Орешко Н. И., Геппенер В. В. Декомпозиция на эмпирические моды с параболической интерполяцией огибающих в задачах очистки сигналов от шума // Цифровая обработка сигналов: научно-технический журнал / КБ волоконно-оптических приборов. М. 2011. № 2. С. 51-60: ил. ISSN 1684-2634.

5. Клионский Д. М. // Доклады 13-й Международной конференции «Цифровая обработка сигналов и ее применение». Москва. 2011. С. 120–123.

6. Huang N. E., et al. The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis // Proc. Royal Soc. London. 1998. Vol. 454. P. 903-995.

7. Huang N. E., Shen S. S. P. Hilbert-Huang Transform and Its Applications. World Scientific, 2005. 350 p.

8. Клионский Д. М., Орешко Н. И., Геппенер В. В. Декомпозиция на эмпирические моды и ее использование при анализе дробного броуновского движения // Цифровая Обработка Сигналов. 2008. № 3. С. 37-45.

9. Ронкин М. А., Зенков Л. Р. Функциональная диагностика нервных болезней. Руководство для врачей. Изд. 5-е, Издательство МЕДпресс-информ, 2013, 488 с.

10. Арбузов С. М., Степанов А. Б. Применение методов вейвлет-анализа в электроэнцефалографии. СПб.: Линк, 2009. 104 с.

ABOUT SIGNAL ANALYSIS METHODS BASED ON DECOMPOSITION INTO EMPIRICAL

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

This paper is devoted to a review of the main methods of signal analysis using the empirical mode decomposition algorithm. The very concept of empirical mode is given and considered, as well as the main advantages and disadvantages of this method are considered, in comparison with the analysis using the Fourier transform mechanism or wavelet analysis. Special attention is paid to the signal decomposition algorithm itself. The possibility of applying the algorithm to specific signals to clear the latter of noise components, as well as identify trend components, is being evaluated.

Key words *mathematical methods of signal analysis, empirical modes, Fourier transform, wavelet analysis, signal filtering, electroencephalogram, electrocardiogram*

УДК 677. 070
ГРНТИ 64.29.35

ИССЛЕДОВАНИЕ СВОЙСТВ ПАРААРАМИДНЫХ НИТЕЙ ПОД ВОЗДЕЙСТВИЕМ ЭКСПЛУАТАЦИОННЫХ ФАКТОРОВ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Н. П. Лебедева[1], А. Б. Степанова[2]

[1] Санкт-Петербургский государственный университет промышленных технологий и дизайна
[2] Санкт-Петербургский политехнический университет Петра Великого

Рассмотрены исследования, проведенные ранее и посвященные изучению влияния повышенных и пониженных температур, различных агрессивных сред и микроорганизмов на механические свойства параарамидных нитей. С учетом условий эксплуатации, данные нити нашли широкое применение, в т.ч. в условиях пониженных температур. Для расчета полученных результатов использовались современные программы для обработки данных.

параарамидные нити, влияние температур, механические свойства

Параарамидные волокна и нити благодаря своим уникальным свойствам широко применяются для изготовления различных изделий технического назначения, в частности для:

– средств индивидуальной бронезащиты (Кевлар, Русар и т. п. – изделия подвергаются воздействию температур, влаги и ультрафиолетовым излучениям);
– средств спасения и безопасности (Русар, Кевлар, Тварон, Технора и т. п. – изделия из данных волокон и нитей способны удерживать ударные нагрузки: тросы, канаты, ленты, кабели, страховочные пояса и т.д.);
– защитной оплетки для кабелей (Кевлар, Тварон, СВМ, Русар, Армос – изделия, подвергаются механическим воздействиям, а также пониженным и повышенным температурам и агрессивным средам);
– композиционных материалов для ракетно-космической промышленности (Кевлар и т. п. – изделия, эксплуатируются в условиях ионизирующего излучения и воздействия температур);
– теплоизолирующей продукции, рукавов, приводных ремней, кабелей, канатов, проводов зажигания и т. п. (воздействие высоких механических нагрузок, агрессивных сред и температур);

– трансмиссионные ремни, автомобильные шланги, шины, конструкционные пластики для автомобильной, кораблестроительной промышленности и пр. (изделия, для которых существенное значение имеют температурный фактор и агрессивные среды [1-5].

Параарамидные нити представляют собой высокотехнологические материалы, которые сочетают в себе повышенную прочность, устойчивость к различным агрессивным средам. В процессе эксплуатации они подвергаются воздействию как высоких температур, так и экстремально пониженных температур, особенно в условиях Арктики.

Наибольшее применение нашли волокна и нити под торговыми марками Технора® (Япония), Тварон® (Нидерланды), Русар® и Армос® (Россия).

Однако в процессе эксплуатации, когда данные нити подвергаются воздействию различных эксплуатационных факторов длительное время (как по отдельности, так и совместно), это может привести к постепенному изменению структуры волокна и свойств изделий из них.

В связи с вышесказанным, возникает необходимость проведения следующих исследований:

– прогнозирование поведения параарамидных волокон и нитей как при кратковременном, так и при длительном воздействии эксплуатационных факторов;
– исследование свойств параарамидных волокон и нитей при комплексном воздействии различных факторов.

Ранее проводились исследования влияния влаги и различных факторов окружающей среды на свойства следующих параарамидных нитей: Русар (Россия, ОАО «Каменскволокно»), Кевлар 49 (США, Du Pont de Nemour), Тварон 1000, 2000 и 2200 (Нидерланды, Teijin Twaron b. v.), Технора Т200 (Япония, Teijin) [3]. В частности, проводились исследованиz влияния влаги и факторов окружающей среды на свойства параарамидных нитей, в рамках которых изучались:

– тепловые эффекты сорбции и десорбции, необходимые в дальнейшем для расчета и оптимизации условий процессов массопереноса;
– гистерезисные явления при сорбции и десорбции водяного пара;
– изменения свойств параармидных нитей под воздействием микроорганизмов;
– исследования изменения свойств параарамидных нитей под воздействием различных атмосферных факторов.

Результаты проведенных исследований приведены в работах [6-9].

Однако, хотелось бы отметить, что в ходе обширного ряда экспериментов было выявлено, что при длительном пребывании нитей в воде, на их поверхности начинают активно развиваться микроорганизмы. Деструкция нитей приводит к дальнейшему снижению разрывных характеристик нитей.

Также были проведены исследования и выполнен сравнительный анализ следующих образцов Тварон 1000, 2000 и 2200 (Нидерланды, Teijin Twaron b. v.), Технора Т200 (Япония, Teijin) при экстремальных воздействиях высоких температур и агрессивных сред [4]:

– проведены исследования кратковременного и длительного воздействия высоких температур на механические свойства параарамидных нитей;
– выполнены исследования при суммарном воздействии высоких температур и агрессивных сред;
– изучен вопрос влияния ионизирующего излучения на механические свойства параарамидных нитей;
– выполнен сравнительный анализ образцов параарамидных нитей при комплексном воздействии различных факторов.

В ходе выполнения работы было выявлено, что данные нити обладают не только повышенной термостойкостью, но и повышенной хемостойкостью.

Более детальные результаты проведенных исследований приведены в работах [10-15].

Однако, вышеприведенные исследования касались в основном исследований свойств параарамидных нитей при воздействии высоких температур и не рассматривали влияния отрицательных температур на изменения свойств параарамидных нитей, в частности, при экстремальных отрицательных температурах в условиях Арктики.

Стоит отметить, что по данным Teijin, данные нити широко применяются в качестве составляющей тросов для нефтегазовых платформ в арктических условиях, что значительно увеличило срок службы данных тросов, однако существуют определенные сложности с устойчивостью к влаге данных изделий.

Следует также отметить о необходимости проведения дальнейших исследований для разработки модели поведения данных нитей в изделиях, подверженных воздействию экстремально низких температур, с целью предотвращения из разрушения в изделиях.

В процессе выполнения исследовательских работ всегда возникает вопрос о корректной обработке большого объема данных.

С этой целью для проведенных исследований [2, 3] использовались программы Excel и ORIGIN. Программа Excel позволяет анализировать, преобразовывать данные, тем самым упрощая и значительно ускоряя процесс обработки данных.

