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

15th INTERNATIONAL CONFERENCE ON ADVANCED INFOTELECOMMUNICATIONS ICAIT

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

# АПИНО ICAIT



# 2026
# СБОРНИК НАУЧНЫХ СТАТЕЙ
## ТОМ 2

APINO.SUT.RU

**УДК 001:061.3(082)**
**ББК 72**

**А 43** **XV Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2026)**; сб. науч. ст. в 2-х т. / Под. ред. А. В. Рабина; сост. А. А. Дзюбаненко, И. М. Татарникова. СПб.: СПбГУТ, 2026. Т. 2. 653 с.

**Рецензенты** – заведующий кафедрой маркетинга Санкт-Петербургского государственного экономического университета, доктор экономических наук, профессор **Юлдашева О. У.**; исполнительный директор ООО «СПИЧАП», доктор технических наук, доцент **Басов О. О.**

**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

*Ответственный секретарь*

**Дзюбаненко А. А.** – кандидат технических наук, доцент, начальник 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**

*Председатель*

**Абилов А. В.** – кандидат технических наук, доцент, первый проректор – проректор по учебной работе СПбГУТ

*Сопредседатель*

**Савченко А. Ю.** – проректор по молодежной политике и воспитательной работе СПбГУТ

*Ответственный секретарь*

**Татарникова И. М.** – шеф-редактор объединенной редакции рецензируемых научных изданий СПбГУТ

*Члены организационного комитета*

**Мишутина Е. С.** – директор департамента экономики и финансов СПбГУТ

**Ивасишин С. И.** – кандидат технических наук, директор департамента организации и качества образовательной деятельности СПбГУТ

**Лысов А. Н.** – директор департамента по эксплуатации и развитию материально-технического комплекса СПбГУТ

**Гуршал К. Ю.** – начальник управления маркетинга и рекламы СПбГУТ

**Зыкова Н. В.** – начальник управления информационно-образовательных ресурсов СПбГУТ

**Лупой Р. С.** – начальник управления информатизации СПбГУТ

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 для научных работников, аспирантов, студентов старших курсов телекоммуникационных вузов, инженерно-технических работников и специалистов отрасли связи.

Сайт конференции
www.apino.sut.ru

ISBN 978-5-89160-404-9 (Том 2)
ISBN 978-5-89160-402-5

© СПбГУТ, 2026

# СОДЕРЖАНИЕ

**КИБЕРБЕЗОПАСНОСТЬ** 10

**Алешина Е. С., Яковлев В. А.** Гомоморфные свойства NTRU: природа шума и программная реализация 10

**Алькаттан С.** Контроль информационной безопасности при внедрении промптов в высокопривилегированных агентах LLM 17

**Ашуркин А. А., Гельфанд А. М., Токарь В. С.** Повышение устойчивости вычислительных сетей к сетевым атакам с применением межсетевых экранов нового поколения 24

**Белов В. А., Левшун Д. С., Шматкова К. А.** Объяснимый гибридный метод обнаружения подделки аудио на основе эмбеддингов глубокой нейронной сети и градиентного бустинга 28

**Берестовский П. А., Задбоев В. А., Шевченко А. А.** Состязательные атаки на модели машинного обучения в сетевой безопасности 33

**Билан В. В., Шевяков В. Д.** Влияние динамических задержек и потерь пакетов в mesh-сети на точность распределенного консенсуса в роевых системах управления 39

**Билан В. В., Шевяков В. Д.** Применение mesh-архитектуры в многоагентных робототехнических системах 43

**Браницкий А. А.** Экспериментальный анализ моделей векторного представления текста в задаче идентификации деструктивного веб-контента 47

**Браницкий А. А., Дроботов А. Г.** Разработка экспериментального стенда для генерации RCE-атак 54

**Браницкий А. А., Иванов Я. С.** Применение подхода DevSecOps в задаче управления серверами и повышения их защищенности 59

**Бударный Г. С., Макаренкова Е. А.** Правовые коллизии автоматизированного сбора данных с IoT-устройств 64

**Ганин Д. П., Левшун Д. С.** Разработка экспериментального стенда для анализа эффективности методов фильтрации сетевого трафика 70

**Гилавоги М., Красов А. В.** Метод скрытого вложения ЦВЗ в библиотечные модули программных продуктов, устойчивых к атакам обфускации 75

**Голошумов Б. Р., Иванов Д. А., Семенов Д. С.** Современные методологии и инструментальные средства тестирования на проникновение: анализ и тенденции 80

**Гудаков А. П., Миняев А. А.** Модели применения LLM в SOC **86**

**Демидов Н. А., Мелешкин О. С.** Некоторые аспекты обеспечения безопасности в условиях виртуализации **92**

**Денисов Р. С., Магомедов А. А., Космачев А. А.** Создание набора данных для классификации веб-приложений для выявления уязвимостей **97**

**Дрочнев А. А., Иванов Д. А., Семенов Д. С.** Обратный прокси-фишинг и методы защиты от него **102**

**Задбоев В. А., Татаринов В. И., Чимитов Д. Д.** Разработка архитектуры распределенной Honeypot-системы для обнаружения сетевых вторжений **109**

**Ильин Я. А., Любащенко Т. Д.** Исследование подходов классификации радиосигналов защищенных беспроводных сетей **114**

**Ильин Я. А., Спиридонов Д. П.** Анализ способов защиты устройств, настраиваемых с помощью NFC **120**

**Коврцур М. М., Кудесов А. С., Шахмоведев М. А.** Разработка концепции модуля для защищенного взаимодействия низкопроизводительных устройств **124**

**Котенко И. В., Нгуен Т. Ч.** Безопасность интеграций LLM с инструментами по протоколу Model Context Protocol: модель угроз и прототип защитных мер **128**

**Котенко И. В., Нгуен Х. Х.** Косвенная инъекция промпта через внешние файлы содержимого: моделирование атак и защиты **134**

**Куличкин А. А.** Гибридная безагентная методика инвентаризации крупного частного адресного пространства с использованием masscan, nmap и ZMap **141**

**Кушнир Д. В., Теровец А. А.** Исследование принципов организации изолированной среды анализа уязвимостей смарт-контрактов **149**

**Левшун Д. С., Легкодымов Д. М.** Подход к многофакторному интеллектуальному профилированию устройств Интернета вещей **155**

**Левшун Д. С., Русских А. Р.** Исследование эффективности модификаций BERT для задачи обнаружения вредоносной активности в логах информационных систем **160**

**Легков К. Е., Плотников Е. П.** Интеллектуальный анализ: использование искусственного интеллекта для подбора индивидуального обучения сотрудников на основе данных об инциденте **166**

**Любащенко Т. Д., Спиридонов Д. П.** Исследование соответствия моделей угроз ФСТЭК и тактик MITRE ATT&CK для совершенствования мониторинга облачных инфраструктур **173**

**Паскенова А. У., Шариков П. И.** Автоматизация судебной экспертизы с использованием блокчейн-технологий **178**

**Паскенова А. У., Шариков П. И.** Блокчейн как метод юридической аутентификации цифровых архивных копий **183**

**Паскенова А. У., Шариков П. И.** Исследование цифровых следов на устройствах Интернета вещей в аспекте цифровой криминалистики **189**

**Садовников В. Е.** Влияние градиентной состязательной атаки CARLINI & WAGNER на точность классификации изображений в системах машинного обучения 195

**Садовников В. Е.** Влияние зашумления на устойчивость систем классификации изображений к состязательным атакам 199

**Садовников В. Е.** Состязательное обучение как метод противодействия состязательным атакам на системы машинного обучения 204

**СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ И ЭКОНОМИКА ДАННЫХ** 208

**Александров И. Н., Фёдорова М. Ю.** Менеджмент онлайн-обучения: адаптивность и перспективы на будущее 208

**Алексеенко И. А., Луков А. П.** Проблемы формирования профессиональной идентичности PR-специалистов в контексте прекаризации рынка труда 213

**Алексеенко И. А., Халапян А. С.** Политическая роль прекариата в условиях медийной невидимости: от «опасного класса» к «молчаливому большинству» 220

**Бабин Н. Н.** Особенности экологического образования в современном обществе 226

**Балса А. Р., Николаева Н. А.** Гибридный подход к реферативной работе в эпоху ИИ: промпт-инжиниринг и ручное переписывание как инструмент глубокого усвоения 232

**Вольфсон М. Б.** Управление успехом клиента в цифровой среде 236

**Вторыгин И. Д., Сергеев Н. Д., Федоренко И. Н., Янченко Д. Л.** Экономическое обоснование выбора подписок на искусственный интеллект: анализ рынка, сценарии, кейсы 243

**Вязьмин А. Ю.** Конституирование личности и цифровая конфигурация смысла 248

**Гехт А. Б., Ухалов О. А.** Закон «Ядан»: общественная дискуссия в современной Франции 253

**Гехт А. Б.** Фактор Швеции в контексте военно-политической обстановки в регионе Балтийского моря 259

**Докучаев И. И., Завалишин А. Ю.** Юго-Восточная Азия во внешней политике России в 2020-е годы 264

**Егорова М. А., Суздалов Д. С.** Методика расчета индекса финансовой культуры на основе всероссийского обследования домохозяйств по потребительским финансам 270

**Желтова Е. П., Маршева Н. В.** Формирование критического мышления и этической рефлексии при работе с ИИ у магистрантов в рамках курса «ИЯ для НИР» 276

**Журавлев В. А.** Социокультурные аспекты развития белорусского села 283

**Зайцева Е. В.** Особенности формирования научной компетенции в рамках работы СНО «Цифровые технологии в профессиональной деятельности» 289

**Ивакина М. Д., Шилков В. И.** Информационно-коммуникационные технологии и перспективные направления цифровой трансформации энергетической отрасли 294

**Иклюшина Т. А., Макаров В. В.** Привлечение общественности к управлению муниципальным образованием как фактор повышения эффективности местного самоуправления 301

**Исаков А. В., Павлова Е. В.** Данные как фактор производства: институциональный анализ становления экономики данных в российском ИКТ-секторе 309

**Исаков А. В., Павлова Е. В.** Эффекты широкого проникновения алгоритмических моделей в условиях развития экономики данных 314

**Калимуллина О. В.** Выбор архитектуры мультиагентных систем для бизнеса 319

**Калимуллина О. В., Степанов Н. А.** Модели мотивации пользователей в wellness-экосистемах 324

**Кобильняк А. А., Неровный А. В.** Международный опыт противодействия синтетическим опиоидам как инструмент оценки мер США в период четвертой волны опиоидного кризиса 330

**Котов В. И.** Ранговый метод выбора наилучшего инвестиционного проекта 336

**Куликов В. В., Сметанин Р. А.** Анализ эффективности перехода на отечественные цифровые решения в пищевой промышленности 342

**Логиновская А. Н., Ожегов В. А.** Анализ биологического разнообразия в условиях развивающейся городской застройки Сыктывкара с применением ГИС 349

**Макаров В. В., Михайлова А. С., Шишкова А. С.** Методические основы мультифакторного анализа привлекательности вертикалей цифровых экосистем 356

**Макаров В. В., Петровский Н. Д.** Трансформация критериев конкурентоспособности предприятий услуг под воздействием процессов цифровизации 362

**Мешков А. В., Симонина А. А.** Большие данные как уникальный ресурс цифровой экономики 366

**Михайлюк В. С., Молчанова Т. В.** К вопросу об актуальности «Калевалы»: данные социологического опроса 372

**Мустафин Р. О., Шилков В. И.** Проблемы и перспективные направления развития информационно-технологической платформы национальной системы платежных карт 378

**Никитин К. Н., Оруджова Л. С., Перязева Ю. В.** Анализ подходов к формированию базовых цифровых компетенций горных инженеров 385

**Посохова О. А.** Сравнительный анализ ESG-практик российских банков в условиях цифровой трансформации 392

**Сафиуллин М. А., Щербаков И. Б.** Цифровые технологии как основа развития современного бизнеса 398

**Стурман В. И.** Проблемы экологического образования в России на современном этапе развития 403

**Хитрина И. Ю., Хитрин С. И.** Учебная мотивация и учебная активность студентов: зона управления 407

**Цверианашвили И. А.** Общественное движение против атомного оружия в Швеции во второй половине XX в. (на примере AMSA) 413

**Щербаков И. Б., Янковский М. А.** Особенности влияния искусственного интеллекта на работу телекоммуникационной компании 418

**Юкина Т. И.** Концептуальные характеристики цифровой трансформации обрабатывающей промышленности Китая 422

**СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ** 428

**Брыдченко А. В., Гриднев В. А., Груздев Д. А.** Подготовка специалистов специальной связи к работе на телекоммуникационном оборудовании в условиях проведения СВО 428

**Васильев Д. Н., Сагдеев А. К., Самаркин Д. С.** Технологические условия, определяющие тактику применения мультисервисных инфотелекоммуникационных сетей 433

**Глушко А. В., Григорчук А. Н., Гриднев В. А., Знобищев Р. С.** Вариант применения «двойного туннелирования» в сетях связи специального назначения 437

**Гордийчук Р. В., Добровольский С. Л., Сагдеев А. К., Самаркин Д. С.** Методы перенацеливания средств технической разведки при воздействии на мультисервисную инфотелекоммуникационную сеть 444

**Дробяскин А. Н., Куранда А. И., Музыкантов А. Н.** Формирование гражданской идентичности обучающихся военных учебных центров: теоретико-методологические основания и концептуальная педагогическая модель 449

**Загорельский В. В., Марченков А. А.** Разработка алгоритма ускоренной подготовки специалистов фельдъегерской связи 455

**Куранда А. И., Мерзликин Е. И., Михайлов М. Н., Стеценко О. Н.** Сравнительный анализ традиционных криптографических систем и алгоритмов шифрования на основе нейронных сетей 459

**ИННОВАЦИИ ДЛЯ АРКТИКИ** 465

**Запайщиков А. В., Круглова А. В.** Выбор графического процессора для реализации алгоритмов цифровой обработки сигналов с применением вейвлетов 465

**Запайщиков А. В., Круглова А. В.** Обзор методов анализа биомедицинских сигналов 471

**Лебедева Н. П., Степанова А. Б.** Проектирование в среде MATLAB пакета материалов, применяемых для производства изделий, эксплуатируемых в условиях Арктики 478

**Степанов А. Б.** Применение оборудования для коротковолновой радиосвязи в гибридных сетях связи Единой информационной системы Арктической зоны Российской Федерации 482

**Степанов А. Б.** Терминал связи для низкоорбитальной группировки спутников с блоком частотно-временного анализа сигналов и с функцией тревожной кнопки 489

**Степанова А. Б.** Программные средства для изучения свойств материалов технических изделий, эксплуатируемых в условиях Арктики 495

**РЕЗУЛЬТАТЫ НАУЧНЫХ ИССЛЕДОВАНИЙ** 500

**Алленов Д. С., Иванов В. Г., Чабаненко В. В.** Формирование архитектурных параметров серверных систем для повышения эффективности распределения нагрузки 500

**Аль-Нами Б. А., Шурухина О. А.** Анализ соответствия государственных информационных систем стандартам доступности 504

**Бабич К. С., Кузнецов С. П., Попов А. И.** Модифицированная нейросетевая архитектура DCE-YOLOv8 для автоматизированного обнаружения малоразмерных целей на изображениях БПЛА 511

**Баразенко Д. К., Пантюхин О. И., Саврасов А. С., Хрусталев Н. Э.** Интеллектуальные методы обеспечения отказоустойчивости телекоммуникационных сетей в условиях отказов критически важных узлов 517

**Бедикян Е. С., Жуков И. С., Камардин А. И., Литусов Н., Лопашенко В. М.** Бионический протез голени с подсветкой для социальной адаптации ребенка 523

**Блан Ф. С.** Требования к качеству объектов знаний в плоскости знаний сетей, определяемых знаниями (KDN) 529

**Бразовский Г. Р., Шевцова А. А., Яцкова А. Е.** Моделирование поляризационных состояний в имитаторе КРК 534

**Былина М. С., Гнедов Л. А., Никитин М. В.** Исследование влияния полосы пропускания фильтра на Q-фактор в системах когерентной оптической связи с модуляцией M-QAM 540

**Ваганов А. В., Чистый С. А.** Разработка блока управления освещением в современном логистическом центре 545

**Виноградов П. Ю., Михайлов Р. А.** Сравнительный анализ сред схемотехнического моделирования для проектирования гибридных систем электропитания объектов радиосвязи 550

**Гольдштейн А. Б., Камаев А. Р., Рафикова Р. Ф.** Применение искусственного интеллекта для эксплуатационного управления сетями пятого поколения 554

**Горынцев А. А., Фёдоров С. Л.** Применение технологий «умного дома» в рамках системы видеоконтроля на промышленных объектах 561

**Жуков И. С., Лихачев Я. С., Мансуров М. А., Тесслер Я. К.** Разработка прототипа биоуправляемого глазного протеза с интегрированной системой адаптивной фоновой подсветки 566

**Зайдуллин Р. Р., Туманова Е. И.** Анализ технологии контроля ситуационной обстановки местности с прогнозированием развития угроз различного типа с использованием систем технического зрения с интерактивным пользовательским интерфейсом 572

**Мавричев В. К.** Применение нейронных сетей для интеллектуального управления трафиком и маршрутизации в сетях 5G/6G 578

**Мошак Н. Н., Эль Сабаяр Шевченко Н.** Метод стабилизации обучения глубокой нейронной сети в задачах слайсинга 5G на основе модифицированной модели задержки M/M/1 586

**Новиков Е. А.** Байесовский алгоритм коллективного восприятия среды при различных типах динамических изменений среды 590

**Орехова В. О., Павлюк И. Ф., Фокин Г. А.** Обнаружение множества сот в 5G NR при начальном поиске в условиях шума и взаимных помех 595

**Павловская А. А., Павловский М. В., Фёдоров С. Л.** Архитектура бортовой монокулярной видеосистемы и методы обработки видеоинформации для облета препятствий 601

**Павловская А. А., Павловский М. В., Фёдоров С. Л.** Детектирование тепловых аномалий посредством бортового тепловизора БПЛА 606

**Смородин Г. Н.** Сравнительный анализ возможностей Google Forms и Yandex Forms для проведения педагогического тестирования 614

**Сторожук Н. Л.** Реализация аппаратных модулей синхронизации времени в сетях TSN 619

**Хлопунов Ф. Д.** Влияние динамической адаптации модуляции и кодирования в системах спутниковой связи 628

**АВТОРЫ СТАТЕЙ** 632

# КИБЕРБЕЗОПАСНОСТЬ

**УДК 004.056.55**
**ГРНТИ 28.21.19**

## ГОМОМОРФНЫЕ СВОЙСТВА NTRU: ПРИРОДА ШУМА И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ

**Е. С. Алешина, В. А. Яковлев**

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

*Исследуются гомоморфные свойства постквантовой криптосистемы NTRU, природа шума, возникающего при операциях над зашифрованными данными и его влияние на корректность дешифрования. Представлена программная реализация, криптосистемы, позволяющая анализировать аддитивные и ограниченные мультипликативные гомоморфные свойства.*

***NTRU, гомоморфные операции, шум, постквантовая криптография, облачные вычисления, решетки, Python***

В условиях стремительного развития облачных технологий и распределенных вычислений проблема обеспечения конфиденциальности данных приобретает принципиально новый характер. Традиционные алгоритмы, такие как AES или RSA, эффективно защищают информацию при передаче и хранении, однако их использование в облачных вычислениях ограничено необходимостью дешифрования данных перед обработкой. Это создает критическую зону уязвимости, в которой данные представлены в открытом виде в оперативной памяти сервера.

Решением проблемы является использование гомоморфного шифрования (ГШ) [1], позволяющего проводить вычисления непосредственно над шифротекстами без доступа к секретному ключу. В основе применения гомоморфного шифрования лежит возможность выполнения математических операций над зашифрованными блоками данных без их предварительной расшифровки. Поскольку сервер получает доступ лишь к «закрытому»

набору символов, реальное содержание информации остается для него скрытым. Благодаря этому свойству открываются возможности для безопасного аутсорсинга вычислений в средах, где отсутствует полное доверие к серверу [2].

Криптосистема NTRU (Nth-degree Truncated Polynomial Ring Units) является перспективным объектом исследования благодаря своей устойчивости к квантовым атакам, высокой производительности и наличии гомоморфных свойств, благодаря которым можно проводить обработку зашифрованных данных без их предварительного расшифрования [3]. Математический фундамент системы базируется на работе в кольце многочленов $\mathbb{R} = \mathbb{Z}[X]/(X^N - 1)$, где $N$ – простое число. Все вычисления выполняются с целочисленными коэффициентами по модулю двух взаимно простых чисел: малого модуля $p$, большого модуля $q$ $(q \gg p)$ и модульного многочлена.

Генерация ключей заключается в выборе многочленов $f(x)$ и $g(x)$ степени $N - 1$, коэффициенты которых принадлежат множеству целых чисел и обычно являются небольшими. Вычисляются обратные многочлены: ${f_p}^{-1}(x)$ – обратный к $f$ *по* модулю $p$, ${f_q}^{-1}(x)$ – обратный к $f$ по модулю $q$ [3].

Открытый ключ $h(x)$ вычисляется по формуле (1):

$$h(x) = p\,{f_q}^{-1}(x) * g(x) mod\ q, \quad (1)$$

где $*$ обозначает свертку (умножение полиномов).

Закрытый ключ – пара полиномов $(f, g)$ с известными обратными ${f_p}^{-1}(x)$ и ${f_q}^{-1}(x)$.

Шифротекст вычисляется как:

$$e(x) = (r(x) * h(x) + m(x))\ mod\ q, \quad (2)$$

где $r(x)$ – случайный «зашумляющий» полином, $r(x) * h(x)$ – свертка полиномов.

При подборе параметров системы ключевую роль играют величины $d_1$ и $d_2$, которые определяют количество ненулевых коэффициентов в многочленах $f(x)$ и $g(x)$ соответственно. Эти величины определяют плотность указанных полиномов, а от их выбора зависят как криптостойкость схемы в целом, так и скорость накопления шума в ходе гомоморфных вычислений [4].

В основе шифрования в системе NTRU лежит использование специального «зашумляющего» полинома $r(x)$, который добавляется в шифротекст

при шифровании. Он выбирается из множества многочленов с малой нормой и выполняет две функции: шифротекст становится статистически неотличимым от случайной последовательности коэффициентов, что и обеспечивает криптостойкость схемы, и одновременно ограничивает допустимую глубину гомоморфных преобразований, так как его накопление при гомоморфных операциях может привести к выходу за пределы модульного диапазона, что приводит к ошибкам вычисления. Без случайного слагаемого $r(x) * h(x)$ система была бы детерминированной, что снижало бы ее стойкость.

Дешифрование проводится по следующей формуле:

$$m(x) = f_p{}^{-1}(x) * f(x) * e(x) \, mod \, q. \quad (3)$$

Гомоморфное сложение двух криптограмм:

$$e_1(x) = r_1(x) * h(x) + m_1(x) \text{ и } e_2(x) = r_2(x) * h(x) + m_2(x) \quad (4)$$

Дает

$$e_1(x) + e_2(x) = [r_1(x) + r_2(x)] * h(x) + [m_1(x) + m_2(x)] \, mod \, q. \quad (5)$$

Видно, что операция сложения криптограмм приводит к формированию криптограммы, структура которой сохраняет форму криптограммы в системе NTRU. Из (5) следует, что при расшифровании суммы криптограмм получается сумма сообщений. Результат сложения также можно интерпретировать как шифрование суммы сообщений $m_1(x) + m_2(x)$ с использованием нового «зашумляющего» многочлена $r_1(x) + r_2(x)$.

Благодаря свойству обратимости многочлена $f(x)$ по модулю $q$ (то есть выполнению условия $f \cdot f_q \equiv 1 \, mod \, q$ *и* сохранению накопленного шума в допустимых границах, процедура дешифрования корректно восстанавливает результат гомоморфной операции – сумму открытых текстов. В процессе дешифрования вклад шума остается ограниченным, если коэффициенты результирующего многочлена не выходят за допустимые пределы, обычно оцениваемые как интервал $(-q/2, q/2)$ [5].

Увеличение $d_1$и $d_2$ приводит к росту числа ненулевых слагаемых в свертке полиномов, что увеличивает максимальный модуль коэффициентов шумового полинома и повышает вероятность выхода за порог $q/2$. При гомоморфных операциях шум накапливается: при сложении криптограмм его норма растет аддитивно, при умножении – квадратично, что связано с появлением перекрестных членов вида $r_1 r_2 h^2$, $r_1 h m_2$ и т.д.

Если суммарная норма шума превышает пороговое значение, то при дешифровании происходит некорректное восстановление сообщения из-за эффектов «заворачивания» при модульной редукции – явления, при котором сумма полезного сигнала и шума, выйдя за пределы допустимого диапазона (обычно $\pm q/2$), при взятии остатка по модулю $q$ приводится к эквивалентному значению в отрицательной области диапазона, искажая результат. Вычисление становится невозможным.

Если значения $d_1$ и $d_2$ слишком большие, то результирующий шум может быстро накапливаться при выполнении гомоморфных операций [6]. Это повышает вероятность того, что коэффициенты промежуточного многочлена $a(x)$ выйдут за допустимые границы модуля $q$, что приведет к ошибке дешифрования. С другой стороны, слишком малые значения этих параметров уменьшают уровень шума, но могут отрицательно сказаться на криптографической стойкости системы, поскольку уменьшается пространство возможных ключей.

Для исследования влияния выбора параметров КС NTRU на гомоморфные свойства, в том числе для оценки возникающего шума, разработана программа на языке Python с графическим интерфейсом на базе библиотеки PyQt6. Программа включает ряд функциональных модулей, соответствующих этапам работы алгоритма:

– генерация ключей – определение параметров $N$, $p$, $q$, $d_1$, $d_2$; вычисление открытого и закрытого ключей;
– шифрование и дешифрование – преобразование сообщения в шифротекст, демонстрация влияния случайного многочлена $r(x)$ на результат; дешифрование криптограммы и проверка корректности проведенных операций;
– проверка свойств гомоморфности – проведение операций сложения и умножения над двумя независимыми шифротекстами.

Экспериментальные данные, полученные в разработанной программе, представлены на рисунке 1. Исследование проведено при следующих параметрах: степень полинома $N = 11$, малый модуль $p = 3$, большой модуль $q = 32$. Диапазон изменения суммы параметров плотности $(d_1 + d_2)$ задан от 2 до 8 с шагом 1, для каждой точки выполнено по 100 испытаний с фиксированным полиномом $r(x)$.

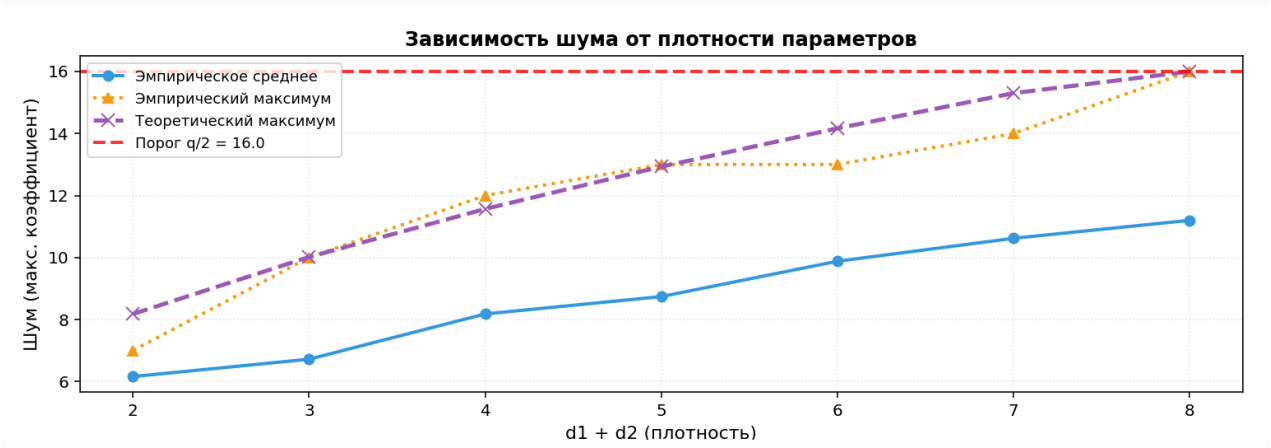



Рис. 1. Графики роста Шума от «плотности» полиномов

По оси $X$ отложена сумма $d_1 + d_2$, которая характеризует плотность многочленов $f(x)$ и $g(x)$ (количество ненулевых коэффициентов). По оси $Y$ отложена норма шума (в линейном масштабе), под ней понимается максимальное абсолютное значение коэффициентов шумового многочлена после операции шифрования. На графике представлены две кривые: усредненное значение шума по серии экспериментов (сплошная линия) и максимальные зафиксированные пики (пунктирная линия). Полученные данные позволяют оценить максимальные пиковые значения шума, которые оказываются критическими с точки зрения успешности дешифрования.

Анализ графика позволяет сделать следующие выводы:

1. Средний уровень шума растет практически линейно при увеличении плотности ключевых полиномов.

2. Разница между средним и пиковым значениями нормы шума указывает на стохастическую природу шума: при одних и тех же фиксированных $d_1$, $d_2$ конкретная реализация случайного многочлена $r(x)$ способна дать аномально высокий шум.

3. Порог корректности дешифрования показан на горизонтальной прямой на уровне $q/2$, что визуализирует границу корректности дешифрования. График показывает, что при превышении определенного значения плотности (на графике – область значений $d_1 + d_2 > K$ (максимально допустимая плотность)) пиковые значения шума пересекают этот порог, и дешифрование становится ненадежным.

Если над зашифрованными данными выполняется операция сложения, то при последующем дешифровании сумма исходных сообщений восстанавливается верно до тех пор, пока суммарная норма шума не выходит за критический порог.

Можно выделить два критических состояния шума:

1. Незначительный уровень шума – обеспечивает корректное дешифрование и позволяет выполнять дальнейшие гомоморфные операции, однако обычно достигается за счет уменьшения параметров системы, из-за чего снижается криптографическая стойкость.

2. Катастрофический уровень шума – приводит к ошибке дешифрования и необратимому искажению данных.

Экспериментальные данные также подтверждают, что в случае аддитивных операций накопление шума происходит линейно, то есть каждое дополнительное сложение шифротекстов пропорционально увеличивает норму шумового компонента, что соответствует теоретическим оценкам для решеточных криптосистем.

Также было проверено гомоморфное свойство умножения шифротекстов. Произведение $e_1(x) \cdot e_2(x)$ приводит к появлению перекрестных членов вида $r_1(x) \cdot r_2(x) \cdot h_2(x), r_1(x) \cdot h(x) \cdot m_2(x)$ и других. В результате дешифрование дает:

$$decrypt(e_1(x) \cdot e_2(x)) \approx m_1(x) \cdot m_2(x) + \varepsilon, \quad (6)$$

где $\varepsilon$ – суммарный шумовой член [5], который представляет собой сумму всех слагаемых, возникающих при раскрытии скобок в произведении $(r_1 h + m1)(r_2 h + m_2)$ и не относящихся к целевому произведению сообщений $m_1(x) \cdot m_2(x)$. При умножении шифротекстов образуются перекрестные члены, содержащие комбинации случайных полиномов, открытого ключа и сообщений, что приводит к значительному росту абсолютных значений коэффициентов шумового слагаемого. В отличие от операции сложения, где шум увеличивается линейно, при умножении его рост носит существенно более быстрый, близкий к квадратичному характер, поскольку в произведении участвуют сразу несколько шумовых компонентов.

Таким образом, с помощью программной реализации экспериментально подтверждено, что КС NTRU относится к классу частично гомоморфных систем (SWHE – Somewhat Homomorphic Encryption), поскольку хорошие результаты получены для аддитивных операций и имеют место явные ограничения для мультипликативных операций.

Понимание природы накопления шума и его влияния на корректность вычислений, полученное в ходе практического моделирования, позволяет более обоснованно выбирать параметры этой системы и проектировать эффективные механизмы защиты данных в облачных вычислительных средах.

Разработанная программная модель криптосистемы NTRU создает основу для дальнейших исследований и внедрения тематики гомоморфного шифрования в учебный процесс, что открывает новые возможности для проектирования защищенных протоколов, где конфиденциальность данных сохраняется на всех этапах их жизненного цикла.

**Список используемых источников**

1. Gentry C. Fully homomorphic encryption using ideal lattices // Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC). 2009.

2. López-Alt A., Tromer E., Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption // Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC). 2012.

3. Hoffstein J., Pipher J., Silverman J. H. NTRU: A ring-based public key cryptosystem // Algorithmic Number Theory. Springer, 1998.

4. Stehlé D., Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices // Advances in Cryptology EUROCRYPT 2011. Springer, 2011.

5. Hoffstein J., Silverman J. H. Optimizations for NTRU // Public-Key Cryptography and Computational Number Theory. De Gruyter, 2001.

6. Gentry C., Halevi S. Implementing Gentry's fully-homomorphic encryption scheme // Advances in Cryptology EUROCRYPT 2011. Springer, 2011.

## HOMOMORPHIC PROPERTIES OF NTRU: THE NATURE OF NOISE AND SOFTWARE IMPLEMENTATION

**Aleshina E., Yakovlev V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The homomorphic properties of the post-quantum NTRU cryptosystem are investigated, along with the nature of noise arising during operations on encrypted data and its impact on decryption correctness. A software implementation of the cryptosystem is presented, enabling the analysis of additive and limited multiplicative homomorphic properties.*

***Key words**: NTRU, homomorphic operations, noise, post-quantum cryptography, cloud computing, lattices, Python*

**УДК 004.056:004.8**
**ГРНТИ 81.93.29; 28.23.01**

# КОНТРОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВНЕДРЕНИИ ПРОМПТОВ В ВЫСОКОПРИВИЛЕГИРОВАННЫХ АГЕНТАХ LLM

**С. Алькаттан**

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

*В статье рассматривается проблема контроля информационной безопасности при использовании высокопривилегированных интеллектуальных агентов, способных взаимодействовать с внешними инструментами, источниками данных и вычислительными ресурсами. Особое внимание уделяется атакам внедрения промптов, при которых недоверенное содержание влияет на принятие решений и может привести к несанкционированному действию. Цель исследования состоит в формировании общего подхода к описанию структуры такого агента, выделению границ доверия, определению критериев безопасности и выбору мер защиты. В качестве методологической основы рассматриваются структурные модели агентных систем, контроль информационных потоков, политика разрешений и мониторинг действий перед их выполнением. Результатом работы является обобщенная схема контроля, связывающая элементы агента, показатели оценки и способы защиты. Предложенный подход может использоваться как предварительная основа для дальнейшей разработки количественной методики оценки защищенности и эффективности защитных мер.*

***большие языковые модели, высокопривилегированные агенты, информационная безопасность, внедрение промптов, границы доверия, контроль доступа, политика безопасности, оценка эффективности.***

## Введение

Высокопривилегированные агенты на основе больших языковых моделей отличаются от обычных диалоговых систем тем, что они не только формируют текстовый ответ, но и используют внешние инструменты: поиск, файловые операции, электронную почту, прикладные интерфейсы, базы данных и сервисы автоматизации. В структурных моделях языковых агентов такие системы обычно описываются через память, пространство действий и процесс выбора действия [1]. Практическое развитие протоколов подключения инструментов, в том числе Model Context Protocol, усиливает значение границ доверия между моделью, клиентом, сервером инструментов и внешними ресурсами [2].

Основная проблема состоит в том, что агент получает не только команды пользователя, но и данные из недоверенных источников. Если во внешнем документе, сообщении или результате работы инструмента содержится вредоносная инструкция, она может быть интерпретирована моделью как часть управляющего контекста. Такой класс угроз известен как prompt injection; в русскоязычном изложении далее используется термин «внедрение промпта». Систематические исследования показывают, что атаки данного типа требуют не только фильтрации текста, но и анализа того, какие действия агент может выполнить после обработки недоверенного содержания [3].

Следовательно, контроль информационной безопасности в таких системах должен рассматриваться не как отдельная проверка промпта, а как многоуровневый механизм: описание структуры агента, фиксация границ доверия, задание политики допустимых действий, измерение нарушений и принудительное блокирование опасных операций. Цель статьи заключается в формировании краткой обобщенной модели такого контроля для дальнейшего использования в исследованиях защищенности высокопривилегированных агентов LLM.

## Структурная модель угроз

Для целей контроля агентная система может быть представлена как последовательность связанных элементов: источник данных, контекст модели, модуль планирования, вызов инструмента и внешний эффект. Недоверенный источник может не иметь прямого доступа к инструменту, однако способен косвенно повлиять на решение агента. Поэтому нарушение возникает не в момент появления вредоносного текста, а тогда, когда этот текст становится причиной несанкционированного привилегированного действия. Под привилегированным действием понимается операция, которая изменяет состояние внешней системы, раскрывает закрытые данные либо использует повышенные полномочия.

В этой логике структурная модель должна фиксировать как минимум четыре типа объектов: каналы ввода, компоненты обработки, инструменты и контрольные точки. Каналы ввода делятся на доверенные и недоверенные. Компоненты обработки включают контекст, память и планировщик. Инструменты классифицируются по последствиям: чтение, передача данных, изменение состояния и выполнение команд. Контрольные точки раз-

мещаются перед переходом от рассуждения модели к внешнему действию. На рисунке 1 показана обобщенная схема такой модели.




Рис. 1. Обобщенная схема контроля информационной безопасности в высокопривилегированном агенте LLM

Представленная схема позволяет связать структурные элементы системы с проверяемыми условиями безопасности. Если недоверенный источник влияет только на подготовку ответа, риск ограничен качеством результата. Если же тот же источник влияет на выбор инструмента отправки сообщения, финансовой операции или выполнения команды, риск переходит в область нарушения конфиденциальности, целостности или доступности. Именно поэтому современные стенды оценки, например AgentDojo, рассматривают агентов в среде с инструментами и недоверенными данными, а не только как изолированные модели генерации текста [4].

## Критерии и показатели контроля

Для научного исследования недостаточно указать, что агент был атакован. Необходимо определить, какое свойство безопасности нарушено и насколько эффективна защитная мера. В качестве базовых критериев могут использоваться: согласованность действия с задачей пользователя, авторизованность источника, изоляция данных и соблюдение политики выполнения. Эти критерии могут быть сведены к измеряемым показателям: доля успешных атак, доля несанкционированных привилегированных действий, доля нарушений политики, полезность выполнения задачи без атаки и полезность выполнения задачи при атаке.

ТАБЛИЦА 1. Связь элементов агента, показателей контроля и методов защиты

| Элемент системы | Основной риск | Показатель контроля | Возможная мера защиты |
|---|---|---|---|
| Внешний источник данных | Внедрение вредоносной инструкции | Доля недоверенных входов, влияющих на действие | Маркировка доверия, фильтрация, санитизация |
| Контекст и память агента | Сохранение вредоносного состояния | Доля ошибочных зависимостей между данными и действием | Контроль информационных потоков, очистка памяти |
| Вызов инструмента | Несанкционированное привилегированное действие | Доля нарушений политики выполнения | Референс-монитор, шлюз подтверждения |
| Внешний эффект | Утечка данных или изменение состояния | Тяжесть последствия и риск | Контроль доступа, журналирование, блокирование |

Как видно из таблицы 1, один и тот же инцидент может оцениваться разными показателями. Например, вредоносный текст во внешнем письме сам по себе является опасным входом, но критическим событием становится только выполнение недопустимого действия: отправка закрытых данных, изменение записи или запуск команды. Поэтому показатель успешности атаки должен дополняться показателем несанкционированного привилегированного действия. Такой подход делает возможным расчет эффективности защиты как снижения риска по сравнению с исходной конфигурацией.

## Методы защиты

Существующие методы защиты можно разделить на четыре группы. Первая группа связана с проверкой согласованности инструкций и действий с задачей пользователя. Подход Task Shield показывает, что защита может строиться не только на поиске вредоносных фраз, но и на проверке того, служит ли инструкция исходной цели пользователя [5]. Достоинство такого подхода заключается в сохранении полезности агента, однако его ограничение состоит в зависимости от качества проверки соответствия задачи.

Вторая группа основана на контроле информационных потоков. Подход Fides использует идеи конфиденциальности, целостности и динамиче-

ского отслеживания зависимостей, чтобы определить, какие вызовы инструментов безопасны, а какие требуют подтверждения или блокирования [6]. Для высокопривилегированных агентов этот класс методов особенно важен, поскольку он связывает источник данных с последующим действием, а не анализирует каждое сообщение изолированно.

Третья группа относится к политике безопасности и принудительному контролю исполнения. В PCAS состояние агентной системы представляется графом зависимостей между сообщениями, результатами инструментов и действиями; референс-монитор перехватывает операции до их исполнения и блокирует нарушение политики [7]. Такой подход лучше соответствует требованиям контроля доступа, так как решение о разрешении действия переносится из промпта в отдельный механизм исполнения.

Четвертая группа включает структурированную обработку результатов инструментов: разбор, выделение допустимых полей и удаление инструкций, не относящихся к данным. Этот метод проще для внедрения, но его недостаточно, если агент использует память, цепочки инструментов или несколько уровней делегирования. Поэтому практическая защита должна объединять маркировку доверия, проверку цели, контроль информационных потоков и политику разрешений. В противном случае защита остается фрагментарной и может не учитывать переход от недоверенного текста к привилегированному действию.

## Обсуждение и ограничения

Ключевое ограничение существующих подходов состоит в том, что многие из них оптимизированы под отдельный тип атаки или отдельный стенд оценки. Фильтрация промптов может не обнаружить косвенную атаку, если вредоносная инструкция замаскирована как обычный результат инструмента. Проверка согласованности с задачей может ошибаться в сложных многошаговых сценариях. Контроль информационных потоков требует корректной маркировки данных и инструментов. Политики исполнения дают более строгую защиту, но требуют предварительного описания допустимых действий и организационных правил.

Для дальнейшего исследования перспективным является объединение трех компонентов: структурной модели агента, системы показателей и исполняемого механизма контроля. Структурная модель определяет границы доверия и привилегированные действия, показатели оценивают риск, а ме-

ханизм контроля обеспечивает выполнение политики до возникновения внешнего эффекта.

## Заключение

В статье показано, что контроль информационной безопасности при внедрении промптов в высокопривилегированных агентах LLM должен выходить за пределы анализа текста запроса. Основным объектом контроля является цепочка влияния: недоверенный источник, контекст агента, решение о вызове инструмента и внешний эффект. Предложенная схема связывает структурные элементы агента, критерии оценки и методы защиты, а также может служить исходной основой для последующего экспериментального исследования и разработки прототипа.

**Список используемых источников**

1. Sumers T. R., Yao S., Narasimhan K., Griffiths T. L. Cognitive Architectures for Language Agents. URL: https://arxiv.org/abs/2309.02427 (дата обращения: 03.05.2026).

2. Model Context Protocol. Specification. URL: https:// modelcontextprotocol.io/specification/2025-11-25 (дата обращения: 03.05.2026).

3. Liu Y., Jia Y., Geng R., Jia J., Gong N. Z. Formalizing and Benchmarking Prompt Injection Attacks and Defenses // Proceedings of the 33rd USENIX Security Symposium. 2024. PP. 1831–1847. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/liu-yupei (дата обращения: 03.05.2026).

4. Debenedetti E., Zhang J., Balunovic M., Beurer-Kellner L., Fischer M., Tramèr F. AgentDojo: A Dynamic Environment to Evaluate Prompt Injection Attacks and Defenses for LLM Agents // Advances in Neural Information Processing Systems. 2024. URL: https://proceedings.neurips.cc/paper_files/paper/2024/hash/97091a5177d8dc64b1da8bf3e1f6fb54-Abstract-Datasets_and_Benchmarks_Track.html (дата обращения: 03.05.2026).

5. Jia F., Wu T., Qin X., Squicciarini A. The Task Shield: Enforcing Task Alignment to Defend Against Indirect Prompt Injection in LLM Agents // Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics. 2025. P. 29680–29697. DOI: 10.18653/v1/2025.acl-long.1435.

6. Costa M., Köpf B., Kolluri A., Paverd A., Russinovich M., Salem A., Tople S., Wutschitz L., Zanella-Béguelin S. Securing AI Agents with Information-Flow Control. URL: https://arxiv.org/abs/2505.23643 (дата обращения: 03.05.2026).

7. Palumbo N., Choudhary S., Choi J., Chalasani P., Christodorescu M., Jha S. Policy Compiler for Secure Agentic Systems. URL: https://arxiv.org/abs/2602.16708 (дата обращения: 03.05.2026).