Программа ORIGIN представляет обширные инструменты для анализа и графического отображения полученных результатов, включая двухмерные и трехмерных графики. Программа позволяет автоматически обновлять результаты при изменении вводимых данных и благодаря этому можно создать шаблоны для однотипных данных.

В отличие от двух указанных программ, среда MATLAB представляет широкий выбор инструментов не только для анализа полученных данных, для качественной обработки и графического отображения полученных результатов, таким образом, совмещая эти функции и значительно ускоряя процесс обработки, а также позволяет автоматизировать процесс обработки данных за счет написания пользовательских скриптов и функций. Проводя исследования, достаточно один раз загрузить полученные данные и далее приступить к анализу.

При эксплуатации изделий в условиях Арктики, параарамидные волокна и нити подвергаются воздействию переменных экстремальных пониженных температур, микроорганизмов и агрессивных сред. Поэтому исследования воздействия данных факторов на волокна и нити являются необходимыми для прогнозирования срока эксплуатации данных изделий, а дополнительные разработки по окончательной поверхностной обработке параамидных волокон и нитей может привести к значительному увеличению срока службы изделий, созданных на их основе.

Список используемых источников

1. Волохина А. В., Щетинин А. М. Создание высокопрочных, термо- и огнестойких синтетических волокон // Химические волокна. 2001. № 2. С. 14-21.

2. Степанова А. Б. Влияние условий эксплуатации на механические свойства параарамидных нитей: дис. канд. техн. наук: 05.19.01 / Степанова Анна Борисовна. Санкт-Петербург, 2014. 241 с.

3. Лебедева Н. П. Влияние эксплуатационных воздействий на свойства параарамидных нитей технического назначения: дис. канд. техн. наук: 05.19.01 / Лебедева Наталья Павловна. Санкт-Петербург, 2007. 239 с.

4. Кустов А. В., Рожкова Е. А., Бордачев В. А. Композиционные материалы в ракетно-космической отрасли. // Наука, технологии, общество - НТО-II-2022. сб. науч. ст. по материалам II Всероссийской науч. конф., Красноярск, 2022. С. 101-109.

5. Сайт производителя волокон Технора® [Электронный ресурс]: https://fibrxl.com/fibrxl-performance/fibers/technora/ (дата обращения 09.08.2025).

6. Перепелкин К. Е., Гребенников С. Ф., Лебедева Н. П. Сорбция водяных паров высокопрочными параарамидными нитями // Химические волокна. 2007. № 5. С. 50-52.

7. Перепелкин К. Е., Гребенников С. Ф., Лебедева Н. П., Зайцева Е. И. Взаимодействие параарамидных волокнистых материалов с водой // Известия высших учебных заведений. Технология легкой промышленности. 2008. Т. 2. № 2. С. 37-43.

8. Гребенников С. Ф., Лебедева Н. П., Бусыгин К. Н., Мачалаба Н. Н. Физико-химические свойства волокнообразующих параарамидных полимеров. Обзор. Часть 1. Структура и термические свойства // Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 34-41.

9. Лебедева Н. П., Гребенников С. Ф., Бусыгин К. Н., Мачалаба Н. Н., Москалюк О. А. Физико-химические свойства волокнообразующих параарамидных полимеров. Обзор. Часть 3. Влияние эксплуатационных факторов на деформационные свойства АПА // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 36. № 2. С. 45-53.

10. Дьянкова Т. Ю., Лебедева Г. Г., Мещерякова Г. П., Степанова А. Б. Влияние агрессивных сред и температуры на механические свойства параарамидных нитей // Дизайн. Материалы. Технология. 2013. № 5 (30). С. 48-50.

11. Басок М. О., Дянкова Т. Ю., Степанова А. Б. Изменение термических свойств параарамидных нитей после воздействия агрессивной среды // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2013. № 3. С. 13-16.

12. Мещерякова Г. П., Дянкова Т. Ю., Степанова А. Б. Исследование термических характеристик параарамидных нитей методами термического анализа // Известия высших учебных заведений. Технология легкой промышленности. 2013. Т. 22. № 4. С. 16- 18.

13. Мещерякова Г. П., Степанова А. Б., Иванькова Е. М. Изменение свойств параарамидных нитей после действия ионизирующего излучения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2012. № 3. С. 49-52.

14. Мещерякова Г. П., Степанова А. Б. Изменение механических свойств параарамидных нитей под воздействием агрессивной среды // Известия высших учебных заведений. Технология легкой промышленности. 2012. Т. 18. № 4. С. 3-6.

15. Лебедева Г. Г., Мещерякова Г. П., Степанова А. Б. Изменение механических свойств параарамидных нитей после воздействия высоких температур // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2013. № 3. С. 17-20.

RESEARCH OF THE PROPERTIES OF PARA-AMIDE NITES UNDER THE INFLUENCE OF OPERATIONAL FACTORS USING MODERN SOFTWARE

Lebedeva N., Stepanova A.
[1]Saint Petersburg State University of Industrial Technologies and Design
[2]Peter the Great Saint Petersburg Polytechnic University

The article reviews previous research on the effect of elevated and low temperatures, various aggressive environments, and microorganisms on the mechanical properties of para-aramid fibers. Given the specific conditions of use, these fibers have found widespread applications, including in low-temperature environments. The article uses modern data processing software to calculate the results.

Key words: *para-aramid threads, temperature effects, and mechanical properties*

УДК 621.39
ГРНТИ 49.13

ОСОБЕННОСТИ ПОСТРОЕНИЯ СЕТИ ПЕРЕДАЧИ ДАННЫХ В ДЕРЕВНЕ ЛЕТНЯЯ ЗОЛОТИЦА АРХАНГЕЛЬСКОЙ ОБЛАСТИ С ПРИМЕНЕНИЕМ УКВ ПРИЕМОПЕРЕДАТЧИКОВ АЛИСА-С

А. Б. Степанов

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

Работа посвящена описанию особенностей построения сети передачи данных в деревне Летняя Золотица Архангельской области с применением УКВ приемопередатчиков АЛИСА-С, разработанных под научным руководством автора данной статьи. Приводятся описание и характеристики приемопередатчиков АЛИСА-С, предлагаемая конструкция мачтового оборудования для проведения исследований, методика проведения испытаний оборудования в составе гибридной сети связи.

УКВ приемопередатчики, мачтовое оборудование, гибридная сеть связи, ретранслятор, АЛИСА-С

Обзор документов, посвященных Арктической зоне Российской Федерации [1–3], показал, что задача организации связи в арктических регионах остается одной из важнейших. Предложенная ранее [4] концепция Единой информационной системы Арктической зоны Российской Федерации подразумевает включение в состав гибридной сети связи оборудования различного типа, в том числе позволяющего организовывать передачу данных по радиоканалу на различных расстояниях. На расстояниях в десятки километров могут применяться УКВ приемопередатчики и ретрансляторы различной мощности. Автором данной работы предложены следующие модификации УКВ приемопередатчиков и ретрансляторов, позволяющие передавать данные различного типа (голосовые сообщения, текстовые сообщения, изображения, видеоданные и пр.):

1. Приемопередатчик АЛИСА-С АТ1.1 и ретранслятор АЛИСА-С РТ1.1, обладающие мощностью 0,1 Вт и позволяющие осуществлять передачу данных на расстояние до 4 км (при условиях прямой видимости). Приемопередатчик подключается к любому устройству с поддержкой Bluetooth. Приемопередатчик и ретранслятор реализованы на базе микроконтроллера, что обеспечивает низкое энергопотребление устройств. Они прошли успешные испытания в рамках Арктических технологических экспедиций СПбГУТ.

2. Приемопередатчик АЛИСА-С АТ1.2 и ретранслятор АЛИСА-С РТ1.2, обладающие мощностью 2 Вт. Дальность передачи сообщений – 16 км. Приемопередатчик подключается к любому устройству с поддержкой Bluetooth. Приемопередатчик и ретранслятор реализованы на базе микроконтроллера, обладают низким энергопотреблением. Устройства были испытаны в рамках III Арктической технологической экспедиции СПбГУТ.

3. Миниатюрный приемопередатчик АЛИСА-С АТ1.3 со встроенной в корпус малогабаритной антенной. Мощность приемопередатчика 0,1 Вт. Дальность передачи сообщений – 2 км. Приемопередатчик реализован на базе микроконтроллера, обладает низким энергопотреблением, удобен для хранения и использования с размещением в кармане одежды. Размеры сопоставимы с размерами шариковой ручки.

4. Компактный приемопередатчик АЛИСА-С АТ2.1 со встроенной в корпус малогабаритной антенной. Мощность приемопередатчика 0,1 Вт. Дальность передачи сообщений – 2 км. Приемопередатчик выполнен в формате устройства, имеющего сенсорный экран и встроенные датчики, имеет операционную систему, обладает функциями, аналогичными смартфону. При необходимости может быть оборудован модулем LTE. Приемопередатчик реализован на базе одноплатного компьютера.

5. Приемопередатчик АЛИСА-С АТ2.2 обладает аналогичными параметрами с приемопередатчиком АЛИСА-С АТ2.1. Отличается наличием дополнительной раскладной штыревой антенны, при использовании которой дальность радиосвязи увеличивается до 4 км.

6. Приемопередатчик АЛИСА-С АТ2.3 обладает аналогичными параметрами с приемопередатчиком АЛИСА-С АТ2.2, но имеет мощность 2 Вт. Дальность радиосвязи – до 16 км.

7. Приемопередатчик АЛИСА-С АТ3.1 обладает мощностью 2 Вт, возможностью установки различных антенн, имеет формат планшета, позволяет передавать сообщения до 16 км. Устройство может быть подключено к стационарной антенне, в том числе направленной, за счет чего расстояние для организации сеанса связи может быть значительно увеличено.

На любом из устройств АЛИСА-С может быть предусмотрена процедура шифрования сообщений с использованием, например шифра Grain-128a или его модификаций [5]. Применяемая при разработке технология позволяет подключать в единую сеть связи любые приемопередатчики и ретрансляторы АЛИСА-С. На приемопередатчики (в том числе обладающие сенсорным экраном) может быть дополнительно установлена кнопочная

клавиатура, обеспечивающая удобную работу с устройством при низких температурах даже в перчатках. Все устройства обладают компактными размерами, малым весом, являются носимыми, могут размещаться в кармане одежды, на ее поверхности на специальных креплениях, в рюкзаке или сумке. Электроснабжение приемопередатчиков и ретрансляторов может осуществляться от аккумуляторов или от электросети. К сети приемопередатчиков и ретрансляторов АЛИСА-С могут быть подключены различные устройства, такие, как:

– автоматический портативный электроэнцефалограф «Катюша» [6];
– автоматическая портативная метеорологическая станция;
– датчики контроля периметра;
– тревожные кнопки;
– прочие датчики и устройства.

Использование одноплатного компьютера позволяет выполнять цифровую обработку сигналов от различных устройств или датчиков (встроенных или подключаемых). Так, благодаря предложенному математическому аппарату синтезированных вейвлетов [7], адаптированных к конкретному типу сигналов, может выполняться частотно-временной анализ сигналов, локализация информационных признаков в сигнале, его сжатие, определение переходных процессов и пр., а по каналу связи передаваться непосредственно результаты обработки, обладающие малым объемом. Такой подход позволяет снизить объем передаваемых данных по каналу радиосвязи и обеспечить оперативность передачи критически важной информации.

Часть из описанных приемопередатчиков и ретрансляторов были испытаны в рамках Трех арктических технологических экспедиций СПбГУТ в пгт. Диксон (2022 г.), на Онежский полуостров (2023 г.), в пгт. Тикси (2024 г.).

В рамках Четвертой арктической технологической экспедиции СПбГУТ, посвященной 130-летию изобретения радио, в деревне Летняя Золотица Архангельской области планируется развернуть сеть передачи данных, которая будет включать различные образцы приемопередатчиков и ретрансляторов АЛИСА-С. Приемопередатчики и ретрансляторы должны быть организованы по принципу mesh-сети. Однако, планируется, что при проведении испытаний, на одном из его этапов, один из приемопередатчиков будет установлен в режим базовой станции с возможностью сбора, обработки и хранения сообщений, а также анализа параметров сети. Такой приемопередатчик будет установлен в центральной части деревни на мачтовом оборудовании. С этой целью разработана разборная конструкция мачты связи высотой 12 м. В качестве основных

элементов конструкции мачты выбраны армированные пластиковые трубы, усиленные канатами, размещенные в их полости. Устойчивость конструкции обеспечивают растяжки и якоря, заглубляемые в грунт. Особенностью мачты является также возможность ее простой сборки и демонтажа, а также изменения высоты, что достигается за счет использования модульного принципа. Каждый модуль собирается из четырех вертикальных и четырех горизонтальных секций. Каждая из вертикальных секций имеет длину 1 м, а длина горизонтальных варьируется в диапазоне от 0,15 м до 1 м. При сборке используются болты и гайки, выполненные из нержавеющей стали. Такой подход обеспечивает мобильность при транспортировке мачты, легкость конструкции, простоту ее установки и демонтажа, возможность адаптации по высоте под конкретный рельеф местности, а также устойчивость к ветровым нагрузкам.

Испытания приемопередатчиков и ретрансляторов АЛИСА-С в рамках Четвертой арктической технологической экспедиции СПбГУТ включают в себя построение на их основе элементов гибридной сети связи и проведение следующих экспериментов:

1. Определение предельной дальности при организации радиосвязи с применением различных приемопередатчиков и ретрансляторов АЛИСА-С в условиях прямой видимости, в условиях застройки, леса и других препятствий, а также в условиях помех.

2. Исследование влияния водной поверхности на организацию радиосвязи.

3. Исследование влияния погодных условий на организацию радиосвязи.

4. Оценка возможности изменения скорости передачи пакетов данных и их длины при различных условиях передачи.

5. Исследование приемопередатчика в режиме базовой станции со сбором, накоплением и обработкой сообщений, анализом параметров сети, а также при подключении другого оборудования, в том числе автоматического портативного электроэнцефалографа, автоматических портативных метеорологических станций, тревожных кнопок и пр.

6. Исследования в интересах выбора оптимальных настроек алгоритма шифрования.

7. Исследования приемопередатчиков, в том числе в режиме базовой станции, и ретрансляторов при взаимодействии с другими элементами гибридной сети связи, в том числе с использованием спутникового оборудования.

8. Другие испытания.

В качестве заключения отметим, что предлагаемые приемопередатчики и ретрансляторы АЛИСА-С могут применяться для организации радиосвязи как

между отдельными абонентами, так и в составе гибридной сети связи. Они могут быть использованы при организации Единой информационной системы Арктической зоны Российской Федерации, предложенной ранее [4].

Список используемых источников

1. Распоряжение Правительства Российской Федерации от 24 ноября 2023 года №3339-р об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года. URL: http://static.government.ru/media/files/Pc7fHuejbNvqv17b0RJNv0RIqTo20lUV.pdf (дата обращения 01.06.2025).

2. Указ Президента Российской Федерации от 26.10.2020 г. № 645 «О Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года». URL: http://www.kremlin.ru/acts/bank/45972 (дата обращения 01.06.2025).

3. Решение Архангельской городской Думы от 30.11.2022 № 598 «Об утверждении Стратегии социально-экономического развития городского округа «Город Архангельск» на период до 2035 года». URL: https://www.arhcity.ru/data/2946/str2022.pdf (дата обращения: 01.06.2025).

4. Степанов А. Б. Разработка автоматического портативного электроэнцефалографа с возможностью интегрирования в Единую информационную систему Арктической зоны Российской Федерации. Электросвязь. 2024. № 12-2. С. 53-60.

5. Соколов Н. С., Степанов А. Б. О применении шифрования при разработке энергоэффективных УКВ приемопередатчиков. Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвященная Дню радио. 2025. № 1 (80). С. 111-114.

6. Степанов А. Б. Автоматический портативный электроэнцефалограф. В сборнике: Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021). Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции. Санкт-Петербург, 2022. С. 150-153.

7. Stepanov A. Polynomial, Neural Network, and Spline Wavelet Models for Continuous Wavelet Transform of Signals. Sensors. 2021. Т. 21. № 19. С. 6416.