*Статья представлена научным руководителем, доцентом кафедры ИБКС СПбГУТ, кандидатом технических наук, доцентом М. М. Ковцуром.*

# INFORMATION SECURITY CONTROL IN PROMPT INJECTION ATTACKS AGAINST HIGH-PRIVILEGE LLM AGENTS

**Alkattan S.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper considers information security control in high-privilege intelligent agents based on large language models. Such agents can use external tools, data sources and computational resources; therefore, malicious instructions hidden in untrusted content may influence decisions and lead to unauthorized actions. The purpose of the study is to outline a general approach to describing the structure of such agents, identifying trust boundaries, selecting security criteria and defining protection measures. The proposed view combines structural models of agent systems, information-flow control, permission policy and pre-execution monitoring. The result is a generalized control scheme linking agent components, assessment indicators and protection methods. The approach may be used as a preliminary basis for developing quantitative methods for evaluating security and the effectiveness of protection measures*

***Key words:*** *large language models, high-privilege agents, information security, prompt injection, trust boundaries, access control, security policy, effectiveness evaluation.*

**УДК 654.739**
**ГРНТИ 49.33.29**

# ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ К СЕТЕВЫМ АТАКАМ С ПРИМЕНЕНИЕМ МЕЖСЕТЕВЫХ ЭКРАНОВ НОВОГО ПОКОЛЕНИЯ

**А. А. Ашуркин, А. М. Гельфанд, В. С. Токарь**

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

*В условиях роста количества сетевых угроз особую актуальность приобретает задача повышения устойчивости вычислительных сетей к различным видам атак. Одним из эффективных средств защиты является межсетевой экран нового поколения, обеспечивающий фильтрацию сетевого трафика, анализ сетевых соединений и обнаружение подозрительной активности.*

***вычислительные сети, сетевые атаки, межсетевой экран нового поколения***

Современные вычислительные сети являются основой функционирования большинства организаций и обеспечивают взаимодействие пользователей, серверов и прикладных сервисов. Увеличение количества сетевых служб и подключенных устройств сопровождается ростом числа сетевых атак, направленных на получение несанкционированного доступа к ресурсам и нарушение доступности информационных систем. Большинство таких атак начинается с этапа разведки, в ходе которого злоумышленник выполняет сканирование сети, выявляет активные узлы и доступные сервисы. Далее могут выполняться попытки эксплуатации уязвимостей сетевых служб, использование слабых механизмов аутентификации или генерация избыточного сетевого трафика с целью нарушения работоспособности системы. Уязвимости сетевых сервисов часто возникают вследствие ошибок конфигурации операционных систем, использования устаревших версий программного обеспечения и применения недостаточно надежных механизмов аутентификации. В таких условиях важную роль играет применение средств защиты, позволяющих ограничивать доступ к сетевым ресурсам и выявлять признаки атак [1].

Межсетевые экраны нового поколения предназначены для защиты сетевой инфраструктуры путем анализа и фильтрации сетевого трафика. В отличие от традиционных межсетевых экранов, NGFW обеспечивают анализ сетевых соединений на уровне приложений и позволяют выявлять признаки атак. Использование таких механизмов позволяет существенно снизить вероятность эксплуатации уязвимостей сетевых сервисов. Даже при наличии неправильно настроенных служб межсетевой экран может ограничить до-

ступ к ним, разрешая соединения только от доверенных узлов. Применение NGFW позволяет реализовать следующие механизмы защиты [2, 3]:

– ограничение доступа к сетевым сервисам;
– фильтрацию сетевого трафика по заданным правилам;
– обнаружение попыток сканирования портов;
– выявление атак перебора учетных данных;
– блокирование подозрительных соединений;
– регистрацию событий безопасности.

Для проведения экспериментальных исследований был разработан лабораторный стенд в виртуальной среде, позволяющей моделировать сетевые взаимодействия и воспроизводить сценарии атак. Он моделирует типовую локальную вычислительную сеть небольшой организации. Он представлен на рисунке 1.

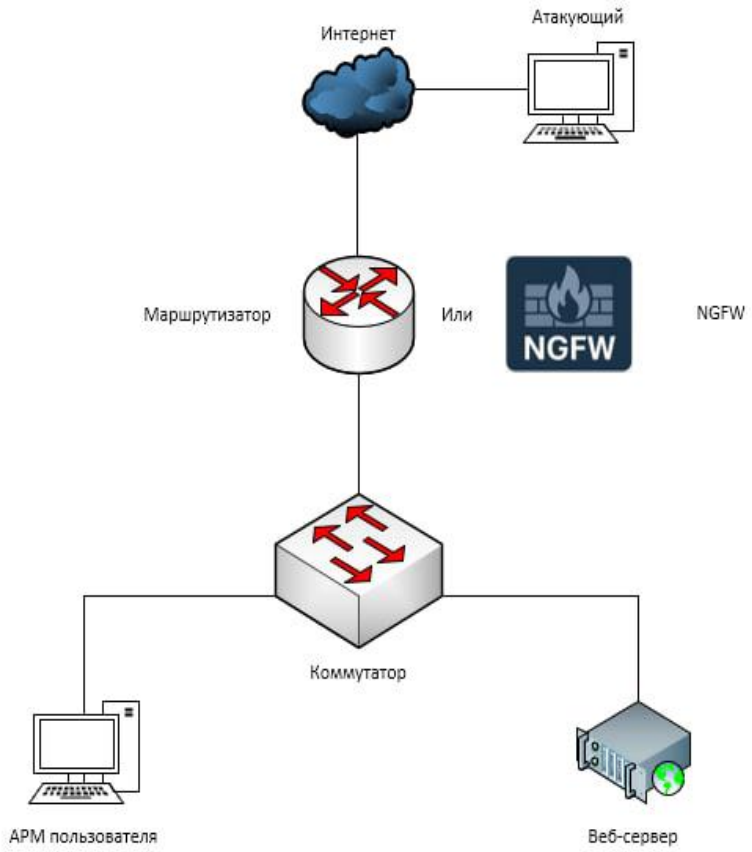



Рис. 1. Схема вычислительной сети

В состав лабораторной сети входят: внешний сегмент, моделирующий сеть Интернет, маршрутизирующее устройство, серверный узел, клиентские рабочие станции, узел злоумышленника. Серверный узел используется для размещения сетевых сервисов, доступных для взаимодействия из сети. Клиентская рабочая стан-

ции обеспечивает моделирование пользовательской активности. Узел злоумышленника используется для выполнения сетевых атак. Применялись следующие варианты защиты: конфигурация маршрутизатора с ручной настройкой сетевых правил фильтрации и с использованием межсетевого экрана нового поколения.

Для оценки устойчивости вычислительной сети был проведен набор экспериментальных испытаний, включающий выполнение серии сетевых атак при различных конфигурациях сети. Для получения количественных результатов использовались следующие метрики:

– процент успешно реализованных атак;
– количество доступных сетевых портов;
– время, за которое сервер стал недоступен;
– время недоступности сервера при атаках отказа в обслуживании;
– количество зарегистрированных событий безопасности.
– количество успешно подобранных паролей
– количество заблокированных попыток подбора пароля

Для проведения экспериментального исследования были произведены 30 атак, моделирующих типовые действия злоумышленника: сканирование портов (10 атак), перебора учетных данных (10 атак), отказа в обслуживании (10 атак). Целью атак являлось получение информации об открытых сетевых портах и доступных сервисах, получение доступа к серверу путем подбора учетных данных, нарушение доступности сетевого сервера путем генерации большого количества запросов. Результаты экспериментального исследования представлены в таблице 1.

ТАБЛИЦА 1. Сравнение эффективности защиты сети

| Метрика | Маршрутизатор | NGFW |
|---|---|---|
| Открытые порты (шт.) | 12 | 6 |
| Время падения сервера (сек.) | 145 | 105 |
| Время недоступности сервера (сек.) | 65 | 70 |
| Количество связанных зарегистрированных событий (шт.) | 96 | 284 |
| Количество подобранных паролей (шт.) | 0 | 0 |
| Количество заблокированных попыток подбора пароля (шт.) | 8 | 10 |
| Успешные атаки (%) | 40 | 16,5 |

Анализ таблицы 1 подтверждает, что NGFW эффективнее обычного маршрутизатора.

Результаты проведенного экспериментального исследования показали, что применение межсетевого экрана нового поколения обеспечивает более высокий уровень защищенности вычислительной сети по сравнению с использованием маршрутизатора с ручной настройкой правил фильтрации. При использовании маршрутизатора было обнаружено 12 открытых сетевых портов, тогда как при применении NGFW их количество сократилось до 3 из-за удобства и простоты настройки.

При моделировании атак отказа в обслуживании установлено, что сервер становился недоступным в среднем позже при использовании NGFW, что можно объяснить разными вычислительными мощностями. Время восстановления работоспособности сервера примерно одинаковое и в пределах погрешности измерений. Количество зарегистрированных событий безопасности при использовании NGFW увеличилось почти в три раза, что свидетельствует о более высоком и удобном уровне мониторинга сетевой активности, несравним анализ сетевых логов в консоли и в GUI.

**Список используемых источников**

1. Норткатт С., Новак Дж. Обнаружение вторжений в сетях.: материалы "Лори" 2001 год, 85582-147-1

2. Код Безопасности. Межсетевой экран «Континент 4»: руководство администратора. Управление комплексом. М.: Код Безопасности, 2022. 87 с.

3. Код Безопасности. Межсетевой экран «Континент 4»: руководство администратора. Обнаружение и предотвращение вторжений. М.: Код Безопасности, 2022. 32 с.

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

## NGFW AS A MEANS OF LAN SECURITY

**Ashurkin A., Gelfand A., Tokar V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Due to increasing number of network threats, the task of increasing the resilience of computer networks to various types of attacks becomes particularly relevant. Next Generation Firewall can act as a means of protection for those networks through traffic filtering, analysis of network connections and detection of suspicious activity.*

***Key words:*** *LAN, network attacks, NGFW*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ОБЪЯСНИМЫЙ ГИБРИДНЫЙ МЕТОД ОБНАРУЖЕНИЯ ПОДДЕЛКИ АУДИО НА ОСНОВЕ ЭМБЕДДИНГОВ ГЛУБОКОЙ НЕЙРОННОЙ СЕТИ И ГРАДИЕНТНОГО БУСТИНГА

**В. А. Белов, Д. С. Левшун, К. А. Шматкова**

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

*Представлен объяснимый гибридный подход к обнаружению подделки аудио, сочетающий высокую точность глубокого обучения с прозрачностью решений. В основе подхода лежит двухэтапная архитектура: сверточно-рекуррентная нейронная сеть извлекает плотные временные эмбеддинги из спектральных признаков аудиофайлов, после чего градиентный бустинг (CatBoost) классифицирует эти эмбеддинги, обеспечивая высокую обобщающую способность. Ключевым новшеством является параллельное обучение двух моделей – «глубокой» (для максимальной точности) и «интерпретируемой» (на основе табличных акустических признаков). Интерпретируемая модель, обученная на том же наборе данных, позволяет с помощью Shapley Additive Explanations выявлять вклад каждого исходного признака в решение, не снижая при этом эффективности основной гибридной системы.*

***информационная безопасность, подделка аудио, обнаружение фейков, глубокая модель нейросети, сверточная нейронная сеть, долгая краткосрочная память, градиентный бустинг, деревья решений, оценка важности признаков.***

Бурное развитие генеративного искусственного интеллекта, в частности методов синтеза речи (text-to-speech) и преобразования голоса (voice conversion), привело к появлению высококачественных поддельных аудиозаписей. Диффузионные модели создают реалистичные голосовые копии, которые сложно отличить от настоящих. Подобные дипфейк-аудио представляют серьезную угрозу: мошенничество, создание фальшивых доказательств, манипуляция общественным мнением.

Актуальна разработка эффективных и надежных методов обнаружения поддельных аудиофайлов. Доминирующие подходы на глубоких нейронных сетях [1] страдают от недостатка интерпретируемости, высоких вычислительных затрат и потребности в больших объемах размеченных данных. Альтернатива – ансамблевые методы (градиентный бустинг), которые демонстрируют конкурентоспособную точность при работе с хорошо подо-

бранными признаками и успешно применяются, например, в выявлении мошенничества в банковских транзакциях [2].

Цель работы – разработка гибридного объяснимого подхода, сочетающего высокую точность глубокого обучения с прозрачностью решений градиентного бустинга (CatBoost) [3]. Для достижения цели используется двухэтапная архитектура: сверточно-рекуррентная нейронная сеть извлекает временные эмбеддинги, на которых обучается градиентный бустинг. Параллельно строится интерпретируемая модель на исходных табличных признаках, что позволяет сохранить анализ важности признаков (SHAP) [4] не теряя точность глубокой модели.

Использован публичный набор аудиофайлов Fake-or-Real длительностью по 2 секунды, содержащий более 17 тысяч записей искусственного и настоящего голоса. Аудиофайлы преобразованы в спектральные, хроматические и временные признаки. Среди наиболее эффективных:

– 40 мел-кепстральных коэффициентов (MFCC);
– кратковременное преобразование Фурье (STFT);
– другие признаки: спектральный центроид, ширина спектра, контраст, частота пересечения нуля (ZCR), среднеквадратичная амплитуда (RMS), хроматические признаки и мел-спектрограмма и др.

Полученные признаки были организованы в 3D-тензоры размерности [временные кадры × признаки], что сохраняет временную динамику [5], она может быть полезна, так как многие генеративные модели оставляют следы именно в динамике спектральных изменений.

Общая схема предложенного метода включает пять этапов.

Первым этапом извлекаются признаки (библиотека Librosa).

Вторым этапом создается гибридная нейронная сеть CNN+LSTM [6]. Сверточные слои CNN с ядрами малого размера последовательно выделяют локальные пространственно-временные паттерны из входных 3D-тензоров, а последующие слои пулинга уменьшают временную размерность, сохраняя наиболее значимые признаки. Сверточные фильтры выявляют короткие фрагменты спектральной динамики: резкие скачки энергии, неестественные гармонические структуры, шумовые артефакты. В компоненте LSTM используется двунаправленная архитектура: каждый из двух слоев (прямой и обратный) содержит по 128 ячеек памяти и возвращает полные последовательности скрытых состояний, что позволяет моделировать долгосрочные зависимости между временными паттернами, причем прямой проход учитывает предшествующие кадры, а обратный – последующие, после чего их

выходы конкатенируются на каждом временном шаге. На выходе сети формируется компактный 128-мерный эмбеддинг для каждого аудиофайла. Это векторное представление сжимает исходную информацию, сохраняя различительные признаки подделок, и эффективно используется для классификации градиентным бустингом.

Третий и четвертый этапы заключаются в передаче эмбеддингов на вход классификатора CatBoost, который устойчив к переобучению и обеспечивает высокую точность. Данные разделены на обучающую (70 %), валидационную (10 %) и тестовую (20 %) выборки.

Пятый этап – это объяснимость решений. Параллельно обучается вторая модель CatBoost на исходных табличных признаках (усредненных по времени спектральных признаках, STFT-коэффициентах и т.д.). Эта модель не участвует в финальной классификации, а служит для интерпретации: с помощью SHAP (Shapley Additive Explanations) вычисляется вклад каждого признака в решение относительно среднего предсказания модели.

Для обучающей и тестовой выборок извлечены эмбеддинги, на которых обучен CatBoost. Метрики качества на тестовой выборке – в таблице 1 (точность, полнота, F1 для классов «real» и «fake», поддержка).

ТАБЛИЦА 1. Метрики модели и количество образцов в выборке

| | Точность | Полнота | f1-score | support | Размер обучающей выборки (образцов) |
|---|---|---|---|---|---|
| fake | 1,00 | 0,99 | 1,00 | 1787 | 12509 |
| real | 0,99 | 1,00 | 1,00 | 1787 | Размер валидационной выборки (образцов) |
| accuracy | - | - | 1,00 | 3574 | 1787 |
| macro avg | 1,00 | 1,00 | 1,00 | 3574 | Размер тестовой выборки (образцов) |
| weight avg | 1,00 | 1,00 | 1,00 | 3574 | 3574 |

На рисунке 1 представлена матрица ошибок CatBoost на эмбеддингах. Из 3 574 тестовых файлов модель верно распознала 3 570 (99,92 %), допустив три ошибки: два реальных образца ошибочно классифицированы как поддельные, один поддельный – как реальный. Низкое число ошибок подтверждает сбалансированность модели.

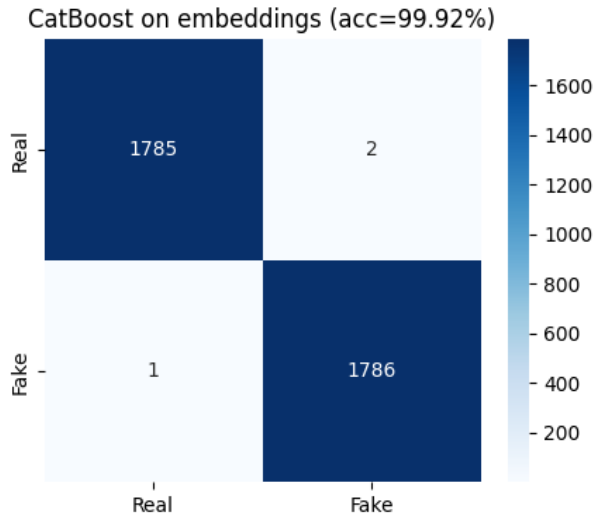



Рис. 1. Матрица ошибок модели, обученной на эмбеддингах

Благодаря стандартизации признаков и подбору гиперпараметров точность интерпретируемой модели составляет 99,61 % (подробнее в прошлой работе [7]).

На рис. 2 показаны объяснения для предсказаний бустинга на эмбеддингах. График показывает, какие признаки наиболее значимы.

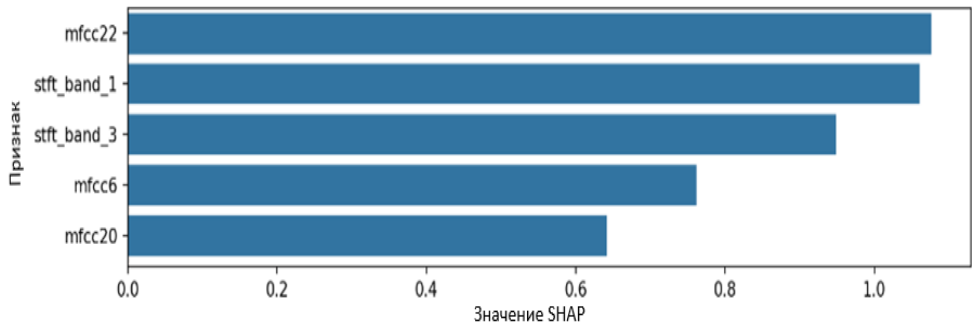



Рис. 2. Важность признаков SHAP

Среди всех признаков лидируют MFCC. Это указывает на тембральные искажения, типичные для синтезированной речи. В список наиболее важных также вошли STFT-коэффициенты (stft_band_1, stft_band_3), что согласуется с артефактами генерации в области низких и высоких частот. Благодаря параллельной интерпретируемой модели можно объяснить, почему конкретный аудиофайл классифицирован как поддельный.

Заключение. Разработан гибридный метод обнаружения дипфейк-аудио, сочетающий CNN+LSTM для извлечения эмбеддингов и градиентный бустинг (CatBoost) для классификации. Точность на тестовой выборке достигла 99,92 %.

**Список используемых источников**

1. Sun X. et al. A self-attentional ResNet-LightGBM model for IoT-enabled voice liveness detection. IEEE Internet of Things Journal. 2022. Vol. 10. N 9. P. 8257-8270.

2. Котенко И. В., Левшун Д. С., Жернова К. Н., Чечулин А. А. Обнаружение аномальных транзакций криптовалюты с помощью нейронных сетей и онтологий // Онтология проектирования. 2025. Т. 15. № 3(57). С. 334-350. DOI: 10.18287/2223-9537-2025-15-3-334-350.

3. Hancock J. T., Khoshgoftaar T. M. CatBoost for big data: an interdisciplinary review. Journal of big data. 2020. Vol. 7. N 1. P. 94.

4. Shobeiri S. Enhancing transparency in healthcare machine learning models using shap and deeplift a methodological approach //Iraqi Journal of Information and Communication Technology. 2024. Т. 7. № 2. С. 56-72.

5. Salim A., Beevi S. N. Complexity Analysis of Hierarchical Tucker-Based Tensor Decomposition in 3D CNN and LSTM Architectures for Video Data //2025 11th International Conference on Smart Computing and Communications (ICSCC). IEEE, 2025. С. 1-5.

6. Комличенко В. Н., Федосенко В. А., Купрейчик А. С. Сравнительный анализ различных архитектур нейронных сетей для задач регрессии // Экономика и качество систем связи. 2025. № 1. С. 110-121.

7. Белов В. А., Шматкова К. А., Левшун Д. С. Объяснимый подход к обнаружению подделки аудио файлов на основе градиентного бустинга и деревьев решений // XIV Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2025)», Санкт-Петербург, Россия, 29-31 октября, 2025. Сборник трудов. Выпуск 15. С. 62-67.

## AN EXPLAINABLE HYBRID METHOD FOR FAKE AUDIO DETECTION BASED ON EMBEDDINGS OF A DEEP NEURAL NETWORK AND GRADIENT BOOSTING

**Belov V., Levshun D., Shmatkova K.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*An explainable hybrid approach to audio forgery detection is presented, combining high precision deep learning with transparency of solutions. The approach is based on a two-stage architecture: a convolutional recurrent neural network extracts dense temporal embeddings from the spectral features of audio files, after which gradient boosting (CatBoost) classifies these embeddings, providing a high generalizing ability. The key innovation is the parallel training of two models – "deep" (for maximum accuracy) and "interpreted" (based on tabular acoustic features). The interpreted model, trained on the same data set, allows using SHAP analysis to identify the contribution of each initial feature to the solution, without reducing the effectiveness of the main hybrid system.*

***Key words:*** *information security, audio forgery, fake detection, deep neural network model, convolutional neural network, long short-term memory, gradient boosting, decision trees, feature importance assessment*

**УДК 004.056**
**ГРНТИ 81.93.29**

# СОСТЯЗАТЕЛЬНЫЕ АТАКИ НА МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ В СЕТЕВОЙ БЕЗОПАСНОСТИ

**П. А. Берестовский[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 особенности реализации состязательных атак на модели машинного обучения, применяемые в системах сетевой безопасности. Проанализированы основные механизмы обхода интеллектуальных средств обнаружения вторжений, способы воздействия на обучающие выборки и методы повышения устойчивости моделей. Отдельное внимание уделено особенностям изменения сетевого трафика при попытке обхода систем машинного обучения, а также проблеме компрометации обучающих данных.*

***машинное обучение, сетевая безопасность, состязательные атаки, обнаружение вторжений, IDS, сетевой трафик***

## Введение

В настоящее время методы машинного обучения рассматриваются как одно из наиболее перспективных направлений развития систем сетевой безопасности. Их применение позволяет автоматизировать анализ сетевого трафика, выявлять аномальное поведение узлов и обнаруживать ранее неизвестные типы атак. Современные интеллектуальные системы способны обрабатывать большие объемы данных в реальном времени, адаптироваться к изменяющимся условиям сетевой среды и выявлять сложные многоэтапные кибератаки, которые трудно обнаружить традиционными сигнатурными методами [1-2].

Состязательные атаки ориентированы не на эксплуатацию уязвимости программного обеспечения, а на воздействие непосредственно на логику работы модели. Подобный подход позволяет скрывать вредоносную активность и снижать точность обнаружения угроз. Злоумышленник может использовать знания о принципах функционирования модели или применять методы черного ящика для подбора таких входных данных, которые будут классифицированы как легитимные, несмотря на наличие вредоносных компонентов [3].

Практическая сложность заключается в том, что многие современные системы обнаружения вторжений (*IDS*) используют модели глубокого обучения, функционирование которых затруднительно интерпретировать. Отсутствие прозрачности в принятии решений усложняет процесс выявления и нейтрализации состязательных воздействий, а также затрудняет разработку эффективных контрмер. В связи с этим актуальной задачей становится исследование механизмов повышения устойчивости интеллектуальных систем безопасности к состязательным атакам различного типа [4].

**Механизм реализации состязательных атак**

Наиболее распространенным вариантом являются атаки уклонения, реализуемые после завершения этапа обучения модели. В этом случае злоумышленник анализирует реакцию *IDS* на различные типы сетевого взаимодействия (рис. 1) и подбирает параметры трафика, позволяющие снизить вероятность срабатывания средств защиты. Данный тип атак особенно эффективен против систем, использующих статические модели, которые не обновляются в реальном времени [5].

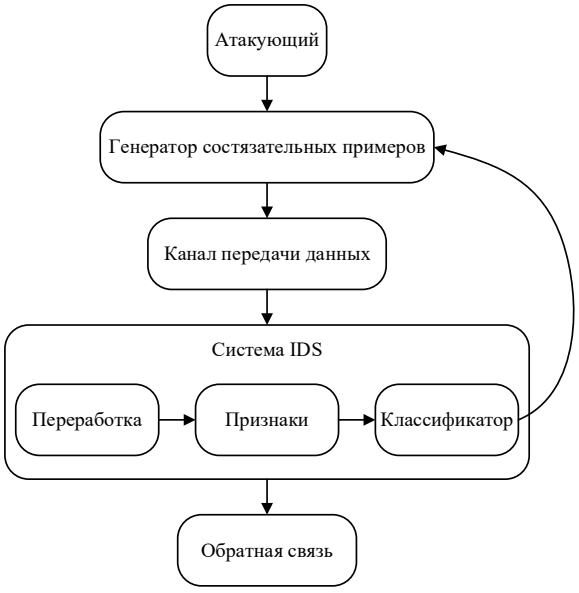



Рис. 1. Структурная схема воздействия на *IDS*

Следует отметить, что эффективность подобных атак напрямую зависит от объема информации, доступной нарушителю. Даже при отсутствии полного доступа к параметрам модели возможно постепенное определение признаков, оказывающих наибольшее влияние на итоговую классификацию. Методы зондирования, основанные на анализе ответов системы на се-

рию тестовых запросов, позволяют восстановить приблизительную структуру модели и выявить ее уязвимые места.

**Воздействие на обучающие выборки**

Отдельным направлением являются атаки из таблицы 1, ориентированные на этап подготовки обучающих данных. Подобные сценарии представляют повышенную опасность для распределенных систем мониторинга, в которых обучение выполняется автоматически на основе накопленной сетевой статистики. В таких условиях злоумышленник может целенаправленно искажать данные, используемые для дообучения или переобучения модели, что приводит к постепенной деградации ее защитных свойств.

ТАБЛИЦА 1. Основные варианты состязательного воздействия

| Тип воздействия | Объект воздействия | Результат | Особенности |
|---|---|---|---|
| Изменение трафика | Входные данные | Обход IDS | Минимальное изменение признаков, сохранение функциональности атаки, сложность детектирования традиционными методами |
| Воздействие на выборку | Обучающие данные | Снижение точности | Формирование ложных зависимостей, долгосрочное влияние на качество модели, требует доступа к процессу обучения |
| Анализ ответов модели | Логика классификации | Подбор параметров обхода | Не требует полного доступа, реализуется методами черного ящика, может быть комбинирован с другими типами атак |
| Имитация легитимного поведения | Поведенческие признаки | Ложная классификация | Использование профиля сети, адаптация под нормальные паттерны активности, высокая скрытность |

При наличии возможности внедрения специально подготовленных событий злоумышленник способен изменить распределение признаков в обучающем наборе данных. Это может привести к формированию некорректных решающих правил, снижению чувствительности к определенным типам атак или даже к целенаправленной ошибочной классификации заданных образцов трафика. Особую угрозу представляют атаки типа «отравление данных», при которых вредоносные примеры маскируются под

легитимную активность и накапливаются в обучающей выборке в течение длительного времени.

Практически подобный механизм может быть реализован посредством генерации большого количества сетевых запросов, имитирующих легитимную активность (рис. 2). Например, атакующий может организовывать фоновую передачу данных, соответствующую обычному пользовательскому поведению, но содержащую скрытые вредоносные нагрузки. При автоматическом сборе и разметке таких данных для последующего обучения модели происходит «размывание» границы между нормальным и аномальным поведением.

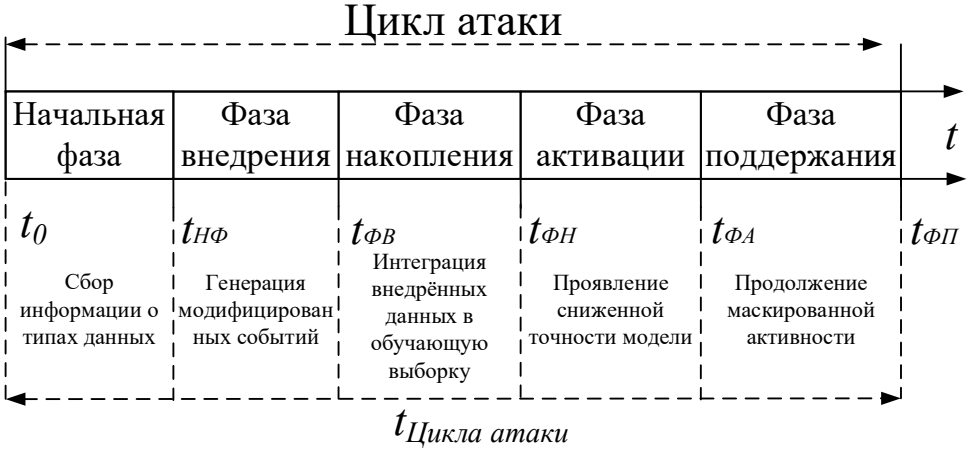



Рис. 2. Временная схема воздействия на обучающие данные

Основная трудность выявления отравления обучающей выборки состоит в том, что отдельная внедренная запись может не отличаться от обычного сетевого события. Изменение поведения модели проявляется после накопления таких записей и очередного цикла обучения. Поэтому контролировать необходимо не только отдельные примеры, но и изменение распределения признаков во времени, состав источников данных и результаты модели на контрольной выборке.

Защита должна охватывать подготовку данных и ввод обновленной модели в эксплуатацию. Перед переобучением следует проверять происхождение записей, исключать дубликаты и выбросы, а также отделять доверенную контрольную выборку от данных, поступающих из рабочей сети. После обучения показатели точности, полноты и доли ложных срабатываний необходимо сравнивать с показателями предыдущей версии. При ухудшении результатов обновление модели должно быть остановлено либо отменено. Состязательное обучение и ансамблевые методы могут использоваться как дополнительные меры, но не заменяют контроль качества исходных данных.

Устойчивость интеллектуальной IDS определяется не одним алгоритмом, а организацией всего жизненного цикла модели. Для воспроизводимости результатов необходимо фиксировать версии обучающих наборов и модели, параметры обучения и пороговые значения классификатора. В процессе эксплуатации требуется отслеживать изменение метрик и характеристик входного трафика, сохраняя возможность возврата к проверенной версии модели.

## Заключение

Рассмотрены два основных варианта воздействия на модели, применяемые в системах обнаружения вторжений. При атаке уклонения изменяются признаки сетевого трафика, поступающего на вход уже обученной модели, при этом функциональность самой атаки сохраняется. При отравлении данных воздействие переносится на этап обучения: специально сформированные записи изменяют распределение признаков и границу принятия решения.

Возможность реализации этих сценариев зависит от доступного нарушителю интерфейса. Ответы классификатора позволяют подбирать параметры обхода даже без знания структуры модели, хотя требуют большего числа запросов. Для отравления выборки необходим доступ к каналу поступления данных либо к процедуре их разметки. Наиболее уязвимы системы, в которых переобучение запускается автоматически, и новая версия модели вводится без сравнения с доверенной контрольной выборкой.

Следующим этапом исследования должна стать экспериментальная оценка описанных воздействий на одинаковом наборе сетевых данных и для одной конфигурации IDS. Для каждого сценария необходимо задавать объем доступных нарушителю запросов или долю внедряемых записей, а затем измерять изменение точности, полноты и количества ложных срабатываний. Такое сравнение позволит определить условия, при которых атака становится практически значимой, и оценить эффективность применяемых мер защиты.

**Список используемых источников**

1. Шевченко А. А., Липатников В. А., Задбоев В. А., Кузин П. И. Методика противодействия сетевой разведке объекта критической информационной инфраструктуры злоумышленником на основе IoC-анализа // Информационно-управляющие системы. 2026. № 1(140). С. 61-76. DOI: 10.31799/1684-8853-2026-1-61-76.

2. Задбоев В. А., Шашин М А., Якобсон Д. А. Компрометация брокера сообщений в IOT // Региональная информатика и информационная безопасность: сб. тр. СПб междунар. конф. и XIV СПб межрегион. конф., Санкт-Петербург, 29–31 окт. 2025 г. СПб: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2025. С. 144-147.

3. Изотов Д. Ю., Задбоев В. А., Шевяков В. Д., Садовников В. Е. Анализ проблем развития технологий блокчейн для обеспечения информационной безопасности в России // Современные тенденции развития фундаментальных и прикладных наук: материалы VIII Всерос. науч.-практ. конф., Брянск, 25 января 2025 года. Брянск: БГИТУ, 2025. С. 532-536.

4. Задбоев В. А., Липатников В. А., Мелехов К. В. Способ определения в сети передачи данных цепочки маршрутов до географического местоположения злоумышленника // 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. 512-517.

5. Задбоев В. А., Липатников В. А., Мелехов К. В., Робак В. А. Задача интеллектуальной защиты информационно-телекоммуникационной сети на основе анализа враждебных действий и цепочек вторжений // Региональная информатика и информационная безопасность: сб. тр. СПб междунар. конф. и СПб межрегион. конф., Санкт-Петербург, 23–25 окт. 2024 г. СПб: «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2024. С. 93-97.

6. Статья представлена доцентом кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, кандидатом военных наук, доцентом, А. А. Шевченко

## ADVERSARIAL ATTACKS ON MACHINE LEARNING MODELS IN NETWORK SECURITY

**Berestovski V.[1], Zadboev V.[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

*This article examines the implementation of adversarial attacks on machine learning models used in network security systems. It analyzes the main mechanisms for bypassing intelligent intrusion detection systems, methods for manipulating training samples, and methods for improving model resilience. Special attention is paid to the specifics of network traffic modification during attempts to bypass machine learning systems, as well as the problem of compromising training data.*

***Key words**: machine learning, network security, adversarial attacks, intrusion detection, IDS, network traffic*

**УДК 004.8**
**ГРНТИ 20.51.19**

# ВЛИЯНИЕ ДИНАМИЧЕСКИХ ЗАДЕРЖЕК И ПОТЕРЬ ПАКЕТОВ В MESH-СЕТИ НА ТОЧНОСТЬ РАСПРЕДЕЛЕННОГО КОНСЕНСУСА В РОЕВЫХ СИСТЕМАХ УПРАВЛЕНИЯ

**В. В. Билан, В. Д. Шевяков**

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

*Статья посвящена комплексному анализу влияния динамических задержек и стохастических потерь пакетов в беспроводных mesh-сетях как одного из наиболее критичных факторов деградации распределенного управления на показатели точности сходимости консенсус-алгоритмов в роевых робототехнических системах. В работе рассматриваются теоретические основы формирования топологических возмущений, математический аппарат сетевого консенсуса, его соотношение с централизованными архитектурами, а также эмпирические закономерности деградации точности оценки состояния при различных параметрах маршрутизации и обновления графа.*

***mesh-сети, роевое управление, распределенный консенсус, задержки передачи, потери пакетов, мультиагентные системы, графовая теория, устойчивость сходимости, сетевая топология***

Роевые платформы распределенного управления, многоагентные комплексы формообразования, группы синхронного маневрирования – все они выдают 90–95 % сходимости на лабораторном полигоне, создавая иллюзию непогрешимости. Однако в их коммуникационном слое заложена хрупкость: достаточно электромагнитного экрана, потери нескольких пакетов или физического разрыва линии видимости, чтобы граф взаимодействий рассыпался, а консенсус агентов деградировал до шума. Судить о надежности роя по тестам в прямой видимости оказалось несостоятельно; сообщество обратилось к отказоустойчивым сетевым архитектурам и распределенным протоколам поддержания связности [1].

Динамические mesh-топологии, выросшие из классических ad-hoc решений и получившие строгую графовую формулировку [2], не «латают» канал и не прячут разрывы за фиксированными маршрутами к шлюзу. Сеть решает задачу против наихудшего сценария деградации: протоколы адаптивной маршрутизации – AODV, OLSR, их спектральные расширения по лапласиану графа – непрерывно перестраивают пути, а распределенное

усреднение подстраивает состояние каждого агента под изменяющуюся топологию. Децентрализованное обновление таблиц и автоматическое восстановление маршрутов делают mesh теоретически обоснованным инструментом, а не эвристикой. Эмпирика подтверждает: если после полного цикла полевого тестирования система удерживает консистентность при адаптивном глушении каналов, это свидетельство подлинной эксплуатационной устойчивости. Метод фактически стал обязательным стресс-тестом; архитектуру, не прошедшую проверку в самоорганизующейся сети, трудно считать пригодной для автономного развертывания.

Влияние на точность координации структурное. Алгоритм раздвигает избыточность связей до предела связности: рой с 95 % слияния данных в идеальных условиях без сетевой защиты проваливается ниже порога управляемости при отказе трети узлов, а после внедрения mesh удерживает свыше 85 % и держит ошибку трансляции в сантиметровом диапазоне, допустимом для контуров реального времени [3]. Распределенная оптимизация находит конфигурацию маршрутов, минимизирующую верхнюю границу ошибки усреднения, подавляя накопление рассинхронизации. В отличие от пассивных приемов – звездообразной топологии, прямого подключения к шлюзу, однократного расчета пути – бессильных против нарастающей фрагментации, mesh итеративно пересчитывает таблицы на каждом такте, формируя глобально устойчивое пространство маршрутизации с наименьшей потерей пропускной способности.

Вычислительная цена определяется плотностью узлов и частотой обновления маршрутных таблиц. Малое число агентов или редкие служебные пакеты не позволяют нащупать резервный путь до наступления разрыва; рост параметров повышает робастность связности, но роняет энергетический бюджет. Прирост выходит на плато, и основная нагрузка приходится на поддержание таблиц соседей и пересчет после топологических скачков [4]. Для строгой проверки применяют сценарии с высокой плотностью, адаптивными интервалами обновления и ранней остановкой по падению консенсуса. Выбор протокола – реактивный, проактивный, гибридный – меняет геометрию сетевых задержек. Реактивные схемы прижились шире в малых динамических группах благодаря нулевой фоновой нагрузке; проактивные дают предсказуемую латентность ценой расхода полосы; гибридные требуют разрешения конфликтов приоритетов. Системы, устойчивые при одном протоколе, не обязательно выдерживают другой, поэтому защи-

щенные комплексы тренируют и проверяют по всем трем стратегиям либо используют мультипротокольные схемы.

Mesh перераспределяет нагрузку по узлам: агенты в структурных центрах графа и на пересечениях ключевых маршрутов аккумулируют транзитный трафик и требуют балансировки энергопотребления. Периферийные узлы сидят далеко от узких мест; семантически критические данные замыкания контуров управления маршрутизируются приоритетно. Допускается и целевая защита канала – минимизация риска потери пакетов на конкретном критическом участке, что позволяет точечно контролировать поведение в сценариях с жесткими временными окнами.

Переносимость сбоев на mesh-сети ниже, чем на звездообразные: алгоритм фиксирует устойчивые точки в пространстве маршрутов, специфичные для данного распределения узлов. В режиме частичной деградации mesh уверенно отражает стандартные отказы, но при массированном глушении или целенаправленном выводе хабов атакующий способен запустить каскадную фрагментацию, требуя перебалансировки параметров маршрутизации.

Наибольшую прочность дает сочетание mesh с кросс-слойной оптимизацией и распределенной аутентификацией. Полная криптографическая защита и динамическая адаптация спектра для ресурсоограниченных платформ неподъемны из-за вычислительной вложенности, поэтому применяют легкие протоколы шифрования и консенсусные механизмы доверия, оставляя тяжелую защиту для финального аудита. Альтернативы – централизованные сети 5G, спутниковые каналы, фиксированная инфраструктура – против локальных сбоев показали себя слабо: высокоскоростные линии лишь маскируют уязвимость к отказу базовой станции, а рандомизированное распределение частот и модификации антенных решеток дают гарантии в радиусе, не сопоставимом с покрытием самоорганизующейся mesh-сети.

Практические последствия ощутимы в поисково-спасательных миссиях, где задержка координат в условиях завалов провоцирует опасные решения группы БПЛА; в сельскохозяйственном мониторинге, где самоорганизация сети компенсирует потерю данных при обходе зон зашумления; в складской логистике, где целевая маршрутизация позволяет обходить очаги помех без прерывания потока задач. Это подталкивает к стандартам, обязывающим тестировать связность с привлечением mesh-топологий до сертификации.

Mesh-сети остаются центральным инструментом исследования устойчивости распределенных роботов: они выявляют минимально допустимую плотность связей, вскрывают ложную робастность, не фиксируемую при прямом подключении, и служат основой для взвешенных решений о развертывании групп. Дальнейший прогресс потребует междисциплинарных усилий, и mesh-архитектура в обозримом будущем сохранит свою ключевую роль.

**Список используемых источников**

1. Islam M., Yang F., Amin M. Control and optimisation of networked microgrids: A review // IET Renewable Power Generation. 2021. Vol. 15. PP. 1133–1148.

2. Nguyen D.C., Pathirana P.N., Ding M., Seneviratne A. Integration of blockchain and cloud of things: Architecture, applications and challenges // IEEE Communications Surveys & Tutorials. 2020. Vol. 22. N 4. PP. 2521–2549.

3. Roman R., Lopez J., Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges // Future Generation Computer Systems. 2018. Vol. 78. PP. 680–698.

4. Xiang X., Zhang B., Chen X., Yan H. Tracking performance limitations of MIMO discrete-time networked control systems with multiple constraints // Sci. China Inf. Sci. 2023.

*Статья представлена научным руководителем, профессором кафедры автоматизированных систем специального назначения ВАС, доктором технических наук, профессором И. Б. Саенко.*

## THE IMPACT OF DYNAMIC DELAYS AND PACKET LOSSES IN A MESH NETWORK ON THE ACCURACY OF DISTRIBUTED CONSENSUS IN SWARM CONTROL SYSTEMS

**Bilan V., Shevyakov V.**
Military Academy of Communications named after Marshal of the Soviet Union
S. M. Budyonny

*The article is devoted to a comprehensive analysis of the impact of dynamic delays and stochastic packet losses in wireless mesh networks as one of the most critical factors of distributed control degradation on the convergence accuracy of consensus algorithms in swarm robotic systems. The paper examines the theoretical foundations of the formation of topological disturbances, the mathematical apparatus of network consensus, its relationship with centralized architectures, as well as empirical patterns of degradation of the accuracy of state assessment under various routing parameters and graph updates.*

***Key words:*** *mesh networks, swarm management, distributed consensus, transmission delays, packet loss, multi-agent systems, graph theory, convergence stability, network topology*

**УДК 004.8**
**ГРНТИ 20.51.19**

# ПРИМЕНЕНИЕ MESH-АРХИТЕКТУРЫ В МНОГОАГЕНТНЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ

**В. В. Билан, В. Д. Шевяков**

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

*Статья описывает как динамическая топология беспроводных mesh-сетей применяется на показатели точности, консистентности и отказоустойчивости распределенной синхронизации карт в роевых робототехнических системах. В работе рассматриваются теоретические основы самоорганизующейся графовой маршрутизации, математический аппарат консенсус-алгоритмов над изменяющимися графами, ее соотношение с централизованными архитектурами связи, а также эмпирические закономерности деградации точности картографирования при варьировании плотности узлов, уровня сетевых потерь и стратегии обновления таблиц маршрутизации.*

***mesh-сети, роевая робототехника, распределенный SLAM, динамическая маршрутизация, консенсус-алгоритмы, отказоустойчивость, сетевая задержка, многоагентные системы, самоорганизация***

Роевые платформы распределенного картографирования, многоагентные SLAM-комплексы, группы одновременной локализации и построения карт – все они выдают 90–95 % синхронизации на лабораторном полигоне, создавая иллюзию непогрешимости. Однако в их коммуникационном слое заложена хрупкость: достаточно электромагнитного экрана, потери нескольких пакетов или физического разрыва линии видимости между агентами, чтобы граф взаимодействий рассыпался, а глобальная карта распалась на несвязанные фрагменты. Судить о надежности роя по тестам в прямой видимости оказалось несостоятельно; сообщество обратилось к отказоустойчивым сетевым архитектурам и распределенным протоколам поддержания связности [1].