FEATURES OF BUILDING A DATA TRANSMISSION NETWORK IN THE VILLAGE OF LETNYAYA ZOLOTITSA, ARKHANGELSK REGION, USING VHF ALISA-S TRANSCEIVERS

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

The work is devoted to the description of the features of building a data transmission network in the village of Letnyaya Zolotitsa (Arkhangelsk region) using VHF ALISA-S transceivers developed under the scientific guidance of the author of this article. The description and characteristics of ALISA-S transceivers, the proposed design of mast equipment for conducting research, and the methodology for testing equipment as part of a hybrid communications network are given.

Key words: *VHF transceivers, mast equipment, hybrid communication network, repeater, ALISA-S*

УДК 519.6, 677.070
ГРНТИ 64.01.77, 64.29.35

ИСПОЛЬЗОВАНИЕ СРЕДЫ MATLAB ДЛЯ ВЫПОЛНЕНИЯ РАСЧЕТОВ ПРИ ИССЛЕДОВАНИИ СВОЙСТВ ПАРААРАМИДНЫХ НИТЕЙ

А. Б. Степанова

Санкт-Петербургский политехнический университет Петра Великого

При выполнении исследований и при получении большого объема данных всегда возникает вопрос о правильной обработке полученных данных. В частности, при проведении исследований свойств параарамидных нитей, был получен большой объем данных, которых необходимо было правильно и корректно обработать. Среда MATLAB помогает правильно и корректно обработать полученные результаты работы, получать наглядные графики.

параарамидные нити, среда MATLAB, обработка данных

Параарамидные волокна и нити известны своими уникальным свойствам и широко используются в различных областях науки и техники: для создания композиционных материалов для ракетной и космической промышленности, средств индивидуальной бронезащиты, защитной оплетки кабелей различного назначения, в автомобильной промышленности (для шинного корда, ремней трансмиссионных, автомобильных шлангов), для теплоизолирующей продукции (рукавов, приводов и т. п.), в качестве спецодежды для металлургов и пожарных.

Среди таких волокон и нитей отдельно стоит выделить волокна и нити под торговыми марками Русар® и Армос® (ОАО «Каменскволокно», Россия), Технора® (Teijin, Япония), Тварон® (Teijin Twaron b. v., Нидерланды), Кевлар (Du Pont de Nemour, США).

В процессе эксплуатации параарамидные волокна и нити в составе изделий подвергаются воздействию различных эксплуатационных факторов: температур (как повышенных, так и экстремально пониженных), агрессивных сред, влажности, микроорганизмов, УФ-излучение [1-7]. Несмотря на то, что данные материалы обладают высокими прочностными характеристиками, при воздействии эксплуатационных факторов может происходить значительное снижение прочности. Поэтому необходимо точно спрогнозировать поведение параарамидных волокон и нитей непосредственно при

воздействии суммарных факторов: например, таких как температура и агрессивные среды, УФ-излучение и температуры (в частности низкие температуры, например, используемых в кабелях для буровых установок), воздействие влаги и экстремально низких температур и т. п. Полученные данные помогут расширить ассортимент изделий с их применением, а также понять какие дополнительные изменения нужно внести для улучшения долговечности изделий.

Основным методом оценки прочностных характеристик нитей является испытание на одноосное растяжение. Для получение статистических данных, необходимо провести большой ряд исследований для получения:

– диаграмм растяжения,
– относительного разрывного удлинения, $\Delta\varepsilon$
– относительной величины деформации, $\Delta\sigma$
– относительной разрывной нагрузки, P_{ts}/P_o
– удлинения при разрыве, $\varepsilon_{\text{ts}}/\varepsilon_o$,
– модуля деформации, E, ГПа.

После получения большого объема данных, всегда возникает вопрос о правильной обработке полученных данных и о их корректном графическом отображении.

Для этой цели можно использовать различное программное обеспечение, но для упрощения работы и сокращения времени обработки данных можно использовать среду MATLAB.

Среда MATLAB имеет интуитивно понятный интерфейс с большим множеством функций, что немаловажно при работе с новой программой, когда необходимо быстро и качественно обработать данные. Благодаря интерактивной среде, можно выполнять команды и тут же вносить изменения, видя результаты запущенных команд. Однако, для получения правильных расчетов, детальной обработки данных и получения точной визуализации необходимо обладать рядом необходимых знаний. В частности, среда MATLAB обладает мощными математическими возможностями. Следует также отметить, что программа содержит большую библиотеку функций (в т. ч. для обработки графиков, что немаловажно особенно когда необходимо грамотно отобразить полученные данные) [8].

Среда MATLAB позволяет создавать графики различной сложности.

Для графического отображения полученных данных можно использовать графику двух типов:

– двумерная, трехмерная растровая графика;

– дескрептовая графика (handle).

Для визуализации данных в среде MATLAB можно выбрать один из множества встроенных графиков [9].

Для построения двумерных графиков можно использовать встроенную функцию «plot» (данная функция позволяет выполнять построение графиков в декартовой системе координат): для графика в линейном масштабе, например, для оформления диаграмм растяжения. При этом использование функции «readtable» позволяет импортировать данные из файла в таблицу.

Встроенные функции «xlabel ()», «ylabel ()», "xtickangle ()» и "ytickangle ()» позволяют наносить создаваемые метки и настраивать их положение на осях «x» и «y» соответственно [10].

Также, в среде MATLAB существуют другие полезные встроенные функции: например, с помощью функции «bar» можно выполнять построение диаграмм. Аналогичная команда «barh» позволяет отображать столбцы диаграммы в горизонтальном положении. Функция «errorbar» – выполняет построение графика с указанием интервала погрешности.

Функция «hist» выполняет построение гистограмм (данная функция может полезна для отображения данных о температуре начала термического разложения на воздухе и в среде азота).

Следует отметить и о других полезных встроенных функциях, позволяющих настраивать надписи и пояснения к графикам («text» – добавление к графику текста; «title» – создание заголовков для двумерных и трехмерных графиков; «legend» – для создания пояснений к графику; «clabel» – для маркировки линий уровня на контурных графиках).

Наибольший интерес для исследовательских работ представляет возможность создавать собственные скрипты и функции с возможностью их запуска из командной строки MATLAB или из других скриптов и функций.

Среда MATLAB позволяет автоматизировать задачи с помощью скриптов. Возможно комбинировать команды для создания скриптов, автоматизирующий процесс работы. Можно добавлять высокоуровневые конструкции, операторы / циклы, для сложной логики, автоматизируя рутинные и сложные задачи.

Еще одним преимуществом является наличие редактора «Live», с помощью которого можно создать скрипт как исполняемую записную книжку: код, его вывод и визуализации будут отображаться рядом друг с другом.

Немаловажным является гибкость выполнения задач: например, можно запустить целиком скрипт, как программу или запустить отдельными секциями по мере необходимости.

И что немаловажным является, особенно когда идет речь о командных исследованиях, возможно задокументировать выполненную работу, используя отформатированный текст, изображения и т.п., для того, чтобы в дальнейшем поделиться готовым интерактивным документом.

Также, можно добавлять аннотации для наглядности: можно использовать различные визуальные элементы, такие как изображения, различный текст, возможные уравнения, гиперссылки или ссылки непосредственно на определенные функции MATLAB и т.п., тем самым делая работу более понятной для восприятия [9].

В заключение стоит отметить, что среда MATLAB соединяет в себе не только возможность выполнять сложные вычисления, осуществлять визуализацию числовых данных, но и выполнять сложные задачи с помощью программирования, что создает оптимальную среду не только для обработки данных и их визуализации, но и для создания прогноза поведения тех или иных объектов исследования при определенных условиях.

Список используемых источников

1. Дьянкова Т. Ю., Лебедева Г. Г., Мещерякова Г. П., Степанова А. Б. Влияние агрессивных сред и температуры на механические свойства параарамидных нитей // Дизайн. Материалы. Технология. 2013. № 5 (30). С. 48-50.

2. Лебедева Г. Г., Мещерякова Г. П., Степанова А.Б. Изменение механических свойств параарамидных нитей после воздействия высоких температур // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2013. № 3. С. 17-20.

3. Перепелкин К. Е., Гребенников С. Ф., Лебедева Н. П. Сорбция водяных паров высокопрочными параарамидными нитями // Химические волокна. 2007. № 5. С. 50-52.