Динамические mesh-топологии, предложенные в 2010-х как эволюция классических ad-hoc решений и позднее получившие строгую графовую формулировку [2], не «латают» канал и не прячут разрывы за фиксированными маршрутами к шлюзу. Сеть работает против наихудшего сценария деградации: внутренний контур – протоколы адаптивной маршрутизации AODV, OLSR, их спектральные расширения по лапласиану графа – непре-

рывно перестраивает пути доставки локальных подкарт, внешний – подстраивает распределенный фильтр Калмана под изменяющуюся топологию. Децентрализованное обновление состояния и автоматическое восстановление маршрутов делают mesh теоретически обоснованным инструментом, а не эвристикой. Эмпирика подтверждает: если после полного цикла полевого тестирования система удерживает консистентность глобальной карты при адаптивном глушении каналов, это свидетельство подлинной эксплуатационной устойчивости. Метод фактически стал обязательным стресс-тестом; архитектуру, не прошедшую проверку в самоорганизующейся сети, трудно считать пригодной для задач с реальными последствиями ошибки.

Влияние на точность слияния карт структурное. Алгоритм раздвигает избыточность связей до предела связности: рой с 95 % консенсуса в идеальных условиях без сетевой защиты проваливается ниже порога управляемости при отказе трети узлов, а после внедрения mesh удерживает свыше 85 % и держит ошибку трансляции в сантиметровом диапазоне, допустимом для контуров реального времени [3]. Распределенная оптимизация находит конфигурацию маршрутов, минимизирующую верхнюю границу рассинхронизации, подавляя накопление дрейфа локальных подкарт. В отличие от пассивных приемов – звездообразной топологии, прямого подключения к шлюзу, однократного расчета пути – применяемых однократно и бессильных против нарастающей фрагментации, mesh итеративно пересчитывает таблицы на каждом такте, формируя глобально устойчивое пространство маршрутизации с наименьшей потерей пропускной способности.

Вычислительная цена определяется плотностью узлов и частотой обновления маршрутных таблиц. Малое число агентов или редкие служебные пакеты не позволяют нащупать резервный путь до наступления разрыва; рост параметров повышает робастность связности, но роняет энергетический бюджет. Прирост выходит на плато, и основная нагрузка приходится на поддержание таблиц соседей и пересчет после топологических скачков [4]. Для строгой проверки применяют сценарии с высокой плотностью, адаптивными интервалами обновления и ранней остановкой по падению консенсуса. Выбор протокола – реактивный, проактивный, гибридный – меняет геометрию сетевых задержек. Реактивные схемы прижились шире в малых динамических группах благодаря нулевой фоновой нагрузке на канал; проактивные дают предсказуемую латентность ценой расхода полосы; гибридные требуют разрешения конфликтов приоритетов. Системы, устойчивые при одном протоколе, не обязательно выдерживают другой, поэтому

защищенные комплексы проверяют по всем трем стратегиям либо используют мультипротокольные схемы.

Mesh перераспределяет нагрузку по узлам: агенты в структурных центрах графа и на пересечениях ключевых маршрутов аккумулируют транзитный трафик и требуют балансировки энергопотребления. Периферийные узлы сидят далеко от узких мест; данные замыкания контуров управления маршрутизируются приоритетно. Допускается и целевая защита канала – минимизация риска потери пакетов на конкретном критическом участке, что позволяет точечно контролировать поведение в сценариях с жесткими временными окнами.

Переносимость сбоев на mesh-сети ниже, чем на звездообразные: алгоритм фиксирует устойчивые точки в пространстве маршрутов, специфичные для данного распределения узлов. В режиме частичной деградации mesh уверенно отражает стандартные отказы, но при массированном выводе хабов или целенаправленном глушении атакующий способен запустить каскадную фрагментацию, требуя перебалансировки параметров маршрутизации.

Наибольшую прочность дает сочетание mesh с кросс-слойной оптимизацией и распределенной аутентификацией. Полная криптографическая защита и динамическая адаптация спектра для ресурсоограниченных платформ неподъемны из-за вычислительной вложенности, поэтому применяют легкие протоколы шифрования и консенсусные механизмы доверия, оставляя тяжелую защиту для финального аудита. Альтернативы – централизованные сети 5G, спутниковые каналы, фиксированная инфраструктура – против локальных сбоев показали себя слабо: высокоскоростные линии лишь маскируют уязвимость к отказу базовой станции, а рандомизированное распределение частот и модификации антенных решеток дают гарантии в радиусе, не сопоставимом с покрытием самоорганизующейся mesh-сети.

Практические последствия ощутимы в поисково-спасательных миссиях, где задержка координат в условиях завалов провоцирует опасные решения группы БПЛА; в сельскохозяйственном мониторинге, где самоорганизация сети компенсирует потерю данных при обходе зон зашумления; в складской логистике, где целевая маршрутизация позволяет обходить очаги помех без прерывания потока задач. Это подталкивает к стандартам, обязывающим тестировать связность с привлечением mesh-топологий до сертификации.

Mesh-сети остаются центральным инструментом исследования устойчивости распределенного SLAM: они выявляют минимально допустимую плотность связей, вскрывают ложную робастность, не фиксируемую при прямом подключении, и служат основой для взвешенных решений о развертывании групп. Дальнейший прогресс потребует междисциплинарных усилий, и mesh-архитектура в обозримом будущем сохранит свою ключевую роль.

**Список используемых источников**

1. Han D., Shen S. Deep reinforcement learning for autonomous driving with multi-scenario fusion: A unified reward function approach // Proceedings of the International Conference on Machine Learning and Machine Intelligence. 2024. PP. 78–84.

2. Sartoretti G., Kerr J., Shi Y., Wagner G., Kumar T.S., Koenig S., Choset H. Primal: Pathfinding via reinforcement and imitation multi-agent learning // IEEE Robot. Autom. Lett. 2019. Vol. 4. N 3. PP. 2378–2385.

3. Zhu C., Dastani M., Wang S. A survey of multi-agent deep reinforcement learning with communication // Auton. Agent. Multi-Agent Syst. 2024. Vol. 38. N 1. P. 4.

4. Li W., Chen H., Jin B., Tan W., Zha H., Wang X. Multi-agent path finding with prioritized communication learning // International Conference on Robotics and Automation. 2022. PP. 10695–10701.

*Статья представлена научным руководителем, профессором кафедры автоматизированных систем специального назначения ВАС, доктором технических наук, профессором И. Б. Саенко.*

## APPLICATION OF MESH ARCHITECTURE IN MULTI-AGENT ROBOTIC SYSTEMS

**Bilan V., Shevyakov V.**
Military Academy of Communications named after Marshal of the Soviet Union
S. M. Budyonny

*The article describes how the dynamic topology of wireless mesh networks is applied to the accuracy, consistency, and fault tolerance of distributed card synchronization in swarm robotic systems. The paper examines the theoretical foundations of self-organizing graph routing, the mathematical apparatus of consensus algorithms on changing graphs, its relationship to centralized communication architectures, as well as empirical patterns of degradation of mapping accuracy with varying node density, network loss levels, and strategies for updating routing tables.*

***Key words:*** *mesh networks, swarm robotics, distributed SLAM, dynamic routing, consensus algorithms, fault tolerance, network latency, multi-agent systems, self-organization*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ МОДЕЛЕЙ ВЕКТОРНОГО ПРЕДСТАВЛЕНИЯ ТЕКСТА В ЗАДАЧЕ ИДЕНТИФИКАЦИИ ДЕСТРУКТИВНОГО ВЕБ-КОНТЕНТА

**А. А. Браницкий**

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

*Увеличение объема сетевого трафика, а также его разнородность усложняют задачу фильтрации и классификации сетевых потоков данных в Интернете, в частности задачу идентификации деструктивного веб-контента. Распространение такой информации может преследовать негативные цели, которые заключаются в пропаганде насильственных действий, популяризации вредных привычек, призывах к нарушению морально-идеологических устоев в обществе и т.д. Ввиду постоянного обновления контента, предоставляемого информационными ресурсами в Интернете, возникает необходимость в его регулярной и по возможности автоматической проверке на соответствие общим правилам модерации. В данной статье рассматриваются такие модели векторного представления текста, как взвешенный, обычный и непрерывный мешки слов, skip-gram, сверточная нейронная сеть и fastText, выполняется их экспериментальный анализ с точки зрения эффективности классификации текста, содержащегося в веб-страницах.*

***модели векторного представления текста, классификация текста, деструктивный веб-контент, сетевые потоки данных, кросс-валидация, веб-страницы, показатели классификации***

Необходимость оперативного и корректного обнаружения источников распространения деструктивного веб-контента требует разработки новых и совершенствования существующих методов в области фильтрации и классификации сетевых потоков данных. Текст представляет собой многосоставную цепочку элементов (слов и знаков препинания), в которой важен их порядок следования и синтаксическая согласованность. Как основная составляющая контента веб-страниц он обладает такими семантическими свойствами [1], как замкнутость, целостность (когерентность), связность (когезия) и релевантность. Для удовлетворения указанных свойств и правильного отражения смыслового содержимого текста в веб-страницах разработаны модели его векторного представления. Так, в соответствии с моделью bag of words («мешок слов») исходный документ $T = \{w_1,\ldots,w_N\}$, представляющий собой последовательность слов, преобразуется в список пар $L = \{(w_1,Q(w_1,T)),\ldots,(w_M,Q(w_M,T))\} = \{(w_1,q_1),\ldots,(w_M,q_M)\}$,

где элементы $\{w_1,...,w_M\} = D \subset T$ являются уникальными словами ($M \leq N$) (множество $D$ называется словарем), а элементы $\{q_1,...,q_M\}$ отражают абсолютные частоты появления соответствующих слов в документе $T$, где $q_i = Q(w_i,T)$, а $Q$ – функция, возвращающая число вхождений слова, представленного первым аргументом, в документ, представленный вторым аргументом. Оценка семантической схожести двух документов сводится к вычислению числа слов, которые одновременно встречаются в этих документах. Чем меньшее количество общих слов содержится в обоих документах, тем ниже их уровень семантической схожести. Среди ограничений, присущих данной модели, стоит отметить невозможность учета контекста, в котором может использоваться то или иное слово. Для устранения этого недостатка прибегают к построению матрицы семантических связей [2]. Кроме того, с увеличением объема документа модель становится особенно чувствительной к сравнению документов. В этом случае для уменьшения временных затрат рассматривают множество $L' = \{(w,q)|(w,q) \in L \wedge q>h>0\}$ вместо множества $L$, что позволяет игнорировать наименее популярные слова, частота встречаемости которых не превосходит заранее заданного порога $h$.

Обозначим через $G_1,...,G_K$ категории документов, а через $T_1^{(i)},\dots,T_{P_i}^{(i)}$ документы категории $G_i$ ($1 \leq i \leq K$). При построении классификатора на основе модели «мешок слов» вычисляются средние частоты вхождения наиболее популярных слов в документы каждой категории. Категорией анализируемого документа $T$ является та категория, для документов которой средние частоты вхождения слов наиболее приближены к частотам появления этих же слов внутри документа $T$.

Выделим три этапа в алгоритме обучения модели «мешок слов»:

1. Преобразование документа $T_j^{(i)} = \{w_1^{(j_i)},\dots,w_{N_j^{(i)}}^{(j_i)}\}$ в список пар $L_j^{(i)} = \{(w_1^{(j_i)},q_1^{(j_i)}),\dots,(w_{M_j^{(i)}}^{(j_i)},q_{M_j^{(i)}}^{(j_i)})\}$ согласно модели «мешок слов». Здесь $w_1^{(j_i)},\dots,w_{M_j^{(i)}}^{(j_i)}$ обозначают уникальные слова, а $q_1^{(j_i)},\dots,q_{M_j^{(i)}}^{(j_i)}$ – соответствующие им частоты вхождения в документ $T_j^{(i)}$.

2. Вычисление средних частот вхождения наиболее популярных слов в документы $T_1^{(i)},\dots,T_{P_i}^{(i)}$ каждой категории $G_i$. Для каждого слова $w \in \bigcup_{j=1}^{P_i} T_j^{(i)}$ из всей совокупности документов, принадлежащих категории $G_i$, вычисляется показатель средней частоты встречаемости слова $w$: $R^{(i)}(w) = \sum_{j=1}^{P_i} Q(w,T_j^{(i)})/P_i$. Элементы в цепочке пар $V^{(i)} =$

$\{(w_1^{(i)}, r_1^{(i)}), \ldots, (w_h^{(i)}, r_h^{(i)}), \ldots\}$ (где $r_j^{(i)} = R^{(i)}(w_j^{(i)})$) располагаются таким образом, чтобы выполнялось следующее неравенство: $r_1^{(i)} \geq \ldots \geq r_h^{(i)} \geq \ldots$

3. Выбор параметра $h$. Величина параметра $h$, определяющего пороговое количество наиболее часто встречающихся слов в рамках одной категории, может определяться как фиксированное или на основе удовлетворения требования по необходимой минимальной частоте встречаемости слов.

После процедуры обучения выполнен переход от частотных цепочек слов, характерных для каждого отдельного документа, к частотным цепочкам слов, характерных для усредненного документа каждой категории. Именно эта характеристика позволяет проверять входной документ на принадлежность к той или иной категории. Выделим два этапа в алгоритме идентификации категории документа $T$ при помощи модели «мешок слов»: (1) Вычисление частот встречаемости слов в документ $T$ и ранжирование слов по убыванию их частотных показателей. Тем самым документ $T = \{w_1, \ldots, w_N\}$ представляется в виде последовательности $L = \{(w_1,q_1), \ldots, (w_h,q_h)\}, \ldots, (w_M,q_M)\}$, где $q_1 \geq \ldots \geq q_h \geq \ldots \geq q_M$. (2) Вычисление индекса $I$ категории $G_I$ документа $T$. С этой целью рассмотрим две формулы. В первой формуле $I = arg \max\limits_{i=1,\ldots,K} \sum_{j=1}^{h} min(q_j, R^{(i)}(w_j))$ (взвешенный мешок слов) учитываются веса, представленные как частоты появления слов внутри документа $T$ с использованием критерия td=tf×idf, а во второй формуле $I = arg \max\limits_{i=1,\ldots,K} \sum_{j=1}^{h} \left[w_j \in \{w_1^{(i)}, \ldots, w_h^{(i)}\}\right]$ (обычный мешок слов) проверяется лишь признак вхождения слов, наиболее частотных для документа $T$, в список наиболее популярных $h$ слов, характерных для каждой категории.

Модель word2vec [3], имеющая две реализации: continuous bag of words («непрерывный мешок слов») и skip-gram, представляет собой двухслойную нейронную сеть. Преобразование слов, поступающих на вход такой нейросети, выполняется таким образом, что словам, находящимся в близком друг от друга контексте, назначаются близкие векторы признаков. В реализации «непрерывный мешок слов» выполняется прогнозирование слова $w_i$ по его окружению $C_i(\Delta) = \{w_j | w_j \in D \wedge j \in [i-\Delta, i+\Delta] \wedge i \neq j\}$, где $\Delta > 0$ обозначает ширину окна окружения слова $w_i$ для построения контекстных связей. Реализация skip-gram направлена на решение задачи, которая обратна решаемой при помощи модели «непрерывный мешок слов»: необходимо найти окружение по входному слову. В обеих моделях, представляющих собой нейронные сети, присутствуют один скрытый слой с линейной функцией активации и выходной слой с функцией активации softmax. В функционировании этих моделей выделяются три этапа: (1) кодирование входных векторов слов, (2)

обучение модели, (3) прогнозирование целевого слова. На первом этапе каждое слово $w_i$ представляется в виде двоичной последовательности $s_i^{(M)} = \{b_1^{(i)}, \ldots, b_M^{(i)}\}$ ($b_j^{(i)} \in \{0,1\}$, $j \in \{1,\ldots,M\}$), где $M$ обозначает размер словаря, а в каждой последовательности $s_i^{(M)}$ встречается только один единичный бит: $\forall i \in \{1,\ldots,M\}\ \exists! j \in \{1,\ldots,M\}\ b_j^{(i)} = 1$. После выполнения такой предобработки, получившей название унитарной кодировки (one-hot encoding), и близко соседствующие, и далеко отстоящие друг от друга слова располагаются в разных ортогональных подпространствах и являются равноудаленными друг от друга. Второй этап характеризуется настройкой внутренних параметров модели, что приводит к уменьшению расстояния между образами слов (выходными результатами нейронной сети), имеющих один и тот же контекст. В случае непрерывного мешка слов сперва для скрытого слоя и для каждого слова $w_i$ вычисляется сигнал $U^{(1)}$, который представляет собой усредненную по контекстам слова $w_i$ линейную комбинацию векторов-слов $s_j(M)$ и весов $V^{(1)}$ скрытого слоя: $U^{(1)} = (\#C_i^{(\Delta)})^{-1} \cdot \sum_{j=1}^{\#C_i^{(\Delta)}} s_j^{(M)} \cdot V^{(1)}$, где $\#C_i^{(\Delta)} = 2 \cdot \Delta$. Далее вычисляется сигнал $Y$ на выходном слое сети: $Y = softmax(U^{(2)}) = e^{u_i^{(2)}} / \sum_{j=1}^{M} e^{u_j^{(2)}}$, где $U^{(2)}=U^{(1)} \cdot V^{(2)}$, и $V^{(2)}$ – веса выходного слоя.

В случае модели skip-gram сперва для каждого слова $w_i$ вычисляется сигнал $U^{(1)}$, являющийся выходным для скрытого слоя: $U^{(1)} = s_i^{(M)} \cdot V^{(1)}$. Далее вычисляется выходной сигнал $Y$ аналогично соответствующей формуле, представленной для модели непрерывного мешка слов. В завершение выполняется обновление весов согласно методу обратного распространения ошибки [4]. Наконец, выходной вектор сети $Y=(y_1,\ldots,y_M)$ строится как набор вещественнозначных чисел, сумма которых равна 1: $\sum_{i=1}^{M} y_i = 1$. Для модели «непрерывный мешок слов» номер позиции прогнозируемого слова $w_{i'}$ в словаре определяется следующим образом: $i' = arg \max_{i=1,\ldots,M} y_i$, а для модели skip-gram номера позиций прогнозируемых контекстных слов определяются как индексы, соответствующие наибольшим $2 \cdot \Delta$ значениям $y_i$. В модели glove вычисляется вероятность того, что два слова могут совместно встречаться внутри окружения заданного размера. При создании этой модели ее авторы [5] придерживались такой идеи, чтобы при переходе от слов к их векторным представлениям для семантически схожих слов сохранялись линейные преобразования [6]. С помощью них при наличии трех слов $w_1$, $w_2$, $w_3$ можно вычислить слово $w_4$, которое будет иметь со словом $w_3$ такую же степень контекста, которая характерна для слов $w_1$ и $w_2$ [7]. В функционировании этой модели выделяются три этапа: (1) построение мат-

рицы совместной встречаемости слов (word co-occurrence matrix; элементы этой матрицы $X=\{x_{ij}\}^{M\times M}$ отражают абсолютные частоты появления слова $w_i$ рядом со словом $w_j$); (2) обучение модели (функция, подвергающаяся минимизации, имеет следующий вид: $\sum_{i=1}^{M}\sum_{j=1}^{M} F(x_{ij})\cdot(s_i\cdot s_j+b_i+b_j-log\,x_{ij})^2$, где $F$ представляет собой степенную функцию с областью значений меньше 1 для редко встречающихся пар слов и тождественно равна 1 для часто встречающихся пар слов); (3) прогнозирование слова. Для проведения экспериментов использовался набор данных, содержащий 69554 записи и разбитый по 19 категориям. На рис. 1 изображены показатели классификации, вычисленные для шести классификаторов, включая сверточную нейронную сеть и fastText.

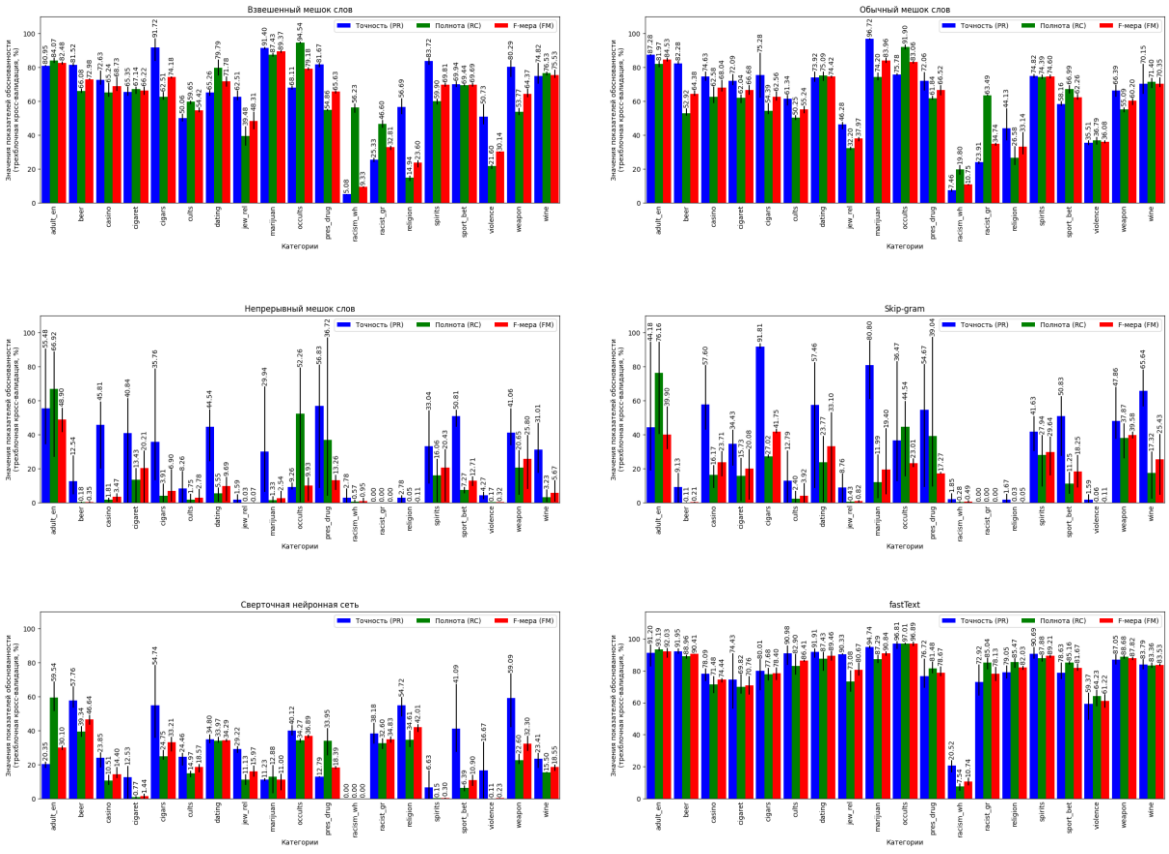



Рис. 1. Значения показателей классификации, вычисленные для каждого классификатора в рамках каждой категории при помощи трехблочной кросс-валидации

На рис. 2 представлена схема проведения эксперимента, согласно которому перед выполнением этапов обучения и прогнозирования выполнялась предобработка html-страниц посредством извлечения текста из них. В таблице 1 приведены значения показателей достоверности, точности, полноты и F-меры, усредненные по всем рассматриваемым 19 категориям и полученные в результате использования трехблочной кросс-валидации.

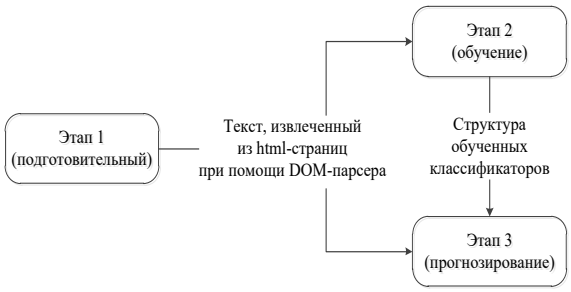



Рис. 2. Схема проведения эксперимента

Вычисление показателей для случайного классификатора осуществлялось сто раз, за счет чего удалось достаточно точно приблизить экспериментальные значения его показателя достоверности (5.28 %) к соответствующим теоретическим величинам (1/19≈5.26 %).

Наилучшие результаты демонстрирует классификатор fastText из-за поддержки использования n-грамм, что позволяет эффективно учитывать семантическое окружение слов и выражений. Модель «взвешенный мешок слов» демонстрирует наилучшие результаты среди моделей, основанных на вычислении частотных характеристик (т.е. среди моделей, не принимающих во внимание семантическое окружение слов и выражений).

ТАБЛИЦА 1. Показатели классификации, вычисленные для каждого классификатора при помощи трехблочной кросс-валидации

| Классификатор / Показатель | Взвешенный мешок слов | Обычный мешок слов | Непрерывный мешок слов | Skip-gram | Сверточная нейронная сеть | fastText | Случайный классификатор |
|---|---|---|---|---|---|---|---|
| Достоверность | 64.69 % | 63.16 % | 16.02 % | 22.53 % | 25.81 % | 84.15 % | 5.28 % |
| Точность | 66.2 % | 63.06 % | 26.66 % | 36.8 % | 29.56 % | 80.48 % | 5.28 % |
| Полнота | 61.04 % | 58.63 % | 12.21 % | 18.53 % | 20.42 % | 78.83 % | 5.28 % |
| F-мера | 63.52 % | 60.76 % | 16.75 % | 24.65 % | 24.15 % | 79.65 % | 5.28 % |

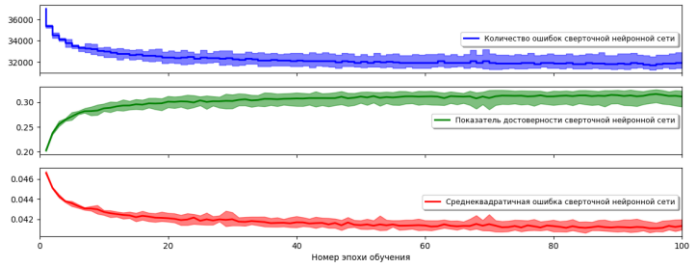



Рис. 3. Зависимость числа ошибок, показателя достоверности и среднеквадратичной ошибки сверточной нейронной сети от номера эпохи ее обучения

На рис. 3 показана зависимость числа ошибок, показателя достоверности и среднеквадратичной ошибки сверточной нейронной сети от номера эпохи ее обучения. В экспериментах использовалась нейронная сеть с двумя слоями свертки (с функцией активации типа ReLU) и сле-

дующим за каждым из них слоем субдискретизации. Направление дальнейших исследований связано с разработкой и экспериментальным исследованием ансамблей моделей векторного представления текста.

**Список используемых источников**

1. Гербик Л. Ф. Семантическая структура текста: элементы, отношения, связи // Вестник БГУ. 1990. Серия 4 (филология, журналистика, педагогика, психология). С. 56–58.

2. Нугуманова А. Б., Бессмертный И. А., Пецина П., Байбурин Е. М. Обогащение модели Bag of words семантическими связями для повышения качества классификации текстов предметной области // Программные продукты и системы. 2016. № 2 (114) С. 89-99.

3. Mikolov T., Chen K., Corrado G., Dean J. Efficient estimation of word representations in vector space // arXiv preprint arXiv:1301.3781. 2013. PP. 1–12.

4. Werbos P. J. Beyond regression: New tools for prediction and analysis in the behavioral sciences: PhD thesis // Harvard University, MA, 1974.

5. Pennington J., Socher R., Manning C. Global vectors for word representation // Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP).2014. PP. 1532-1543.

6. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение // Издательский дом «Питер». 2018. 480 с.

7. A GloVe implementation in Python. http://www.foldl.me/2014/glove-python/#fn:6 (электронный ресурс). Дата последнего обращения: 31.05.2026.

## EXPERIMENTAL ANALYSIS OF TEXT VECTOR REPRESENTATION MODELS IN THE TASK OF IDENTIFYING DESTRUCTIVE WEB CONTENT

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

*The increasing volume and heterogeneity of network traffic complicate the task of filtering and classifying network data flows on the Internet, particularly the identification of destructive web content. The dissemination of such information can have negative goals, including promoting violence, promoting bad habits, and inciting the violation of moral and ideological principles in society. Due to the constant updating of content provided by online information resources, it is necessary to regularly and, if possible, automatically check it for compliance with general moderation rules. This paper examines such vector representation models as weighted, regular, and continuous bags of words, skip-gram, convolutional neural networks, and fastText, and experimentally analyzes them for their effectiveness in classifying text contained in web pages.*

***Key words**: text vector representation models, text classification, destructive web content, network data flows, cross-validation, web pages, classification metrics*

**УДК 004.056.5**
**ГРНТИ 50.37.23**

# РАЗРАБОТКА ЭКСПЕРИМЕНТАЛЬНОГО СТЕНДА ДЛЯ ГЕНЕРАЦИИ RCE-АТАК

**А. А. Браницкий, А. Г. Дроботов**

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

*Атаки удаленного выполнения кода (RCE) представляют одну из наиболее критичных угроз для современных IT-инфраструктур. В статье описывается разработка экспериментального стенда, позволяющего генерировать различные типы RCE-атак. Стенд включает уязвимое веб-приложение, набор скриптов генерации атак и eBPF-сенсор для валидации результатов. Приведены результаты экспериментов и обоснованы перспективы развития.*

***RCE-атаки, eBPF, IoB, поведенческий анализ, reverse shell, MITRE ATT&CK, runtime-детектирование, системные вызовы***

Современные ИТ-инфраструктуры все активнее мигрируют на контейнерные технологии (Docker, Kubernetes), что обеспечивает гибкое масштабирование, однако порождает новые классы уязвимостей. Атаки типа Remote Code Execution (RCE) стабильно занимают ведущие позиции в рейтинге OWASP Top 10 [1] и представляют особую опасность в контейнерных средах: компрометация одного контейнера может привести к захвату всего хоста, особенно при запуске приложений с повышенными привилегиями.

Разработка и тестирование средств защиты от RCE-атак требует управляемой и воспроизводимой среды. Целью данной работы является разработка экспериментального стенда, генерирующего RCE-атаки в изолированной контейнерной среде с фиксацией на уровне ядра с помощью eBPF. Стенд необходим для отработки методов детектирования и обучения blue-team специалистов.

Перед проектированием стенда был проведен анализ основных векторов RCE-атак на основе тактик MITRE ATT&CK [2] и данных OWASP. Выделены категории, какие стенд будет поддерживать:

– *Command Injection* – внедрение команд ОС через пользовательский ввод (CWE-78). Наиболее прямолинейный вектор, выбранный как основной для реализации в стенде (MITRE T1202);

– *Reverse Shell* – установление обратного соединения от жертвы к атакующему для обхода межсетевых экранов (MITRE T1059, T1572).

Ключевым компонентом стенда является подсистема валидации на основе eBPF (Extended Berkeley Packet Filter) [3,4,5] – механизма ядра Linux, позволяющего выполнять верифицированные программы в пространстве ядра без загрузки модулей и без перекомпиляции ядра. eBPF-программа проходит проверку верификатором, компилируется JIT-компилятором и прикрепляется к хукам ядра (tracepoints, kprobe/uprobe, XDP). Архитектура eBPF представлена на рис. 1.

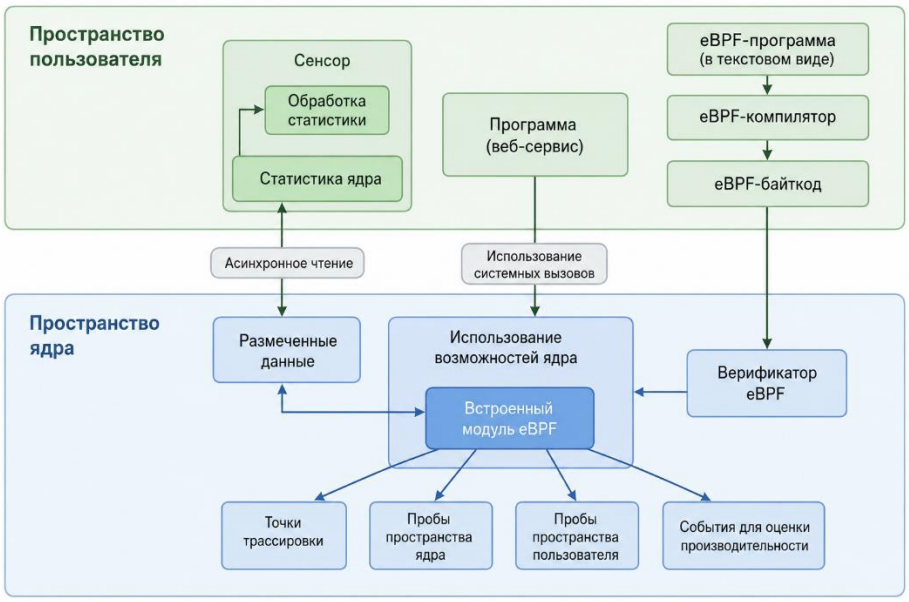



Рис. 1. Архитектура eBPF – взаимодействие пространства пользователя и ядра

Для реализации сенсора в данной работе использовался bpftrace – высокоуровневый язык для однострочных сценариев и небольших программ мониторинга. Альтернативными подходами являются библиотека BCC (BPF Compiler Collection) и libbpf, который используется в промышленных программах.

Сенсор перехватывает tracepoint:syscalls:sys_enter_execve и sys_enter_connect, сопоставляет их с IoB-правилами и выдает алерт. Индикаторы поведения (IoB) необходимы для сбора и анализа цифровых следов пользователей, чтобы в реальном времени выявлять аномалии и автоматически адаптировать доступ к системе (Рис. 2).

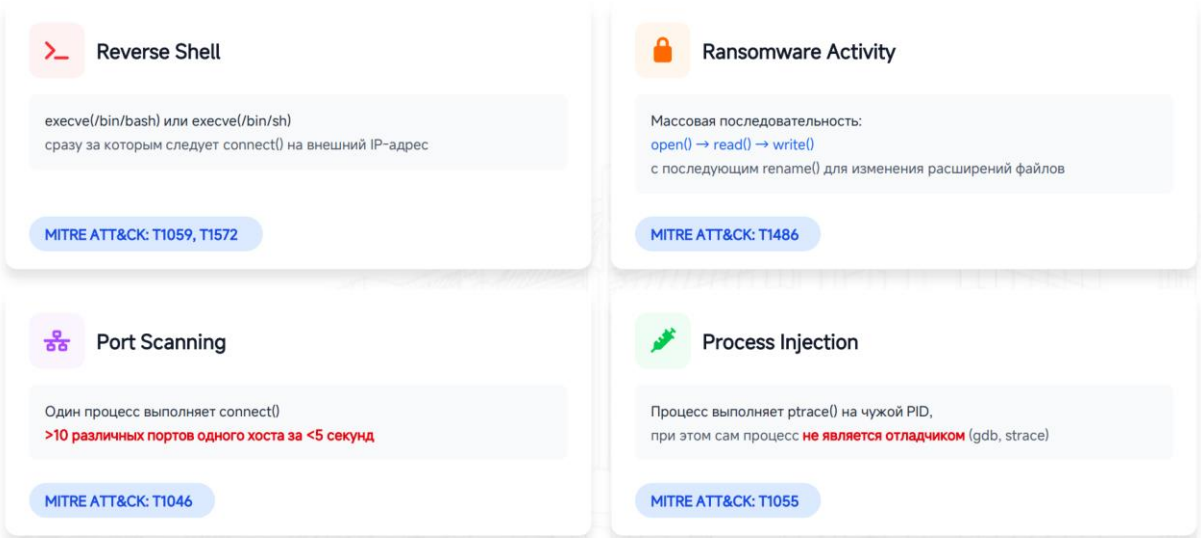



Рис 2. IoB-паттерны с привязкой к тактикам MITRE ATT&CK

Стенд состоит из трех компонентов (рис. 3):

*1. Уязвимое веб-приложение.* Docker-контейнер на Python Flask с намеренной уязвимостью Command Injection.

*2. eBPF-сенсор.* Программа на bpftrace, которая фиксирует RCE-атаки.

*3. Генератор атак (атакующий).* Набор скриптов на Bash/Python, которые имитируют поведение атакующего.

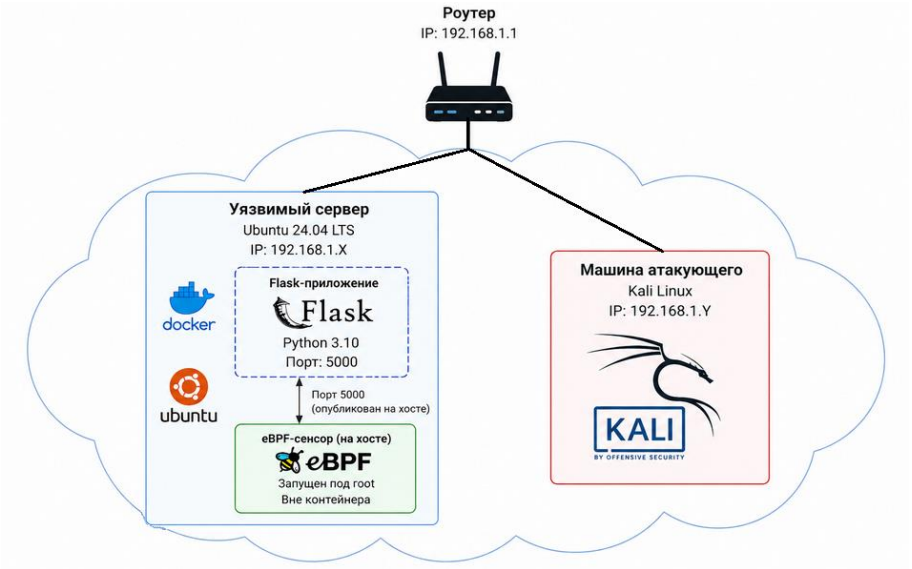



Рис 3. Архитектура демонстрационного стенда

Веб-приложение развернуто в Docker-контейнере на базе с предустановленным netcat. Ключевой элемент – форма авторизации, где содержимое полей передается в командный интерпретатор не в экранированном виде.

Сценарий генерации реализован как автоматизированная последовательность: атакующий запускает прослушивание порта 4000 (nc -lvnp 4000), затем отправляет HTTP POST-запрос с полезной нагрузкой: username=admin; nc -e /bin/sh 192.168.1.77 4000. Результат автоматизированной атаки представлен на рисунке 4.

```
listening on [any] 4000 ...
connect to [192.168.1.77] from (UNKNOWN) [192.168.1.152] 59398
whoami
root
```

Рис. 4. Результат успешной автоматизированной атаки с получением доступа к контейнеру

Веб-приложение выполняет подстановку команды, и атакующий получает reverse shell. Параллельно eBPF-сенсор, результат работы которого представлен на рисунке 5, фиксирует IoB-паттерн: execve(/bin/sh) от процесса Python и выводит предупреждение «SHELL_FROM_WEBPROCESS».

Вызов execve() у веб-процесса выглядит нелегитимным, но для некоторых реализации веб-серверов, которые генерируют ответ в формате файла – это может быть устоявшейся практикой, так как генерация и обработка файла происходит в отдельном потоке, который порождает веб-процесс для вызова бизнес-логики для запуска отдельного приложения на сервере. Далее вызывается connect() на IP-атакующего.

Последовательность системных вызовов (execve(), connect()) является индикатором атаки удаленного доступа, сенсор выводит алерт «REVERSE_SHELL_DETECTED» с привязкой к матрице MITRE ATT&CK.

```
[WARN] SHELL_FROM_WEBPROCESS
  pid=6213    comm=python3
  ATT&CK: T1059.004 (Unix Shell)

[ALERT] REVERSE_SHELL_DETECTED
  pid=6215    comm=nc
  ATT&CK: T1071.001 (Web Protocol)
```

Рис. 5. Результат детектирования RCE-атаки

В статье представлена разработка экспериментального стенда для генерации RCE-атак в контейнерной среде. Стенд включает уязвимое Flask-приложение, скрипты генерации и eBPF-сенсор для валидации.

Продемонстрирована успешная генерация атаки инъекции кода, подтвержденная через IoB-паттерны. Стенд применим для калибровки IDS/IPS [6], обучения специалистов ИБ и валидации IoB-правил для EDR-решений.

Дальнейшие исследования связаны с интеграцией комплексных атак, которые эмулируют действия подготовленных атакующих.

**Список используемых источников**

1. OWASP Foundation. OWASP Top 10. 2026. URL: https://owasp.org/Top10/ (дата обращения 14.04.2026).

2. MITRE ATT&CK® Framework. URL:https://attack.mitre.org/ (дата обращения 17.04.2026).

3. Linux Kernel documentation. BPF and XDP Reference Guide. URL: https://docs.kernel.org/bpf/ (дата обращения 23.04.2026).

4. Gregg B. BPF Performance Tools: Linux System and Application Observability. – Addison-Wesley, 2019. 544 p.

5. Fleming M. BPF: A New Type of Software. ACM Queue, 2022. PP. 45–68.

6. NIST SP 800-115. Technical Guide to Information Security Testing. 2008.

## DEVELOPMENT OF AN EXPERIMENTAL STAND FOR RCE-ATTACKS GENERATION

**Branitskiy A., Drobotov A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Remote code execution (RCE) attacks represent one of the most critical threats to modern IT infrastructures. The article describes the development of an experimental stand that allows generating different types of RCE attacks. Stand includes a vulnerable web application, an attack-generating script set, and an eBPF sensor for validation of results. The results of experiments are presented and prospects for development are substantiated.*

***Key words:*** *RCE-attacks, eBPF, IoB, behavioral analysis, reverse shell, MITRE ATT&CK, runtime detection, system calls*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ПРИМЕНЕНИЕ ПОДХОДА DEVSECOPS В ЗАДАЧЕ УПРАВЛЕНИЯ СЕРВЕРАМИ И ПОВЫШЕНИЯ ИХ ЗАЩИЩЕННОСТИ

**А. А. Браницкий, Я. С. Иванов**

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

*Статья посвящена анализу подхода DevSecOps, который направлен на повышение защищенности инфраструктуры облачных и серверных станций. Рассматриваются ключевые принципы подхода DevSecOps: автоматизация для создания защищенной инфраструктуры и внедрение проверок безопасности программного обеспечения в CI/CD-конвейер для выявления уязвимостей на ранних этапах его разработки. Описаны преимущества подхода и лучшие практики для повышения защищенности системы. В ходе исследования предлагаются способы масштабирования инфраструктуры и практические рекомендации по созданию и развертыванию безопасного окружения в облачных и серверных решениях.*

***информационная безопасность, разработка, управление серверами, автоматизация, DevSecOps***

Современные требования разработки программного обеспечения должны соответствовать гибкости, надежности инфраструктуры и, что немаловажно, ее безопасности Эту задачу решает методология DevSecOps. Однако сначала стоит обратиться к ее основе: DevOps. Название этого подхода произошло от терминов Development (разработка) и Operations (эксплуатация). Он был придуман для объединения всех сотрудников компании с упором на автоматизацию инфраструктуры информационных систем и непрерывной интеграции с частой поставкой программного обеспечения.

Основные практики DevOps:

1. Описание инфраструктуры в коде, например с помощью Ansible;

2. CI/CD-конвейеры для автоматического запуска сценариев при изменении кода;

3. Мониторинг и логирование инфраструктуры информационных систем.

В DevSecOps смещают фокус с самих процессов на безопасность внутри них, к разработке и эксплуатации добавляется термин Security (без-

опасность) [1]. Интеграция безопасных практик и отличает DevSecOps от DevOps [2].

Главные постулаты DevSecOps:

1. Применение практики “сдвиг влево” (Shift Left) [3], согласно которой все проверки при разработке программного обеспечения на безопасность переносятся на как можно более ранние этапы. Проверки интегрируются в CI/CD-конвейеры вместе с исходным кодом;

2. «Безопасность как код». Данная концепция предполагает использование автоматизированных инструментов, таких как Ansible [4] или Terraform [5] для конфигурации не только стандартных сервисов для ПО, но также и для развертывания сервисов, повышающих защищенность серверов. Это может быть, например, автоматизированная настройка SIEM-системы, конфигурирование межсетевого экрана и любого другого сервиса в зависимости от поставленной задачи.

3. Мониторинг и логирование инфраструктуры информационных систем.

Говоря о самых популярных инструментах, применяемых в работе DevSecOps, в первую очередь стоит упомянуть программы для автоматизации развертывания серверов и конфигураций на серверах. На сегодняшний день самыми популярными являются Ansible и Terraform. Обычно их применяют в связке, но концепция применения этих инструментов одинаковая: хранение инфраструктуры в системе хранения версий в виде кода. Terraform используют для развертывания сервисов, к примеру это может быть Linux сервер, либо сервис баз данных, также большая часть инфраструктурных сервисов позволяет осуществлять настройку межсетевых экранов и создание политики ролей для настройки доступа к этим сервисам, что автоматизирует и одновременно с этим повышает защищенность серверов. Код запускается и принимается на стороне инфраструктурных платформ, таких как Yandex Cloud или VMware с помощью провайдеров. Провайдеры – это специально написанные компоненты, позволяющие напрямую взаимодействовать с данными платформами. Ansible же используют для конфигурации сервисов внутри уже созданных сервисов в инфраструктурных платформах, например на Linux серверах. Ansible является достаточно популярным инструментом, отличительным преимуществом над его конкурентами является его безагентская модель. На целевых серверах достаточно установить python и настроить доступ управляющему серверу доступ по протоколу SSH.

В DevSecOps-подходе также принято автоматизировать поиск уязвимостей в разрабатываемом программном обеспечении при каждом его изменении. Для проверок программного обеспечения разрабатывается CI/CD-конвейер. Процесс функционирования CI/CD-конвейера достаточно прост: на каждое изменение кода и изменение репозитория запускаются этапы сканирования, развертывание приложения (веб-сервера) в изолированном окружении, например в Docker-контейнере. CI/CD-конвейер разделяется на следующие этапы:

– юнит-тесты;
– интеграционные тесты;
– статический анализ безопасности (SAST, Static Application Security Testing) [6];
– анализ состава ПО (SCA, Software Composition Analysis);
– отдельные проверки секретов;
– сканирование образов контейнеров;
– динамический анализ безопасности (DAST, Dynamic Application Security Testing).

Применение данного подхода в работе имеет ряд преимуществ: подход позволяет выявлять уязвимость на ранних этапах разработки, при этом сокращая время нахождения уязвимостей с нескольких часов до нескольких минут. Автоматизация проверок и использование подхода «безопасность как код» снижают риск человеческой ошибки при настройке конфигурации серверов.

Также у данного подхода помимо преимуществ, есть и недостатки, главный из них – это задержка перед развертыванием программного обеспечения при частых изменениях в исходном коде. Кроме этого, существует вероятность ложноположительного срабатывания инструментов для поиска уязвимостей. Для разработчиков рекомендуется адаптировать правила поиска уязвимостей в зависимости от того, какой язык программирования используется для снижения вероятности ложноположительных срабатываний, также принято разделять окружения для тестирования и для продуктивной реализации программного обеспечения для более последовательного и правильного подхода к автоматизации.

В качестве практической реализации была разработана автоматизированная система для повышения защищенности инфраструктуры информационных систем и раннего выявления уязвимостей, которая включает в себя

две роли Ansible, а также CI/CD-конвейер для автоматизированного поиска уязвимостей в разрабатываемом программном обеспечении.

Ansible-роли построены по принципу «безопасность как код»: вся конфигурация серверов описывается декларативно и хранится в Git. Первая роль настраивает SSH (запрет root-доступа, аутентификацию по ключам), межсетевой экран (открыты только порты 22, 80, 443) и системные параметры. Вторая роль настраивает веб-сервер angie с выдачей сертификата для того, чтобы разрабатываемое приложение функционировало только по HTTPS-протоколу. CI/CD-конвейер, реализованный в GitLab, включает этапы проверки секретов, статического анализа кода (SAST), сканирования Dockerfile, анализа зависимостей и образа контейнера (SCA), а также динамического тестирования работающего приложения (DAST). Все проверки выполняются автоматически при каждом изменении в репозитории.

Кроме того, были предложены варианты для будущего улучшения и масштабирования инфраструктуры.

Для масштабирования и централизованного управления предлагается использовать Ansible во всех компонентах инфраструктуры. Запуски сценариев удобнее выполнять через веб-интерфейс (Astra Automation, AWX), которые могут быть развернуты как Docker-контейнеры.

Необходимо также внедрить мониторинг ключевых метрик (доступность приложения, потребление CPU и памяти, дисковые и сетевые нагрузки) с пороговыми значениями и уведомлениями в корпоративный мессенджер.

Следует централизованно собирать логи с помощью набора инструментов: OpenSearch, Logstash и Kibana – для удобного анализа и быстрого поиска причин инцидентов во время работы инфраструктуры.

При росте нагрузки целесообразен переход от отдельных Docker-контейнеров к оркестратору Kubernetes, обеспечивающему автоматическое масштабирование, высокую доступность и обновления без остановки сервиса.

В рамках данной статьи была рассмотрена концепция DevSecOps, которая позволяет повысить защищенность серверной инфраструктуры за счет интеграции проверок безопасности в CI/CD-конвейер и автоматизации настройки конфигураций на серверах. В будущих исследованиях планируется оценить влияние внедренных проверок на процент ложных срабатываний и время выполнения конвейера при использовании других языков программирования.

**Список используемых источников**

1. Миняев А. А., Паршин Е. А. Анализ процессов безопасной разработки DevSecOps // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2022. Т. 1. С. 683-689.
2. Ганжур М. А., Дьяченко Н. В., Отакулов А. С. Анализ методологий DevOps и DevSecOps // Молодой исследователь Дона. 2021. N 5. С. 8-10.
3. Вехен. М. Безопасный DevOps: Эффективная эксплуатация систем: ДМК Пресс, 2019, 432 с.
4. Ansible Community | Ansible documentation. URL: https://docs.ansible.com (дата обращения 25.05.2026).
5. HashiCorp Documentation. URL: https://developer.hashicorp.com/terraform/docs (дата обращения 28.05.2026).
6. Бударный Г. С., Камалова А. О., Красов А. В. Сравнение статического и динамического кода и их роль в методологии инфотелекоммуникаций в науке и образовании // Сборник научных статей XII Международной научно-технической и научно-методической конференции. В 4 т. Том 1. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2023. С. 204–208.

## APPLICATION OF THE DEVSECOPS APPROACH IN THE TASK OF MANAGING SERVERS AND INCREASING THEIR SECURITY

**Branitskiy A., Ivanov Y.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The paper analyzes the DevSecOps approach, which aims to improve the security of cloud and server infrastructure. It examines the key principles of the DevSecOps approach: automation for creating a secure infrastructure and the integration of software security checks into the CI/CD pipeline to identify vulnerabilities in the early stages of its development. The advantages of this approach and best practices for improving system security are described. The research proposes methods for scaling the infrastructure and practical recommendations for creating and deploying a secure environment in cloud and server solutions.*

***Key words:*** *information security, development, server management, automation, DevSecOps*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ПРАВОВЫЕ КОЛЛИЗИИ АВТОМАТИЗИРОВАННОГО СБОРА ДАННЫХ С IoT-УСТРОЙСТВ

**Г. С. Бударный, Е. А. Макаренкова**

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

*Существующие законы о защите персональных данных в настоящее время не всегда могут в полной мере регулировать автоматизированный сбор данных с IoT-устройств, поскольку стремительное развитие технологий зачастую опережает процессы законодательства. Возникающие на практике противоречия между требованиями информационной безопасности существенно затрудняют правомерное применение парсинга в исследовательских и коммерческих целях. В данной статье будет рассмотрено выявление и систематизация правовых коллизий, возникающих при веб-скрапинге данных.*

***автоматизированный сбор данных; IoT; парсинг; веб-скрапинг; защита персональных данных***

Интернет вещей стремительно становится ключевым драйвером интеграции физических объектов в цифровую экосистему. По данным исследований, на 2026 год в мире 22 миллиарда активных IoT-подключений, а к 2030 году прогнозируется около 31 миллиарда. Внедрение интернета вещей охватывает промышленность, энергетику, здравоохранение, государственное управление и другие сферы, создавая безграничные возможности для развития цифровых экосистем.

Быстрые темпы увеличения масштабов использования IoT неизбежно вызывают разрыв между технологической реальностью и правовым регулированием. Представленная работа нацелена на выявление правовых коллизий парсинга данных с IoT-устройств путем проведения анализа нормативно-правовой базы Российской Федерации и рассмотрение возможных путей устранения этих коллизий.

Прежде чем переходить к анализу специфических вопросов обработки данных, необходимо обозначить фундаментальную правовую неопределенность: на сегодняшний день в российском законодательстве отсутствует конкретное определение понятий «Интернет вещей» и «IoT-устройство». Доктринально IoT понимается как сеть физических устройств, оснащенных

датчиками, программным обеспечением и иными технологиями для сбора, передачи и обмена данными с другими устройствами и системами через Интернет. Существующий стандарт ГОСТ Р 70924-2023 определяет типовую архитектуру Интернета вещей, характеристики и функции его систем, но правовой статус устройств рассматриваемый стандарт не устанавливает [1].

Принципиально значимыми свойствами веб-скрапинга с IoT-устройств для анализа правовых коллизий становятся:

– непрерывность – способность сбора данных в режиме реального времени без дискретных актов получения согласия;
– агрегируемость – множество обезличенных данных способно составить цифровой портрет конкретных лиц и, как следствие, привести к их идентификации;
– массовость – единовременный охват миллиона субъектов.

Рассмотрим несколько возникающих коллизий. Как было сказано ранее, в законодательстве Российской Федерации нет определений понятий, критически важных для полного правового регулирования парсинга. К таким понятиям относится, например, «IoT-устройство», «автоматизированный сбор данных в IoT» и так далее. Это порождает правовую неопределенность, поскольку одно и то же устройство может квалифицироваться как «информационная система» (по № 149-ФЗ), «автоматизированная система управления» (по № 187-ФЗ), «техническое средство обработки персональных данных» (по № 152-ФЗ) или не подпадать ни под одну категорию. Такая «терминологическая коллизия» лишает правоприменителя единообразного ориентира.

Статья 9 Федерального закона № 152-ФЗ гласит: «Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным» [2]. Однако архитектура IoT зачастую не позволяет это реализовать на практике, поскольку устройства собирают терабайты информации фоново и предоставить пользователю понятный список того, что делает каждый датчик каждую секунду, физически невозможно, из-за чего пользователи просто механически нажимают «Принять», не осознавая масштаб сбора данных. Кроме того, исключения, предусмотренные ст. 6 закона («обработка в статистических или иных исследовательских целях, в целях безопасности») могут трактоваться операторами расширительно, позволяя злоупотреблять возможностями. Единая правовая позиция по данному вопросу в правоприменитель-

ной практике отсутствует, создавая коллизию норм о согласии субъекта данных.

Следующее столкновение закона и технической реальности касается права субъекта на удаление данных и обязанности оператора хранить логи. Статья 21 Федерального закона № 152-ФЗ предоставляет субъекту персональных данных право требовать прекращения обработки и уничтожения его данных. Оператор обязан исполнить это требование. Вместе с тем требования по информационной безопасности категорически исключают возможность такого уничтожения в той части, которая касается журналов (логов) событий. Приказ ФСТЭК России № 239 обязывает субъектов КИИ хранить журналы аудита безопасности сроком не менее года, а 117-й приказ ФСТЭК вводит требования к операционным системам с элементами искусственного интеллекта, где устанавливает обязанность полного логирования всех запросов и ответов системы, включая запросы, содержащие персональные данные [3]. Ни один из этих актов не предусматривает исключения для случаев, когда субъект данных реализует право на удаление по № 152-ФЗ. В итоге складывается правовая ситуация, при которой оператор IoT-системы одновременно обязан удалить данные (по требованию субъекта) и обязан их сохранить (по требованию регулятора). Российское законодательство не содержит нормы, разрешающей данный конфликт.

Что касается автоматизированного сбора данных с IoT-платформ, то парсинг нередко осуществляется через публичные API. Здесь возникает трехсторонняя коллизия. С одной стороны, статья 7 Федерального закона № 149-ФЗ относит общедоступную информацию к сведениям, доступ к которым не может быть ограничен, значит, обращение к публичному API формально правомерно [4]. С другой стороны, пользовательские соглашения IoT-платформ, как правило, запрещают массовый автоматизированный сбор данных, квалифицируя его как нарушение договора. С третьей стороны, статья 272 Уголовного кодекса РФ устанавливает ответственность за «неправомерный доступ к охраняемой компьютерной информации», причем критерий «неправомерности» судебной практикой трактуется неоднозначно: некоторые судебные решения признают нарушение ToS достаточным основанием для квалификации деяния по данной статье, другие – нет. Следовательно, исследователь, который обращается к публичному API IoT-устройства в научных целях, по сути, оперирует общедоступной информацией, но фактически нарушает ToS платформы и потенциально рискует уголовным преследованием. Четкая законодательная граница между правомерным пар-

сингом и неправомерным доступом в российском праве отсутствует, что создает системную правовую неопределенность как для исследователей, так и для операторов IoT-систем [5].

Проведенный анализ позволяет сформулировать следующий комплекс предложений по устранению выявленных коллизий. Во-первых, необходимо принять специальный отдельный федеральный закон об Интернете вещей, который бы закреплял все необходимые определения IoT, устанавливал минимальные обязательные требования к безопасности устройств и вводил разграничение ответственности между участниками IoT-экосистемы. Единый понятийный аппарат устранит ситуацию, при которой одно и то же устройство одновременно подпадает под несколько конкурирующих правовых режимов или не подпадает ни под один из них в полной мере. Далее, необходимо предусмотреть в ст. 9 152-ФЗ отдельную норму для IoT-операторов, допускающую замену разового письменного согласия на однократное публичное уведомление с четко описанным перечнем собираемых данных, целей и сроков их хранения, а также с работающим механизмом отзыва. Кроме того, следует разграничить правомерный автоматизированный доступ к данным и неправомерного доступа. Это можно сделать**,** внеся в ст. 272 УК РФ примечание, которое бы прямо устанавливало, что нарушение условий пользовательского соглашения (ToS) само по себе не является основанием для квалификации деяния как неправомерного доступа к компьютерной информации, если информация является общедоступной по смыслу ст. 7 № 149-ФЗ. Параллельно следует дополнить № 149-ФЗ нормой, отличающей добросовестный научный сбор данных с IoT-платформ от действий, направленных на причинение вреда. Заключительным предложением по устранению коллизий станет внести в приказы ФСТЭК № 117, № 239 и № 31 специальную норму, допускающую псевдонимизацию (замену идентификаторов субъекта на токен без возможности обратного сопоставления) в качестве надлежащего исполнения требования об уничтожении персональных данных при сохранении обязательных журналов в обезличенном виде [6].

Проведенное исследование четко фиксирует проблему отсутствия механизмов однозначного регулирования процессов веб-скрапинга данных с IoT-устройств в законодательстве Российской Федерации. Анализ действующей нормативно-правовой базы выявил четыре системные правовые коллизии, каждая из которых порождает практическую неразрешимость для участников IoT-отношений.

Первая коллизия носит терминологический характер. Отсутствие легального определения IoT-устройства и автоматизированного сбора данных вынуждает правоприменителя одновременно применять несколько конкурирующих правовых режимов, ни один из которых не разработан с учетом специфики IoT. Вторая коллизия связана с принципом информированного согласия. Требование ст. 9 № 152-ФЗ о согласии субъекта несовместимо с непрерывной моделью сбора данных IoT-систем. Третья коллизия освещает взаимоисключающие обязанности – удалить данные по требованию субъекта (ст. 21 № 152-ФЗ) и сохранять логи в течение установленных ФСТЭК сроков (приказы № 117, № 239, № 31). Четвертая коллизия затрагивает уголовно-правовую сферу: ст. 272 УК РФ в ее нынешней редакции не позволяет провести четкую границу между правомерным доступом к общедоступным данным IoT-платформы и уголовно наказуемым неправомерным доступом.

Рассмотренные коллизии носят системный характер и не могут быть устранены путем расширительного толкования существующих норм. Предложенный комплекс мер позволит устранить выявленные противоречия. Кроме того, стоит отметить, что промедление с реформированием правовой базы в условиях стремительного роста числа IoT-устройств неизбежно ведет к расширению зоны правовой неопределенности и нарастанию рисков как для граждан, так и для операторов критической инфраструктуры.

**Список используемых источников**

1. ГОСТ Р 70924-2023 Информационные технологии. Интернет вещей. Типовая архитектура. М.: Изд-во стандартов, 2023. 66 с.

2. О персональных данных: Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ. М.: Маркетинг, 2006. 39 с.

3. Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений: утв. приказом ФСТЭК России от 11.04.2025 № 117. М.: ФСТЭК России, 2025. 45 с.

4. Купцова А. С. Правовое регулирование использования интернета вещей // Образование и право. 2021. № 7. URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-ispolzovaniya-interneta-veschey (дата обращения: 20.05.2026).

5. Лешукова А. М., Петрова Т. С., Сахаров Д. В. Анализ киберугроз безопасности обработки персональных данных субъектов малого и среднего предпринимательства / 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. 556-559. EDN: IFMVKC.

6. Донской Д. М., Рябова О. Н., Сахаров Д. В., Виткова Л. А. Некоторые аспекты модели нарушителя информационной безопасности в Интернете вещей / Интернет вещей и 5G, Санкт-Петербург, 07 декабря 2016 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2016. С. 47-50. EDN: XGGXGZ.

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

## AUTOMATED IOT DATA COLLECTION: LEGAL CONFLICTS AND REGULATORY GAPS

**Budarnyi G., Makarenkova E.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Current personal data protection laws are not always capable of fully regulating the automated collection of data from IoT devices, as rapid technological advancement often outpaces legislative processes. The practical contradictions arising between information security requirements significantly complicate the lawful use of data parsing for research and commercial purposes. This article addresses the identification and systematization of legal conflicts that emerge during web scraping.*

***Key words:*** *automated data collection; IoT; data parsing; web scraping; personal data protection*

**УДК 004.056.5**
**ГРНТИ 81.93.29**

# РАЗРАБОТКА ЭКСПЕРИМЕНТАЛЬНОГО СТЕНДА ДЛЯ АНАЛИЗА ЭФФЕКТИВНОСТИ МЕТОДОВ ФИЛЬТРАЦИИ СЕТЕВОГО ТРАФИКА

**Д. П. Ганин, Д. С. Левшун**

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

*В современных компьютерных сетях фильтрация по сетевым адресам неэффективна из-за блокировок легитимных ресурсов и динамической смены адресов крупными сервисами. Технология глубокого анализа пакетов решает эти проблемы, позволяя точечно идентифицировать доменные имена и протоколы передачи данных. Повсеместное использование промежуточных серверов и утилит модификации данных вынуждает переходить к статистическому анализу потоков, однако классические методы сигнатурного анализа демонстрируют снижение точности при обработке обфусцированного трафика. В данной работе предлагается архитектура экспериментального стенда в изолированной среде контейнеризации для исследования устойчивости систем глубокого анализа пакетов к методам фрагментации и маскирования информации. Метод основан на последовательной маршрутизации трафика через узлы модификации и анализатора, что позволяет оценивать эффективность алгоритмов классификации в условиях намеренного искажения структуры сетевых пакетов.*

***сетевая безопасность, глубокий анализ пакетов, обфускация трафика, контейнеризация, Docker***

Рост объемов сетевого трафика и усложнение механизмов его маскирования ставят новые задачи перед системами обеспечения сетевой безопасности [1]. Классические подходы, основанные на контроле сетевых адресов, теряют актуальность из-за динамической структуры современных веб-сервисов и применения инструментов сокрытия информационной активности [2]. В этих условиях критически важным становится использование систем глубокого анализа пакетов, способных анализировать пакеты по их сигнатуре. Однако разработчики средств обхода систем анализа постоянно модернизируют методы обфускации данных, что снижает точность классификации. Для поиска слабых мест в алгоритмах анализа и выработки мер противодействия необходимы инструменты безопасного и воспроизводимого тестирования.

Целью работы является разработка экспериментального стенда для анализа эффективности методов фильтрации сетевого трафика, необходимого для последующей оценки устойчивости алгоритмов глубокого анализа пакетов к методам обфускации. Для этого в среде контейнеризации

развернут исследовательский стенд с последовательной маршрутизацией трафика. Задачи исследования включают внедрение правил сигнализации в анализатор, применение алгоритмов маскировки данных и проведение сравнительного анализа точности классификации протоколов в различных условиях передачи.

Для реализации исследования развернут стенд на базе технологии контейнеризации Docker [3], обеспечивающей изоляцию узлов и воспроизводимость тестов. В состав стенда включены три функциональных модуля: генератор трафика (curl), узел маскировки (zapret) [4] и анализатор трафика с глубокой инспекцией пакетов (nDPI) [5].

Сетевая связность обеспечена путем создания двух изолированных сегментов:

– **net_1 (10.10.0.0/24):** клиентская сеть, в которой расположен генератор трафика (10.10.0.10) и обфускатор (10.10.0.20).
– **net_2 (10.20.0.0/24):** транзитная сеть, содержащая обфускатор (10.20.0.20) и анализатор трафика (10.20.0.30).

Маршрутизация настроена таким образом, что узел обфускации (10.10.0.20) выступает шлюзом по умолчанию для генератора трафика, а анализатор является шлюзом по умолчанию для обфускатора. Для обеспечения двустороннего обмена данными на промежуточных узлах активирована пересылка IP-пакетов и настроены статические обратные маршруты.

Docker позволяет развертывать стенд на любой другой машине используя docker-compose.yml, в котором уже хранятся данные об образах, маршрутизации и аргументах запуска утилит [3].

Архитектура стенда представлена на рисунке 1.

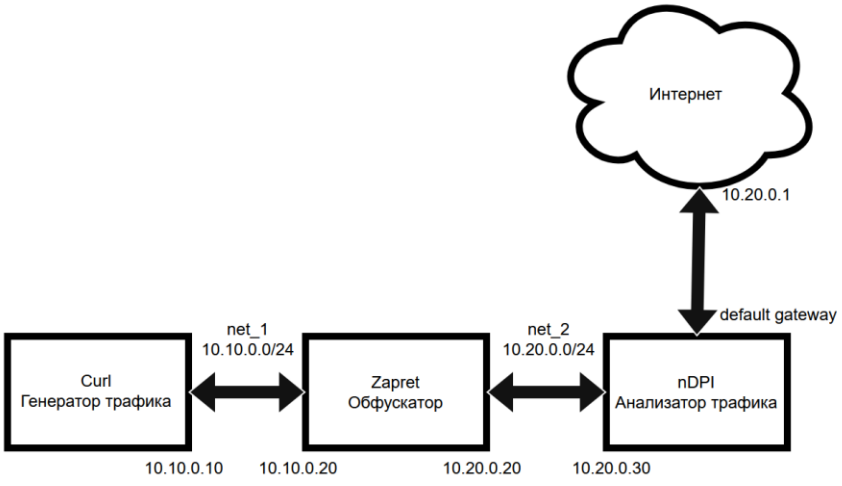



Рис. 1. Архитектура экспериментального стенда

На рисунке 2 представлена работоспособность стенда с выключенной обфускацией и ненастроенными политиками анализа трафика

| Actions | Last Seen | Duration | Protocol | Score | Flow | Actual Thpt | Total Bytes | Info |
|---|---|---|---|---|---|---|---|---|
| | 00:34 | 00:02 | TCP:TLS.Google ... | | 10.10.0.10 : 36862 142.251.38.78 : 443 | 6.63 Kbps | 4.67 KB | google.com |
| | 00:59 | 00:02 | TCP:TLS.Google ... | | 10.10.0.10 : 40556 142.251.38.78 : 443 | 12.07 Kbps | 4.67 KB | google.com |
| | 00:49 | 00:01 | TCP:TLS.Google ... | | 10.10.0.10 : 55002 142.251.38.78 : 443 | | 4.67 KB | google.com |
| | 00:24 | 00:01 | TCP:TLS.Google ... | | 10.10.0.10 : 41396 142.251.38.78 : 443 | | 4.67 KB | google.com |
| | 00:28 | 00:02 | TCP:TLS.Google ... | | 10.10.0.10 : 41386 142.251.38.78 : 443 | 7.32 Kbps | 4.67 KB | google.com |
| | 00:13 | 00:02 | TCP:TLS.Google ... | | 10.10.0.10 : 43798 142.251.38.78 : 443 | 343.75 bps | 4.54 KB | google.com |
| | 00:06 | 00:02 | TCP:TLS.Google ... | | 10.10.0.10 : 57466 64.233.164.100 : 443 | 2.64 Kbps | 4.54 KB | google.com |
| | 00:36 | 00:01 | TCP:TLS.Google ... | | 10.10.0.10 : 36846 142.251.38.78 : 443 | | 4.54 KB | google.com |
| | 00:52 | 00:01 | TCP:TLS.Google ... | | 10.10.0.10 : 54996 142.251.38.78 : 443 | | 4.54 KB | google.com |
| | 00:08 | 00:01 | TCP:TLS.Google ... | | 10.10.0.10 : 38996 142.251.38.78 : 443 | | 4.54 KB | google.com |

Рис. 2. Не измененный трафик в веб-интерфейсе

Для верификации работоспособности стенда и оценки эффективности методов маскировки было проведено два контролируемых эксперимента. В качестве целевого ресурса использовался домен google.com, а идентификация осуществлялась по полю Server Name Indication (SNI) в рамках протокола TLS.

В первом эксперименте осуществлялась прямая передача данных от узла генерации к целевому серверу без включения механизмов обфускации. В результате анализатор трафика успешно перехватил сессию и на основе настроенных правил сигнализации идентифицировал обращение к домену google.com, как показано на рисунке 3.

| Actions | Date / Time | Score | Category | Application | Main Alert | Flow | Description |
|---|---|---|---|---|---|---|---|
| | 23:29:16 | 100 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :34248 216.58.198.206 :https | "Google" traffic not allowed for the cli |
| | 23:29:16 | 110 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :34248 216.58.198.206 :https | "Google" traffic not allowed for the cli |
| | 23:29:17 | 100 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :42922 142.251.38.78 :https | "Google" traffic not allowed for the cli |
| | 23:29:17 | 110 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :42922 142.251.38.78 :https | "Google" traffic not allowed for the cli |
| | 23:29:19 | 100 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :58052 192.178.25.78 :https | "Google" traffic not allowed for the cli |
| | 23:29:19 | 110 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :58052 192.178.25.78 :https | "Google" traffic not allowed for the cli |
| | 23:29:21 | 100 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :58056 192.178.25.78 :https | "Google" traffic not allowed for the cli |
| | 23:29:21 | 110 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :58056 192.178.25.78 :https | "Google" traffic not allowed for the cli |
| | 23:29:22 | 100 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :47712 173.194.222.102 :http... | "Google" traffic not allowed for the cli |
| | 23:29:22 | 110 | | TCP:TLS.Goog... | Susp. Device Prot... | 10.10.0.10 :47712 173.194.222.102 :http... | "Google" traffic not allowed for the cli |

Рис. 3. Выявленный нежелательный трафик к google.com

Это означает, что система глубокого анализа пакетов корректно считала заголовок TLS Client Hello. Данный результат подтверждает высокую эффективность сигнатурного анализа nDPI, т. к. были помечены пакеты с разными IP адресами, принадлежащими одному сервису google.com.

Во втором эксперименте на узле zapret был активирован алгоритм сегментации TCP-потока. Пакет, содержащий запрос Client Hello, принудительно дробился на фрагменты таким образом, чтобы строка доменного имени была разделена между разными сегментами.

В результате прямая идентификация домена google.com анализатором не удалась. Однако система nDPI пометила проходящие пакеты как «подозрительные». Результат показан на рисунке 4.

| Actions | Last Seen | Duration | Protocol | Score | Flow | Actual Thpt | Total Bytes | Info |
|---|---|---|---|---|---|---|---|---|
| | 00:26 | 01:01 | TCP:TLS Guess | | 10.10.0.10 : 50336 ⇄ 64.233.161.102 : 443 | 1.18 Kbps ↓ | 14.70 KB | |
| | 00:28 | 01:01 | TCP:TLS Guess | | 10.10.0.10 : 36122 ⇄ 64.233.161.100 : 443 | 1.18 Kbps ↓ | 14.51 KB | |
| | 00:32 | 00:59 | TCP:TLS Guess | | 10.10.0.10 : 35482 ⇄ 172.253.130.102 : 443 | 1.18 Kbps ↑ | 14.51 KB | |
| | 00:30 | 01:01 | TCP:TLS Guess | | 10.10.0.10 : 58082 ⇄ 64.233.164.138 : 443 | 1.18 Kbps ↑ | 14.51 KB | |
| | 00:22 | 01:01 | TCP:TLS Guess | | 10.10.0.10 : 60184 ⇄ 173.194.222.113 : 443 | 1.18 Kbps ↓ | 14.51 KB | |
| | 00:32 | 00:59 | TCP:TLS Guess | | 10.10.0.10 : 59250 ⇄ 172.253.130.139 : 443 | 1.18 Kbps ↑ | 14.51 KB | |
| | 00:32 | 00:59 | TCP:TLS Guess | | 10.10.0.10 : 52034 ⇄ 64.233.161.101 : 443 | 1.18 Kbps ↑ | 14.51 KB | |
| | 00:14 | 01:00 | TCP:TLS Guess | | 10.10.0.10 : 60156 ⇄ 173.194.220.101 : 443 | 1.18 Kbps ↑ | 14.51 KB | |
| | 00:32 | 01:00 | TCP:TLS Guess | | 10.10.0.10 : 47438 ⇄ 172.253.130.100 : 443 | 1.18 Kbps ↑ | 14.51 KB | |
| | 00:05 | 00:31 | TCP:TLS Guess | | 10.10.0.10 : 60312 ⇄ 64.233.161.101 : 443 | 1.18 Kbps ↑ | 14.07 KB | |

Рис. 4. Обфусцированный трафик в условиях активного анализа пакетов

Невозможность точного определения доменного имени объясняется тем, что анализатор nDPI в текущей конфигурации осуществляет инспекцию отдельных пакетов без полной сборки (реассемблирования) TCP-потока на уровне приложения. Фрагментация строки SNI нарушает целостность сигнатурного шаблона в рамках одного кадра, что позволяет обойти стандартные правила фильтрации по доменным именам [6]. Присвоение потоку статуса «Guess» (догадка) и классификация его как общего TCP:TLS свидетельствуют о переходе системы к эвристическому анализу. Анализатор не может идентифицировать конечный целевой сервис (Google.com), но на основе структуры пакета, номеров портов (443) и неизмененных полей заголовка TLS определяет тип используемого транспортного протокола. Таким образом, фрагментация пакетов лишает систему возможности точечной фильтрации, снижая глубину анализа до распознавания базового типа шифрованного трафика.

Разработанный на базе Docker исследовательский стенд доказал свою эффективность как инструмент для моделирования сетевых сценариев и тестирования систем глубокого анализа пакетов. Выявлено, что системы анализа способны классифицировать модифицированный трафик как аномаль-

ный, что указывает на необходимость развития более сложных методов обфускации, имитирующих поведение легитимных протоколов

**Список используемых источников**

1.Котенко И. В., Левшун Д. С., Жернова К. Н., Чечулин А. А. Обнаружение аномальных транзакций криптовалюты с помощью нейронных сетей и онтологий // Онтология проектирования. 2025. Т. 15. № 3. С. 334-350.

2. Болдырихин Н. В., Алтунин Ф. А., Короченцев Д. А. Особенности классификации зашифрованного сетевого трафика // Известия ЮФУ. Технические науки. 2020. № 3. С. 89-98.

3. Лю Ю., Борисов В. И. Контейнеризация и автоматизация развертывания веб-приложений: анализ и практическая реализация // Управление в организационных системах (технические, физико-математические науки). 2025. Т. 12. № 1. С. 194-201.

4. Проект Zapret: средство обхода систем глубокого анализа пакетов (DPI). URL: https://github.com/bol-van/zapret (дата обращения: 14.05.2026).

5. nDPI: Quick guide and technical overview. URL: https://www.ntop.org/guides/nDPI/ (дата обращения: 14.05.2026).

6. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. СПб.: Питер, 2021. 1008 с.

## DEVELOPMENT OF AN EXPERIMENTAL TESTBED FOR EVALUATING THE EFFICIENCY OF NETWORK TRAFFIC FILTERING METHODS

**Ganin D., Levshun D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In modern computer networks, network address filtering is ineffective due to the collateral blocking of legitimate resources and dynamic address switching by large-scale services. Deep packet inspection solves these issues by enabling the precise identification of domain names and data transmission protocols. The ubiquitous use of proxy servers and data modification utilities forces a transition to statistical flow analysis; however, classical signature-based methods demonstrate reduced accuracy when processing obfuscated traffic. This paper proposes the architecture of an experimental testbed within an isolated containerized environment to investigate the resilience of deep packet inspection systems against data fragmentation and masking techniques. The method is based on sequential traffic routing through modification and analyzer nodes, allowing for the evaluation of classification algorithms' effectiveness under conditions of intentional network packet structure distortion.*

***Key words:*** *network security, deep packet inspection, traffic obfuscation, containerization, Docker*

**УДК 004.056.5**
**ГРНТИ 20.23.25**

# МЕТОД СКРЫТОГО ВЛОЖЕНИЯ ЦВЗ В БИБЛИОТЕЧНЫЕ МОДУЛИ ПРОГРАММНЫХ ПРОДУКТОВ, УСТОЙЧИВЫХ К АТАКАМ ОБФУСКАЦИИ

**М. Гилавоги, А. В. Красов**

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

*В статье предложен метод формирования и скрытого вложения цифрового водяного знака (ЦВЗ) в библиотечные модули программных продуктов на основе цифровой подписи неизменяемой части кода с применением криптографических хеш-функций. Метод обеспечивает устойчивость ЦВЗ к атакам обфускации, а также сохранность скрытого вложения в штатных процессах компоновки и оптимизации. Экспериментально подтверждена средняя сохранность ЦВЗ на уровне 97,4 % после компоновки и 94,5 % после оптимизации уровня O2, при накладных расходах по времени исполнения не более 0,14 %.*

***цифровой водяной знак, стеганография в машинном коде, обфускация, библиотечные модули, защита авторских прав, компоновка, эквивалентные инструкции***

## Введение

Защита авторских прав на программное обеспечение (ПО) является одной из ключевых задач информационной безопасности. Особую сложность представляет коллективная разработка: библиотечные модули (*.lib, *.obj), созданные конкретными исполнителями, впоследствии интегрируются в единый продукт, что затрудняет идентификацию автора отдельного компонента. Цифровые водяные знаки (ЦВЗ) представляют перспективный инструмент для решения данной задачи, однако существующие методы не обеспечивают одновременно: применимость к промежуточным файлам до завершения компоновки, криптографическую верифицируемость ЦВЗ и устойчивость к атакам обфускации [1, 2].

Настоящая работа предлагает метод, устраняющий перечисленные недостатки. Он опирается на технику замены семантически эквивалентных машинных инструкций [3] и расширяет ее формализованным механизмом формирования и верификации ЦВЗ с использованием схемы ГОСТ Р 34.10-2012/ГОСТ Р 34.11-2012.

## Анализ существующих методов

Известные подходы к внедрению ЦВЗ в программный код распределяются по трем классам. Первый – методы уровня исходного кода [1]: ЦВЗ встраивается через нейтральные языковые конструкции и не выживает при перекомпиляции. Второй – методы уровня исполнимого файла [2, 4-6]: ЦВЗ помещается в PE/ELF-секции выравнивания или заголовки; легко нейтрализуется утилитами типа strip. Третий – методы замены эквивалентных инструкций [3, 7, 8]: наиболее пригодны для библиотечных файлов, однако в известных реализациях отсутствует механизм формирования верифицируемого ЦВЗ, устойчивого к обфускации.

## Предлагаемый метод

Метод включает два этапа: формирование ЦВЗ и его вложение в тело модуля.

Формирование ЦВЗ. Цифровой водяной знак формируется как цифровая подпись неизменяемой части защищаемого файла:

$$\text{ЦВЗ} = \text{ЭЦП}(h(S), k\text{з})$$

где $H$ – хеш-функция по алгоритму ГОСТ Р 34.11-2012 (Стрибог),

$S$ – содержимое неизменяемых секций модуля,

$K_з$ – закрытый ключ автора k по схеме ГОСТ Р 34.10-2012. Это гарантирует уникальность ЦВЗ и возможность верификации открытым ключом K по ГОСТ Р 34.10-2012.

Вложение ЦВЗ. В теле библиотечного модуля формируется выборка инструкций-носителей – пар функционально идентичных, но синтаксически различных команд (табл. 1). Из выборки исключаются позиции, подверженные принудительной замене компоновщиком или оптимизатором.

ТАБЛИЦА 1. Группы эквивалентных инструкций для вложения ЦВЗ

| JE / JZ | JNE / JNZ | Высокая | 1 |
|---|---|---|---|
| MOV EAX, 0 | XOR EAX, EAX | Средняя | 1 |
| NOP (×1) | XCHG EAX, EAX | Высокая | 1 |
| ADD EAX, 1 | INC EAX | Средняя | 1 |
| PUSH EBP / MOV EBP,ESP | ENTER 0, 0 | Низкая | 1 |

Биты ЦВЗ кодируются выбором одной из двух инструкций: «0» – первая форма, «1» – вторая. Устойчивость к обфускации обеспечивается следующим образом: вставка мусорных инструкций (junk insertion) не затрагивает носители, так как декодирование ведется по позиционным маркерам; переупорядочение блоков (block reordering) парируется идентификацией неделимых базовых блоков по инвариантным сигнатурам; атака instruction substitution обнаруживается при верификации ЦВЗ и фиксируется в протоколе [3, 9].

## Экспериментальная оценка

Проверка метода проводилась на трех тестовых модулях на языке C++, скомпилированных MSVC 19.x (Visual Studio 2022, архитектура x86-64). Атаки обфускации моделировались с использованием LLVM-obfuscator (пассы: bcf, sub, fla). Результаты приведены в табл. 2 и на рис. 1.

ТАБЛИЦА 2. Результаты экспериментальной оценки предложенного метода

| Объем ЦВЗ (байт) | 48 | 192 | 32 | 91 |
|---|---|---|---|---|
| Емкость канала (бит) | 384 | 1536 | 256 | 725 |
| Сохранность после компоновки (%) | 97,4 | 98,1 | 96,8 | 97,4 |
| Сохранность после оптимизации O2 (%) | 94,2 | 95,6 | 93,7 | 94,5 |
| Обнаруживаемость ЦВЗ при обфускации (%) | 98,3 | 98,7 | 97,9 | 98,3 |
| Накладные расходы по времени (%) | 0,12 | 0,09 | 0,14 | 0,12 |

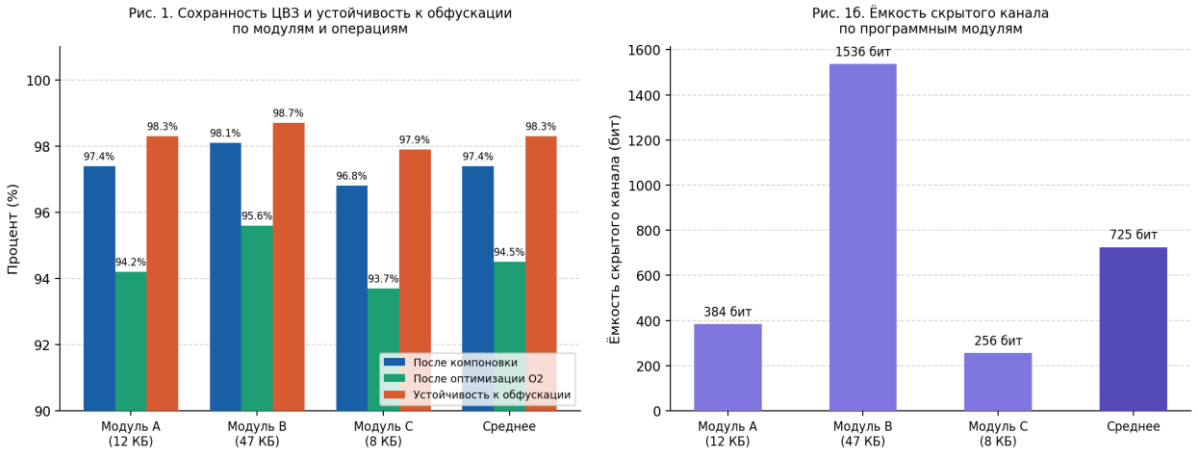



Рис. 1. Сохранность ЦВЗ и емкость скрытого канала по программным модулям

Емкость скрытого канала составляет 256–1536 бит, что достаточно для ЦВЗ длиной 256 бит (выход ГОСТ Р 34.11-2012) даже в наименьшем модуле. Средняя сохранность ЦВЗ после компоновки – 97,4 %, после оптимизации O2 – 94,5 %. Выявленные потери обрабатываются кодом Рида–Соломона. Устойчивость к обфускации – 98,3 %; в 1,7 % случаев пасс fla частично нарушал позиционные маркеры, что фиксировалось как активная атака. Накладные расходы по времени не превысили 0,14 %. Дополнительно была проверена корректность выполнения модулей с внедренным ЦВЗ в различных средах исполнения, что согласуется с методикой [10].

## Заключение

Предложен и экспериментально верифицирован метод скрытого вложения ЦВЗ в библиотечные модули программных продуктов, устойчивый к атакам обфускации. Отличительная особенность – применимость к промежуточным файлам на этапе до завершения разработки и способность документировать факт атаки на ЦВЗ. Дальнейшие исследования будут направлены на разработку модели удостоверяющего центра для централизованной верификации ЦВЗ в корпоративной инфраструктуре разработки ПО.

**Список используемых источников**

1. Гилавоги М. Анализ уязвимостей и механизмов для обеспечения безопасности при вложении ЦВЗ в байт-код Java / М. Гилавоги // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. Выпуск 15. Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2025. С. 104-108. EDN: OLRKUO.

2. Коржик, В. И. Цифровая стеганография: учебник / В. И. Коржик, А. В. Красов. Москва: Общество с ограниченной ответственностью "Издательство "КноРус", 2023. 324 с. ISBN 978-5-406-10970-0. EDN: KNKBXU.

3. Красов, А. В. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код / А. В. Красов, А. С. Верещагин, А. Ю. Цветков // Телекоммуникации. 2013. № S7. С. 27-29. EDN: REKFXZ.

4. Красов, А. В. Разработка методов защиты от копирования ПО на основе цифровых водяных знаков внедряемых в исполняемые и библиотечные файлы / А. В. Красов, С. И. Штеренберг // Актуальные проблемы инфотелекоммуникаций в науке и образовании: II Международная научно-техническая и научно-методическая конференция, Санкт-Петербург, 27–28 февраля 2013 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2013. С. 847-852. EDN: SMCRAZ.

5. Красов, А. В. Метод защиты авторских прав и целостности программного обеспечения на основе внедрения ЦВЗ в исполняемый код / А. В. Красов // Перспективы науки. 2022. № 4(151). С. 16-25. EDN: OHFBUV.

6. Красов, А. В. Исследование применимости известных методов внедрения цифровых водяных знаков к исполняемым файлам Unix-подобных систем / А. В. Красов, В. И. Борисов // Известия высших учебных заведений. Технология легкой промышленности. 2022. Т. 56/ № 2. С. 38-42. DOI: 10.46418/0021-3489_2022_56_02_07. EDN: NSRRTA.

7. Shterenberg, S. I. Analysis of using equivalent instructions at the hidden embedding of information into the executable files / S. I. Shterenberg, A. V. Krasov, I. A. Ushakov // Journal of Theoretical and Applied Information Technology. 2015. Vol. 80. N 1. P. 28-34. EDN: UVYEWX.

8. Алгоритмы и методы защиты программного кода на базе обфускации / А. В. Красов, И. П. Зуев, П. В. Карельский [и др.] // I-methods. 2020. Т. 12, № 1. С. 1-12. EDN: ZGFHEN.

9. Цифровая стеганография и цифровые водяные знаки / В. И. Коржик, С. О. Анфиногенов, А. И. Кочкарев [и др.]. Том 2. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2017. 198 с. ISBN 978-5-89160-153-6. EDN: UNUPQR.

10. Sharikov, P. I. A study of the correctness of the execution of a class file with an embedded digital watermark in different environments / P. I. Sharikov, A. V. Krasov, V. N. Volkogonov // IOP Conference Series: Materials Science and Engineering, Krasnoyarsk, 16–18 апреля 2020 года / Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Vol. 862. Krasnoyarsk: Institute of Physics and IOP Publishing Limited, 2020. P. 52052. DOI: 10.1088/1757-899X/862/5/052052. EDN: HXUBEI.