4. Перепелкин К. Е., Гребенников С. Ф., Лебедева Н. П., Зайцева Е. И. Взаимодействие параарамидных волокнистых материалов с водой // Известия высших учебных заведений. Технология легкой промышленности. 2008. Т. 2. № 2. С. 37-43.

5. Мещерякова Г. П., Степанова А. Б. Изменение механических свойств параарамидных нитей под воздействием агрессивной среды // Известия высших учебных заведений. Технология легкой промышленности. 2012. Т. 18. № 4. С. 3-6.

6. Басок М. О., Дянкова Т. Ю., Степанова А. Б. Изменение термических свойств параарамидных нитей после воздействия агрессивной среды // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2013. № 3. С. 13-16.

7. Мещерякова Г. П., Степанова А. Б., Иванькова Е. М. Изменение свойств параарамидных нитей после действия ионизирующего излучения // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2012. № 3. С. 49-52.

8. Дьяконов В. П. MATLAB. Полный самоучитель. М.: ДМК Пресс, 2012. 768 с. ISBN 9785940746522.

9. MATLAB. Официальный сайта компании. URL: https:// www.mathworks.com/products/matlab/programming-with-matlab.html (дата обращения 13.08.25).

10. Manish Kumar Saini. How to Create Custom Axis Labels in MATLAB. URL: https:/www.tutorialspoint.com/how-to-create-custom-axis-labels-in-matlab (дата обращения 13.08.2025).

USING THE MATLAB ENVIRONMENT TO PERFORM CALCULATIONS IN THE STUDY OF PARA-AMIDE NITES PROPERTIES

Stepanova A.
Peter the Great Saint Petersburg Polytechnic University

When conducting research and obtaining a large amount of data, the question of how to properly process the data arises. In particular, when conducting research on the properties of para-aramid fibers, a large amount of data was obtained that needed to be processed correctly and accurately. The MATLAB environment helps to process the results of the work correctly and accurately, and to generate visual graphs.

Key words: *para-aramid threads, MATLAB environment, data processing*

УДК 677. 070
ГРНТИ 64.29.35

ОБЗОР ИССЛЕДОВАНИЙ СВОЙСТВ ПАРААРАМИДНЫХ НИТЕЙ ПРИ ВОЗДЕЙСТВИИ НИЗКИХ ТЕМПЕРАТУР

А. Б. Степанова

Санкт-Петербургский политехнический университет Петра Великого

Параарамидные нити благодаря своим уникальным свойствам получили широкое применение в различных отраслях науки и техники. В частности, они используются для изготовления защитной одежды для полярных экспедиций. Тросы из Twaron применяются для буровых установок. В статье рассмотрены, результаты исследований, проводимых по изучению свойств параарамидных волокон (нитей) при воздействии отрицательных температур. Приведены методики проведения испытаний и представлены полученные данные.

параарамидные нити, влияние температур, механические свойства

Параарамидные нити обладают рядом уникальных свойств, благодаря чему нашли широкое применение в различных изделиях. Защитная оплетка для различных кабелей, средства индивидуальной защиты (в т. ч. бронежилеты), средства спасения и безопасности (тросы, канаты, веревочные лестницы, страховочные ремни и т.п.), теплоизолирующая продукция, трансмиссионные ремни, автомобильные шланги, композиционные материалы для ракетной и космической промышленности, конструктивные пластики для кораблестроительной промышленности и т.п. – это лишь немалый перечень, где данные волокна и нити нашли свое применение [1-5].

Экстремальные условия Арктики, такие как температура -40^{0}С и ниже, агрессивные среды, сильные ветра и т.п., требуют применения материалов с особенными свойствами, способными выдерживать особенные климатические условия.

Рассмотрим основные свойства параарамидных нитей, благодаря которым их возможно использовать в непростых климатических условиях Арктики:

– термостабильность (является одним из самых наиболее важных факторов, благодаря которому данные нити могут применяться в качестве многих изделий, связанных с воздействием как экстремально отрицательных, так

и повышенных температур) – сохранение свойств при воздействии температур в пределах от -196^{0}С до +400^{0}С;
– высокая прочность при малом весе (прочность нити Технора Т200 достигает 3,0 – 3,4 ГПа, в то время как нитей Тварон, Кевлар – данные показатель достигает 2,7 – 3,5 ГПа, у Армоса и Русара этот показатель значительно выше 4,5 – 5,5 ГПа);
– низкая теплопроводность (благодаря чему параарамидные волокна и нити могут использоваться в теплоизолирующей продукции и в элементах техники, где требуются использование данных свойств);
– данные нити химически устойчивы к воздействию различных агрессивных сред: нефтепродуктов, многих видов химикалиев, микроорганизмов и т.п. [6].

Благодаря своему химическому составу и особенностям производства, параарамидные нити обладают комплексом физико-механических свойств (включая высокие прочностные показателей нитей). При этом у данных нитей отсутствует хрупкость (что присуща некоторых видам полимеров). Они имеют минимальное тепловое расширение, что особенно важно при использовании для композитных конструкций. Поэтому они нашли применение в т.ч. в условиях Арктики для различных технических изделий.

Вследствие низкой теплопроводности данные нити можно применять для защитной одежды полярников с многослойными мембранами (перчатки, элементы обуви – т.к. данные нити устойчивы к истиранию и обледенению). По данным компании DuPont [7], по сравнению с традиционными материалами, применяемыми для изготовления защитной одежды для полярников, использование параарамидных нитей приводит к уменьшению теплопотерь на 30 %.

Также, данные нити применяются для изготовления ряда технических изделий, эксплуатируемых в условиях экстремально пониженных температур:
– тросов и канатов (например, используемых на нефтегазовых платформах, а также для буровых установок);
– для армирования трубопроводов и резервуаров;
– в качестве композитных материалов спутников (здесь происходит воздействие экстремальных отрицательных температур);
– для усиления шин снегоходов и вездеходов;
– термостойкие чехлы для защиты техники и т.п.

Стоит отметить еще один положительный момент применения нитей Кевлар для армирования термопластиковых труб: благодаря своей устойчивости к коррозии, прочности и гибкости данные изделия легко монтировать и позволяет использовать трубы с более высоким номинальным давлением.

Однако, существуют и некоторые отрицательные свойства данных нитей: параарамидные нити, при набухании могут терять до 7 % прочности; в условиях воздействия мощного арктического солнца существует риск разрушения от сильного УФ-воздействия на протяжении длительного времени.

Рассмотрим некоторые исследования, посвященные изучению свойств параарамидных волокон и нитей в условиях экстремально низких температур.

В работе [8] проведены исследования по изучению повышенных и пониженных температур на механические свойства параамидных тканей, изготовленных из нитей Русар. Приведена методика испытаний. полученные в ходе эксперимента данные, а также разработанная математическая модель, позволяющая прогнозировать механические свойства нитей в зависимости от величины воздействия температуры и длительности воздействия. Образцы исследований подвергались замораживанию, а затем воздействию повышенных температур (в пределах от -25^0C до $+300^0$C). Разработанная математическая модель позволяет прогнозировать механические свойства нитей в зависимости от величины воздействия температуры и длительности воздействия.

Наиболее подробные и системные исследования [6] проводились компанией DuPont. Например, проведены сравнительные исследования по изучению свойств нити Кевлар с сверхвысокомолекулярным полиэтиленом высокой плотности (СВМПЭ) и сталью. В ходе исследований было выявлено, что использование материала Кевлар обеспечивает лучшую ползучесть по сравнению с (СВМПЭ) и при этом обладает наибольшей прочностью по сравнению со сталью. Эти немаловажные показатели говорят о том, что Кевлар является более надежным материалом для работы в тяжелых морских климатических условиях, может эксплуатироваться как более надежная и гибкая альтернатива по сравнению со приведенными материалами.

Остальные исследования по изучению свойств параарамидных нитей в условиях низких температур, свойственных для климатических условий Арктики и находящихся в открытом доступе носят разрозненный данные.