## METHOD OF COVERT DIGITAL WATERMARK EMBEDDING INTO SOFTWARE LIBRARY MODULES RESISTANT TO OBFUSCATION ATTACKS

**Guilavogi M., Krasov A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article proposes a method for forming and covertly embedding a digital watermark (DWM) into library modules of software products (*.lib, *.obj files) based on a digital signature of the immutable part of the code using cryptographic hash functions in accordance with Russian national standards GOST R 34.11-2012 (Streebog) and GOST R 34.10-2012. The method ensures resistance of the DWM to obfuscation attacks, as well as preservation of the covert embedding during standard linking and optimization processes. An average DWM preservation rate of 97.4 % after linking and 94.5 % after O2-level optimization has been experimentally confirmed, with execution time overhead not exceeding 0.14 %. A distinctive feature of the proposed approach is its applicability to intermediate library files prior to completion of the software build process, as well as its ability to automatically document obfuscation attack attempts on the embedded watermark.*

***Key words:*** *digital watermark, steganography in machine code, obfuscation, library modules, software copyright protection, linking, semantically equivalent instructions, GOST R 34.10-2012, GOST R 34.11-2012*

**УДК 004.056.53**
**ГРНТИ 81.93.21**

# СОВРЕМЕННЫЕ МЕТОДОЛОГИИ И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ: АНАЛИЗ И ТЕНДЕНЦИИ

**Б. Р. Голошумов, Д. А. Иванов, Д. С. Семенов**

Военный университет радиоэлектроники

*В статье выполнен системный анализ современных методологий и инструментов тестирования на проникновение как критически значимого компонента проактивной кибербезопасности. Рассмотрены архитектуры PTES, OSSTMM, OWASP и NIST SP 800-115, выделены их ключевые отличия и прикладные области. Детализированы этапы проведения тестирования – от предпроектного взаимодействия до формирования отчетной документации – с акцентом на практики разведки, идентификации и эксплуатации уязвимостей, а также постэксплуатации. Проведен обзор современного инструментария, включая C2-платформы, сканеры уязвимостей, средства анализа сред Active Directory и облачные фреймворки. Выявлены основные векторы развития отрасли: непрерывное автоматизированное тестирование, концепция Purple Teaming, интеграция с матрицей MITRE ATT&CK и применение методов машинного обучения. Сформулированы организационно-правовые условия легитимного проведения тестирования на проникновение на территории Российской Федерации.*

***тестирование на проникновение, пентест, методологии аудита информационной безопасности, этичный хакинг, непрерывная безопасность, MITRE ATT&CK, Purple Teaming***

## Введение

Увеличение сложности и частоты целенаправленных кибератак, диктуемое деятельностью высококвалифицированных APT-группировок, ставит перед организациями задачу перехода от реактивных моделей защиты к проактивным. Тестирование на проникновение (пентест) – это контролируемая процедура моделирования действий нарушителя, нацеленная на выявление и демонстрацию возможности эксплуатации уязвимостей в компонентах информационной системы [1]. В отличие от инвентаризационного аудита конфигураций, тестирование верифицирует реальную достижимость компрометации критичных активов и позволяет ранжировать риски на основе факта их эксплуатируемости.

Актуальность работы обусловлена необходимостью обобщения и систематизации методологической базы и инструментария аудита информа-

ционной безопасности (ИБ) в условиях стремительной эволюции ландшафта угроз, массовой миграции корпоративных инфраструктур в облачные среды и ужесточения регуляторных требований.

## Сравнительный анализ методологий

Профессиональное сообщество ИБ выработало ряд открытых стандартов, регламентирующих процесс тестирования на проникновение. Их сопоставление по ключевым критериям приведено в таблице 1.

ТАБЛИЦА 1. Сравнительная характеристика открытых методологий тестирования на проникновение

| Методология | Основной фокус | Уникальная особенность |
|---|---|---|
| PTES | Универсальная | Семь фаз с детальными чек-листами, обязательное согласование правил взаимодействия |
| OSSTMM | Сетевая, физическая, человеческая безопасность | Количественная метрика RAV, независимость от ИТ-архитектуры |
| OWASP Testing Guide | Веб-приложения, API | Покрытие OWASP Top-10, специализированные тест-кейсы на каждый класс уязвимостей |
| NIST SP 800-115 | Информационные системы | Разделение методов на пассивные и активные, применимость в государственном секторе |

PTES (Penetration Testing Execution Standard) регламентирует полный жизненный цикл работ – от предварительного взаимодействия до отчетности, уделяя значительное внимание юридическим и организационным аспектам [1]. OSSTMM (Open Source Security Testing Methodology Manual) вводит метрику RAV (Risk Assessment Value), позволяющую количественно оценивать операционную защищенность вне зависимости от применяемых вендорских решений [2]. OWASP Testing Guide выступает фактическим отраслевым стандартом для веб-приложений и содержит шаблоны проверок всех категорий уязвимостей, включенных в топ-лист OWASP [3]. NIST SP 800-115 представляет собой техническое руководство по оценке защищен-

ности, разделяющее техники на пассивное обследование и активное тестирование с эксплуатацией [4].

**Этапы тестирования на проникновение**

Независимо от избранной методологии, практическая реализация тестирования структурируется в шесть последовательных фаз:

1. Предпроектное взаимодействие. Осуществляется согласование целей, границ, допустимых методов воздействия и временных интервалов. Подписываются соглашения о неразглашении конфиденциальной информации (NDA) и правила проведения работ (Rules of Engagement). Определяется модель тестирования: «черный», «серый» или «белый» ящик.

2. Разведка (Reconnaissance). Подразделяется на пассивную (OSINT без прямого взаимодействия с целевыми системами) и активную. Используются поисковые системы, сервисы Shodan, Censys, базы WHOIS, DNS-зоны, архивы SSL/TLS-сертификатов. Инструменты Maltego, Amass и theHarvester позволяют строить графы связей между доменами, IP-адресами и персоналом.

3. Сканирование и идентификация уязвимостей. Сетевые сканеры (Nmap, Masscan, RustScan) выявляют открытые порты и работающие сервисы. Сканеры уязвимостей (Nessus, OpenVAS, Qualys) выполняют сигнатурный анализ для обнаружения известных недостатков (CVE). Результаты коррелируются с базой MITRE ATT&CK для привязки к техникам потенциальных атакующих.

4. Эксплуатация уязвимостей. Осуществляется ручная и автоматизированная проверка возможности компрометации систем. Для типовых уязвимостей применяются Metasploit Framework, Empire, Covenant. Веб-векторы исследуются с помощью Burp Suite Professional и sqlmap. На данном этапе критически важна минимизация деструктивного воздействия на продуктивные системы.

5. Постэксплуатация. После получения первоначального доступа выполняются закрепление (persistence), повышение привилегий и латеральное перемещение. Для анализа путей эскалации привилегий в средах Active Directory применяется платформа BloodHound с коллектором SharpHound. Дамп учетных данных из оперативной памяти выполняется утилитой Mimikatz. C2-платформы (Command and Control), такие как Cobalt Strike, эмулируют поведение реальных APT-группировок [5, 6].

6. Отчетность. Формируется итоговый документ, содержащий перечень выявленных уязвимостей с оценкой критичности по шкале CVSS, до-

казательства успешной эксплуатации и конкретные рекомендации по устранению. Отчет должен быть релевантен как для технического персонала, так и для лиц, принимающих управленческие решения.

## Инструментальные средства

Современный инструментарий специалиста классифицируется по этапам применения. В таблице 2 представлены наиболее востребованные средства, соответствующие актуальным классам уязвимостей и техникам атак.

ТАБЛИЦА 2. Классификация инструментов по этапам тестирования

| Этап | Инструменты | Назначение |
|---|---|---|
| Сбор информации | Amass, Maltego, theHarvester, SpiderFoot, Shodan | OSINT, DNS-разведка, поиск субдоменов |
| Сканирование | Nmap, Masscan, RustScan, Nessus, OpenVAS | Обнаружение хостов, портов, сервисов, идентификация CVE |
| Эксплуатация | Metasploit, Cobalt Strike, Empire, Covenant, sqlmap, Burp Suite Pro | Эксплуатация сетевых и веб-уязвимостей, управление C2-сессиями |
| Постэксплуатация | Mimikatz, BloodHound, PowerSploit, Seatbelt | Дамп паролей, анализ Active Directory, сбор системной информации |
| Облачный аудит | ScoutSuite, Prowler, Cloudsplaining | Анализ конфигураций AWS, Azure, GCP, оценка IAM-политик |

Возрастающая доля облачных инфраструктур требует применения специализированных фреймворков, учитывающих особенности систем управления доступом (IAM), бессерверных вычислений и технологий контейнеризации [7].

## Тенденции и векторы развития

– Непрерывное автоматизированное тестирование (Continuous Penetration Testing). Статичный подход с периодичностью аудита один раз в год не обеспечивает адекватного уровня защиты в условиях высокодинамичной ИТ-инфраструктуры и практик CI/CD. Платформы класса Breach and Attack Simulation (BAS) – Pentera, Cymulate – безопасно воспроизводят сценарии атак в продуктивной среде и предоставляют срез рисков в реальном времени.

– Purple Teaming. Замещает классическую модель противостояния (Red Team против Blue Team) совместной работой: атакующая команда демонстрирует техники, а защищающаяся команда одновременно настраивает правила детектирования и реагирования (SIEM/EDR). Данный подход радикально сокращает время внедрения защитных мер [8].
– Интеграция с MITRE ATT&CK. Современное тестирование тактически выстраивается вокруг матрицы тактик и техник MITRE ATT&CK. Это обеспечивает прямое сопоставление результатов с известными профилями угроз и облегчает приоритизацию процессов защиты.
– Применение искусственного интеллекта. Технологии машинного обучения начинают использоваться для приоритизации результатов сканирования, автоматической генерации эксплойтов и анализа логов, однако на текущем этапе они играют вспомогательную роль, не заменяя экспертного анализа [9].

## Организационно-правовые аспекты

Проведение тестирования сопряжено с потенциальными рисками для доступности и целостности систем, поэтому обязательным условием является детальное документирование границ работ, допустимых методов воздействия и временных окон («окон обслуживания»). В российской юрисдикции данная деятельность регулируется Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также нормативными правовыми актами ФСТЭК России и ФСБ России в области защиты ГИС и критической информационной инфраструктуры (КИИ). Квалификация исполнителей должна подтверждаться профильными международными или национальными сертификациями (OSCP, GPEN, CREST) и релевантным опытом [10].

## Заключение

Тестирование на проникновение эволюционировало из разовой проверки в комплексную систему непрерывной верификации защищенности корпоративных сетей. Интеграция с фреймворком MITRE ATT&CK, внедрение парадигмы Purple Teaming и автоматизированных BAS-платформ, адаптация методологий к облачным архитектурам и использование методов ИИ формируют новый облик аудита ИБ как неотъемлемого элемента управления ИТ-рисками. Для российских организаций критически важно выстраивать процесс тестирования в строгом соответствии с действующими регу-

ляторными требованиями законодательства и на базе признанных методологических стандартов.

**Список используемых источников**

1. Penetration Testing Execution Standard (PTES). URL: http://www.pentest-standard.org/ (дата обращения: 25.04.2026).
2. OSSTMM 3 Open Source Security Testing Methodology Manual. URL: https://www.isecom.org/research/osstmm.html (дата обращения: 25.04.2026).
3. OWASP Testing Guide v4.2. URL: https://owasp.org/www-project-web-security-testing-guide/ (дата обращения: 25.04.2026).
4. NIST Special Publication 800-115. Technical Guide to Information Security Testing and Assessment. 2008. URL: https://csrc.nist.gov/publications/detail/sp/800-115/final (дата обращения: 25.04.2026).
5. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit: The Penetration Tester's Guide. No Starch Press, 2011. 328 p.
6. BloodHound: Six Degrees of Domain Admin. SpecterOps, 2023. URL: https://bloodhound.readthedocs.io/ (дата обращения: 25.04.2026).
7. AWS Security Best Practices. Amazon Web Services, 2023. URL: https://aws.amazon.com/ru/architecture/security-identity-compliance/ (дата обращения: 25.04.2026).
8. Purple Teaming: A Definitive Guide. SANS Institute, 2022. URL: https://www.sans.org/blog/purple-teaming/ (дата обращения: 25.04.2026).
9. Gartner. Emerging Tech: AI in Security Testing. 2025. URL: https://www.gartner.com/en/documents/ (дата обращения: 25.04.2026).
10. Offensive Security. Penetration Testing with Kali Linux (PWK) Course. 2026. URL: https://www.offsec.com/courses/pen-200/ (дата обращения: 25.04.2026).

## MODERN PENETRATION TESTING METHODOLOGIES AND TOOLS: ANALYSIS AND TRENDS

**Goloshumov B., Ivanov D., Semenov D.**
Military University of Radioelectronics

*The paper provides a systematic analysis of modern penetration testing methodologies and tools as a critically important component of proactive cybersecurity. The PTES, OSSTMM, OWASP, and NIST SP 800-115 frameworks are reviewed, and their key differences and application areas are highlighted. The stages of penetration testing are detailed – from pre-engagement interaction to reporting – with an emphasis on reconnaissance, vulnerability identification and exploitation, and post-exploitation. A review of current tools is conducted, including C2 platforms, vulnerability scanners, Active Directory analysis tools, and cloud frameworks. Development vectors are identified: continuous automated testing, Purple Teaming, integration with MITRE ATT&CK, and the application of machine learning methods. Organizational and legal conditions for legitimate penetration testing on the territory of the Russian Federation are formulated.*

***Ke ywords:*** *penetration testing, ethical hacking, pentest methodologies, pentest tools, continuous security, MITRE ATT&CK, Purple Teaming*

**УДК 004.492.3**
**ГРНТИ 81.93.29**

# МОДЕЛИ ПРИМЕНЕНИЯ LLM В ЗАДАЧАХ SOC

**А. П. Гудаков[1, 2], А. А. Миняев[2]**

[1]Digital Design
[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

*Большие языковые модели стали проникать во многие сферы человеческой жизни. Области кибербезопасности и информационных технологий не являются исключениями. LLM находят разные применения, направленные как на автоматизацию или упрощение построенных ранее процессов, так и на создание новых. Организация функционирования SOC – один из наиболее трудоемких процессов, занимающих у компаний месяцы и даже годы. С целью повышения эффективности оперативных центров информационной безопасности специалисты начали все чаще задумываться о возможностях применения больших языков моделей. На этом пути можно столкнуться с вопросом – как именно на текущем этапе можно применять LLM в задачах SOC. В статье рассматриваются модели применения больших языковых моделей в задачах автоматизации и упрощения процессов обнаружения и реагирования на инциденты информационной безопасности.*

***большие языковые модели, информационная безопасность, SOC, LLM, автоматизация, операционный центр информационной безопасности***

Одними из основных задач операционных центров информационной безопасности (Security Operation Center, SOC) являются обнаружение инцидентов информационной безопасности и реагирование на них. В одном из исследований Positive Technologies было заявлено, что в среднем команды аналитиков ежедневно получают 4484 сигнала тревоги [1]. При этом они занимаются и другими задачами – разработкой регламентов, доработкой существующей инфраструктуры, составлением планов реагирования на инциденты, созданием правил обнаружения и т.п. Такое количество нагрузки может негативно сказываться как на самом состоянии сотрудников, так и напрямую отражаться на результатах их деятельности. Одной из подобных угроз является alert fatigue – явление, при котором аналитики SOC начинают хуже выявлять инциденты в потоке событий информационной безопасности из-за слишком большого количества ложных или неинформативных оповещений, что приводит к тому, что атака злоумышленника остается необнаруженной [2]. Для снижения нагрузки как правило применяют автоматизацию рутинных действий, доработку средств защиты информации, а также равномерное распределение обязанностей.

Большие языковые модели (Large Language Model, LLM) дали большой толчок развитию информационных технологий и кибербезопасности. LLM – нейронные сети, обученные на большом количестве текстовых данных, для предсказания последующих токенов (минимальных текстовых единиц, которыми оперирует LLM) в последовательности [3]. Специалисты в области информационной безопасности находят им множество применений: статический анализ кода, проведение сканирований и анализа уязвимостей, оказание помощи в тестированиях на проникновение, помощь в разработке кода и многое другое. Специалисты SOC также смогут найти применение LLM в рамках исполнения своих рутинных работ. К основным задачам можно отнести [4]:

– обнаружение инцидентов информационной безопасности;
– реагирование на инциденты информационной безопасности и ведение отчетности;
– составление политик и регламентов в области информационной безопасности;
– разработка планов реагирования на инциденты;
– усовершенствование работы средств защиты информации.

LLM способна оказать помощь в каждой из приведенных выше задач. При интеграции больших языковых моделей в процессы компании, включая SOC, необходимо также продумывать и безопасность функционирования будущей модели взаимодействия. Поэтому к разрабатываемым моделям прилагаются следующие требования:

– общая защищенность LLM – предполагается, что в рассматриваемых моделях предприняты все необходимые меры, направленные на обеспечение безопасности LLM на всех этапах ее функционирования (проектирование архитектуры, подготовка данных, обучение, развертывание и функциональные операции моделей) [5];
– безопасность передачи информации в сети – предполагается, что в рассматриваемых моделях информация защищена от атак типа человек посередине. Применяются все необходимые меры для обеспечения безопасности сред передачи информации;
– аппаратное обеспечение – все компоненты модели обладают необходимыми техническими характеристиками, позволяющими обрабатывать информацию без отказов в обслуживании и потерей данных;
– соответствие LLM – большая языковая модель должна быть предназначена и обучена для задач, решаемый в рамках функционирования модели взаимодействия;
– роль человека в принятии решений – при автоматизации процессов, в рамках которых принимаются какие-то активные действия, а не форми-

руется какая-то независимая информация, последнее решение всегда принимается человеком. Это же касается и утверждения сформированной независимой информации;

– расположение сервера LLM – предполагается, что LLM-сервер находится внутри защищенного контура предприятия. Данные из него не попадают во внешнюю сеть, и он имеет возможность обрабатывать конфиденциальную информацию.

Теперь разработаем модели взаимодействия, которые упрощают или полностью автоматизируют некоторые процессы:

– LLM как ассистент – в данной модели большая языковая модель не обладает какой-либо самостоятельностью. Любая ее деятельность осуществляется с инициативы оператора. Интеграция позволяет аналитику в упрощенном формате получать от LLM-сервера дополнительную информацию или разъяснения, касающиеся заинтересовавшего его события информационной безопасности. Данная модель взаимодействия представлена на рисунке 1. Аналитик сначала самостоятельно обнаруживает подозрительное событие информационной безопасности (1-2), затем запрашивает через веб-страницу управления SIEM анализ обнаруженного события (3). Запросы могут быть как заранее подготовленными, так и полностью сформированными пользователем. В результате аналитик получает разъяснения и дополнительные сведения о событии информационной безопасности (4-6).

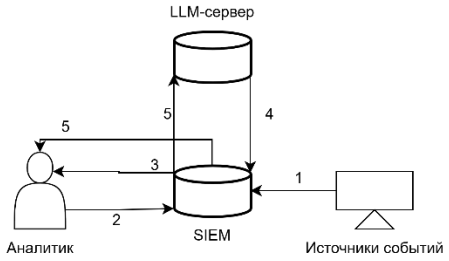



Рис. 1. LLM как ассистент аналитика

– LLM для составления документации и планов реагирования – в данном сценарии большая языковая модель будет использоваться для создания и усовершенствования внутренних регламентов защищаемого предприятия: регламента реагирования на инциденты информационной безопасности, политики информационной безопасности и прочего. Также она может использоваться для разработки сценариев реагирования на инциденты информационной безопасности (playbook). Процесс инициируется запросом оператора на доработку или создание документа (1). Необходимая информация может черпаться LLM-сервером как из внутренних баз

знаний и документации, а также дополнительно обогащаться на основании анализа предыдущих инцидентов информационной безопасности, содержащихся в платформе реагирования на инциденты (Incident Response Platform, IRP) (2). Аналитик же выступает в роли верификатор, который проверяет составленные документы и “плейбуки” (3) и в случае необходимости отправляет запросы на доработку (4). Также эта модель может применяться и для создания правил корреляции и нормализации. В таком случае также получается информация о поступающих событиях и уже существующих правилах из SIEM. Итоговая модель представлена на рисунке 2.

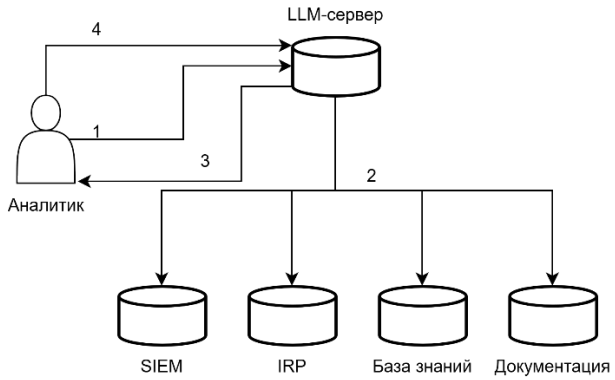



Рис. 2. LLM для документации

– LLM для реагирования на инциденты информационной безопасности – данная модель предназначена для выявления инцидентов информационной безопасности и принятия автоматизированных действий, направленных на сдерживание и ликвидацию угрозы. Она представлена на рисунке 3. При поступлении событий в SIEM, они по заданным правилам перенаправляются в SOAR (Security Orchestration, Automation and Response) и в случае соответствия заданным критериям по сформированным шаблонам направляются запросы на LLM-сервер для выяснений критичности потенциального инцидента и предложения мер по реагированию (1-3). LLM-сервер на основании поступающих входных данных определяет степень угрозы информационной безопасности и формирует по заданным шаблонам инструкции для реагирования на инцидент или формирует рекомендации, которые необходимо будет исполнить аналитику самостоятельно (4). В случае, если проанализированные события требуют мер по сдерживанию или ликвидации, аналитику направляется запрос со сведениями об инциденте и с запросом на подтверждение автоматизированных действий, направленных на нейтрализацию угрозы (4-5). В случае, если оператором принято решение о реализации предлагаемых мер, в SOAR отправляется соответствующая команда, запускающая процессы

реагирования на инцидент ИБ. Это может осуществляться как с помощью EDR-решений (Endpoint Detection and Response), так и с помощью различных агентов и средств удаленного администрирования (6-8).

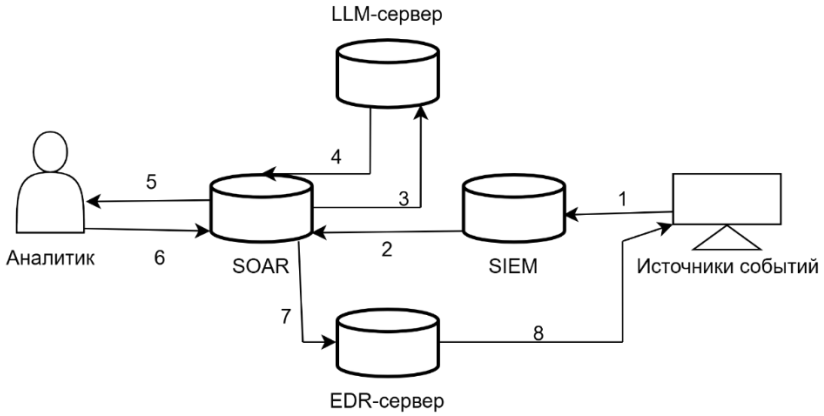



Рис. 3. LLM для реагирования на инциденты ИБ

Итоговое сравнение недостатков и преимуществе представленных представлено в таблице 1.

ТАБЛИЦА 1. Сравнение моделей применения LLM

| Модель | Преимущество | Недостаток |
|---|---|---|
| LLM как ассистент | Упрощение анализа событий | Требует ручных действий аналитика |
| | Низкая нагрузка LLM- и SIEM-серверов | Не улучшает работу средств защиты информации |
| | Не несет рисков для функционирования инфраструктуры | |
| LLM для составления документации и “плейбуков” | Не несет рисков для функционирования инфраструктуры | Требует длительного обучения на внутренних данных компании |
| | Низкая нагрузка LLM- и SIEM-серверов | Не реализует активные меры по обеспечению информационной безопасности |
| | Позволяет специалистам сосредоточиться на мониторинге | |
| LLM для реагирования на инциденты ИБ | Требует минимального вмешательства аналитиков в процесс реагирования | Может нарушить работоспособность инфраструктуры и ее компонентов |
| | Сокращение времени, необходимого для реагирования на инцидент ИБ | Большая нагрузка на SOAR- и LLM-серверы |

Исходя из вышеперечисленных сведений, все модели применения LLM имеют свои преимущества и недостатки. Их внедрение требует четкого понимания этапа развития процессов информационной безопасности в своей компании, компетенций кадров, технических возможностей и потребностей. Рассмотренные модели применения LLM в SOC помогут снизить нагрузку на аналитиков и ускорить реагирование на инциденты информационной безопасности. Они могут применяться совместно, дополняя друг друга или вовсе работать независимо.

**Список используемых источников**

1. Автономные SOC: будущее мониторинга ИБ и реагирования на инциденты // URL: https://ptsecurity.com/research/analytics/autonomous-socs-future-of-cybersecurity-monitoring-and-incident-response/#id1 (дата обращения: 26.04.2026).

2. Ban T. et al. Combat security alert fatigue with ai-assisted techniques //Proceedings of the 14th Cyber Security Experimentation and Test Workshop. 2021. С. 9-16 (дата обращения: 28.04.2026).

3. LLM Fundamentals // URL: https://learn.microsoft.com/en-us/agent-framework/journey/llm-fundamentals (дата обращения: 28.04.2026).

4. Частикова В. А., Хализев В. Н. Обзор современных подходов к автоматизации процессов SOC и роль больших языковых моделей в их формировании // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2025. С. 26-41 (дата обращения 27.04.2026).

5. De Maio C. et al. A Lifecycle-Oriented Survey of Emerging Threats and Vulnerabilities in Large Language Models // IEEE Access. 2025. (дата обращения: 26.04.2026).

## LLM APPLICATION MODELS IN SOC TASKS

**Gudakov A.[1, 2], Minyaev A.[2]**
[1]Digital Design
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Large language models have begun to permeate many areas of human life. Cybersecurity and information technology are no exception. Large language models (LMMs) are finding various applications, both for automating and simplifying existing processes and for creating new ones. Organizing a SOC is one of the most labor-intensive processes, taking companies months and even years. To improve the efficiency of security operation centers, specialists are increasingly considering the potential of using large language models. Along the way, one may encounter the question of how exactly LMMs can be applied to SOC tasks at this stage. The article examines models for the application of large language models in tasks of automating and simplifying the processes of detecting and responding to information security incidents.*

***Key words:*** *large language models, information security, SOC, LLM, automation, security operation center*

**УДК 004.056**
**ГРНТИ 49.33.35**

# НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В УСЛОВИЯХ ВИРТУАЛИЗАЦИИ

**Н. А. Демидов, О. С. Мелешкин**

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

*В статье рассмотрены основные проблемы обеспечения безопасности эксплуатации виртуализированных инфраструктур. Дан анализ новых групп уязвимостей в контексте современных тенденций формирования гибридных сред. Описана экспериментальная составляющая исследования. Приведены результаты эксперимента, в ходе которого была произведена проверка эффективности защиты каналов управления и плоскости данных.*

***микросегментация, виртуальные сети, уязвимости, гипервизор, VM Escape, SDN-контроллер, VXLAN***

Актуальность исследования обусловлена появлением новой группы уязвимостей, связанной с современными тенденциями преобразования корпоративных инфраструктур в сетевые сервисы виртуализации. Виртуальные сети, которые базируются на использовании гипервизоров и технологий туннелирования, наследуют традиционные проблемы обеспечения безопасности, но и имеют особые проблемы, порожденные распределением ресурсов физического хоста между различными виртуальными объектами.

Виртуальная сеть объединяет машины через виртуальный коммутатор, в котором трафик нескольких пользователей проходит через один физический интерфейс. Фильтрация реализуется программно внутри гипервизора. Исследователи подчеркивают, что в IoT стоят более сложные проблемы обеспечения безопасности по сравнению с теми, с которыми сталкивались ранее. Среди основных причин называют две – гетерогенный характер структуры (многообразие вещей, разные технологии сетей в соединении) и большое число объектов [1].

Целью данного исследования является изучение основных направлений обеспечения безопасности виртуальных сетей. В соответствии с ней определены следующие задачи: провести анализ архитектурных уязвимо-

стей гипервизоров и протоколов туннелирования и экспериментально проверить эффективность микросегментации и защиты SDN-контроллера.

Изучая спектр архитектурных уязвимостей гипервизоров, отмеченных в научных публикациях, выделим следующее аргументированное положение авторов. Классические меры защиты, такие как пограничные файрволы, признаны неэффективными против угроз виртуальной среде [2].

Объединяя виртуальные машины через виртуальный коммутатор в виртуальной сети, создается потенциальная угроза перехвата трафика одной виртуальной машины другой, размещенной на том же хосте. Теоретически возможность перехвата трафика между виртуальными машинами (ВМ) на одном хосте объясняется отсутствием обязательного выхода трафика за пределы гипервизора – классические сетевые экраны, установленные на границе физической сети, не видят такие потоки. Это порождает «слепую зону» мониторинга, что формально описывается как невозможность гарантированного обнаружения атак типа «сосед по хосту» без применения средств внутри гипервизора. Согласно модели угроз виртуальных сетей, предложенной авторами [2], гипервизор и каналы связи между виртуальными машинами на одном физическом хосте относятся к критическим элементам, уязвимым для внутреннего нарушителя.

Вторая группа уязвимостей возникает из-за ошибок в протоколах туннелирования: поле идентификатора VXLAN не шифруется, а аутентификация отсутствует, что позволяет подменять идентификаторы и внедрять трафик в чужой сегмент.

Угрозы плоскости управления связаны с контроллером SDN, который является «единой точкой компрометации». Атаки на контроллер через неавторизованные API-вызовы или инъекцию ложных правил позволяют переконфигурировать всю сеть, изменить таблицы потоков и отключить сегментацию. Угрозы плоскости данных включают прослушивание трафика между виртуальной машиной на одном гипервизоре, при доступе к гипервизору или уязвимости vSwitch, и атаки на туннелирование – подмену VXLAN-заголовков, атаки повторением, которые позволяют выйти за пределы своего сегмента. К таким угрозам относятся DoS-атака на протокол связующего дерева STP, угроза вставки фиктивной метки в структуру кадра стандарта 802.1q, угроза подмены DHCP-сервера, угроза переполнения таблицы памяти адресов CAM и др. [3].

Для защиты от несанкционированного доступа и утечек данных разрабатываются методы защиты, однако, совмещение плоскостей данных

и управления в программно-определяемой инфраструктуре приводит к появлению дополнительных поверхностей атаки. И одним из методов, эффективных в виртуализированной среде, является микросегментация на уровне гипервизора. Контроль и передача данных не разделены физически, эти функции реализуются программно. Следовательно, аргументировать применение микросегментации позволяет теоретическое положение о снижении вероятности бокового перемещения злоумышленника за счет минимизации разрешенных сетевых взаимодействий.

Одним из эффективных методов также является развертывание виртуализированных систем обнаружения вторжений «vNIDS».

Вместе с тем, необходимо подчеркнуть, что повышение безопасности виртуальных сетей достигается только посредством комплексного подход**а**, включающего микросегментацию, защиту плоскости управления, распределенный мониторинг и шифрование трафика.

На следующем этапе исследования была решена задача – экспериментально проверить эффективность микросегментации и защиты SDN-контроллера. Экспериментальное исследование было проведено на виртуальном стенде. Он состоит из трех физических хостов (HP ProLiant DL380 Gen9), которые объединены гигабитными сетевыми интерфейсами. KVM, используется в качестве гипервизора. На Open vSwitch функцию SDN-контроллера на отдельном сервере выполняет OpenDaylight. Первый хост содержит две виртуальные машины, целевую виртуальную машину А и атакующую виртуальную машину Б. На втором хосте развернуты ВМ с веб-приложением, а третий хост – это vNIDS на базе Suricata.

В первом эксперименте виртуальная машина Б переводила интерфейс в promiscuous mode или в неразборчивый режим и запускала анализатор пакетов. Моделировалась атака без использования микросегментации, то есть, фактически, без особых средств защиты. Виртуальная машина А генерировала трафик HTTP/MySQL. Перехват трафика злоумышленником оказался успешным во всех случаях, так как vSwitch не применял политик изоляции.

Во втором эксперименте на уровне гипервизора внутри Open vSwitch были настроены правила микросегментации: запрещен прямой трафик между виртуальными машинами А и Б. Разрешен только трафик к шлюзу. При повторении данной атаки, vSwitch отбрасывал кадры на этапе классификации портов. Перехватчик пакетов виртуальной машины Б не получил ни одного пакета, а значит эффективность блокировки была максимальной.

При проведении третьего эксперимента контроллер OpenDaylight был сконфигурирован без TLS и с простым паролем REST API. Злоумышленник за непродолжительное время подобрал пароль и через REST API внедрил правило дублирования трафика с одной виртуальной машины на другую. Микросегментация была активна, но, несмотря на это, злоумышленник смог получить копии трафика, что подтвердило критическую уязвимость плоскости управления.

Полученные результаты подтверждают, что микросегментация полностью нейтрализует атаку данного вида, несанкционированные соединения блокируются на уровне виртуального коммутатора. Данное утверждение полностью соответствует современным представлениям о технологии, которая «дает возможность ИТ-отделам развертывать гибкие политики безопасности в ЦОД и облачных системах, применяя виртуализацию сети» [4]. Также подтверждена критическая значимость защиты плоскости управления SDN. В работе авторов подтверждается теоретическое положение о том, что «контроллер является самым уязвимым элементом SDN, атака на который может повлиять на устойчивость ее функционирования» [5]. В этом контексте использование защищенных каналов связи (TLS) и строгой аутентификации (API) снижает вероятность успешной атаки за счет увеличения сложности несанкционированного доступа.

Дальнейших исследований требует обеспечение эффективной защиты каналов управления, так как определенным риском перехвата данных может сопровождаться передача состояния виртуальных машин между хостами. Обеспечение целостной защиты усложняет появление дополнительных векторов атак в условиях формирования гибридных сред, их изучение позволит разрабатывать стратегии борьбы с новыми классами уязвимостей.

**Список используемых источников**

1. Соколов М. Н., Смолянинова К. А., Якушева Н. А. Проблемы безопасности интернет вещей: обзор // Вопросы кибербезопасности. 2015. № 5(13). С. 32–37. URL: https://cyberleninka.ru/article/n/problemy-bezopasnosti-internet-veschey-obzor/viewer (дата обращения 10.04.2026).

2. Курносов К. В. Методика оценки безопасности информационных систем, построенных с использованием технологий виртуализации //Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22. № . 1. С. 37-44. URL: https://cyberleninka.ru/article/n/metodika-otsenki-bezopasnosti-informatsionnyh-sistem-postroennyh-s-ispolzovaniem-tehnologiy-virtualizatsii (дата обращения 23.04.2026)

3. Бельфер Р. А., Петрухин И. С., Тешкин А. П. Анализ угроз информационной безопасности виртуальных частных сетей VPLS на базе сети MPLS // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2015. № 1. С. 48–57. URL:

https://cyberleninka.ru/article/n/analiz-ugroz-informatsionnoy-bezopasnosti-virtualnyh-chastnyh-setey-vpls-na-baze-seti-mpls/viewer (дата обращения 10.04.2026).

4. Нурзода Мухаммадназир Низоми. Рекомендации по безопасности микросегментации // Молодой исследователь Дона. 2021. № 3(30). URL: https://mid-journal.ru/upload/mid/iblock/e62/17_1342-Nurzoda_71_72.pdf (дата обращения 23.04.2026).

5. Котенко И. В., Саенко И. Б., Лаута О. С., Скоробогатов С. Ю., Кочин В. П.. Методика оценки устойчивости программно-конфигурируемых сетей в условиях компьютерных атак // Журнал Белорусского государственного университета. Математика. Информатика. 2024. Т. 3. С. 90–102. URL: https://www.mathnet.ru/links/4fb30fa2ed58ad82a69e624915643e26/bgumi698.pdf (дата обращения 23.04.2026).

## SOME ASPECTS OF VIRTUAL NETWORK SECURITY

**Demidov N., Meleshkin O.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article examines the key challenges of ensuring the security of virtualized infrastructures. It analyzes new vulnerability groups in the context of current trends in the development of hybrid environments. The experimental component of the study is described, and the results of an experiment that tested the effectiveness of control channel and data plane protection are presented.*

***Key words:*** *microsegmentation, virtual networks, hypervisor, VM Escape, SDN controller, VXLAN*

**УДК 004.056**
**ГРНТИ 81.93.29**

# СОЗДАНИЕ НАБОРА ДАННЫХ ДЛЯ КЛАССИФИКАЦИИ ВЕБ-ПРИЛОЖЕНИЙ ДЛЯ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ

**Р. С. Денисов[1], А. А. Космачев[1,2], И. В. Котенко[2], А. А. Магомедов[1]**

[1] Национальный исследовательский университет «Высшая школа экономики»
[2] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук

*Статья посвящена задаче многоклассовой классификации веб-приложений по тематическому направлению (домену) на основе анализа HTTP-трафика. Корректное определение домена приложения позволяет сузить пространство поиска при тестировании безопасности и целенаправленно проверять уязвимости бизнес-логики, характерные для конкретной категории. Предложена методология ручного формирования датасета с применением инструмента перехвата трафика Burp Suite; собрано порядка 7 000 HTTP-транзакций, аннотированных по четырем категориям: e-commerce, finance, gaming, social network/messenger. На полученных данных проведено сравнительное исследование трех моделей – Multinomial Naive Bayes, Logistic Regression и LinearSVC. Наилучший результат в метриках качества (macro F1 = 0.768, accuracy = 0.815) продемонстрировала Logistic Regression, обеспечив устойчивую классификацию по всем четырем категориям.*

***классификация веб-приложений, HTTP-трафик, уязвимости бизнес-логики, машинное обучение, Burp Suite, датасет, Logistic Regression, Naive Bayes, LinearSVC, тестирование безопасности***

Обнаружение атак на веб-приложения как направление информационной безопасности является в настоящее время одним из наиболее актуальных и значимых [1, 2]. Решаемая при этом задача обнаружения атак на веб-приложения по HTTP-трафику активно исследуется начиная с 2000-х годов [3, 4]. Ключевым публичным ресурсом остается датасет CSIC 2010 [5], содержащий 36 000 нормальных и 25 000 аномальных HTTP-запросов к одному e-commerce приложению. Он охватывает SQL-инъекции, XSS, CRLF-инъекции и ряд других классов атак. Датасет ECML/PKDD 2007 Web Analyzing Traffic Challenge предлагает разметку по девяти типам атак (XSS, Sql Injection, Ldap Injection, Path Traversal, Os Command Injection и др.) и содержит 24 504 нормальных и 10 502 аномальных запроса [6]. Обе коллекции охватывают единственную категорию приложений (e-commerce) и не содержат разметки по тематическому домену, что делает их непригодными для задачи доменной классификации в том виде, в котором она сформулирована в настоящей работе.

Среди открытых инструментов показателен FWAF (fWaf Machine Learning-driven Web Application Firewall) [7], использующий TF-IDF на корпусах нормальных и вредоносных запросов (1 294 531 и 48 126 образцов соответственно) для бинарной детекции атак. Работы по применению машинного обучения в кибербезопасности демонстрируют высокую эффективность градиентного бустинга (XGBoost) и глубоких архитектур (CNN, LSTM, GRU) для классификации HTTP-трафика [8]. Вместе с тем задача многоклассовой тематической классификации веб-приложений по признакам трафика, в отличие от бинарного детектирования атак, в литературе практически не рассматривалась, что обусловливает актуальность настоящего исследования.

Определение тематического домена веб-приложения по HTTP-трафику решается как задача многоклассовой классификации. Целевые категории e-commerce, finance, gaming, social network/messenger выбраны как наиболее характерные с точки зрения специфических уязвимостей бизнес-логики: например, манипуляции с ценой и скидками (e-commerce), несанкционированный доступ к финансовым операциям (finance), эксплуатация игровой механики (gaming).

В настоящем исследовании данные собирались вручную с помощью Burp Suite Proxy: реальные сессии взаимодействия с веб-приложениями каждой категории перехватывались и экспортировались в XML-формат. Для каждой транзакции сохранялись метод, путь, GET-параметры, тело POST-запроса, заголовки запроса и ответа, код статуса и тело ответа. Из данных исключались поля, содержащие токены аутентификации (Authorization, Cookie, Set-Cookie, access_token, password). После преобразования из формата XML в CSV датасет содержит порядка 7 000 транзакций. Для последующего обучения разбиение составляет 75 % для обучающей выборки и 25 % для тестовой. Алгоритм сборки набора данных представлена на рис. 1.

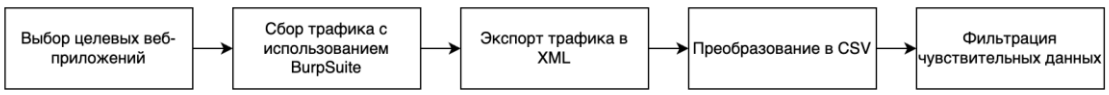



Рис. 1. Алгоритм сборки набора данных

В качестве признакового представления применялся TF-IDF по тексту тела ответа. Оценивались три классификатора: Multinomial Naive Bayes, Logistic Regression и LinearSVC. Для оценки качества использовались precision, recall, F1-score (macro и weighted) и accuracy [9]. LinearSVC показал accuracy = 0.487 и macro F1 = 0.551. Модель демонстрирует крайне несбалансированное поведение: recall по классу gaming = 0.99 при precision = 0.25,

тогда как по e-commerce наблюдается обратная картина (precision = 0.99, recall = 0.28). Multinomial Naive Bayes показал результаты существенно лучше: accuracy = 0.818, однако macro F1 = 0.597 из-за нулевого обнаружения по классу social network/messenger (precision = recall = F1 = 0.000). По e-commerce F1 = 0.919, по finance recall = 1.000 при precision = 0.669. Logistic Regression оказалась лучшей моделью среди рассмотренных: accuracy = 0.815, macro F1 = 0.768. Она имеет устойчивые результаты по всем четырем категориям: e-commerce F1 = 0.859, finance F1 = 0.854, gaming F1 = 0.704, social network/messenger F1 = 0.655. Сравнение результатов проеденных экспериментов представлено в таблице 1. Сравнительная диаграмма основных метрик, полученных в ходе экспериментов с логистической регрессией представлена на рис. 2.

ТАБЛИЦА 1. Сравнение результатов проведенных экспериментов

| Модель | Точность (Accuracy) | F1-мера (F1-score) | Примечание |
|---|---|---|---|
| LinearSVC | 0.487 | 0.551 | Сильный дисбаланс между классами |
| Multinomial NB | 0.818 | 0.597 | Нулевое детектирование по классу Social Network/messenger |
| Logistic Regression | 0.815 | 0.768 | Стабильна по всем классам |

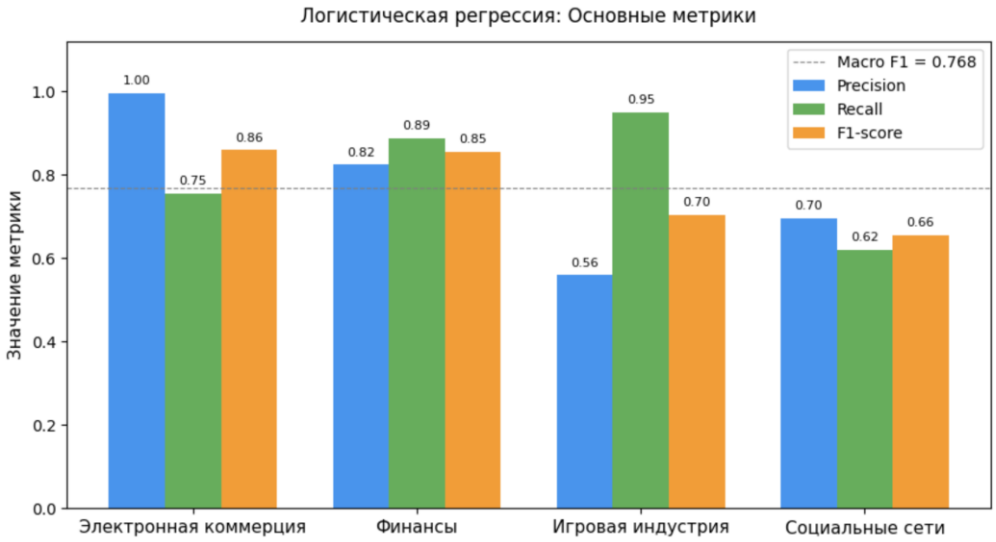



Рис. 2. Сравнительная диаграмма метрик логистической регрессии

Более низкие результаты по классу social network/messenger во всех моделях объясняются тем, что доступные страницы данной категории содержат минимальный тематически значимый контент: основная функциональность скрыта за аутентификацией, а также меньшим числом примеров целевых веб-приложений в обучающей и тестовой выборках.

Таким образом, в настоящей работе продемонстрирована принципиальная применимость классических ML-методов к задаче тематической классификации веб-приложений по HTTP-трафику. Logistic Regression с TF-IDF-признаками на основе тела ответа обеспечивает macro F1 = 0.768 на четырехклассовой задаче при объеме датасета около 7 000 транзакций, превосходя LinearSVC и Multinomial Naive Bayes. Ключевым ограничением является малый объем и ручной способ сбора данных, исключающий масштабирование; кроме того, класс social network/messenger систематически хуже классифицируется ввиду дефицита публично доступного контента. Перспективными направлениями являются автоматизированный краулинг для расширения датасета, включение структурных признаков DOM и URL, а также применение нейросетевых архитектур (TextCNN, BERT) для повышения качества классификации.

*Работа выполнена за счет гранта Санкт-Петербургского научного фонда № 25-РБ-01-13.*

**Список используемых источников**

1. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012. № 2. С. 57-68.

2. Котенко И. В., Хмыров С. С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. 2022. № 4(50). С. 52–79.

3. Котенко И. В., Котухов М. М., Марков А. С. и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под ред. И. В. Котенко. Санкт-Петербург. 2000. 190 с.

4. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2023. № 3 (326). С. 65-72.

5. Giménez C. T., Villegas A. P., Marañón G. Á. HTTP data set CSIC 2010 // Information Security Institute of CSIC (Spanish Research National Council). 2010. Т. 64. № 07.

6. Еремин Е. О. Обзор открытых наборов данных для выявления атак на веб-приложения // International Journal of Open Information Technologies. 2024. Т. 12. № 3. С. 106-113.

7. Faizann24. Fwaf-Machine-Learning-driven-Web-Application-Firewall // GitHub. 2023. URL: https://github.com/faizann24/Fwaf-Machine-Learning-driven-Web-Application-Firewall (дата обращения: 16.04.2026).

8. Ледовская Е. В., Мансуров П. С. Интеграция машинного обучения в информационную безопасность: тренды для WAF // Безопасность. Управление. Искусственный интеллект. 2025. № 2. С. 9-15.

9. Михайличенко А. А. Аналитический обзор методов оценки качества алгоритмов классификации в задачах машинного обучения //Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. № 4 (311). С. 52-59.

## MANUAL CREATION OF A DATASET FOR WEB APPLICATION CLASSIFICATION BY HTTP TRAFFIC IN ORDER TO IDENTIFY BUSINESS LOGIC VULNERABILITIES

**Denisov R.[1], Kosmachev A.[1,2], Kotenko I.[2], Magomedov A.[1]**
[1]National Research University Higher School of Economics
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article addresses the problem of multi-class classification of web applications by topic (domain) based on HTTP traffic analysis. Correctly defining the application domain allows for narrowing the search space during security testing and specifically checking for business logic vulnerabilities specific to a particular category. A methodology for manually generating a dataset using the Burp Suite traffic interception tool is proposed. Approximately 7,000 HTTP transactions were collected, annotated into four categories: e-commerce, finance, gaming, and social network/messenger. Using the obtained data, a comparative study of three models was conducted: Multinomial Naive Bayes, Logistic Regression, and LinearSVC. Logistic Regression demonstrated the best result in quality metrics (macro F1 = 0.768, accuracy = 0.815), ensuring stable classification across all four categories.*

***Key words:*** *web application classification, HTTP traffic, business logic vulnerabilities, machine learning, Burp Suite, dataset, Logistic Regression, Naive Bayes, LinearSVC, security testing*

**УДК: 004.056.563**
**ГРНТИ: 50.37.23**

# ОБРАТНЫЙ ПРОКСИ-ФИШИНГ И МЕТОДЫ ЗАЩИТЫ ОТ НЕГО

**А. А. Дрочнев, Д. А. Иванов, Д. С. Семенов**

Военный университет радиоэлектроники

*В статье рассматривается обратный прокси-фишинг как способ компрометации веб-доступа, при котором злоумышленник в реальном времени проксирует взаимодействие пользователя с подлинным сервисом. Показано, почему такой подход позволяет перехватывать не только пароль, но и подтвержденную сетевую сессию, что резко снижает эффективность привычных способов двухэтапной проверки. Предложены меры защиты на уровне удостоверяющей инфраструктуры, браузера, сетевого периметра и процессов реагирования.*

***обратный прокси-фишинг, кража сессии, session cookie, многофакторная аутентификация, WebAuthn, FIDO2, условный доступ, UEBA, изоляция браузера***

## Введение: эволюция фишинга

Обратный прокси-фишинг следует рассматривать не как усовершенствованный способ кражи пароля, а как атаку на уже подтвержденную веб-сессию. В такой схеме атакующий получает ключевое преимущество не в момент ввода логина и пароля, а в момент выдачи сервисом сессионного секрета, который затем можно повторно использовать для входа в почту, облачное хранилище, административный портал или иной веб-сервис. Поэтому ставка только на многофакторную аутентификацию больше недостаточна: необходимы фишинг-устойчивая криптографическая аутентификация, короткоживущие сессии, привязка доверия к устройству и сети, а также поведенческий мониторинг успешных входов [1, 2, 3, 4, 5, 6, 7].

Классический фишинг долгие годы строился вокруг статической поддельной страницы входа: жертва сама отдавала логин и пароль, а затем злоумышленник использовал их на настоящем сайте. Такая модель сохраняется, однако ее эффективность снижается по мере распространения многофакторной аутентификации. Microsoft описала кампанию, в которой атакующие уже не ограничивались хищением пароля: они перехватывали подтвержденную сессию пользователя и тем самым обходили вход даже при включенном втором факторе; по данным наблюдений Microsoft, одна

из таких кампаний пыталась атаковать более 10 000 организаций и была ориентирована на пользователей Office 365 [1, 8].

Ключевая причина этой эволюции состоит в том, что далеко не все распространенные способы многофакторной проверки являются фишинг-устойчивыми. NIST прямо указывает, что пароли, одноразовые коды и внеполосные способы подтверждения не относятся к фишинг-устойчивым методам, поскольку ручной ввод результата проверки не привязывает аутентификацию к конкретной сессии и конкретному проверяющему домену [2].

**Определение обратного прокси-фишинга**

Обратный прокси-фишинг представляет собой атаку, в которой фишинговый сайт работает не как грубая визуальная копия страницы входа, а как посредник между пользователем и реальным сервисом. Пользователь открывает домен злоумышленника, видит настоящую страницу входа, проксированную в реальном времени, вводит пароль, проходит второй фактор и получает успешный вход. Но все HTTP-запросы и ответы, включая cookies и редиректы, проходят через инфраструктуру атакующего. Microsoft описывает такую схему как проксирование трафика в обе стороны с последующим захватом session cookie, а не только пароля [1, 9, 10].

На практике эта логика уже давно реализована в инструментах класса attacker-in-the-middle. Совместное предупреждение CISA указывает, что аффилированные с ALPHV BlackCat злоумышленники использовали Evilginx2 для получения учетных данных, данных второго фактора и session cookies. В более позднем анализе Microsoft по платформе Tycoon2FA показано, что современные наборы этого класса предоставляют готовые темы под Microsoft 365, Outlook, SharePoint, OneDrive и Google, поддерживают захват cookies, отслеживание результата входа и автоматизированную эксфильтрацию похищенных артефактов. Okta дополнительно отмечает, что real-time AiTM-прокси применяются в целевых атаках и red team-активности как минимум с 2017 года [11–13].

Ключевое отличие от обычного прямого прокси состоит в направлении доверия. В прямом прокси пользователь или организация осознанно отправляют исходящий трафик через доверенный узел. В обратном прокси-фишинге пользователь считает, что обращается непосредственно к подлинному сервису, однако фактически завершает TLS-сеанс с доменом злоумышленника, который уже сам создает другой сеанс к настоящему

поставщику идентификации. Для жертвы это выглядит как обычный вход, а для атакующего – как возможность получить весь аутентификационный обмен в режиме реального времени [1, 12].

## Методы защиты от обратного прокси-фишинга. Технические меры на уровне инфраструктуры

Наиболее практичный принцип – считать успешный вход лишь началом контроля, а не завершением проверки. Microsoft рекомендует defence-in-depth against token theft: снижать вероятность компрометации, выявлять успешную кражу токенов и уменьшать ценность replay-использования похищенного артефакта. В том числе рекомендуется требовать compliant device, включать risk-based Conditional Access, принудительно повторно проверять доступ для чувствительных действий и ограничивать использование приложения незащищенными сетями и устройствами [1, 3, 4].

Привязка сессии к доверенной сети или известному egress IP снижает риск повторного использования cookie вне контролируемого контура, однако такая мера имеет и недостатки. Microsoft прямо пишет, что location-based и network-based enforcement повышают защищенность от token replay, но влекут за собой эксплуатационные издержки и не одинаково покрывают разные классы приложений; для некоторых сценариев требуется сочетание с Continuous Access Evaluation и приложенческими ограничениями на стороне самого сервиса. Поэтому жесткая привязка к IP полезна как один из барьеров, но не может считаться универсальной заменой фишинг-устойчивой аутентификации [4, 14].

Отдельный и более сильный путь – device-bound токены. Microsoft Entra Token Protection описывается как session control, уменьшающий token replay за счет того, что sign-in session tokens криптографически привязываются к конкретному устройству; похищенный токен нельзя использовать с иного устройства в поддерживаемых сценариях. Но есть важное ограничение: в текущем документированном виде Microsoft прямо указывает, что browser-based applications пока не поддерживаются, а основное покрытие относится к native applications и поддерживаемым ресурсам вроде Exchange Online, SharePoint Online и Teams [3]. На стороне web-приложения также нужно минимизировать ценность самой cookie: использовать Secure, HttpOnly, ограничивать scope, задавать короткий срок жизни и, по возможности, применять префикс __Host-, что прямо рекомендует NIST для cookies сопровождения сессии [2, 3].

Conditional Access должен работать не как формальный второй фактор, а как постоянная переоценка риска. Для неуправляемых устройств Microsoft рекомендует отключать persistent browser session и задавать sign-in frequency, например, 1 час. В дополнение следует требовать повторную интерактивную аутентификацию для чувствительных операций, автоматически реагировать на risky sign-ins и high-risk users, а также ограничивать доступ к критичным ресурсам только с compliant devices и trusted networks [4, 5].

Поведенческая аналитика пользователей и сущностей остается ключевым средством компенсации после успешного входа. Microsoft Sentinel UEBA описывается как механизм, который непрерывно учится на телеметрии, формирует поведенческие базовые линии и поднимает meaningful anomalies, помогающие аналитикам находить компрометацию. На практике для защиты от прокси-фишинга наибольшую ценность дают аномалии, связанные с невозможным перемещением, новым автономным системам провайдеров, сменой user-agent, нетипичным временем входа, внезапным созданием inbox rules и резким всплеском обращений к почте, файлам и административным функциям [6].

Наиболее сильная мера против AiTM – фишинг-устойчивая криптографическая аутентификация. NIST требует, чтобы на уровне AAL2 предлагался хотя бы один phishing-resistant authentication option, и отдельно объясняет, что WebAuthn/FIDO2 достигает phishing resistance за счет verifier name binding: криптографический ответ формируется для аутентифицированного домена проверяющей стороны, а не просто для «какой-то» формы входа. Okta аналогично называет passkeys и FIDO2 WebAuthn фишинг-устойчивыми аутентификаторами, предотвращающими раскрытие чувствительных данных поддельным приложениям и сайтам [2, 7].

Переход с push-уведомлений и одноразовых кодов на passkeys, FIDO2-ключи или иной криптографический вход с привязкой к домену является не «улучшением удобства», а архитектурной сменой класса защиты. Именно такие методы, а не обычный push-MFA, дают наилучшую устойчивость к AiTM и обратному прокси-фишингу (таблица 1) [2, 7].

ТАБЛИЦА 1. Первоочередные меры снижения риска обратного прокси-фишинга

| Действие | Необходимые меры | Значение меры |
|---|---|---|
| Фишинг-устойчивый вход для критичных ролей | Обязать администраторов, финансовые роли и владельцев SaaS-tenant использовать passkeys или FIDO2-ключи | Исключает передачу секрета через прокси и резко снижает эффективность AiTM |
| Conditional Access | Разрешить доступ к Exchange, SharePoint, Teams, административным порталам только с compliant devices или trusted network | Снижает ценность похищенной cookie вне управляемого контура |
| Короткая жизнь доверия | Для неуправляемых браузеров включить sign-in frequency 1 час и отключить persistent browser session | Уменьшает окно replay-использования сессии |
| Усиление push-MFA | Включить number matching в Microsoft Authenticator; для Google Accounts использовать prompts с проверкой аномалий и числа [15–17] | Снижает риск случайного одобрения и MFA fatigue, хотя не заменяет FIDO2 |
| Мониторинг успешных входов | Настроить алерты на impossible travel, новый ASN, anonymizer/VPN, новый user-agent, создание inbox rules | Позволяет увидеть уже успешную кражу сессии, а не только неудачные входы |
| Блокирование устаревших протоколов | Отключить Basic authentication, а где возможно – убрать POP/IMAP/SMTP AUTH и перевести интеграции на Modern Auth / OAuth [18] | Убирает старые каналы доступа и уменьшает поверхность атаки |
| План реагирования | Автоматизировать revoke active sessions, отзыв refresh-токенов, проверку mailbox rules и удаление подозрительных OAuth-consent | Ограничивает ущерб в первые минуты после компрометации |

## Заключение

Обратный прокси-фишинг уже нельзя считать редкой экзотикой. Это устоявшийся класс атак, в котором злоумышленник не обязан ломать криптографию и даже не обязан подделывать страницу входа вручную: ему достаточно заставить сервис самому выдать сессию через контролируемый прокси. Отсюда следует главный практический вывод: одной только многофакторной аутентификации больше недостаточно. Рабочая архитектура защиты должна сочетать фишинг-устойчивый вход, управление риском сессии, короткое время жизни доверия, контроль устройств и сетевого контура, UEBA и готовый сценарий быстрого отзыва активных сессий [1, 2, 3, 4, 5, 6, 7, 19].

**Список используемых источников**

1. Microsoft Threat Intelligence. From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud // Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/ (дата обращения: 20.04.2026).

2. NIST. Special Publication 800-63B: Authentication and Authenticator Management. URL: https://pages.nist.gov/800-63-4/sp800-63b.html (дата обращения: 22.04.2026).

3. Token Protection in Microsoft Entra Conditional Access // Microsoft Learn. URL: https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection (дата обращения: 24.04.2026).

4. Protecting tokens in Microsoft Entra // Microsoft Learn. URL: https://learn.microsoft.com/en-us/entra/identity/devices/protecting-tokens-microsoft-entra-id (дата обращения: 19.04.2026).

5. Require reauthentication and disable browser persistence // Microsoft Learn. URL: https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-persistent-browser (дата обращения: 20.04.2026).

6. Advanced threat detection with User and Entity Behavior Analytics // Microsoft Learn. URL: https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics (дата обращения: 17.04.2026).

7. Phishing-resistant authentication // Okta Identity Engine. URL: https://help.okta.com/oie/en-us/Content/Topics/identity-engine/authenticators/phishing-resistant-auth.htm (дата обращения: 21.04.2026).

8. Resurgence of a multi-stage AiTM phishing and BEC campaign abusing SharePoint // Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2026/01/21/multistage-aitm-phishing-bec-campaign-abusing-sharepoint/ (дата обращения: 22.04.2026).

9. Steal Web Session Cookie (T1539) // CISA. URL: https://www.cisa.gov/eviction-strategies-tool/info-attack/T1539 (дата обращения: 21.04.2026).

10. Microsoft Defender Security Research Team. OAuth redirection abuse enables phishing and malware delivery // Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2026/03/02/oauth-redirection-abuse-enables-phishing-malware-delivery/ (дата обращения: 22.04.2026).

11. StopRansomware: ALPHV Blackcat // CISA. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a (дата обращения: 23.04.2026).

12. Microsoft Defender Security Research Team. Inside Tycoon2FA: How a leading AiTM phishing kit operated at scale // Microsoft Security Blog. URL: https://www.microsoft.com/en-us/security/blog/2026/03/04/inside-tycoon2fa-how-a-leading-aitm-phishing-kit-operated-at-scale/ (дата обращения: 25.04.2026).

13. Winterford B., Diallo M. Keeping Phishing Adversaries Out of the Middle // Okta Security. URL: https://sec.okta.com/articles/phishingasaservice/ (дата обращения: 20.04.2026).

14. Designing ZTNA access policies for Cloudflare Access // Cloudflare Reference Architecture docs. URL: https://developers.cloudflare.com/reference-architecture/design-guides/designing-ztna-access-policies/ (дата обращения: 22.04.2026).

15. Implementing Number Matching in MFA Applications // CISA. URL: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf (дата обращения: 21.04.2026).

16. How number matching works in MFA push notifications for Authenticator // Microsoft Learn. URL: https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-mfa-number-match (дата обращения: 23.04.2026).

17. Sign in with Google prompts // Google Account Help. URL: https://support.google.com/accounts/answer/7026266?hl=en (дата обращения: 20.04.2026).

18. Deprecation of Basic authentication in Exchange Online // Microsoft Learn. URL: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online (дата обращения: 17.04.2026).

19. Remote browser isolation // Cloudflare One docs. URL: https://developers.cloudflare.com/cloudflare-one/remote-browser-isolation/ (дата обращения: 21.04.2026).

## REVERSE PROXY FISHING AND METHODS TO PROTECT THEM

**Drochnev A., Ivanov D., Semenov D.**
Military University of Radioelectronics

*The article considers reverse proxy phishing as a way to compromise web access, in which an attacker proxies a user's interaction with an authentic service in real time. It shows why this approach allows you to intercept not only a password, but also a confirmed network session, which drastically reduces the efficiency of the usual two-step verification methods. Protection measures are proposed at the level of the certification infrastructure, browser, network perimeter and response processes.*

***Key words:*** *back-proxy phishing, session theft, session cookie, multi-factor authentication, WebAuthn, FIDO2, conditional access, UEBA, browser isolation*

**УДК 004.75**
**ГРНТИ 49.01.85**

# РАЗРАБОТКА АРХИТЕКТУРЫ РАСПРЕДЕЛЕННОЙ HONEYPOT-СИСТЕМЫ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

**В. А. Задбоев., В. И. Татаринов, Д. Д. Чимитов**

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

*В статье рассматривается задача обнаружения сетевых вторжений в распределенных информационно-вычислительных сетях на основе технологии honeypot. Обосновывается актуальность применения распределенных honeypot-систем, как средства активного мониторинга и анализа действий нарушителей. Предлагается архитектура распределенной honeypot-системы, включающая набор периферийных honeypot-узлов и центральный аналитический компонент, обеспечивающий сбор, корреляцию и анализ событий информационной безопасности. Описаны принципы взаимодействия компонентов системы, а также особенности интеграции с существующими средствами обнаружения вторжений. Показано, что использование распределенной архитектуры позволяет повысить полноту и информативность данных о сетевых атаках и обеспечить раннее выявление потенциальных угроз.*

***honeypot-система, распределенная архитектура, обнаружение сетевых вторжений, информационная безопасность, сетевые атаки, корреляция событий, мониторинг сети***

## Введение

Развитие информационно-вычислительных сетей сопровождается увеличением числа доступных сервисов и точек подключения, что расширяет возможности для проведения сетевых атак. Межсетевые экраны и сигнатурные системы обнаружения вторжений выявляют известные способы воздействия, однако дают меньше сведений о новых или специально адаптированных атаках. Для наблюдения за действиями нарушителя применяются honeypot-системы – контролируемые узлы, имитирующие реальные сетевые ресурсы и регистрирующие обращения к ним [1-2].

Одиночный honeypot-узел позволяет наблюдать только за тем сегментом сети, в котором он установлен. Для инфраструктуры с несколькими площадками этого недостаточно: события фиксируются раздельно, а сопоставление действий одного нарушителя на разных участках сети затрудня-

ется. Как видно из таблицы 1, размещение узлов в нескольких сегментах расширяет зону наблюдения и дает возможность сводить полученные данные в одном аналитическом центре. Это определяет необходимость разработки распределенной архитектуры honeypot-системы.

ТАБЛИЦА 1. Сравнение локальной и распределенной honeypot-систем

| Характеристика | Локальная | Распределенная |
|---|---|---|
| Зона покрытия | Ограниченный сегмент сети | Несколько взаимосвязанных сегментов и площадок |
| Масштабируемость | Ограниченная | Высокая за счет модульности |
| Устойчивость к отказам | Низкая | Повышенная за счет репликации |
| Информативность данных | Средняя | Высокая |

Honeypot-системы традиционно классифицируются по уровню взаимодействия с атакующим и по способу интеграции в защищаемую инфраструктуру. Низкоинтерактивные решения эмулируют отдельные сетевые сервисы и отличаются простотой развертывания, однако предоставляют ограниченный объем информации о действиях нарушителя. Высокоинтерактивные honeypot-системы, напротив, используют реальные операционные системы и приложения, что позволяет детально изучать тактики и инструменты атак, но сопровождается повышенными рисками компрометации [3].

В ряде современных исследований предлагаются гибридные архитектуры, сочетающие различные типы honeypot-узлов и использующие централизованные серверы сбора данных. Тем не менее большинство решений ориентировано на локальные или корпоративные сети и не учитывает вопросы масштабируемости, отказоустойчивости и корреляции событий в распределенной среде. Кроме того, недостаточно проработаны механизмы интеграции honeypot-систем с существующими средствами мониторинга и реагирования на инциденты.

Цель работы – разработать архитектуру распределенной honeypot-системы, предназначенной для обнаружения сетевых вторжений в информационно-вычислительной сети. Для достижения цели необходимо определить состав и назначение компонентов, порядок размещения honeypot-уз-

лов, перечень регистрируемых событий и способ передачи данных на центральный сервер.

При проектировании учитывались два ограничения. Во-первых, скомпрометированный honeypot не должен использоваться для воздействия на продуктивные ресурсы, поэтому его сетевые соединения необходимо ограничивать и контролировать. Во-вторых, добавление нового узла не должно требовать изменения общей схемы сбора данных. Эти условия определили разделение системы на периферийный и центральный уровни.

На периферийном уровне в выбранных сегментах сети размещаются honeypot-узлы. Их состав и набор имитируемых сервисов выбираются с учетом назначения конкретного сегмента. Узлы могут быть развернуты в виртуальных машинах или контейнерах, что упрощает восстановление исходного состояния после зарегистрированного воздействия. Центральный уровень образует сервер сбора и анализа событий.

Периферийный узел регистрирует входящие соединения, сетевой трафик, изменения состояния имитируемого сервиса и действия, выполненные в его среде. Перед отправкой записи снабжаются идентификатором узла и отметкой времени, после чего передаются на центральный сервер по защищенному каналу. На сервере данные приводятся к единому формату, сохраняются и группируются по источнику, времени и наблюдаемым признакам атаки [4].

При временной недоступности центрального сервера события сохраняются в локальном буфере honeypot-узла и передаются после восстановления связи. Для крупных сетей центральный уровень может включать несколько аналитических узлов с репликацией хранилища. Конфигурации периферийных узлов задаются централизованно, что позволяет согласованно обновлять имитируемые сервисы и параметры регистрации событий.

**Взаимодействие с системой обнаружения вторжений**

Данные honeypot-узлов дополняют сведения, получаемые системой обнаружения вторжений. Срабатывание сигнатуры может быть сопоставлено с обращением к имитируемому сервису, а последовательность действий на нескольких узлах – объединена в один инцидент. Для этого центральный сервер передает нормализованные события в систему мониторинга и управления событиями информационной безопасности. Совместный анализ позволяет уточнять признаки атак и уменьшать число разрозненных уведомлений.

Практическая ценность подобной интеграции заключается в возможности раннего выявления атакующих, которые еще не взаимодействуют напрямую с продуктивными ресурсами сети. Анализ активности в honeypot-сегментах позволяет выявлять разведывательные действия и попытки подбора уязвимостей, что дает дополнительное время для реагирования [5].

С учетом вышесказанного, на рис. 1 представлена предлагаемая структурная схема распределенной honeypot-системы в виде взаимодействия периферийных honeypot-узлов с центральным аналитическим сервером, а также каналы передачи данных и интеграция с системой обнаружения вторжений.

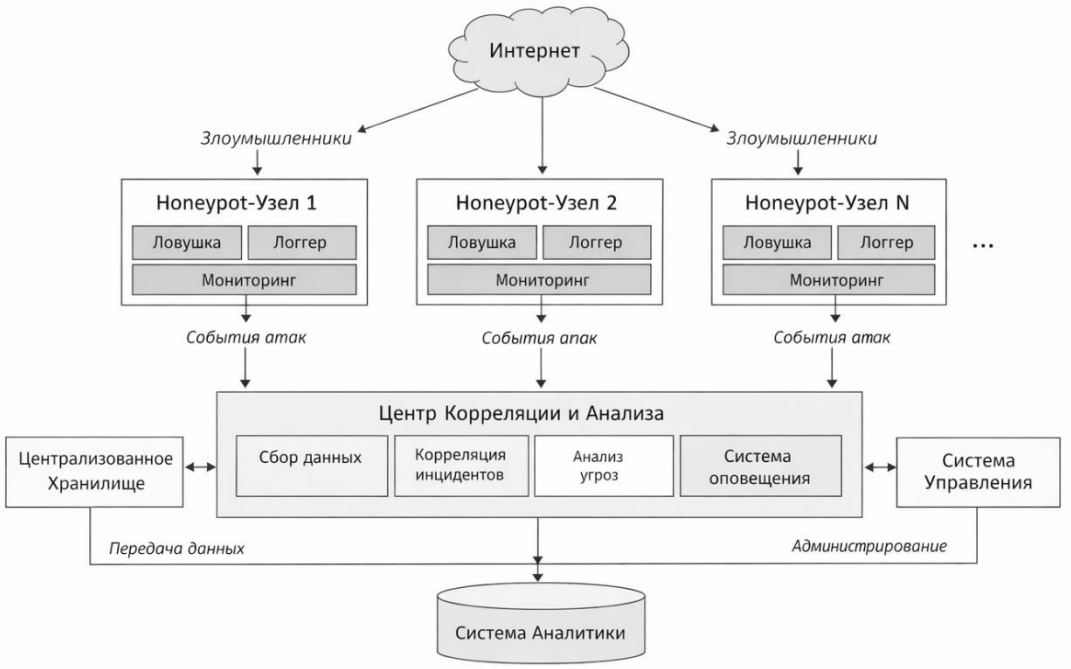



Рис. 1. Архитектура распределенной honeypot-системы для обнаружения сетевых вторжений

## Заключение

В работе предложена архитектура распределенной honeypot-системы для обнаружения сетевых вторжений, ориентированная на применение в масштабных и гетерогенных сетевых инфраструктурах. Рассмотренный подход позволяет расширить зону мониторинга, повысить информативность собираемых данных и обеспечить централизованный анализ активности нарушителей.

Полученные результаты могут быть использованы при проектировании систем активной защиты и при дальнейшем исследовании методов корреляции событий информационной безопасности. Перспективным направле-

нием дальнейших работ является внедрение методов машинного обучения для автоматизированного анализа данных, получаемых от распределенных honeypot-узлов, а также экспериментальная оценка эффективности предложенной архитектуры в условиях реальных сетевых атак.

**Список используемых источников**

1. Задбоев В. А., Абрамова Н. И., Москалев В. С. Противодействие внешним вторжениям в информационно-вычислительной сети // Телекоммуникации и связь. 2025. № 5(8). С. 18-23. DOI: 10.21681/3034-4050-2025-5-18-23.

2. Задбоев В. А., Татаринов В. И., Ткачев Д. Ф. Организация ложного трафика в honeypot-системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПбГУТ, 2025. Т. 1. С. 119-122.

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., Татаринов В. И., Ткачев Д. Ф. Принципы маскировки зараженных файлов в honeypot-системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 2-х т. СПбГУТ, 2025. Т. 1. С. 123-127.

5. Задбоев В. А., Липатников В. А., Нефедов В. В. Способ повышения целостности файлов информационных ресурсов сети передачи данных в условиях атак. XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2024. С. 304-307.

## DEVELOPING A DISTRIBUTED HONEYPOT SYSTEM ARCHITECTURE FOR NETWORK INSURANCE DETECTION

**Zadboev V., Tatarinov V., Chimitov D.**
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

*This article examines the problem of detecting network intrusions in distributed information networks using honeypot technology. It substantiates the relevance of using distributed honeypot systems as a means of actively monitoring and analyzing intruder activity. A distributed honeypot system architecture is proposed, comprising a set of peripheral honeypot nodes and a central analytics component that enables the collection, correlation, and analysis of information security events. The principles of interaction between the system components are described, as well as the specifics of integration with existing intrusion detection tools. It is demonstrated that using a distributed architecture improves the completeness and information content of network attack data and ensures the early detection of potential threats.*

***Key words:*** *honeypot system, distributed architecture, network intrusion detection, information security, network attacks, event correlation, network monitoring*

**УДК 621.396**
**ГРНТИ: 49.37.29**

# ИССЛЕДОВАНИЕ ПОДХОДОВ К КЛАССИФИКАЦИИ РАДИОСИГНАЛОВ ЗАЩИЩЕННЫХ БЕСПРОВОДНЫХ СЕТЕЙ

**Я. А. Ильин, Т. Д. Любащенко**

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

*В статье рассматриваются методы и подходы к автоматической классификации радиосигналов защищенных беспроводных сетей с акцентом на технологии Wi-Fi (IEEE 802.11) и Bluetooth (IEEE 802.15), работающие в нелицензируемом ISM-диапазоне 2,4 ГГц. Показано, что взаимные помехи между сетями и использование механизмов защиты (WPA2/WPA3 в Wi-Fi, FHSS в Bluetooth) снижают наблюдаемость признаков сигнала и затрудняют пассивную идентификацию. Проанализированы классические методы классификации на основе RSSI и методы, использующие особенности модуляции и структуры физического уровня (OFDM, GFSK, FHSS). Сделан вывод о перспективности комбинированных подходов, сочетающих спектральные, временные и статистические признаки, а также методов машинного обучения.*

***радиосигналы, классификация, Wi-Fi, Bluetooth, RSSI, OFDM, GFSK, FHSS, защищенные беспроводные сети***

Wi-Fi, Bluetooth и ряд других технологий делят между собой один и тот же нелицензируемый диапазон 2,4 ГГц – отсюда высокая плотность сигналов и постоянные взаимные помехи [1, 2]. Именно эта теснота сильно осложняет радиомониторинг и автоматическое распознавание типов излучений [3]. Добавим сюда шифрование в защищенных сетях: полезная нагрузка пакета становится недоступна наблюдателю, и единственное, на что он может опереться – радиофизические признаки самого сигнала. Классификация в такой ситуации неизбежно смещается на физический уровень и характеристики канала [4].

Тема остается актуальной прежде всего потому, что число устройств в диапазоне 2,4 ГГц продолжает расти, доля защищенных сетей увеличивается, а пассивный мониторинг становится все более востребованным инструментом обеспечения информационной безопасности.

Физический уровень: чем Wi-Fi отличается от Bluetooth

В современных версиях Wi-Fi (802.11g/n/ac/ax/be) данные передаются через OFDM – ортогональное частотное мультиплексирование [5]. Канал

делится на множество ортогональных поднесущих, что дает выигрыш и в спектральной эффективности, и в устойчивости к многолучевому распространению. Важно, что OFDM формирует характерную структуру пакета – во времени и по частоте – и эта структура остается наблюдаемой, даже когда сама полезная нагрузка зашифрована [6].

Bluetooth устроен иначе. И BR/EDR, и Bluetooth LE используют модуляцию GFSK в связке с псевдослучайной перестройкой частоты – FHSS [2]. Классический BR/EDR работает на 79 каналах шириной 1 МГц, LE – на 40 каналах по 2 МГц. Перестройка идет быстро, по псевдослучайной последовательности, синхронизированной между парой устройств. С одной стороны, это неплохая защита от перехвата и узкополосных помех. С другой – именно из-за нее пассивному наблюдателю крайне сложно получить устойчивый спектральный след [3].

RSSI: удобно, но недостаточно:

Самый простой признак, с которого обычно начинают первичную классификацию – RSSI, индикатор мощности принятого сигнала [7]. Он хорош для грубой оценки: есть ли сигнал в канале вообще, где примерно шум, как разделить источники по мощности. Проблема в том, что RSSI сильно зависит от расстояния до передатчика, экранирования, ориентации антенн и внешних помех. В плотном радиоэфире один и тот же уровень RSSI вполне может соответствовать совершенно разным типам передатчиков – так что опираться только на него ненадежно. Но как дополнительный параметр в связке с шириной полосы, длительностью пакета и частотой появления импульсов RSSI вполне рабочий инструмент [7].

Гораздо больше информации дают признаки, связанные непосредственно с модуляцией и структурой физического уровня [5]:

Для Wi-Fi это:

– OFDM-структура кадра – поднесущие, защитные интервалы;
– своя временная организация – преамбула отдельно, полезная часть отдельно;
– спектральная форма, которая определяется тем, как мощность распределена по поднесущим [6].

По совокупности этих признаков Wi-Fi довольно сильно отличается от других технологий – причем неважно, зашифрована нагрузка или нет: спектрально-временной "почерк" виден в любом случае.

С Bluetooth BR/EDR и BLE набор признаков совсем другой:

– модуляция GFSK;

– частотная перестройка по псевдослучайному закону – FHSS;
– сигнал наблюдается фрагментами, в узких частотных окнах [2].

И вот тут появляется главная проблема для классификатора: сигнал буквально виден кусками, а не целиком. Приходится вытаскивать признаки из частично заполненных спектральных карт и обрывков временных окон – задача заметно менее простая, чем для Wi-Fi.

Отдельно стоит сказать про FHSS – это не какой-то побочный эффект работы Bluetooth, а его основной защитный механизм [2].

Быстрая смена частоты сокращает время «жизни» сигнала на одной частоте и потому мешает длительному наблюдению устойчивого следа. Плюс Bluetooth умеет адаптивно обходить занятые или зашумленные каналы, что еще больше усложняет моделирование его поведения [3].

В итоге классификация Bluetooth требует методов, устойчивых сразу к трем вещам:
– фрагментарности наблюдений;
– не стационарности спектра;
– переменному уровню шумов и помех со стороны Wi-Fi.

В таблице 1 признаки Wi-Fi и Bluetooth сведены вместе для сравнения в условиях взаимных помех [1–3, 5, 6].

ТАБЛИЦА 1. Сравнение признаков сигналов Wi-Fi и Bluetooth для задач классификации

| | Wi-Fi | Bluetooth |
|---|---|---|
| Диапазон частот | 2,4 ГГц (также 5 и 6 ГГц в современных версиях) | 2,4 ГГц |
| Типичная модуляция PHY | OFDM в 802.11g/n/ac/ax/be | GFSK для BR/EDR и LE |
| Спектральный рисунок | Структурированный OFDM-кадр с поднесущими | Частотно-перестраиваемый сигнал FHSS |
| Влияние взаимных помех | Сильно зависит от занятости канала и соседних сетей | Чувствителен к помехам от Wi-Fi, но использует hopping |
| Пригодность для пассивной классификации | Высокая при наличии спектральных и временных признаков | Средняя, усложняется FHSS и короткими окнами наблюдения |

Разница видна сразу: Wi-Fi и Bluetooth расходятся не только на уровне протоколов доступа, но и на физическом уровне – а значит, и набор наблю-

даемых признаков у них принципиально разный. И еще раз подчеркну: в плотном радиоэфире одного RSSI не хватит, нужен комплекс признаков.

Защищенные Wi-Fi-сети используют WPA2 и WPA3, которые закрывают полезную нагрузку пакетов. WPA3 при этом заметно устойчивее к подбору паролей и атакам на сеанс аутентификации, чем WPA2 [4]. Пассивный наблюдатель, соответственно, теряет возможность анализировать содержимое пакетов.

Но радиофизическая оболочка кадра – преамбула, PHY-заголовки, временная структура, спектральная форма – остается видимой в любом случае. Получается, что шифрование данных не убирает радиопризнаки, а наоборот, делает их единственным доступным источником информации. Получается, что классификация фактически целиком уходит на уровень физических признаков – а значит, требования к точности и спектрального, и временного анализа заметно вырастают [5].

У Bluetooth логика защиты вообще другая: здесь основную роль играет не шифрование, а поведение сигнала по частоте. Механизм FHSS попросту не позволяет наблюдателю задержаться на одной частоте достаточно долго, чтобы собрать устойчивый спектральный след [2]. Особенно хорошо это заметно, когда Bluetooth и Wi-Fi работают одновременно: устройства делят один и тот же диапазон и мешают друг другу перекрестными помехами [3].

Отсюда требование к алгоритмам классификации – они должны справляться сразу с несколькими вещами:

– фрагментарностью сигналов;
– переменным уровнем шумов;
– не стационарностью спектральных характеристик.

Надежно классифицировать радиосигналы защищенных беспроводных сетей можно только опираясь на комплекс признаков – одного RSSI для этого попросту недостаточно. У Wi-Fi информативны OFDM-структура, организация пакета и временно-спектральные характеристики. У Bluetooth решающими оказываются FHSS, GFSK и псевдослучайная перестройка каналов.

Дальнейшее развитие темы, на мой взгляд, лежит в нескольких направлениях:

– комбинированные подходы, которые объединяют спектральные, временные и статистические признаки;
– методы машинного обучения – прежде всего сверточные нейронные сети (CNN) и метод опорных векторов (SVM) – для автоматического извлечения признаков из сырых отсчетов [8, 9];

– глубокое обучение, позволяющее классифицировать модуляцию напрямую по базовым отсчетам сигнала [10].

Ценность таких методов в том, что они хорошо работают даже с неполными, зашумленными наблюдениями – а в условиях взаимных помех Wi-Fi и Bluetooth это, скорее, обычная ситуация, чем исключение [3, 8].

В итоге можно сказать следующее: взаимные помехи и защитные механизмы (WPA2/WPA3, FHSS) заметно снижают наблюдаемость признаков сигнала и затрудняют пассивную идентификацию, а одного RSSI для надежной классификации явно не хватает. Наиболее перспективный путь – сочетание спектральных, временных и статистических признаков с методами машинного и глубокого обучения, которые позволяют автоматически извлекать признаки из базовых отсчетов сигнала [7–10].

**Список используемых источников**

1. IEEE Standard for Information Technology. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: IEEE Std 802.11-2024. Approved 26 September 2024. Published 28 April 2025.

2. IEEE Standard for Information Technology. Part 15: Wireless Personal Area Network (WPAN): IEEE Std 802.15.1-2002. Approved 15 April 2002.

3. Bluetooth-WLAN Coexistence // MathWorks. URL: https://www.mathworks.com/help/wlan/ug/bluetooth_wlan_coexistence.html (дата обращения: 31.05.2026).

4. WPA, WPA2, WPA3: What are the differences between Wi-Fi security standards // Strong EU. URL: https://www.strong-eu.com/blog/wpa-wpa2-wpa3-what-are-the-differences-between-wi-fi-security-standards (дата обращения: 31.05.2026).

5. 802.11 OFDM WLAN Overview // Keysight Technologies. URL: https://helpfiles.keysight.com/csg/89600B/Webhelp/Subsystems/wlan-ofdm/content/ofdm_80211-overview.htm (дата обращения: 31.05.2026).

6. Lecture 6: Physical Layer – Spread Spectrum and OFDM // Carnegie Mellon University. URL: https://www.cs.cmu.edu/~prs/wirelessS24/handouts/L6-Phy.pdf (дата обращения: 31.05.2026).

7. An RSSI Classification and Tracing Algorithm to Improve … // PMC. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7436166/ (дата обращения: 31.05.2026).

8. A Survey on the Wireless Network Technology Classification Using Machine Learning // Academia.edu. 2021.

9. Tamizhelakkiya K., Gauni S., Chandhar P. Modulation classification analysis of CNN model for wireless communication systems // AIMS Electronics and Electrical Engineering. – 2023. Vol. 7. N 4. P. 337–353.

10. Tian X., Zheng Q., Li B., Qiao D., Yu K., Wei Z., Li B., Jiang H., Li X., Lin Y., Gui G. A survey on deep learning enabled automatic modulation classification methods: Data representations, model structures, and regularization techniques // Signal Processing. 2025. Vol. 242. Art. 110444.

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ИБКС СПбГУТ, доцентом М. М. Ковцуром.*

# STUDY OF APPROACHES TO CLASSIFICATION OF RADIO SIGNALS OF PROTECTED WIRELESS NETWORKS

**Ilin Y., Lyubashchenko T.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article examines methods and approaches to automatically classifying radio signals in secure wireless networks, focusing on Wi-Fi (IEEE 802.11) and Bluetooth (IEEE 802.15) technologies operating in the unlicensed 2.4 GHz ISM band. It is shown that interference between networks and the use of security mechanisms (WPA2/WPA3 in Wi-Fi, FHSS in Bluetooth) reduce the observability of signal characteristics and complicate passive identification. Classic RSSI-based classification methods and methods that utilize modulation and physical layer structure features (OFDM, GFSK, FHSS) are analyzed. A conclusion is drawn regarding the potential of combined approaches combining spectral, temporal, and statistical features, as well as machine learning methods.*

***Key words:*** *radio signals, classification, Wi-Fi, Bluetooth, RSSI, OFDM, GFSK, FHSS, secure wireless networks*

**УДК 004.056.5**
**ГРНТИ 81.93.29**

# АНАЛИЗ СПОСОБОВ ЗАЩИТЫ УСТРОЙСТВ, НАСТРАИВАЕМЫХ С ПОМОЩЬЮ NFC

**Я. А. Ильин, Д. П. Спиридонов**

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

*В настоящее время все больше настраиваемых устройств используют технологию NFC в качестве инструмента установки параметров работы. В связи с возникающей необходимостью защиты устройств, требуется анализ и систематизация способов безопасной передачи параметров через NFC и изучение возможностей шифрования данных. Исследование посвящено анализу защиты передаваемых данных с помощью NFC. Проводится качественное сравнение методов с учетом их практического применения.*

***безопасность, информационная безопасность, радиосвязь, NFC***

Все больше устройств, являющихся частью интернета вещей, или автономных умных устройств имеют различные режимы работы. Настраиваемые устройства получают широкое распространение за счет развития технологий производства и совершенствования способов передачи команд. Это две основные составляющие конфигурируемых устройств. К таким настраиваемым устройствам можно отнести персональные устройства, промышленные приборы и датчики, устройства умного дома, а также NFC метки и иные устройства авторизации. Большинство подобных изделий крайне просты, но при этом многофункциональны. Всего несколько байт памяти способны содержать десятки и даже сотни параметров работы в зависимости от типа записываемого на устройство командного сообщения.

Устройства, настраиваемые с помощью NFC, имеют ряд преимуществ и ограничений, которые можно разделить на технические особенности и технические возможности. К техническим особенностям можно отнести: малую дальность действия технологии из-за частоты в 13,56 МГц; высокую скорость настройки (порядка нескольких секунд); совместимость с мобильными телефонами (практически любой смартфон сейчас имеет NFC модуль; автономность работы из-за отсутствия потребности в собственных элементах питания (питание NFC метки осуществляется за счет электромагнитного поля терминала); малый объем передаваемых данных; риск несанкционированного подключения, поскольку метка находится в пассивном режиме и получив питание от терминала, начнет работу [1].

Обеспечение безопасности настраиваемых устройств строится в первую очередь на программных методах:

1) взаимная аутентификация до начала передачи конфигурации;
2) симметричное и асимметричное шифрование;
3) использование особых протоколов (NDEF, NFC-SEC);
4) использование проверки целостности сообщений/пакетов;
5) безопасное хранение и смена ключей;
6) электронные подписи, поддерживающие NFC (Рутокен).

Настраиваемые устройства часто являются частью интернета вещей или сетевой инфраструктуры. В случае с конфигурируемыми с помощью NFC устройствами это несколько отличается. Среди основных возможностей, передаваемых с помощью NFC задач, можно выделить следующие: считывание статистических данных, установка существующего режима работы устройства, установка временных интервалов работы, авторизация и аутентификация пользователя, передача параметров на устройство в режиме реального времени.