Наряду с широко известными параарамидными нитями, ведутся разработки по созданию новых волокон, нитей и тканей на их основе. В частно-

сти, в работе [9] описываются исследованные свойства разработанной термостойкой ткани, которая может одновременно эксплуатироваться в экстремальных условиях Арктики и выдерживать температуры до -60^{0}С (в качестве защитной одежды) и при необходимости испытывать повышенные температуры. В частности, была разработана ткань, особенностью которой является то, что она выработана из смесовой двухниточной пряжи, которая включает в себя параарамидные и полиоксидиазольные волокна (для данных волокон свойственна высокая хемостойкость, термостабильность, пониженная горючесть) в соотношении 50х50 (переплетение комбинированное полотняное основных и уточных нитей: основным и уточным репсов – соответственно по основе и утку). Дополнительно данная ткань была обработана фторорганическим препаратом.

Однако для улучшения и продления срока эксплуатации данных изделий требуется проведение дополнительных исследований, что говорит о необходимости проведения дальнейших исследований и разработке новых материалов на основе существующих для расширения области их применения.

Список используемых источников

1. Лебедева Г. Г., Мещерякова Г. П., Степанова А. Б. Изменение механических свойств параарамидных нитей после воздействия высоких температур // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2013. № 3. С. 17-20.

2. Сайт производителя волокон Технора®. URL: https://fibrxl.com/fibrxl-performance/fibers/technora (дата обращения 09.08.2025).

3. Дьянкова Т. Ю., Лебедева Г. Г., Мещерякова Г. П., Степанова А. Б. Влияние агрессивных сред и температуры на механические свойства параарамидных нитей // Дизайн. Материалы. Технология. 2013. № 5 (30). С. 48-50.

4. Кустов А. В., Рожкова Е. А., Бордачев В. А. Композиционные материалы в ракетно-космической отрасли. // Наука, технологии, общество – НТО-II-2022. сб. науч. ст. по материалам II Всероссийской науч. конф., Красноярск, 2022. С. 101-109.

5. Мещерякова Г. П., Степанова А. Б. Изменение механических свойств параарамидных нитей под воздействием агрессивной среды // Известия высших учебных заведений. Технология легкой промышленности. 2012. Т. 18. № 4. С. 3-6.

6. Сайт компании DuPont. URL: https://www.dupont.com/content/aramids/amer/us/en/kevlar/kevlar-for-built-in-performance/oil-and-gas-kevlar.html (дата обращения 14.08.2025).

7. Степанова А. Б. Влияние условий эксплуатации на механические свойства параарамидных нитей: дис. канд. техн. наук: 05.19.01 / Степанова Анна Борисовна. Санкт-Петербург, 2014. 241 с.

8. Курденкова А. В., Шустов Ю. С. Разработка методов оценки влияния температурного воздействия на механические свойства тканей из нитей Русар // Научно-методи-

ческий электронный журнал «Концепт». 2016. Т. 3. С. 41–45. URL: http://e-koncept.ru/2016/56020.htm (дата обращения 14.08.2025).

9. Козлов И. Г., Тарасов В. П., Бородин С. В., Криволапова О. Н., Иванюсь Н. В. Термостойкая ткань из полимерных волокон и изделие, выполненное из этой ткани. Пат. 2614002C1 Российская Федерация; заявитель и патентообладатель Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский технологический университет "МИСиС". – № 2016116711; заявл. 06.04.2016; опубл. 28.04.2016.

REVIEW OF RESEARCH ON THE PROPERTIES OF PARA-AMIDE NITES AT LOW TEMPERATURES

Stepanova A.
Peter the Great Saint Petersburg Polytechnic University

Due to their unique properties, para-aramid threads are widely used in various fields of science and technology. In particular, they are used to make protective clothing for polar expeditions. Twaron cables are used for drilling rigs. This article discusses the results of research conducted to study the properties of para-aramid fibers (threads) under the influence of negative temperatures. The article provides test methods and presents the obtained data.

Key words: *para-aramid threads, temperature effects, and mechanical properties*

АВТОРЫ СТАТЕЙ

АБРАМОВА Нина Ивановна — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, HIAbram@yandex.ru

АВАКЯН Сергей Артурович — студент группы ИКТИ-45м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, avakyan.sa@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

АЛЛИ Рашид Амидуевич — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alli.ra@sut.ru

АНТОНЮК Евгений Артурович — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, evgeniy-antoniuk@rambler.ru

АНТРОПОВА Лидия Александровна — магистрант группы ИКТИ-45м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, antropova.la@sut.ru

АРЛАНЦЕВА Юлия Александровна — техник Студенческого конструкторского бюро Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arlanceva.ua@sut.ru

АРСИРИЙ Алла Ивановна — кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, arsirii.ai@net.sut.ru

БАБАНОВ Захар Дмитриевич — магистрант группы ИКТИ-45м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, babanov.zd@sut.ru

БАБАНОВ Захар Дмитриевич — студент группы ИКТИ-45м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, babanov.zd@sut.ru

БАГАЕВ Егор Сергеевич — аспирант кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bagaev.es@sut.ru

БАДАСЯН Артем Николаевич — студент группы ИКВТ-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, badasian.an@sut.ru

БЕРЕЗИНА Юлия Сергеевна — инженер ООО «Вижен Сервис», Julia.Berezina@mail.ru

БЕРЁЗКИН Александр Александрович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, berezkin.aa@sut.ru

БЕРЕСТОВСКИЙ Павел Андреевич — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, berest.pv@mail.ru

БИКБУЛАТОВ Владислав Родионович — адъюнкт научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, vlaad.bik@icloud.com

БИЛАН Виктория Викоторовна — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, bilan_vv@bk.ru

БОЙКО Игорь Андреевич — ассистент кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, boiko.ia@sut.ru

БОРИСОВ Сергей Викторович — кандидат технических наук, доцент, доцент кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А.Бонч-Бруевича, borisov.sv@sut.ru

БРАГИНА Алёна Эдуардовна — специалист АО «Научно-исследовательский институт «РУБИН», A.E.Bragina@rubin-spb.ru

БУРУМБАЕВ Даниль Ильмирович — старший преподаватель кафедры информационных систем и технологий Уральского технического института связи и информатики (филиал) Сибирского государственного университета телекоммуникаций и информатики, bdi@urtisi.ru

БУЧАТСКИЙ Александр Николаевич — кандидат технических наук, доцент кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, abuchatsky@sut.ru

БУЧИН Даниил Дмитриевич — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, dbuchind@bk.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

ВЕТОШЕВ Владислав Олегович — эксперт Международного центра цифровой криминалистики Санкт-Петербургского Федерального исследовательского центра Российской академии наук, mrgimx@gmail.com

ВИВЧАРЬ Роман Михайлович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vivchar.rm@sut.ru

ВИКУЛОВ Антон Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vikulov.as@sut.ru

ВИТКОВА Лидия Андреевна — кандидат технических наук, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vitkova@comsec.spb.ru

ВЛАДЫКО Андрей Геннадьевич — кандидат технических наук, доцент, декан факультета радиоэлектронных систем и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladyko@sut.ru

ВОЛОСТНЫХ Виктор Анатольевич — кандидат военных наук, доцент, научный сотрудник Военной академии связи имени Маршала Советского Союза С. М. Буденного, ra1alo@mail.ru

ВОЛОШИНОВ Денис Вячеславович — доктор технических наук, профессор, заведующий кафедрой информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, denis.voloshinov@yandex.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

ГЕРЛИНГ Екатерина Юрьевна — кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gerling.eu@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

ГОЛЬДШТЕЙН Александр Борисович — доктор технических наук, профессор кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, goldshtein.ab@sut.ru

ГОНЧАРОВ Владимир Андреевич — магистрант группы ИКПИ-492м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, goncharov.va@sut.ru

ГОРДА Максим Дмитриевич — аспирант, младший научный сотрудник Международного центра цифровой криминалистики Санкт-Петербургского Федерального исследовательского центра Российской академии наук, gordamd@ya.ru

ГОРОБЦОВ Илья Александрович — старший преподаватель кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gorobcov.ia@sut.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

ГРОМОВ Владислав Витальевич — кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gromov.vv@sut.ru

ГУБИН Александр Николаевич — кандидат технических наук, доцент, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gubin.an@sut.ru

ДАВЫДОВА Екатерина Викторовна — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, davydova.ev@sut.ru

ДЕМЕНТЬЕВ Михаил Евгеньевич — студент группы ИКВТ-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dementev.me@sut.ru

ДУЛАЕВ Руслан Аланович — техник Студенческого конструкторского бюро Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dulaev.ra@sut.ru