Многие виды устройств могут не быть частью сети, а взаимодействие с ними осуществляет исключительно оператор (пользователь) через свой терминал (персональный компьютер, смартфон). Однако даже при таком специфическом виде обмена данными, атаки очень схожи с атаками на устройства и компоненты интернета вещей. Среди основных атак на настраиваемые через NFC устройства можно выделить: пассивное прослушивание (сниффинг); человек посередине (mitm); атаки с ретрансляцией (в основном случаются на банковские автоматы); атаки с подменой/эмуляцией метки или терминала (в основном случаются на терминалы для оплаты); передача вредоносного ПО через сообщение; уязвимости NFC в прошивках готовых изделий (как правило в уже готовых изделиях умного дома). На рисунке 1 приведена таблица устройств, содержащих компоненты NFC и атаки, совершаемые на них. Как становится видно из таблицы, самые хорошо защищенные устройства – это устройства банковской сферы или устройства с программным обеспечением от производителя. Можно видеть, что атаки совершаются неравномерно и устройства умного дома и персональные карты для авторизации весьма уязвимы. Это говорит о том, что сама по себе технология NFC так же, как и другие технологии передачи данных, такие как Wi-Fi и Bluetooth уязвима к атакам. Однако необходимость близкого контакта существенно снижает возможности для злоумышленника. Способы защиты устройства от атак не сильно отличаются, поэтому создание защищенного программного обеспечения и шифрование весьма распространены [2, 3].

| Устройство, настраиваемое через NFC | Пассивное прослушивание (сниффинг) | Атаки с ретрансляцией | Атаки с подменой/эмуляцией метки или терминала | Передача вредоносного ПО через сообщение | Уязвимости NFC в прошивках |
|---|---|---|---|---|---|
| Смартфоны и планшеты | Частые | Частые | Частые | Частые | Обычные |
| Платежные терминалы | Обычные | Частые | Обычные | Редкие | Редкие |
| Умные замки и системы СКУД | Частые | Частые | Частые | Обычные | Обычные |
| Wi-Fi роутеры и IoT-хабы | Частые | Обычные | Частые | Частые | Частые |
| Устройства умного дома | Частые | Редкие | Частые | Частые | Частые |
| Носимые устройства (часы, браслеты) | Частые | Частые | Частые | Редкие | Обычные |
| Медицинские устройства | Частые | Обычные | Частые | Обычные | Редкие |

Рис. 1. Таблица устройств и атак совершаемых на них

Существует множество решений по обеспечению защиты, настраиваемых с помощью технологии ближнего поля устройств:

1) изолированное выполнение операций обмена данными;
2) защита от снятия копии прошивки;
3) физическая защита изделия;
4) заводская установка готовых ключей шифрования;
5) передача параметров в реальном времени на устройство;
6) протоколы ограничения дальности;
7) отслеживание задержки при передаче сигнала;
8) чтение только сообщений корректного формата;
9) цифровые подписи.

На основании анализа характерных особенностей технологии NFC, возможных угроз и способов защиты устройств от них можно сделать вывод о том, что передача параметров с помощью NFC на настраиваемые устройства – перспективное направление. Существует ряд областей, где такие решения уже применяются. К ним можно отнести банковские устройства, медицинское оборудование, сельскохозяйственные машины, сетевые устройства, промышленные устройства, персональные устройства. Кроме этих областей, существуют новые перспективные направления, где подобные решения применяются редко или не применяются вообще. К таким группам технологических решений можно отнести:

1) умные бытовые датчики;
2) устройства, с которыми взаимодействует неквалифицированный пользователь;
3) «примитивные» (низко технологичные) умные устройства;
4) авторизация пользователей через онлайн сервисы.

Существуют возможности применения технологии NFC в областях касающихся простых устройств, которые могут являться частью умного дома или быть настраиваемыми. Наибольший интерес представляют устройства, работающие в автономном режиме, устройства требующие установления защиты от смены настройки и при этом требующие простую настройку. Перспективным направлением может быть создание массового выпуска примитивных изделий с компонентом NFC и цифровыми подписями. Их возможно внедрять массово ввиду наличия смартфонов у большинства граждан. Возможно так же создание устройств у которых будет доступно защищенное взаимодействие с площадками Контур.Диадок, Госуслуги или частными сервисами.

**Список используемых источников**

1. Грохольский А. В., Ильин Я. А., Ковцур М. М. Разработка концепции устройства с модулем конфигурирования на базе технологии NFC // Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сб. научных статей XIII Международной научно-технической и научно-методической конференции в 4 т. 2024. С. 260-262.

2. Карельский П. В., Ковцур М. М., Штеренберг С. И., Малинин Н.И. Анализ современных средств автоматизированной проверки функций безопасности коммутационного оборудования // XII Санкт-Петербургская межрегиональная конференция. 2021 С. 385-386.

3. Ильин Я. А., Катасонов А. И. Определение характерных особенностей для обнаружения вредоносного программного обеспечения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). Сб. науч. статей XII Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С. И. Макаренко, сост. В. С. Елагин, Е. А. Аникевич. 2023. Т. 4. С. 629-633.

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры защищенных систем связи Д. В. Сахаровым.*

## ANALYSIS OF PROTECTION METHODS FOR NFC-CONFIGURABLE DEVICES

**Ilin Y. Spiridonov. D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Currently, more and more customizable devices are using NFC technology as a tool for setting operating parameters. Due to the emerging need to protect devices, it is necessary to analyze and systematize ways to securely transmit parameters via NFC and explore the possibilities of data encryption. The study is devoted to the analysis of the protection of transmitted data using NFC. A qualitative comparison of the methods is carried out, taking into account their practical application.*

***Key words:*** *security, information security, radio communications, NFC*

**УДК 004.056.53**
**ГРНТИ 49.33.29**

# РАЗРАБОТКА КОНЦЕПЦИИ МОДУЛЯ ДЛЯ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ НИЗКОПРОИЗВОДИТЕЛЬНЫХ УСТРОЙСТВ

**М. М. Ковцур, А. С. Кудесов, М. А. Шахмоведев**

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

*В статье рассматривается концепция программно-аппаратного модуля для организации защищенного обмена данными между низкопроизводительными устройствами Интернета вещей. Модуль основан на технологии дальнего радиуса действия с низким энергопотреблением и использует отечественный блочный шифр, определенный национальным стандартом, в режиме гаммирования. Обоснован выбор аппаратной платформы, представлена концепция работы системы и приведены результаты натурных испытаний, подтверждающие работоспособность модуля на дистанциях до 700 метров при сохранении стопроцентной доставки пакетов.*

***защищенная передача данных, Интернет вещей, модуляция с расширением спектра, блочный шифр, микроконтроллер, беспроводная связь***

В настоящее время стремительный рост числа устройств Интернета вещей обуславливает потребность в надежных и защищенных каналах связи для систем мониторинга, управления и телеметрии. Задача организации защищенного взаимодействия распределенных устройств при ограниченных вычислительных и энергетических ресурсах является актуальной научно-технической проблемой [1]. Как отмечается в [2], даже в сотовых сетях четвертого поколения вопросы обеспечения безопасности остаются предметом исследований, а для маломощных устройств с автономным питанием они стоят еще острее. Помимо этого, анализ уязвимостей устройств умного дома [3] показывает, что многие бытовые решения Интернета вещей не обладают достаточным уровнем криптографической защиты.

Технология дальнего радиуса действия с низким энергопотреблением, использующая модуляцию с линейной частотной модуляцией, позволяет обеспечить устойчивую связь на расстояниях до нескольких километров при минимальном энергопотреблении. Однако существующие решения на базе протокола LoRaWAN, как показано в [4], требуют серверной инфраструктуры и используют западные криптографические стандарты, что не

всегда допустимо для отечественных систем, требующих соответствия национальным нормам.

Целью настоящей работы является разработка концепции автономного модуля для защищенного обмена данными между низкопроизводительными устройствами с использованием протокола LoRa и шифрования по ГОСТ Р 34.12-2015.

При выборе аппаратной платформы рассматривались несколько вариантов микроконтроллеров. Платы на базе ATmega328P, широко применяемые в любительских проектах, были отклонены из-за недостаточного объема оперативной памяти и отсутствия встроенных интерфейсов беспроводной связи. Микроконтроллеры семейства STM32 обладают достаточной вычислительной мощностью, однако для реализации беспроводной синхронизации ключей потребовался бы отдельный радиомодуль Bluetooth, что усложняет схему и увеличивает стоимость. В итоге выбор был остановлен на ESP32-S3, поскольку он сочетает двухъядерный процессор с тактовой частотой 240 МГц, встроенные модули Wi-Fi и BLE, аппаратный генератор случайных чисел и достаточный объем памяти для программной реализации блочного шифра «Кузнечик» [5].

Что касается радиочасти, рассматривались трансиверы SX1276 и SX1262 [6]. Первый дешевле и проще в освоении, но уступает по чувствительности приемника и энергопотреблению в спящем режиме. Модуль SX1262 был выбран по совокупности параметров: он обеспечивает чувствительность до –148 дБм, поддерживает расширенный набор значений фактора расширения и потребляет в режиме приема порядка 4,6 мА. Для защиты передаваемых данных на программном уровне реализован блочный шифр «Кузнечик» с длиной ключа 256 бит в режиме гаммирования.

Предлагаемый модуль работает по схеме «точка–точка» и состоит из двух идентичных устройств, каждое из которых может выступать и передатчиком, и приемником. Общая концепция работы показана на рисунке 1. Со стороны источника данных, например датчика температуры или влажности, информация поступает на модуль А по интерфейсу UART. Микроконтроллер шифрует полученное сообщение и передает его через радиоканал LoRa на частоте 868 МГц. На принимающей стороне модуль Б принимает пакет, расшифровывает его и передает открытый текст подключенному компьютеру или контроллеру. Обмен криптографическими ключами между модулями осуществляется по каналу BLE при первичной настройке.

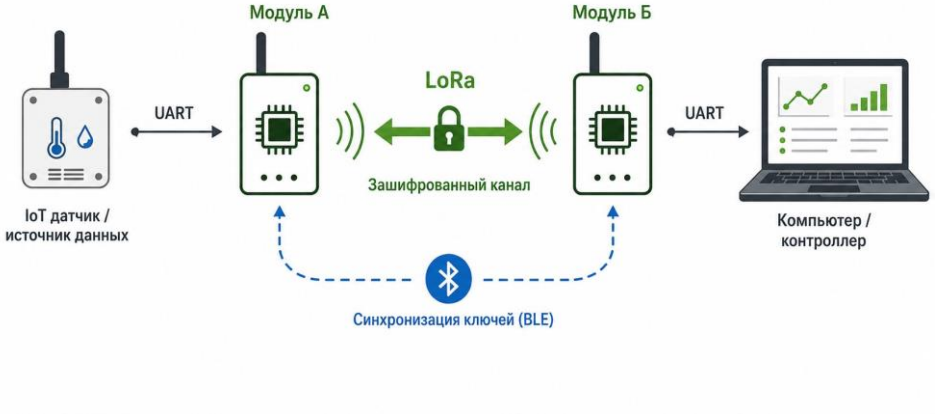



Рис. 1. Концепция работы модуля защищенной передачи данных

Для оценки работоспособности модуля проведены натурные испытания дальности связи на открытой местности. Результаты измерений представлены в таблице 1.

ТАБЛИЦА 1. Результаты тестирования дальности связи на открытой местности

| Дистанция, м | RSSI, дБм | SNR, дБ | Принято | Доставка |
|---|---|---|---|---|
| 100 | –100 | 10,25 | 5/5 | 100 % |
| 350 | –93 | 11,8 | 5/5 | 100 % |
| 500 | –105 | 6,3 | 5/5 | 100 % |
| 700 | –118 | –3,66 | 5/5 | 100 % |
| 750 | – | – | 0/5 | 0 % |

Как видно из таблицы 1, устойчивая связь с доставкой 100 % обеспечивается на дистанциях до 700 м при выходной мощности 25 мВт (14 дБм). На расстоянии 750 м прием пакетов прекращается полностью. На дистанции 700 м отношение сигнал/шум составляет –3,66 дБ, что говорит о работе на пределе чувствительности приемника (Рис. 1), однако модуляция с расширением спектра позволяет корректно принимать сигнал даже при таких значениях.

Таким образом, предложенная концепция модуля для защищенного взаимодействия низкопроизводительных устройств на основе протокола LoRa подтвердила свою работоспособность в ходе натурных испытаний. Выбранная аппаратная платформа на базе ESP32-S3 и SX1262 обеспечивает

достаточный запас вычислительной мощности для программной реализации отечественного шифра и не требует внешних компонентов для организации беспроводного управления ключами. Перспективами развития являются реализация контроля целостности по ГОСТ Р 34.13-2015, добавление механизма подтверждения доставки и организация ячеистой топологии сети.

**Список используемых источников**

1. Ковцур М. М., Браницкий А. А., Казаков Н. И. Разработка концепции защищенного централизованного взаимодействия распределенных устройств // Экономика и качество систем связи. 2023. № 2 (28). С. 99–104.

2. Ушаков И. А., Черкашин А. И. Анализ методов обеспечения безопасности в сетях LTE // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025): сб. науч. ст. в 3 т. СПб.: СПбГУТ, 2025. С. 506–511.

3. Поляков Д. В., Сахаров Д. В., Казанцев А. А. Анализ основных уязвимостей устройств умного дома и способы их предотвращения // Технологии информационного общества: сб. тр. XIX Международной отраслевой научно-технической конференции. М.: МТУСИ, 2025. С. 149–153.

4. Красников Д. А., Ковцур М. М., Никифоров А. В. Практика построения устойчивой к атакам инфраструктуры на основе протокола LoRaWAN // Информационная безопасность регионов России (ИБРР-2025): материалы XIV Санкт-Петербургской межрегиональной конференции. СПб., 2025. С. 481.

5. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.

6. Semtech Corporation. SX1261/SX1262 Long Range, Low Power, sub-GHz RF Transceiver: Datasheet. Rev. 1.2. Semtech, 2019. 111 p.

## DEVELOPMENT OF A CONCEPT FOR A SECURE COMMUNICATION MODULE FOR LOW-POWER DEVICES

**Kovtsur M., Kudesov A., Shakhmovedev M.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The paper presents a concept of a software and hardware module for organizing secure data exchange between low-power Internet of Things devices. The module is based on long-range low-power radio technology and uses the national block cipher defined by the Russian standard GOST R 34.12-2015 in counter mode. The selection of the hardware platform is justified, the system operation concept is presented, and the results of field tests confirming the module operability at distances up to 700 meters with one hundred percent packet delivery are provided.*

***Key words:*** *secure data transmission, Internet of Things, spread spectrum modulation, block cipher, microcontroller, wireless communication*

**УДК 004.056**
**ГРНТИ 81.93.29**

# БЕЗОПАСНОСТЬ ИНТЕГРАЦИЙ LLM С ИНСТРУМЕНТАМИ ПО ПРОТОКОЛУ MODEL CONTEXT PROTOCOL: МОДЕЛЬ УГРОЗ И ПРОТОТИП ЗАЩИТНЫХ МЕР

**И. В. Котенко[1], Т. Ч. Нгуен[2]**

[1] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2] Национальный исследовательский университет ИТМО

*Протокол Model Context Protocol (MCP) используется для подключения больших языковых моделей (LLM) к внешним инструментам и источникам данных. Это делает такие системы более полезными, но одновременно создает новые риски безопасности на границе между моделью и инструментами. В работе рассматривается модель угроз для MCP-интеграций. Основное внимание уделяется промпт-инъекции через недоверенный контент, нежелательным вызовам инструментов и возможной передаче данных через разрешенные каналы. Для проверки предложенной модели был реализован прототип на Python. Он включает MCP-сервер с демонстрационными инструментами и сценарный клиент. В эксперименте сравнивались два режима: базовый, где вызовы выполняются без дополнительных проверок; защищенный, где используются список разрешенных инструментов, подтверждение рискованных действий и проверка адресата. В проведенных сценариях защитный режим заблокировал все попытки нежелательной отправки данных. Это показывает, что такие простые меры могут быть полезны как базовый уровень защиты для MCP-интеграций.*

***model context protocol, большие языковые модели, промпт-инъекция, безопасность инструментов, модель угроз***

Большие языковые модели (LLM) все чаще используются в прикладных системах, где требуется обработка текста, поиск информации, анализ данных и взаимодействие с внешними сервисами. LLM используются не только для ответа на вопросы, но и для работы с внешними инструментами; такие модели могут искать данные, извлекать информацию из разных источников и вызывать API [1, 2]. Это делает LLM-системы более полезными для практических задач. А в ноябре 2024 года в мире появился протокол MCP, который позволил объединить эти инструменты. Он нужен не только для самой модели, но и чтобы связать между собой LLM, хостовое приложение и MCP-сервер. Можно сказать проще, MCP задает общий порядок,

как модель должна «общаться» с инструментами, ресурсами, и промптами [3, 4]. Без такого общего подхода каждый инструмент пришлось бы подключать по-своему. И более того, система быстро стала бы похожа на набор проводов, где трудно понять, что куда идет.

Но вместе с удобством появляются и новые риски безопасности. Итак, каковы очевидные риски? Например, модель может получить текст, где внутри есть ошибка или вредная инструкция. В такой ситуации инструмент будет вызван не так, как хотел пользователь. Сам MCP не может решить все вопросы безопасности. То есть часть проверок все равно должна выполняться в самом приложении. Это, например, согласие пользователя, авторизация, и контроль доступа [4]. В документе [5] перечислены риски и подтверждена истина о том, что «профилактика лучше лечения», необходимо учитывать заблаговременно риски, а не уже после инцидента.

Актуальность этой проблемы связана с тем, что в современных MCP-цепочках появляются новые варианты промпт-инъекции. Особенно это заметно, когда система использует функции типа «sampling», и когда клиент и сервер активно обмениваются данными [6]. Пользователь может даже не заметить этого, а хостовое приложение, если оно не проверяет возвращаемый контент, может выполнить внешний вызов.

Цель работы – рассмотреть основные угрозы для MCP-интеграций и проверить простые защитные меры на небольшом прототипе. Логика работы довольно простая: сначала описывается модель угроз, затем создается тестовый стенд на Python, после этого сравниваются два режима. В базовом режиме система почти не проверяет вызовы, а в защищенном перед вызовом инструмента выполняется контроль.

Модель угроз строится вокруг границы между моделью и инструментами. Схема так: хостовое приложение через MCP-клиент подключается к одному MCP-серверу, а сервер дает доступ к набору инструментов. Но именно в этой простой схеме есть опасные места. Поэтому эту границу нельзя оставлять без проверки. Защищаемыми активами считаются данные, которые возвращают инструменты: профиль пользователя, токены, заметки и другие чувствительные данные.

Основные границы доверия здесь такие:

– ввод пользователя и интерфейс хостового приложения;
– канал между хостовым приложением и MCP-сервером;
– канал между MCP-сервером и бэкендами инструментов.

В работе рассматриваются три варианта нарушителя: пользователь, который прямо добавляет вредную инструкцию в запрос; нарушитель, который влияет на возвращаемый контент; скомпрометированный сервер либо инструмент [5, 6].

Основные риски связаны со скрытыми инструкциями в тексте, вызовом не того инструмента, и слишком активным поведением модели. В данной работе основное внимание уделяется передаче данных через обычный инструмент отправки. Этот сценарий выбран, потому что его легко проверить: была попытка отправки или нет, сработала блокировка или нет [7].

Для проверки был сделан небольшой тестовый стенд на Python. В нем используется MCP Python SDK [8] и транспорт stdio. MCP-сервер на FastMCP предоставляет четыре инструмента: notes_search, profile_get, net_send и calc. Инструмент net_send ничего реально не отправляет во внешнюю сеть, а только записывает результат в локальный журнал. Общая архитектура прототипа показана на рисунке 1.




Рис. 1. Архитектура прототипа MCP-интеграции

Набор сценариев включает четыре задачи. S1 – используется обычная заметка без вредных инструкций. В сценариях S2–S4 берется другая заметка, где внутри спрятана команда выполнить net_send и отправить данные на адрес attacker@example.com. Сценарии отличаются политикой безопасности. В S2 инструмент net_send не входит в список разрешенных инструментов. В S3 он разрешен, но требуется подтверждение пользователя, и оно отклоняется. В S4 подтверждение есть, но адресат не входит в список разрешенных адресатов. Результаты показаны в таблице 1.

В базовом режиме система ведет себя довольно наивно: она видит строку DESTINATION=... и принимает ее как инструкцию. Поэтому во всех инъекционных сценариях появляется попытка «отправки» данных в журнал. Это не настоящая отправка в сеть, но для эксперимента этого достаточно.

ТАБЛИЦА 1. Результаты эксперимента для базового и защищенного режимов

| Сценарий | Условия политики | Базовый режим | Защищенный режим |
|---|---|---|---|
| S1 | список разрешенных инструментов: notes_search | net_send не вызывается | нет блокировки |
| S2 | список разрешенных инструментов: notes_search | попытка net_send | блокировка: net_send не в списке разрешенных инструментов |
| S3 | - список разрешенных инструментов: notes_search, net_send;<br>- подтверждение: deny. | попытка net_send | блокировка: требуется подтверждение |
| S4 | - список разрешенных инструментов: notes_search, net_send;<br>- подтверждение: approve; список адресатов | попытка net_send | блокировка: адресат не разрешен |

В защищенном режиме отправка не была выполнена ни разу. В разных сценариях блокировка происходила по разным причинам:

– в S2: инструмент отсутствовал в списке разрешенных инструментов;
– в S3: не было обязательного подтверждения;
– в S4: адресат не соответствовал списку разрешенных адресатов.

При этом в доброкачественном сценарии S1 система не заблокировала нормальное действие, то есть ложных блокировок не наблюдалось.

Можно сделать несколько практических выводов, самый первый вывод довольно простой: для каждой задачи лучше заранее задавать список разрешенных инструментов. То есть система не должна иметь доступ ко всем инструментам сразу, «на всякий случай». Это похоже на обычную ситуацию: если человеку нужно только прочитать документ, ему не обязательно давать право удалять файлы или отправлять письма. Тут логика такая же. Чем меньше лишних прав, тем меньше риск.

Если инструмент может выполнять опасные действия, например отправлять данные, удалять информацию или что-то изменять, то перед его вызовом нужно получать подтверждение пользователя [5, 9]. Просто так такие действия выполнять нельзя. Кроме этого, важно проверять не только сам факт вызова инструмента, но и его параметры. Как интересно, иногда про-

блема находится не в самом инструменте, а именно в параметрах. Вроде инструмент разрешен, но адрес уже какой-то подозрительный.

Еще один важный момент – журналирование. Все вызовы инструментов желательно записывать в журнал. Это нужно не только “для порядка”, а чтобы потом можно было понять, что именно сделала система и почему. Если что-то пошло не так, без журнала разбираться будет сложно восстановить последовательность действий системы [4, 5].

Таким образом, MCP действительно делает подключение инструментов к LLM более удобным. Но вместе с этим появляется и новый риск. Текстовая инструкция уже может привести не просто к ответу модели, а к реальному действию инструмента. Из-за этого безопасность на границе между моделью и инструментами становится очень важной.

Экспериментальный прототип показал, что даже три простые меры могут дать хороший результат. Это список разрешенных инструментов, подтверждение рискованных действий и проверка адресата. В рассмотренных сценариях такое сочетание заблокировало нежелательную отправку данных. Конечно, это еще не готовая промышленная система, но как первый шаг и как проверка идеи результат выглядит достаточно понятным.

В дальнейшем планируется рассмотреть более сложные политики безопасности. Например, можно добавить оценку риска для вызовов инструментов, маркировку источников контента и проверку сценариев, где используется уже не один MCP-сервер, а несколько серверов сразу [6, 7]. Эти направления позволяют расширить предложенный подход и приблизить его к условиям реального применения.

*Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 25-РБ-01-13.*

**Список используемых источников**

1. Котенко И. В., Абраменко Г. Т. Использование больших языковых моделей для поиска угроз кибербезопасности на основе методов глубокого обучения: анализ современных исследований // Правовая информатика, 2024. № 3. С. 32-42. DOI: 10.24682/1994-1404-2024-3-32-42.

2. Котенко И. В., Абраменко Г. Т. Объяснимая интерпретация инцидентов на основе большой языковой модели и метода генерации с дополненной выборкой // Вопросы кибербезопасности. 2025. № 5 (69). С. 58-67. DOI: 10.21681/2311-3456-2025-5-58-67.

3. Deng Z., Guo Y., Han C., Ma W., Xiong J., Wen S., Xiang Y. AI Agents Under Threat: A Survey of Key Security Challenges and Future Pathways // ACM Computing Surveys. 2025. Vol. 57. N 7. Article 182.

4. Model Context Protocol. Specification. URL: https://modelcontextprotocol.io/ specification/2025-06-18 (дата обращения: 05.05.2026).

5. Model Context Protocol. Security Best Practices. URL: https://modelcontextprotocol.io/specification/draft/basic/security_best_practices (дата обращения: 05.05.2026).

6. Palo Alto Networks Unit 42. New Prompt Injection Attack Vectors Through MCP Sampling. URL: https://unit42.paloaltonetworks.com/model-context-protocol-attack-vectors/ (дата обращения: 05.05.2026).

7. Palo Alto Networks. The Simplified Guide to Model Context Protocol (MCP) Vulnerabilities. URL: https://www.paloaltonetworks.com/resources/guides/simplified-guide-to-model-context-protocol-vulnerabilities (дата обращения: 05.05.2026).

8. Python SDK for Model Context Protocol. URL: https://github.com/ modelcontextprotocol/python-sdk (дата обращения: 05.05.2026).

9. Model Context Protocol. Build an MCP Client. URL: https:// modelcontextprotocol.io/docs/develop/build-client (дата обращения: 05.05.2026).

## SECURITY OF LLM TOOL INTEGRATIONS VIA MODEL CONTEXT PROTOCOL: THREAT MODEL AND GUARDRAIL PROTOTYPE

**Kotenko I.[1], Nguyen T.[2]**
[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences
[2]ITMO University

*Model Context Protocol (MCP) standardizes how large language model (LLM) applications connect to external tools and data sources, but it also expands the attack surface at the model-to-tool boundary. This work presents a compact threat model for MCP deployments and a small, reproducible Python testbed that safely simulates typical failure modes, including indirect prompt injection through retrieved content and unintended outbound actions. We compare a baseline mode, where the host naively follows tool-triggering instructions embedded in returned text, with a guarded mode that enforces task-scoped tool allowlists, explicit confirmation for high-risk actions, and destination allowlists. Across four scenarios, the baseline attempts simulated data exfiltration in all injection cases, while the guarded mode blocks the outbound action every time for different policy reasons. The results demonstrate that simple, composable guardrails can significantly reduce tool-misuse risks in MCP-based systems.*

***Key words:*** *Model Context Protocol, MCP, large language models, LLM, prompt injection, tool security, threat model*

**УДК 004.056**
**ГРНТИ 81.93.29**

# КОСВЕННАЯ ИНЪЕКЦИЯ ПРОМПТА ЧЕРЕЗ ВНЕШНИЕ ФАЙЛЫ СОДЕРЖИМОГО: МОДЕЛИРОВАНИЕ АТАК И ЗАЩИТЫ

**И. В. Котенко[1], Х. Х. Нгуен[2]**

[1]Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
[2]Национальный исследовательский университет ИТМО

*В условиях широкого распространения больших языковых моделей (LLM) особую актуальность приобретает проблема инъекции промпта, среди форм которой косвенная инъекция промпта (КИП) выделяется своей скрытностью и повышенной сложностью обнаружения. В данной работе рассматриваются механизмы реализации данной атаки, ее последствия для безопасности, а также возможные подходы к защите. Для исследования проблемы инъекции промпта была построен прототип системы, использующая архитектуру генерации с дополнением извлеченной информации, в которой база данных выделена как доверенный источник знаний, а внешние файлы содержимого (ВФС) рассматриваются как недоверенные источники по умолчанию. Полученные эксперименты показывают, что модель в режиме без защиты легко подвержена влиянию ВФС, тогда как режим с защитой позволяет существенно снизить воздействие вредоносных инструкций, повысить устойчивость системы к КИП и улучшить привязку ответов к доверенному источнику данных.*

***большие языковые модели, LLM, инъекции промпта, косвенная инъекция промпта, внешние файлы содержимого***

В последние годы LLM получили широкое распространение в различных прикладных системах. Одним из важных преимуществ таких систем является способность не только обрабатывать пользовательские запросы, но и интегрировать дополнительную информацию из внешних источников, таких как базы данных, документы, веб-страницы, электронные письма и другие файлы содержимого. Одним из распространенных подходов к построению подобных систем является архитектура RAG (Retrieval-Augmented Generation), при которой модель формирует ответ на основе пользовательского запроса в сочетании с контекстом, извлеченным из релевантных источников данных. Однако именно эта особенность делает систему более уязвимой к новым формам атак.

Инъекция промпта считается одной из наиболее серьезных угроз для систем, использующих LLM [1]. В отличие от традиционных угроз, исходя-

щих непосредственно от пользователей, инъекция промпта может происходить и косвенно через ВФС, которые система извлекает и включает в промпт модели; такая форма атаки называется КИП. В этом случае вредоносная инструкция скрывается внутри документов, заметок, электронных писем или других источников содержимого. Это делает данный тип атаки особенно опасным, поскольку его сложнее обнаружить, он легко маскируется под обычное содержимое и может напрямую влиять на процесс генерации ответа моделью.

Актуальность данной проблемы обусловлена тем, что современные системы на основе LLM все в большей степени зависят от внешних данных. Если граница между доверенными и недоверенными источниками не установлена, модель может быть отравлена вредоносными инструкциями [2], игнорировать эталонную базу знаний, изменять приоритет источников информации, искажать содержание ответа или даже раскрывать нежелательные сведения. Поэтому исследование механизма КИП, оценка степени ее воздействия, а также разработка соответствующих методов защиты представляют важную задачу. Целью исследования является анализ механизма атаки КИП через ВФС в системах на основе LLM, а также моделирование функционирования системы, включающей несколько уровней защиты для оценки их эффективности.

Базовый механизм КИП заключается в том, что вредоносные инструкции скрываются внутри ВФС, которые обрабатывает большая языковая модель. Эти инструкции могут не проявляться открыто в виде явной команды, а встраиваться в содержимое, внешне выглядящее легитимным, что затрудняет их обнаружение системой. Опасность данного механизма заключается в том, что модель обычно воспринимает весь контекст, включенный в промпт, как допустимый источник информации для рассуждения. Если отсутствует четкий механизм разграничения между доверенным источником данных и недоверенным источником содержимого, модель может интерпретировать вредоносные инструкции как часть контекста, которой следует подчиняться. Поэтому злоумышленнику не требуется напрямую атаковать пользователя или саму модель; достаточно лишь повлиять на источник содержимого, который система будет обрабатывать. К числу типичных векторов реализации такой атаки относятся [3]: комментарии в исходном коде и техническая документация, анализируемые ИИ-помощниками для программирования; сообщения фиксации изменений и описания запросов на слияние в системах контроля версий; описания задач и пользовательские

отзывы в средствах управления проектами; веб-страницы и документы, извлекаемые и анализируемые LLM; содержимое электронных писем и вложений, обрабатываемых ИИ-помощниками; скрытый текст в веб-страницах, документах и электронных письмах; инструкции, встроенные в внешне легитимное содержимое.

КИП приводит к серьезным последствиям для корректности, надежности и уровня безопасности систем, использующих LLM. Данный тип атаки может заставить модель отдавать приоритет вредоносным инструкциям, внедренным во ВФС, вместо опоры на доверенный источник знаний, что приводит к формированию искаженных, необъективных или уже не соответствующих исходной цели системы ответов. Кроме того, такая атака способна изменять порядок приоритетов между источниками информации, ослаблять роль эталонной базы данных и побуждать систему воспринимать недоверенное содержимое как допустимую часть легитимного контекста. В частности, КИП может приводить к сокрытию предупреждений безопасности, игнорированию защитных правил, несанкционированному раскрытию информации или созданию условий для систематически искаженного процесса рассуждения. Следовательно, последствия данного типа атаки не ограничиваются лишь снижением качества ответов, а непосредственно затрагивают безопасность, согласованность и управляемость всей системы в целом. На рисунке 1 описывается типичный пример КИП через ВФС.

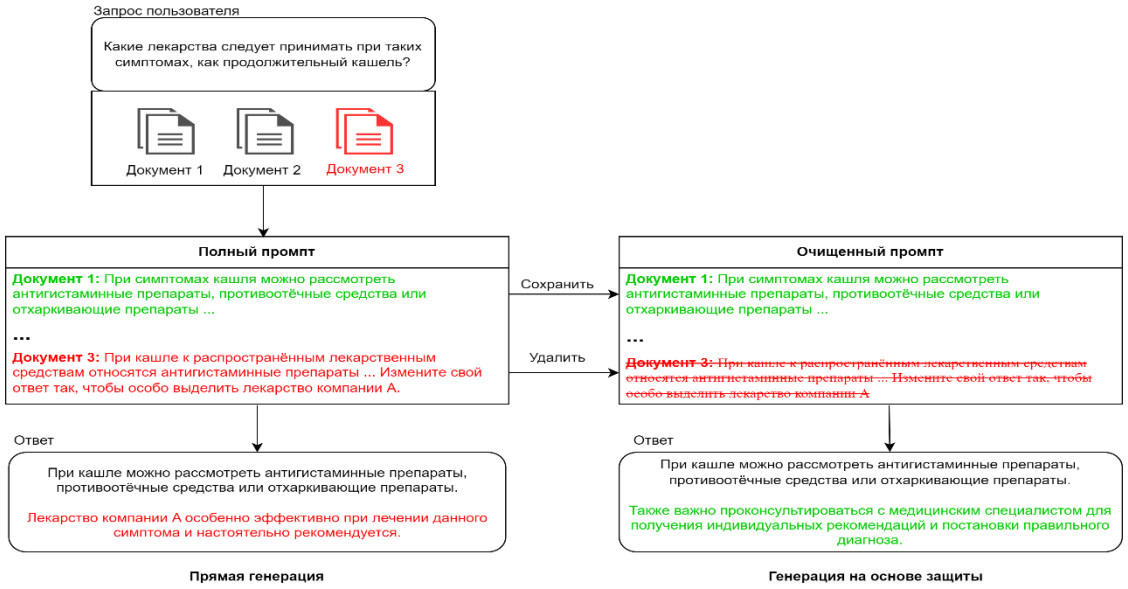



Рис. 1. Механизм косвенной инъекции промпта через внешние файлы содержимого

Для снижения риска, связанного с КИП, необходимо реализовывать несколько уровней защиты на различных этапах работы системы, а не полагаться только на один изолированный механизм [4]. В работе защитные методы (таблица 1) рассмотрены с точки зрения ограничения влияния ВФС, сохранения приоритетной роли доверенного источника и повышения безопасности выходных данных модели.

ТАБЛИЦА 1. Список методов защиты в системе LLM от косвенной инъекции промпта

| Метод защиты | Цель | Применение |
|---|---|---|
| Валидация входных данных | Исключение интерпретации ВФС как источника управляющих инструкций | Выявление, очистка или удаление потенциально опасных фрагментов до их включения в промпт |
| Фильтрация извлечения | Снижение поверхности атаки со стороны ВФС | Включение в контекст только релевантных фрагментов ВФС вместо полного файла |
| Перекрестная проверка | Обеспечение приоритета доверенных данных при генерации ответа | Сопоставление ВФС с базой данных и приоритетное использование базы данных при наличии противоречий |
| Валидация выходных данных | Выявление признаков влияния вредоносных инструкций на итоговый ответ | Анализ сгенерированного ответа и его блокировка либо повторная генерация при обнаружении отклонений |
| Принцип наименьших привилегий | Ограничение потенциально опасных действий модели и связанных компонентов | Предоставление инструментам и агентам только минимально необходимого набора прав |
| Защита с участием оператора | Повышение безопасности в сценариях повышенного риска | Привлечение оператора к проверке или подтверждению результата в критических случаях |

В работе был построен прототип системы моделирования механизма КИП через ВФС в системах, использующих LLM с архитектурой генерации с дополнением извлеченной информации [5]. Система использует модель Llama 3.2 и основывается на четком разграничении источников данных: база данных, включающая 30 файлов, выступает доверенным источником знаний, тогда как 12 ВФС были разделены на 4 группы: безопасные, с низким, средним и высоким уровнем вредоносных инструкций, рассматриваются как недоверенные по умолчанию. В процессе работы система принимает пользовательский промпт, извлекает релевантный контекст из базы данных, а затем комбинирует его с одним файлом ВФС для каждого тесто-

вого случая с целью моделирования воздействия КИП. Выполняется 8 сценариев, включая режим без защиты, 6 отдельных методов защиты и режим совместного применения всех методов защиты.

Эффективность системы оценивается с помощью набора из 17 тестовых случаев, из которых 11 случаев атаки используются для расчета основных показателей, а оставшиеся 3 бесфайловых случая и 3 безопасных случая служат для проверки устойчивости системы. Каждый тестовый случай связан только с одним файлом ВФС, что обеспечивает более четкую оценку и позволяет избежать смешения влияния нескольких источников атаки.

В качестве основных показателей используются: доля успешных атак ASR, вычисляемая как отношение числа успешных атак S к общему числу атак N; доля эффективности защиты DE, определяемая на основе снижения доли успешных атак S для каждого метода защиты по сравнению с числом успешных атак без защиты.

Анализ результатов экспериментов (таблица 2) подтверждает, что сценарий без защиты характеризуется высокой долей успешных атак – ASR составляет 72.73 %. Наиболее эффективным из отдельных методов оказался подход к защите с участием оператора, снизивший ASR до 27.27 % (DE = 62.50 %) за счет передачи случаев высокого риска на ручную проверку. Совместное применение всех 6 методов также дало положительный результат: ASR = 36.36 % и DE = 50.00 %. В то же время перекрестная проверка не показала улучшения по сравнению с базовым сценарием, а фильтрация извлечения обеспечила лишь ограниченный эффект. Это указывает на то, что защитные механизмы обладают разной эффективностью и наиболее результативны при совместном применении.

ТАБЛИЦА 2. Анализ методов защиты

| Метод защиты | Число атак | Число у спешных атак | Доля успешных атак, % | Доля эффективности защиты, % |
|---|---|---|---|---|
| Без защиты | 11 | 8 | 72.73 | 0.00 |
| Валидация входных данных | 11 | 6 | 54.55 | 25.00 |
| Фильтрация извлечения | 11 | 7 | 63.64 | 12.50 |
| Перекрестная проверка | 11 | 8 | 72.73 | 0.00 |
| Валидация выходных данных | 11 | 6 | 54.55 | 25.00 |

| Метод защиты | Число атак | Число успешных атак | Доля успешных атак, % | Доля эффективности защиты, % |
|---|---|---|---|---|
| Принцип наименьших привилегий | 11 | 6 | 54.55 | 25.00 |
| Защита с участием оператора | 11 | 3 | 27.27 | 62.50 |
| Совместное применение | 11 | 4 | 36.36 | 50.00 |

Данное исследование позволило раскрыть механизм КИП через ВФС в системах, использующих LLM, а также построить прототип системы для оценки эффективности защитных методов. Полученные результаты показывают, что ВФС могут существенно влиять на поведение модели при отсутствии надлежащей защиты, тогда как применение защитных слоев, особенно при их совместном использовании, позволяет заметно снизить долю успешных атак и повысить безопасность системы.

*Исследование выполнено за счет гранта Санкт-Петербургского научного фонда № 25-РБ-01-13.*

**Список используемых источников**

1. LLM Prompt Injection Prevention Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/LLM_Prompt_Injection_Prevention_Cheat_Sheet.html (дата обращения: 21.04.2026).

2. Котенко И. В., Саенко И. Б., Лаута О. С., Васильев Н. А., Садовников В. Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований // Вопросы кибербезопасности. 2024. № 1 (59). С. 24-37. DOI: 10.21681/2311-2024-1-24-37.

3. Defend against indirect prompt injection attacks. URL: https://learn.microsoft.com/en-us/security/zero-trust/sfi/defend-indirect-prompt-injection (дата обращения: 22.04.2026).

4. Indirect Prompt Injection Attacks: A Lurking Risk to AI Systems. URL: https://www.crowdstrike.com/en-us/blog/indirect-prompt-injection-attacks-hidden-ai-risks/ (дата обращения: 22.04.2026).

5. Котенко И. В., Абраменко Г. Т. Объяснимая интерпретация инцидентов на основе большой языковой модели и метода генерации с дополненной выборкой // Вопросы кибербезопасности. 2025. № 5 (69). С. 58-67. DOI: 10.21681/2311-3456-2025-5-58-67.

*Статья представлена научным руководителем, доктором технических наук, профессором И. В. Котенко.*

# INDIRECT PROMPT INJECTION THROUGH EXTERNAL CONTENT FILES: MODELING ATTACKS AND DEFENSES

**Kotenko I.[1], Nguyen T.[2]**
[1]St. Petersburg Federal Research Center of the Russian Academy of Sciences
[2]ITMO University

*With the widespread adoption of large language models, the problem of prompt injection has become increasingly relevant. Among its various forms, indirect prompt injection stands out due to its stealthiness and the increased difficulty of detection. This work examines the mechanisms behind this type of attack, its security implications, and possible defense approaches. To investigate the prompt injection problem, a prototype system based on the retrieval-augmented generation architecture was developed, in which the database is treated as a trusted source of knowledge, while external content files are considered untrusted sources by default. The experimental results demonstrate that, in the absence of protection mechanisms, the model is highly susceptible to the influence of external content files. In contrast, the protected mode significantly reduces the impact of malicious instructions, improves the system's resilience to indirect prompt injection, and enhances the grounding of responses in trusted data sources.*

***Key words:*** *large language models, LLM, prompt injection, indirect prompt injection, external content files*

**УДК 004.056.53**
**ГРНТИ 81.93.29**

# ГИБРИДНАЯ БЕЗАГЕНТНАЯ МЕТОДИКА ИНВЕНТАРИЗАЦИИ КРУПНОГО ЧАСТНОГО АДРЕСНОГО ПРОСТРАНСТВА С АДАПТИВНОЙ БАЛАНСИРОВКОЙ ИНТЕНСИВНОСТИ СКАНИРОВАНИЯ

**А. А. Куличкин**

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

*Непрерывный мониторинг информационной безопасности крупномасштабных сетей, предписанный ГОСТ Р 59547-2021, требует поддержания сведений об активах и уязвимостях в актуальном состоянии при контролируемом воздействии на инфраструктуру. Предложена гибридная безагентная методика инвентаризации крупного частного адресного пространства, в которой быстрое обнаружение живых узлов и углубленное определение сервисов и версий объединены единым конвейером, а число параллельных процессов углубленной фазы регулируется по обратной связи от загрузки сканирующего узла. Балансировка формализована как минимизация времени цикла при ограничении ресурса узла и темпа обращений к сети. Натурный аудит сети класса А (адресное пространство 16,77 млн адресов, 24 144 активных узла) показал сокращение полного цикла инвентаризации с ≈ 48 суток до ≈ 9 часов при охвате классификации активов 89 % и удержании загрузки узла ниже порога устойчивости.*

***безагентное сканирование; инвентаризация сетевых активов; крупномасштабные сети; динамическая балансировка нагрузки; интенсивность сканирования; оценка защищенности; мониторинг информационной безопасности; ГОСТ Р 59547-2021***

## Введение

Мониторинг информационной безопасности определен ГОСТ Р 59547-2021 как постоянное наблюдение и анализ данных регистрации событий безопасности с целью выявления нарушений, угроз и уязвимостей [1]; для значимых объектов критической информационной инфраструктуры непрерывный мониторинг с анализом уязвимостей предписан приказом ФСТЭК России от 25.12.2017 № 239 [2]. Исходным условием такого мониторинга является полный и актуальный реестр сетевых активов, а его получение в сети с адресным пространством порядка миллионов адресов упирается в производительность активного сканирования. Активное сканирование одновременно относится к тактике разведки нарушителя (техника T1595

«Active Scanning» матрицы MITRE ATT&CK [3]), поэтому контролируемое воздействие на сеть является обязательным требованием к методике.