ДУНАЙЦЕВ Роман Альбертович — кандидат технических наук, PhD, доцент кафедры сетей связи и передачи данных, заместитель декана факультета инфокоммуникационных сетей и систем по научной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, roman.dunaytsev@sut.ru

ЕЛАГИН Василий Сергеевич — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, v.elagin@sut.ru

ЕЛИСЕЕВ Никита Константинович — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eliseev.nk@sut.ru

ЕЛИСЕЕВ Сергей Михайлович — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, eliseev.sm@sut.ru

ЖЕРНОВА Ксения Николаевна — кандидат технических наук, старший научный сотрудник Международного центра цифровой криминалистики Санкт-Петербургского Федерального исследовательского центра Российской академии наук, zhernova@comsec.spb.ru

ЖУРАВЛЁВ Владимир Анатольевич — кандидат сельскохозяйственных наук, старший научный сотрудник научно-технического отдела Белорусской государственной академии связи, zhuravlyov-77@mail.ru

ЗАДБОЕВ Вадим Александрович — младший научный сотрудник Военной академии связи имени Маршала Советского Союза С. М. Буденного, zadboev89@mail.ru

ЗАЙЦЕВА Зинаида Викторовна — кандидат технических наук, доцент кафедры электроники Санкт- Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaitch@sut.ru

ЗАЙЧИКОВ Кирилл Дмитриевич — техник Студенческого конструкторского бюро Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zaichikov.kd@sut.ru

ЗАПАЙЩИКОВ Александр Викторович — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zapaishikov.av@sut.ru

ЗЕЛЕНЦОВ Виктор Валентинович — кандидат технических наук, доцент кафедры робототехнических систем и мехатроники Московского государственного технического университета им. Н. Э. Баумана, victor.zelentsov@bmstu.ru

ЗИКРАТОВ Игорь Алексеевич — доктор технических наук, декан факультета кибербезопасности Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zikratov.ia@sut.ru

ИВАНЕНКО Тамара Александровна — старший методист военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ivanenko.ta@sut.ru

КАЛИБАБЧУК Артём Олегович — студент группы СМ7-23М Московского государственного технического университета им. Н. Э. Баумана, armterrus@yandex.ru

КАРПЕНКО Даниил Евгеньевич — студент группы ИТИ-41 Гомельского государственного технического университета им. П. О. Сухого, protankist343@gmail.com

КАЧНОВ Андрей Владимирович — аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kachnov.av@sut.ru

КВАША Надежда Владимировна — кандидат экономических наук, доцент, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kvasha.nv@sut.ru

КНИГИНИЦКИЙ Егор Игоревич — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kniginickii.ei@sut.ru

КОВАЛЬСКИЙ Игорь Валериевич — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, kovalskiiv_ru@mail.ru

КОЗЛОВ Андрей Алексеевич — специалист отдела разработки программного обеспечения АО «Научно-исследовательский институт «РУБИН», andrey.kozlov.01@inbox.ru

КОЗЛОВА Алёна Игоревна — студент группы ИКВТ-31, техник Центра перспективных проектов и разработок Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kozlova.ai@sut.ru

КОЛИНКО Инна Павловна — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, kiina131313@gmail.com

КОРЖИК Валерий Иванович — доктор технических наук, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korzhik.va@sut.ru

КОРНЮШКИН Дмитрий Александрович — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kornushkin.da@sut.ru

КОРОВИН Константин Олегович — кандидат физико-математических наук, заведующий кафедрой радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korovin.ko@sut.ru

КОРОВКИНА Екатерина Викторовна — ассистент кафедры систем обработки данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, korovkina1.ev@sut.ru

КОТЛОВА Мария Владимировна — начальник научного отдела государственного учета музейных ценностей Военно-исторического музея артиллерии, инженерных войск и войск связи, mkotlova@gmail.com

КРАСОВ Андрей Владимирович — кандидат технических наук, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krasov.av@sut.ru

КРЫЛОВ Андрей Альбертович — кандидат технических наук, доцент кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, krylov.aa@sut.ru

КУКУНИН Дмитрий Сергеевич — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, kukunin.ds@sut.ru

КУЛЬСИТОВА Карина Акумгалеевна — техник Студенческого конструкторского бюро Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kulsitova.ka@sut.ru

КУРОЧКА Константин Сергеевич — кандидат технических наук, доцент, заведующий кафедрой информационных технологий Гомельского государственного технического университета им. П. О. Сухого, kkostik@inbox.ru

КУШНИР Дмитрий Викторович — кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kushnir.dv@sut.ru

КЮНЕР Андрей Павлович — аспирант Санкт-Петербургского Федерального исследовательского центра Российской академии наук, kunerandrey@mail.ru

ЛАБКОВСКАЯ Римма Яновна — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, labkovskaia.ria@sut.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

ЛЕБЕДЕВА Наталья Павловна — кандидат технических наук, доцент кафедры материаловедения и товарной экспертизы Санкт-Петербургского государственного университета промышленных технологий и дизайна, tms@sutd.ru

ЛЕЩИНСКИЙ Богдан Сергеевич — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, dnr_1910@mail.ru

ЛИПАТНИКОВ Валерий Алексеевич — доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, lipatnikovanl@mail.ru

ЛИТВИНОВ Владислав Леонидович — кандидат технических наук, доцент, заведующий кафедрой информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vlitvinov@sut.ru

ЛОСЕВ Арсений Павлович — аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, losev.ap@ sut.ru

ЛУКАШЕНОК Василий Ильич — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, lukasenokvasilij@gmail.com

ЛЮБИМОВ Александр Геннадьевич — кандидат технических наук, доцент кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Lubimov.ag@sut.ru

ЛЯЛИНА Анна Жановна — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lyalinanna@gmail.com

ЛЯЩУК Михаил Зиновьевич — кандидат технических наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, HIAbram@yandex.ru

МАЙОРОВ Александр Владимирович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Mayorov.AV@sut.ru

МАКАРЕНКО Денис Владимирович — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, nsdivdeni@yandex.ru

МАКСИМЕНКО Сергей Олегович — магистрант группы ИКТИ-45м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, maksimenko.so@sut.ru

МАЛАХОВ Владислав Евгеньевич — аспирант кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета им. проф. М.А. Бонч-Бруевича, младший научный сотрудник Института проблем транспорта им. Н. С. Соломенко Российской академии наук, malahov.ve@sut.ru

МАРОЧКИНА Анастасия Вячеславовна — кандидат технических наук, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, strelchuk.av@sut.ru

МАТЮХИНА Татьяна Владимировна — кандидат технических наук, доцент, заместитель декана факультета радиоэлектронных систем и робототехники по учебной работе Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ius@sut.ru

МЕДВЕДЕВ Сергей Алексеевич — кандидат сельскохозяйственных наук, старший преподаватель кафедры систем обработки данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, medvedev1.sa@sut.ru

МЕЖЕВОВ Павел Александрович — старший преподаватель кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mezhevov.pa@sut.ru

МИХАЙЛИК Егор Артемович — студент группы ИКПИ-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mihailik.ea@sut.ru

МИХНЕВИЧ Светлана Юрьевна — кандидат физико-математических наук, доцент кафедры инфокоммуникационных технологий Белорусской государственной академии связи, s.mikhnevich@bsac.by

МОЛОКОВ Даниил Антонович — техник кафедры систем обработки данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, molokov.da@sut.ru

МОШАК Николай Николаевич — доктор технических наук, доцент, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, профессор кафедры информационной безопасности Санкт-Петербургского государственного университета аэрокосмического приборостроения, moshak.nn@sut.ru

НЕГУРИЦА Анастасия Олеговна — адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного, LadyN98@yandex.ru

НИКОЛАЕВА Полина Арсеновна — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, panicolaeva@mail.ru

НОВИКОВ Евгений Владимирович — кандидат технических наук, доцент, ведущий научный сотрудник отраслевой лаборатории перспективных информационно-коммуникационных технологий Белорусской государственной академии связи, e.novikov@bsac.by

ОСТРОУМОВА Юлия Сергеевна — доктор педагогических наук, доцент, заведующий кафедрой биологической и медицинской физики Военно-медицинской академии им. С. М. Кирова, sinklit@mail.ru

ПАВЛОВСКАЯ Анна Александровна — аспирант кафедры аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, birukova1.aa@sut.ru

ПАВЛОВСКИЙ Михаил Валентинович — аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavlovskii.mv@sut.ru

ПАНКОВ Арсений Владимирович — ассистент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pankov.av@sut.ru

ПАРАМОНОВ Александр Иванович — доктор технических наук, доцент, профессор кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, paramonov@sut.ru

ПАЧИН Андрей Владимирович — кандидат технических наук, доцент кафедры программной инженерии и вычислительной техники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pachin.av@sut.ru

ПЕРЕЛЫГИН Сергей Васильевич — кандидат технических наук, доцент кафедры звукорежиссуры Санкт-Петербургского государственного института кино и телевидения, sergey.perelygin@gmail.com

ПЕРОВ Роман Александрович — кандидат технических наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, perov_ra1245@mail.ru

ПЛОТНИКОВ Павел Владимирович — кандидат физико-математических наук, доцент, заведующий кафедрой высшей математики Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, plotnikov.pv@sut.ru

ПОПОВ Аликс Алексеевич — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, popov2.aa@sut.ru

ПРАСОЛОВ Александр Александрович — кандидат технических наук, доцент кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, prasolov.aa@sut.ru

РАКОВСКИЙ Олег Владимирович — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rakovskii.ov@sut.ru

РЮТИН Константин Евгеньевич — аспирант кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rutin.ke@sut.ru

РЯБИКОВ Дмитрий Сергеевич — аспирант кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ryabikov.ds@sut.ru

САГДЕЕВ Александр Константинович — подполковник, преподаватель кафедры радиорелейной и тропосферной связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sagdeev@sut.ru

САДОВНИКОВ Владимир Евгеньевич — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, bladimir1998@mail.ru

САЕНКО Игорь Борисович — доктор технических наук, профессор кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, saenko_ib@bk.ru

САЗОНОВ Виктор Викторович — кандидат технических наук, доцент, докторант военной академии связи им. Маршала Советского Союза С. М. Буденного, vmktor-sazonov@yandex.ru

САННИКОВА Полина Александровна — магистрант группы ИКТИ-45м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sannikova.pa@sut.ru

СВЕТОВА Анастасия Васильевна — магистрант группы ИКТГ-34м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, svetova.av@sut.ru

СЕМЕНОВ Андрей Борисович — доктор технических наук, профессор кафедры механизации, автоматизации и роботизации строительства Национального исследовательского университета Московского государственного строительного университета, andre52.55@mail.ru

СЕМЕНОВИЧ Алена Юрьевна — преподаватель кафедры инфокоммуникационных технологий Белорусской государственной академии связи, 21alena02@gmail.com

СИДОРКОВИЧ Дарья Романовна — ассистент кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sidorkovich.dr@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

СКОРОБОГАТОВА Светлана Алексеевна — аспирантка кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, skorobogatova.sa@sut.ru

СТЕПАНОВ Андрей Борисович — кандидат технических наук, доцент, заместитель директора института магистратуры по учебной работе, доцент кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stepanov.ab@sut.ru

СТЕПАНОВА Анна Борисовна — кандидат технических наук, старший преподаватель института энергетики Санкт-Петербургского политехнического университета Петра Великого, stepanova-anna-b@yandex.ru

СТРЕМЕДЛОВСКИЙ Александр Валентинович — аспирант Уральского государственного педагогического университета, university-mail@mail.ru

СУДЕНКОВА Анастасия Вячеславовна — студент группы РТ-11 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sudenkova.av@sut.ru

СЫРОВЕТНИК Дмитрий Сергеевич — инженер ООО «Амунго», syrovetnikds@mail.ru

СЫЧУЖНИКОВ Виктор Борисович — кандидат технических наук, старший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, sichujnikov@bk.ru

ТАМБОВЦЕВ Глеб Ильич — инженер студенческого конструкторского бюро Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tambovtsev.gi@sut.ru

ТАНАШЕВ Султан Русланович — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tanashev.sr@sut.ru

ТАРАНУЩЕНКО Александр Павлович — научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, taranuchenkoap@bk.ru

ТАРАСОВ Владимир Анатольевич — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vat-liquidator@bk.ru

ТАТАРИНОВ Владимир Иннокентьевич — кандидат технических наук, заместитель начальник научно-исследовательского отдела Военной академии связи имени Маршала Советского Союза С. М. Буденного, tatar271@mail.ru

ТКАЧЕВ Дмитрий Федорович — кандидат технических наук, начальник отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, dimas.portnoy@inbox.ru

ТУМАНОВА Евгения Ивановна — кандидат технических наук, доцент кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tumanova.ei@sut.ru

ТЭТ Наунг — студент Белорусского государственного университета информатики и радиоэлектроники, s.mikhnevich@bsac.by

УРАЛОВ Михаил Александрович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, uralov_mixa@mail.ru

УШАКОВ Игорь Александрович — кандидат технических наук, и. о. заведующего кафедрой информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakov.ia@sut.ru

ФЁДОРОВ Сергей Леонидович — кандидат технических наук, доцент, заведующий кафедрой цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergey.fedorov@sut.ru

ФЕДОТОВ Андрей Александрович — магистрант группы МАП-2512 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fedotov.aa@sut.ru

ФИЛИППОВ Феликс Васильевич — кандидат технических наук, старший научный сотрудник, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, filippov.fv@sut.ru

ХАНИН Самуил Давидович — доктор физико-математических наук, профессор, профессор кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций имени профессора М. А. Бонч-Бруевича, khanin.sd@sut.ru

ХОАНГ Фыок Ньян — аспирант кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khoang.fn@sut.ru

ХРЕНОВ Андрей Александрович — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hrenov.aa@sut.ru

ХЫА Хю Кыонг — аспирант кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khya.khk@sut.ru

ЧЕНСКИЙ Александр Александрович — инженер Центра перспективных проектов и разработок Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chenskii.aa@sut.ru

ЧЕЧУЛИН Андрей Алексеевич — кандидат технических наук, доцент лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук, andreych@bk.ru

ЧИКАЛОВ Никита Вячеславович — старший инженер-программист отдела разработки программного обеспечения АО «Научно-исследовательский институт «Рубин», nik.chikalow2011@yandex.ru

ЧИПСАНОВА Елена Валерьевна — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chipsanova.ev@sut.ru

ЧУДНОВ Александр Михайлович — доктор технических наук, профессор 31 кафедры автоматизированных систем специального назначения Военной академии связи им. Маршала Советского Союза С. М. Буденного, chudnow@yandex.ru

ЧУПИНА Валентина Александровна — доктор педагогических наук, профессор, профессор кафедры методологии профессионально-педагогического образования Уральского государственного педагогического университета, style@tehno.com

ШВАКОВ Андрей Васильевич — младший научный сотрудник отраслевой лаборатории перспективных информационно-коммуникационных технологий Белорусской государственной академии связи, v-i-a-n-d-y@yandex.by

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

ШЕВЯКОВ Владислав Денисович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Vlad89312239540.la@yandex.ru

ШЕМЯКИН Сергей Николаевич — кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shemyakin.sn@sut.ru

ШИБАЛЕНКОВ Кирилл Артемович — техник Студенческого конструкторского бюро Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shibalenkov.ka@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 имени профессора М. А. Бонч-Бруевича, shumackov_pp@sut.ru

ЭЛЕНТУХ Александр Валерьевич — заместитель начальника отдела разработки средств радиотехнического контроля ООО «Специальный технологический центр», aelentux@yandex.ru

ЭЛЬ САБАЯР ШЕВЧЕНКО Нидал — старший преподаватель кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ius@sut.ru

ЮРЬЕВА Арина Сергеевна — студент группы ИКВТ-31 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iureva.as@sut.ru

XIV МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ (АПИНО 2025)

Сборник научных статей
Том 1

Научное издание

Верстка
М. О. Мотыгина
Корректура
Д. Н. Яшугин
Дизайн логотипа Г. И. Юрьев
Подписано в печать 30.09.2025
Объем 46,5 усл.-печ. л.

Объединенная редакция рецензируемых научных изданий СПбГУТ
193232 СПб., пр. Большевиков, 22, корп. 1

APINO.SUT.RU