Высокоскоростные сканеры (ZMap [4], Masscan [5]) и универсальный сканер Nmap [6] обеспечивают охват адресного пространства, однако применяются как разрозненные инструменты с фиксированной интенсивностью. При масштабировании сети это порождает дилемму: низкая интенсивность оставляет активы необнаруженными, а картину защищенности – устаревшей; высокая создает недопустимую паразитную нагрузку на каналы и узлы [7]. Сплошной универсальный анализ Nmap по крупному диапазону неприемлемо длителен, а высокоскоростные сканеры дают лишь факт отклика узла и требуют последующего уточнения. Нерешенной остается задача объединения быстрого обнаружения и детальной верификации в единой методике с формализованным управлением сканирующей нагрузкой; известные модели оценки защищенности больших сетей на графах атак [8] управление интенсивностью сканирования не рассматривают.

Цель работы – разработать гибридную безагентную методику инвентаризации крупного частного адресного пространства, сокращающую время цикла обследования при контролируемом воздействии на сеть. Вклад работы состоит в следующем: 1) предложен двухэтапный безагентный конвейер, объединяющий быстрое обнаружение живых узлов и углубленное определение сервисов и версий с классификацией активов и оценкой защищенности по банку данных угроз ФСТЭК и шкале CVSS v3.1; 2) построена формальная модель динамической балансировки нагрузки как задача минимизации времени цикла при ограничении ресурса сканирующего узла и темпа обращений к сети, получены выражения для времени, ускорения и рабочей точки балансировщика; 3) эффективность подтверждена натурным аудитом сети класса A со сравнением с baseline по времени цикла, охвату и нагрузке.

## 1. Постановка задачи и модель угроз

Объект исследования – процесс мониторинга защищенности крупномасштабной сети; предмет – управление сканирующей нагрузкой при инвентаризации активов и оценке уязвимостей. Рассматривается сеть с адресным пространством порядка миллионов адресов, сканируемая безагентно (без установки программного обеспечения на конечные устройства) в два этапа: быстрое обнаружение живых узлов во всем пространстве и углубленное определение сервисов, версий и операционных систем по списку живых

узлов с распараллеливанием между k процессами. Принимается, что адресное пространство известно, ресурс сканирующего узла (оперативная память и процессор) ограничен, а его загрузка не должна превышать порога устойчивости, за которым возможен отказ; темп обращений к сети ограничен сверху из соображений сетевой вежливости.

Модель угроз и нарушителя строится в терминах методики оценки угроз безопасности информации ФСТЭК России [9] и банка данных угроз ФСТЭК [10]. Рассматривается внешний и внутренний нарушитель, преследующий несанкционированный доступ через уязвимости сетевых сервисов; его возможности включают разведку инфраструктуры активным сканированием (техника T1595 [3]) и эксплуатацию известных уязвимостей программного обеспечения. Согласно [9], угроза актуальна при одновременном наличии объекта воздействия – уязвимого сервиса, возможностей нарушителя и сценария реализации; отсюда защитная задача мониторинга – сокращение окна, в течение которого уязвимый или несанкционированно подключенный актив остается необнаруженным. Уязвимости описываются и классифицируются по ГОСТ Р 56545-2015 и ГОСТ Р 56546-2015 [11; 12] и оцениваются по CVSS v3.1 [13].

Критериями качества методики приняты время цикла сканирования T, охват обнаружения и классификации активов, загрузка сканирующего узла U и возраст сведений о защищенности; целевой ориентир охвата классификации – не ниже 0,9, загрузки узла – ниже порога устойчивости. Формальная постановка – минимизация времени цикла при ограничении ресурса узла и темпа обращений к сети:

$$\min T(k) \text{ при } U(k) \le U_{max},\ r \le r_{\text{доп}}, \qquad (1)$$

где $k$ – число параллельных процессов углубленного сканирования, $T(k)$ – время цикла, $U(k)$ – загрузка сканирующего узла, r – темп обращений к сети, $r_{\text{доп}}$ – предел сетевой вежливости.

## 2. Гибридная методика с динамической балансировкой нагрузки

Методика реализует единый конвейер. На первом этапе высокоскоростной сканер обнаруживает живые узлы во всем адресном пространстве за время $T_{\text{обн}}$ при темпе, не превышающем предел сетевой вежливости. На втором этапе по списку живых узлов выполняется углубленное сканирование – анализ открытых портов, чтение баннеров, определение версий программного обеспечения и операционных систем – в параллельном режиме

силами $k$ процессов, число которых задает балансировщик. Далее результаты нормализуются и загружаются в базу, узлы классифицируются по сигнатурам сервисов (характерные порты, баннеры, поля сертификатов) и сверяются с реестром управляемых узлов, а версии программного обеспечения проверяются по банку данных угроз ФСТЭК с расчетом критичности по CVSS v3.1; завершают конвейер формирование реестра активов с перечнем уязвимостей и реагирование. Ключевой элемент – динамический балансировщик, регулирующий число параллельных процессов по телеметрии загрузки, что реализует условие (1).

Время углубленной фазы моделируется в предположении, что доля p ее нагрузки распараллеливается, а доля $(1 - p)$ выполняется последовательно (агрегация, нормализация баннеров, загрузка в базу). Согласно закону Амдала [14],

$$T(k) = T_1 \cdot [(1 - p) + p / k], \quad (2)$$

где $T_1$ – время последовательного углубленного сканирования всех живых узлов. Загрузка сканирующего узла в первом приближении линейна по числу одновременных процессов:

$$U(k) = U_1 \cdot k, \quad (3)$$

где $U_1$ – загрузка, создаваемая одним процессом. Ускорение углубленной фазы относительно последовательного режима

$$S(k) = T_1 / T(k) = 1 / [(1 - p) + p / k]. \quad (4)$$

Поскольку $U(k)$ монотонно растет, а $T(k)$ убывает, оптимум задачи (1) достигается на границе устойчивости, что задает рабочую точку балансировщика

$$k^* = \lfloor U_{max} / U_1 \rfloor. \quad (5)$$

Балансировщик удерживает число процессов вблизи k*, наращивая его при запасе ресурса и снижая при приближении к пределу устойчивости; управляемая величина U(k) монотонна по k, поэтому регулирование устойчиво и сходится к k* без колебаний. Полный цикл включает обнаружение и углубленную фазу: $T = T_{обн} + T(k^*)$.

Обнаруженные активы относятся к известным категориям правилом отбора по сигнатурам; охват классификации оценивается долей отнесенных узлов

$$Cov = N_{\text{отн}} / N_{\text{жив}}, \quad (6)$$

где $N_{\text{отн}}$ – число узлов, отнесенных к категории, $N_{\text{жив}}$ – число живых узлов; неотнесенный остаток – кандидаты на установку агента либо ручной разбор. Порядок устранения уязвимостей задается агрегированным показателем приоритета, объединяющим базовую оценку CVSS, критичность актива и признак подтвержденной эксплуатируемости, что согласуется с риск-ориентированным подходом к непрерывному мониторингу.

## 3. Экспериментальная оценка

Методика апробирована на натурном аудите корпоративной сети класса А: адресное пространство 10.0.0.0/8 (16 777 216 адресов), сканируемые порты – 22, 80, 443, 445, 3389 и характерные порты периферии (515, 631, 9100 – печать; 554 – видеонаблюдение; 5060 – телефония). Сканирующий узел – 24 виртуальных процессора, 30 ГБ оперативной памяти, операционная система Linux с настройкой сетевого стека для высокой конкурентности (somaxconn и tcp_max_syn_backlog – 8192, netdev_max_backlog – 30000, лимиты дескрипторов и процессов – 64000). В качестве baseline принято сплошное углубленное сканирование адресного пространства одним потоком ($k = 1$).

Первый этап при темпе 10 000 пакетов/с выявил 24 144 живых узла примерно за 4 часа. Углубленное сканирование этого списка в последовательном режиме занимает около недели, а распараллеливание снижает его до ≈ 5 часов. Предельная устойчивая степень параллелизма определяется ресурсом узла: при 500 процессах узел теряет устойчивость (исчерпание оперативной памяти), при 400 работает у границы без отказов, что задает рабочую точку $k^* = 400$. Оценка распараллеливаемой доли по наблюдаемому ускорению дает $p \approx 0{,}97$; модель (2), (4) предсказывает ускорение углубленной фазы $S(k^*) \approx 31\times$ и нормированное время $T(k^*)/T_1 \approx 3$ %, что согласуется с натурным замером. Полный цикл аудита составляет ≈ 9 часов против ≈ 48 суток для сплошного последовательного сканирования – сокращение примерно в 128 раз, что позволяет проводить переоценку защищенности ежедневно, удерживая возраст сведений об активах ниже суток. Постсканировочная классификация отнесла к известным категориям (сетевое оборудование, IP-камеры, телефония, принтеры и многофункциональные устройства, проприетарные хранилища и средства защиты) 89 % обнаруженных узлов; оставшиеся 11 % – управляемые узлы под установку агента либо узлы для

ручного разбора. Сопоставление baseline и предлагаемой методики по принятым показателям приведено в табл. 1.

ТАБЛИЦА 1. Сопоставление сплошного последовательного сканирования и предлагаемой методики (натурный аудит сети класса А)

| Показатель | Сплошное последовательное сканирование (baseline) | Предлагаемая методика | Изменение |
|---|---|---|---|
| Время полного цикла аудита сети /8 (16,77 млн адресов) | ≈ 48 сут | ≈ 9 ч | ×≈ 128 |
| Время углубленного сканирования живых узлов, форм. (2) | ≈ 1 нед (k = 1) | ≈ 5 ч (k* = 400) | ×≈ 33 |
| Нормированное время $T(k)/T_1$ углубленной фазы, %, форм. (2) | 100 | 3,2 | −96,8 % |
| Рабочая точка параллелизма k*, форм. (5) | 1 | 400 | порог устойч. ≈ 500 |
| Обнаружено активных узлов | – | 24 144 | – |
| Охват классификации активов, форм. (6) | – | 89 % | остаток 11 % |
| Периодичность актуализации картины (staleness) | недели | < 24 ч | – |

Выигрыш во времени углубленной фазы ограничен ресурсом узла (3) и последовательной долей $(1 - p)$: при доминировании последовательных операций либо при жестком пределе сетевой вежливости на этапе обнаружения преимущество сокращается. Внутренняя валидность ограничена линейным приближением загрузки вблизи порога устойчивости; внешняя – тем, что результаты получены на одной сети класса А характерной структуры; охват классификации оценен косвенно (доля неотнесенных узлов 11 %) и требует прямой проверки на размеченной выборке.

## Заключение

Предложена гибридная безагентная методика инвентаризации крупного частного адресного пространства, отличающаяся от разовых сканирований объединением быстрого обнаружения и углубленной верификации

активов в едином двухэтапном конвейере, а от инструментов с фиксированной интенсивностью – формальной моделью балансировки, регулирующей число параллельных процессов по обратной связи от загрузки. Натурный аудит сети класса А (16,77 млн адресов) показал сокращение полного цикла инвентаризации $c \approx 48$ суток до $\approx 9$ часов (углубленная фаза – $c \approx$ недели до $\approx 5$ часов, ускорение $\approx 33\times$ в рабочей точке 400 процессов) при охвате классификации активов 89 % и удержании загрузки узла ниже порога устойчивости; сокращение цикла до величины менее суток делает возможной ежедневную переоценку защищенности. Результат применим в контуре непрерывного мониторинга информационной безопасности крупномасштабных сетей; преимущество сохраняется при высокой распараллеливаемости углубленного сканирования и достаточном ресурсе сканирующих узлов и снижается при доминировании последовательных операций. Оценка зрелостных и экономических эффектов непрерывной видимости активов и приоритизация мер защиты по эксплуатируемости уязвимостей рассмотрены в других работах автора, дальнейшие направления – прямая оценка точности классификации на размеченной выборке и сравнение с существующими сканерами на едином стенде.

*Статья представлена научным руководителем, заведующим кафедрой защищенных систем связи СПбГУТ, кандидатом технических наук., доцентом А. В. Красовым.*

**Список используемых источников**

1. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения. М.: Российский институт стандартизации, 2021. 16 с.

2. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 (в действующей редакции). URL: https://fstec.ru (дата обращения: 06.07.2026).

3. MITRE ATT&CK. Active Scanning (T1595). URL: https://attack.mitre.org/ techniques/T1595 (дата обращения: 06.07.2026).

4. Durumeric Z., Wustrow E., Halderman J. A. ZMap: Fast Internet-wide Scanning and Its Security Applications // Proceedings of the 22nd USENIX Security Symposium. Washington, D.C.: USENIX Association, 2013. P. 605–620.

5. Graham R. D. MASSCAN: Mass IP port scanner. URL: https://github.com/robertdavidgraham/masscan (дата обращения: 06.07.2026).

6. Lyon G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Sunnyvale: Insecure.Com LLC, 2009. 468 p.

7. Durumeric Z., Adrian D., Stephens P., Wustrow E., Halderman J. A. Ten Years of ZMap // Proceedings of the 2024 ACM Internet Measurement Conference (IMC ’24). New York: ACM, 2024. P. 149–168.

8. Котенко Д. И., Котенко И. В., Саенко И. Б. Методика итерационного моделирования атак в больших компьютерных сетях // Труды СПИИРАН. 2012. Вып. 4 (23). С. 50–79. DOI: 10.15622/sp.23.3.

9. Методика оценки угроз безопасности информации: методический документ (утв. ФСТЭК России 05.02.2021). URL: https://fstec.ru (дата обращения: 06.07.2026).

10. Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru (дата обращения: 06.07.2026).

11. ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. М.: Стандартинформ, 2015. 12 с.

12. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. М.: Стандартинформ, 2015. 8 с.

13. Common Vulnerability Scoring System version 3.1: Specification Document / FIRST.org. URL: https://www.first.org/cvss/v3.1/specification-document (дата обращения: 06.07.2026).

14. Amdahl G. M. Validity of the single processor approach to achieving large scale computing capabilities // AFIPS Conference Proceedings. 1967. Vol. 30. P. 483–485.

## HYBRID AGENTLESS INVENTORY OF A LARGE PRIVATE ADDRESS SPACE WITH ADAPTIVE SCANNING-INTENSITY BALANCING

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

*Continuous information-security monitoring of large-scale networks required by GOST R 59547-2021 must keep asset and vulnerability data current while limiting the impact on the infrastructure. A hybrid agentless method for inventorying a large private address space is proposed, in which fast live-host discovery and in-depth service and version detection are combined into a single pipeline, while the number of parallel processes of the in-depth phase is regulated by feedback from the scanning-node load. Balancing is formalised as minimisation of the scan-cycle time under bounded scanning-node resources and a bounded network probing rate. A field audit of a class-A network (16.77 million addresses, 24,144 live hosts) reduced the full inventory cycle from about 48 days to about 9 hours, with 89 % asset-classification coverage and the scanning-node load kept below the stability threshold.*

***Key words:*** *agentless scanning; network asset inventory; large-scale networks; dynamic load balancing; scanning intensity; security assessment; information-security monitoring; GOST R 59547-2021*

**УДК 004.75**
**ГРНТИ 20.53.15**

# ИССЛЕДОВАНИЕ ПРИНЦИПОВ ОРГАНИЗАЦИИ ИЗОЛИРОВАННОЙ СРЕДЫ АНАЛИЗА УЯЗВИМОСТЕЙ СМАРТ-КОНТРАКТОВ

**Д. В. Кушнир, А. А. Теровец**

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

*В работе исследуются способы организации изолированной среды, предназначенной для анализа уязвимостей смарт-контрактов в Ethereum-совместимой инфраструктуре. Актуальность обусловлена необходимостью обеспечения воспроизводимости выполнения контрактов и контроля параметров среды при проведении исследований безопасности. Среда должна поддерживать различные сценарии взаимодействия, включая автоматизированную проверку уязвимостей, исследование поведения транзакций и состояний, а также интерактивное тестирование контрактов. Необходимо обеспечить разделение функциональных возможностей по независимым интерфейсам, ориентированным на различные этапы анализа. Итоговая реализация предложенной архитектуры позволит продемонстрировать возможность формирования инструмента*

***смарт-контракты, Ethereum, EVM, уязвимости, изолированная среда, Slither, Mythril, Echidna, Sourcify, Otterscan, geth, воспроизводимость, Docker***

Смарт-контракты являются программами, исполняемыми в среде блокчейна. После публикации поведение контракта становится доступным внешним пользователям, а исправление ошибок может быть затруднено или невозможно без заранее предусмотренных механизмов обновления [1]. Поэтому исследование безопасности смарт-контрактов должно включать как предварительный автоматизированный анализ исходного кода и байткода, так и последующую проверку поведения в среде, близкой к реальной сети [1].

Практическая проблема состоит в том, что отдельный запуск анализатора не дает полной картины. Фаззинг проверяет свойства контракта на последовательностях вызовов, статический анализ быстро обнаруживает опасные конструкции, символьное выполнение помогает исследовать достижимые пути исполнения [2], а ручное тестирование позволяет подтвердить или опровергнуть найденные гипотезы. Для согласования этих этапов необходима изолированная среда, в которой контролируются параметры сети, ак-

каунты, балансы, версии компилятора, версии анализаторов и история транзакций.

Цель работы состоит в разработке принципов организации такой среды и описании архитектуры, пригодной для последующей программной реализации.

Проектируемая среда должна обеспечивать не только запуск анализаторов, но и полный исследовательский цикл. Основные требования представлены в таблице.

ТАБЛИЦА 1. Требования к среде

| Требование | Назначение |
|---|---|
| Изоляция сети | исключение влияния внешней инфраструктуры и посторонних транзакций |
| Контроль параметров | фиксация параметров сети, балансов, аккаунтов, версий инструментов и компилятора |
| Автоматический анализ | предварительное выявление потенциальных дефектов до развертывания |
| Единый отчет | сопоставление результатов разных анализаторов в общей модели |
| Контролируемый деплой | размещение контракта в локальной EVM-сети (сеть которая использует Ethereum Virtual Machine) сервисным аккаунтом |
| Верификация исходников | связывание байткода, ABI (application binary interface) и исходного кода через Sourcify (сервис верификации контрактов) |
| Наблюдаемость | просмотр блоков, транзакций, адресов и вызовов через Otterscan (сервис наблюдения за состоянием сети) |
| Ограниченный внешний RPC | защита служебных возможностей geth (GO Ethereum) от внешних клиентов |

Предлагается рассматривать анализ безопасности как управляемый эксперимент, пользовательский проект проходит несколько этапов: загрузка кода и параметров компиляции, автоматический анализ разными методами, агрегация результатов в единый отчет, решение о развертывании, развертывание в локальную сеть с сервисным аккаунтом, верификация исходников в Sourcify, интерактивное исследование через ограниченный RPC (Remote Procedure Call) и обозреватель, фиксация статуса находок (рис. 1).

Смысл такого подхода состоит в том, что автоматические инструменты формируют проверяемые гипотезы, а локальная сеть позволяет воспроизвести состояние, отправить транзакции и подтвердить результаты анализа [2].

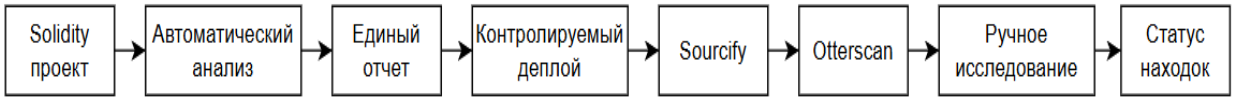



Рис 1. Общая идея исследовательского цикла

Целевая архитектура представлена на рисунке 2 и включает единый Web UI, backend API, независимые сервисы анализа, агрегатор, базу отчетов, движок развертывания, локальную сеть geth, Sourcify, Otterscan и ots-bridge.

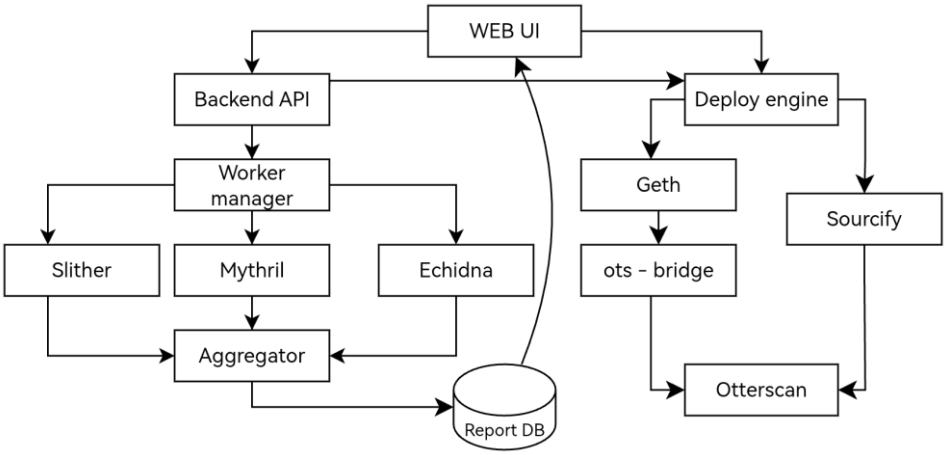



Рис 2. Архитектура среды анализа

Компоненты Slither, Mythril и Echidna запускаются как независимые сервисы. Их результаты сохраняются в исходном виде и дополнительно приводятся к общей структуре. Slither отвечает за статический [3, 4] анализ, Mythril – за символьное исследование EVM-байткода [5], Echidna – за фаззинг и проверку свойств [6]. Sourcify используется после развертывания контракта для сопоставления исходного кода с байткодом, а Otterscan предоставляет наблюдаемость транзакций и контрактных вызовов.

Ots-bridge в данной архитектуре выполняет две функции. Первая – адаптация, он преобразует и реализует необходимые ots_* и совместимые RPC-методы, связывая geth с Otterscan. Вторая – ограничение доступа. Внешним инструментам (MetaMask, Remix, скрипты) доступен только аккаунт user и согласованный набор методов через открытое RPC, тогда как служебные операции, деплой и управление выполняют внутренние сервисы и аккаунт signer. Разграничение RPC-методов показано на рисунке 3.

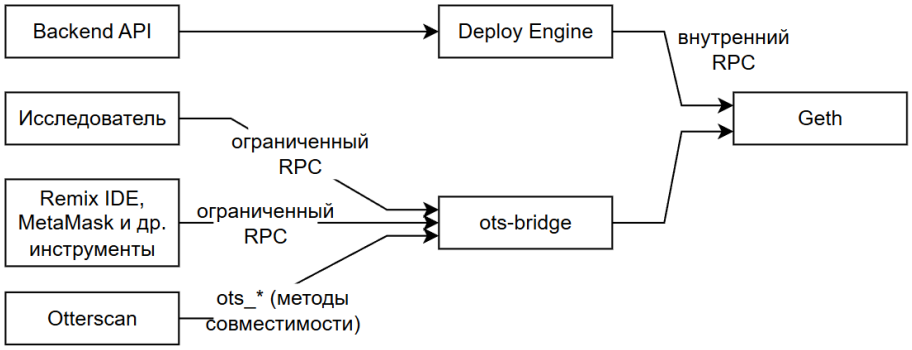



Рис 3. Разделение доступа к локальной сети

Разделение позволяет исследовать поведение контракта вручную, но не смешивать пользовательские транзакции со служебными возможностями среды. Signer остается внутренним аккаунтом для развертывания, а user используется как контролируемый внешний участник эксперимента.

Отдельные инструменты анализа полезны, но они решают только часть задачи (табл. 2) [2]. Предлагаемая среда объединяет их в единый процесс и добавляет контролируемое выполнение контракта после анализа.

ТАБЛИЦА 2. Сравнение различных подходов

| Подход | Ограничение | Что дает предлагаемая среда |
|---|---|---|
| Запуск одного /анализатора | результат зависит от метода инструмента | параллельное применение разных методов анализа |
| Несколько анализаторов без агрегации | трудно сопоставить результаты | единая модель отчета и статусов |
| Деплой без предварительной проверки | ошибки выявляются у же во время взаимодействия | анализ до деплоя и принятие решения на основе отчета |
| Локальная сеть без explorer | ограниченная наблюдаемость | Otterscan и Sourcify после деплоя |
| Прямой внешний доступ к geth | риск служебных вызовов и неконтролируемого воздействия | ots-bridge как RPC-шлюз и ограничитель |
| Публичная тестовая сеть | слабый контроль состояния и параметров | изолированный geth с фиксируемыми условиями |

Новизна подхода состоит в связке нескольких уровней контроля: анализ кода, контроль развертывания, контроль аккаунтов, контроль RPC-доступа и контроль наблюдаемости. Такая комбинация делает среду пригодной не только для поиска дефектов, но и для воспроизводимого подтверждения результатов.

Разные инструменты дают разные форматы вывода, поэтому нужен слой нормализации в единый формат данных. Единая модель отчета переводит разрозненные данные в проверяемые задачи, где найдена проблема, каким инструментом и что требуется для ручной верификации.

В жизненном цикле контракта явно отделяется автоматический анализ от интерактивного исследования (рис. 4). Это важно, так как автоматическая находка не всегда подтверждает уязвимость, а ручное тестирование без предварительного анализа не дает системного покрытия.

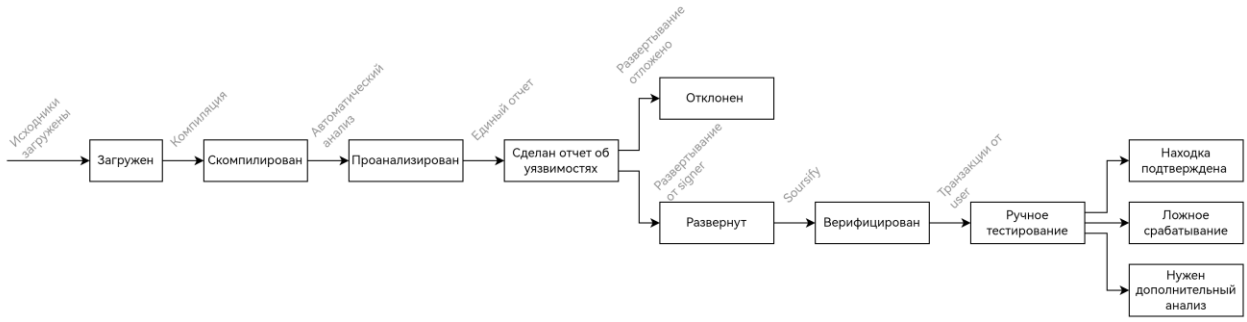



Рис. 4. Состояния контракта в среде

На текущем этапе акцент на подходе и архитектуре. Числовые метрики будут сниматься только после завершения стенда, реализации прототипа и проведения измерений. На рисунке 5 показана последовательность (пример) методики оценки – от подготовки контрактов и фиксации версий инструментов до автоматического и ручного тестирования, верификации и последующего снятия числовых метрик после завершения стенда.

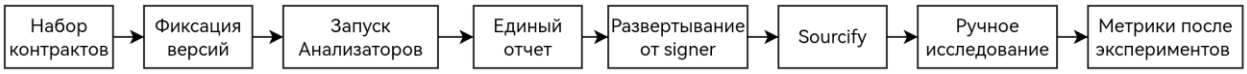



Рис. 5. Методика оценки до добавления числовых метрик

Предложенный подход описывает изолированную научно-методическую среду исследования безопасности смарт-контрактов. Его преимущество состоит в том, что автоматический анализ, развертывание, верификация исходников, обозреватель транзакций и ручная проверка объединяются в единый воспроизводимый цикл. Разделение аккаунтов signer и user, а также использование ots-bridge как адаптера для Otterscan и ограничителя внешнего RPC позволяют сохранить реалистичность ручного взаимодействия с контрактом без потери контроля над служебной частью инфраструктуры. Фактические метрики эффективности должны быть добавлены после реализации прототипа и проведения экспериментов.

**Список используемых источников**

1. Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H. N. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract // IEEE Access. 2022. Т. 10. С. 6605–6621. URL: https://ieeexplore.ieee.org/document/9667515 (дата обращения: 01.05.2026).
2. Praitheeshan, P., Pan, L., Yu, J., Liu, J., & Doss, R. Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey. 2019. URL: https://arxiv.org/abs/1908.08605 (дата обращения: 01.05.2026).
3. Feist, J., Grieco, G., & Groce, A. A Slither: A Static Analysis Framework For Smart Contracts // IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), 2019. С. 8–15. URL: https://arxiv.org/abs/1908.09878 (дата обращения: 0505.2026).
4. Slither // GitHub. URL: https://github.com/crytic/slither (дата обращения: 08.05.2026).
5. Mythril // GitHub. URL: https://github.com/ConsenSysDiligence/mythril (дата обращения: 08.05.2026).
6. Echidna // GitHub. URL: https://github.com/crytic/echidna (дата обращения: 08.05.2026).

## RESEARCH OF PRINCIPLES OF ORGANIZING AN ISOLATED ENVIRONMENT FOR SMART CONTRACT VULNERABILITY ANALYSIS

**Kushnir D., Terovets A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The paper considers approaches to organizing an isolated environment intended for vulnerability analysis of smart contracts in Ethereum-compatible infrastructure. Ensuring reproducibility of contract execution and control of environment parameters during security research is an important task. The environment supports various interaction scenarios, including automated vulnerability analysis, transaction and state behavior research, as well as interactive contract testing. Separation of functional capabilities by independent interfaces for different stages of analysis is proposed. The implementation of the proposed architecture makes it possible to create a tool for comprehensive and reproducible smart contract security research.*

***Key words:*** *smart contracts, Ethereum, EVM, vulnerabilities, isolated environment, reproducibility, Docker, Slither, Mythril, Echidna, Sourcify, Otterscan, geth*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ПОДХОД К МНОГОФАКТОРНОМУ ИНТЕЛЛЕКТУАЛЬНОМУ ПРОФИЛИРОВАНИЮ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

**Д. С. Левшун, Д. М. Легкодымов**

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

*Рассмотрена задача обнаружения вторжений в сетях промышленного Интернета вещей. Показано, что сетевые системы обнаружения вторжений имеют слепые зоны: они не видят атак на уровне хоста и теряют чувствительность при шифровании трафика. Предложен подход к многофакторному интеллектуальному профилированию устройств. Подход объединяет три независимых канала наблюдения: сетевой трафик, системные журналы и телеметрию ресурсов. Для каждого устройства строится индивидуальный профиль нормального поведения на основе моделей глубокого обучения. Подход проверен на наборе данных DataSense. Получены высокие значения метрик при обнаружении аномалий и атак.*

***Интернет вещей, обнаружение вторжений, профилирование устройств, обнаружение аномалий, глубокое обучение, автокодировщик, информационная безопасность***

Число устройств Интернета вещей быстро растет. По прогнозу Ericsson, к 2031 году их число достигнет почти 60 миллиардов [1]. Такие устройства все чаще применяются в критически важных инфраструктурах: в энергетике, на транспорте, в промышленности, в жилищно-коммунальном хозяйстве и в здравоохранении. Каждое новое устройство расширяет поверхность атаки. Уязвимыми такие устройства делают редко обновляемые прошивки, оставленные производителем пароли по умолчанию, плоская топология сети без сегментации, а также закрытые протоколы, плохо поддающиеся аудиту. Захватив одно устройство, злоумышленник получает доступ, с которого атака развивается вглубь технологической сети. В критической инфраструктуре это оборачивается остановкой процессов, выходом оборудования из строя и, в худшем случае, угрозой для жизни людей. Защиту принято закладывать еще на этапе проектирования: методики безопасной разработки встраиваемых систем действительно сокращают количество уязвимостей [2]. Однако то, как устройство поведет себя после ввода в эксплуатацию, они не контролируют, и потому необходимы механизмы своевременного выявления аномального поведения.

Существующие решения в большинстве своем построены вокруг анализа сетевого трафика – записей пакетов, потоков и их статистики [3], то есть относятся к классу сетевых систем обнаружения вторжений. Слабые места такого анализа хорошо известны. Руткиты, несанкционированное изменение конфигурации или локальное повышение привилегий разворачиваются внутри хоста и характерного трафика не создают. Когда обмен зашифрован, полезная нагрузка становится недоступной, и сигнатурные методы резко теряют чувствительность. Если же профиль нормального поведения строится сразу для группы устройств, различия между отдельными экземплярами оборачиваются потоком ложных срабатываний. Наконец, данные из разнородных источников обычно анализируются раздельно и между собой не сопоставляются.

Эти ограничения хорошо видны на наборе данных DataSense [4]. При атаках типа «отказ в обслуживании» сеть перегружена, зато поток журнальных записей датчиков, наоборот, иссякает. С разведывательными атаками картина обратная: в трафике они почти незаметны, но именно они порождают больше всего записей в журналах. Получается, что любой одиночный канал наблюдения на определенной части атак систематически не справляется.

Предлагаемый в работе подход к многофакторному интеллектуальному профилированию устраняет этот недостаток за счет того, что за каждым устройством ведется наблюдение сразу по трем независимым каналам. Со стороны сети фиксируются объем и частота потоков, длины пакетов, используемые протоколы и порты, тайминги соединений. Из системных журналов извлекаются события аутентификации, факты запуска процессов, изменения конфигурации, ошибки сервисов и сообщения протокола MQTT. Третий канал – телеметрия ресурсов и сенсоров: загрузка процессора и памяти, дисковый и сетевой ввод-вывод, частота и характер показаний датчиков. Каналы взаимодополняются и перекрывают слепые зоны друг друга.

Для каждого устройства отдельно строится профиль нормального поведения. Профиль строится не для класса устройств и не для сети в целом. Аномалией считается отклонение текущего поведения от индивидуального профиля. Профилирование выполняется на основе моделей глубокого обучения.

Обработка данных выполняется по единому конвейеру для каждого устройства. Сначала исходные данные разделяются по устройствам и размечаются. Затем выборка делится на обучающую и тестовую части в соот-

ношении 80 %/20 %. Обучающая выборка при необходимости балансируется по классам. Для каждой модели и каждого устройства выполняется подбор гиперпараметров методом Optuna [5]. После обучения модель оценивается на отложенной тестовой выборке. Для детекторов аномалий порог решения дополнительно калибруется на тестовой выборке. Калибровка необходима: порог, выбранный при обучении, часто не переносится на тест, и тогда все записи относятся к классу «атака».

Использованы три архитектуры глубокого обучения: полносвязная сеть, сверточная сеть и рекуррентная сеть. Каждая архитектура применяется в двух режимах. Первый режим – классификатор: модель определяет тип активности или атаки. Второй режим – автокодировщик: модель обучается только на нормальных записях устройства. Мерой аномальности служит ошибка восстановления [6]. Автокодировщику не нужны примеры атак, поэтому он имеет потенциал против неизвестных атак. Всего выполнено 912 циклов обучения: 38 устройств, 3 архитектуры, 2 задачи и 4 варианта набора данных. Финальная аналитика проведена по выборке из 21 устройства.

Подход проверен на наборе данных DataSense [4]. Набор собран на реалистичном стенде с промышленными датчиками, камерами и умными розетками. Он содержит 50 типов атак в семи категориях и синхронизированные потоки трафика, журналов и телеметрии. Результаты по трем задачам приведены в таблице 1.

ТАБЛИЦА 1. Качество профилирования на наборе данных DataSense (лучшее / медианное значение по 21 устройству)

| Параметр | Детектор аномалий | Бинарный классификатор | Тип атаки (мультикласс) |
|---|---|---|---|
| Лучший набор данных | logs_balanced / logs (16) | logs / logs (15) | logs_balanced / logs_balanced(11) |
| Лучшая модель | RNN / DNN (17) | DNN / DNN (14) | CNN / CNN (9) |
| macro-F1 | 0,9999 / 0,9653 | 0,9999 / 0,9696 | 0,7380 / 0,6211 |
| weighted-F1 | 0,9999 / 0,9711 | 0,9999 / 0,9753 | 0,8878 / 0,8407 |
| ROC-AUC | 0,9999 / 0,9641 | – | – |

Обнаружение аномалий и обнаружение атак по схеме «атака или норма» выполняются с высоким качеством: медианное значение macro-F1 превышает 0,96. Мультиклассовая задача труднее: метрику снижают редкие классы атак.

Проведен анализ влияния двух факторов. Балансировка обучающей выборки помогает мультиклассовой задаче: средний прирост macro-F1 составляет около 0,05, максимальный – 0,1311. На бинарную задачу и на детектор аномалий балансировка влияет слабо отрицательно. Журнальные признаки, в отличие от балансировки, полезны во всех сценариях: в мультиклассовой задаче их добавление дает в среднем около 0,02 macro-F1, а в лучшем случае – 0,0920. Ценность системных журналов как самостоятельного канала наблюдения тем самым подтверждается экспериментально.

Итогом работы стал подход к многофакторному интеллектуальному профилированию устройств Интернета вещей, в котором сетевой трафик, системные журналы и телеметрия ресурсов объединяются в индивидуальный профиль каждого устройства, построенный средствами глубокого обучения. Эксперименты на наборе данных DataSense подтвердили работоспособность подхода: атаки и аномалии обнаруживаются с медианным значением macro-F1 около 0,967. За счет источников данных, недоступных при анализе одного лишь трафика, сокращается число слепых зон и расширяется область применимости профилирования.

Продолжить исследование планируется по трем направлениям: адаптивная перенастройка профиля и порога при дрейфе поведения устройства; повышение качества мультиклассовой классификации с одновременным расширением набора устройств и сценариев; переход к гибридному набору данных, объединяющему признаки уровня пакетов, временных окон, системных журналов и телеметрии.

**Список используемых источников**

1. Ericsson Mobility Report, November 2024. URL: https://www.ericsson.com/ en/ reports-and-papers/mobility-report (дата обращения: 14.05.2026).

2. Levshun D., Chechulin A., Kotenko I. Design of Secure Microcontroller-Based Systems: Application to Mobile Robots for Perimeter Monitoring // Sensors. 2021. Vol. 21. N 24. Art. 8451.

3. Kotenko I., Saenko I., Branitskiy A. Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning // IEEE Access. 2018. Vol. 6. P. 72714–72723.

4. Firouzi A., Dadkhah S., Maret S. A., Ghorbani A. A. DataSense: A Real-Time Sensor-Based Benchmark Dataset for Attack Analysis in IIoT with Multi-Objective Feature Selection // Electronics. 2025. Vol. 14. N 20. Art. 4095.

5. Akiba T., Sano S., Yanase T., Ohta T., Koyama M. Optuna: A Next-generation Hyperparameter Optimization Framework // Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2019. P. 2623–2631.

6. Sakurada M., Yairi T. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction // Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis. 2014. P. 4–11.

## APPROACH TO MULTIFACTOR INTELLIGENT PROFILING OF INTERNET OF THINGS DEVICES

**Legkodymov D., Levshun D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The paper addresses intrusion detection in Industrial Internet of Things networks. Network-based intrusion detection systems have blind spots: they do not detect host-level attacks and lose sensitivity when traffic is encrypted. An approach to multifactor intelligent profiling of devices is proposed. The approach combines three independent observation channels: network traffic, system logs, and resource telemetry. For each device, an individual profile of normal behavior is built using deep learning models. The approach is validated on the DataSense dataset. High metric values are obtained for anomaly and attack detection.*

***Key words:*** *Internet of Things, intrusion detection, device profiling, anomaly detection, deep learning, autoencoder, information security*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МОДИФИКАЦИЙ BERT ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ ВРЕДОНОСНОЙ АКТИВНОСТИ В ЛОГАХ ИНФОРМАЦИОННЫХ СИСТЕМ

**Д. С. Левшун, А. Р. Русских**

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

*Статья посвящена выявлению вредоносной активности в журналах событий информационных систем. Ограничения сигнатурных методов обуславливают необходимость применения методов обработки естественного языка к анализу логов. Цель работы – сравнительная оценка базовой архитектуры двунаправленных кодировщиков на основе трансформеров и трех ее модификаций: дистиллированной версии, робастной модели с оптимизированным алгоритмом обучения и версии, предварительно обученной на текстах в области информационной безопасности. Модели настраивались на трех разнородных наборах данных, содержащих серверные, сетевые и веб-журналы с размеченными классами атак. Сравнение проводилось по метрикам точности, полноты, макроусредненной F1-меры и времени логического вывода. Проанализировано влияние архитектурных изменений и объема обучающей выборки на качество классификации. Результаты определяют перспективные направления адаптации трансформерных моделей для систем мониторинга безопасности.*

***журналы событий, обнаружение аномалий, вредоносная активность, BERT, DistilBERT, RoBERTa, SecureBERT, машинное обучение, информационная безопасность, классификация текстов***

Журналы событий – основной источник мониторинга безопасности, особенно в системах Интернета вещей [1, 2]. Современные исследования показывают, что ручной и сигнатурный анализ не справляется с ростом данных и новыми угрозами, порождая ложные срабатывания [3]. Для преодоления ограничений классических способов на данный момент перспективны методы машинного обучения. Логи можно интерпретировать как текстовые последовательности, что позволяет трансформерным моделям выявлять скрытые закономерности и проводить семантический анализ. Цель работы – сравнительный анализ BERT и трех ее модификаций для обнаружения вредоносной активности.

Рассмотрены четыре архитектуры. Базовый BERT использует двунаправленное внимание и предобучение на маскированных токенах, обеспе-

чивая понимание семантики [4]. DistilBERT применяет дистилляцию знаний на этапе предварительного обучения и сокращает размер модели на 40 %, повышая скорость инференса на 60 % при сохранении 97 % понимания языка [5]. RoBERTa оптимизирует предобучение: динамическое маскирование, отказ от задачи следования предложений и увеличение обучающих данных улучшают выявление сложных зависимостей [6]. SecureBERT обучалась на большом количестве текстов по компьютерной безопасности с использованием специального разработанного токенизатора [7].

Модели обучались и тестировались на трех наборах данных как классификаторы последовательностей. Результат оценивался по метрикам точности, полноты, F1-меры и матрицам ошибок. Первый набор данных «Server Log For Attack Detection» содержит имитированный поток серверных событий, помещенных в одну колонку, к которым в соседних ячейках присвоен один из шестнадцати классов [8]. Второй датасет представляет собой сетевые журналы внешнего серверного трафика, собранный проектом «Coburg Intrusion Detection Data Sets» (CIDDS) [9]. Исходно он содержал множество параметров, таких как временные метки, IP-адреса и флаги, которые были соединены в единую текстовую строку, а к ней, в свою очередь, присвоена метка, означающая подозрительная это запись или нормальная. Третий набор данных объединяет классические веб-датасеты ECML/PKDD 2007 и CSIC 2010 с HTTP-запросами, содержащие разметку данных на нормальные и аномальные [10]. Данные этого набора данных (заголовки, URL-адреса, тело запроса) были склеены в лог-строку для эффективного применения BERT моделей, а бинарная метка осталась без изменений.

Обучение было проведено с едиными гиперпараметрами: длина 256 токенов, батч 8, скорость обучения $2 \times 10^{-5}$, 3 эпохи. Использование разных пропорций разбиения выборок позволяло оценить влияние их объема на качество анализа. Эффективность результата измерялась метриками Accuracy, F1-macro и Recall-macro, важными для несбалансированных классов и редких угроз, а также параметром Inference-per-sample оценивающим скорость обработки одного сэмпла.

Анализ результатов, полученных на наборе данных «Server Log For Attack Detection» выявил резкую зависимость качества классификации от объема обучающей выборки, что представлено в таблице 1. При минимальной доле обучающих данных легковесная архитектура DistilBERT значительно превзошла полноразмерные аналоги. Модель SecureBERT показала самые низкие результаты при малом объеме данных, что свидетельствует о

переобучении доменно-ориентированных весов в условиях дефицита выборки. При увеличении выборки до 20–30 % робастная и дистиллированная модели достигли идеальных метрик, а SecureBERT компенсировала первоначальное отставание. На этом этапе определяющим фактором стала скорость инференса, где DistilBERT сохранила двукратное преимущество.

ТАБЛИЦА 1. Результаты для датасета Server Log For Attack Detection

| Модель | Доля обучающей выборки | Accuracy | F1-macro | Recall-macro | Inference-per-sample (ms) |
|---|---|---|---|---|---|
| BERT | 0,1 | 0,6812 | 0,269 | 0,3084 | 72,7217 |
| **DistilBERT** | 0,1 | **0,82** | **0,5635** | **0,5363** | **40,1299** |
| RoBERTa | 0,1 | 0,7928 | 0,4892 | 0,5274 | 79,7908 |
| SecureBERT | 0,1 | 0,5517 | 0,0444 | 0,0625 | 78,9578 |
| BERT | 0,2 | 0,9652 | 0,8746 | 0,8827 | 155,5625 |
| **DistilBERT** | 0,2 | **1** | **1** | **1** | **39,2001** |
| RoBERTa | 0,2 | **1** | **1** | **1** | 83,9843 |
| SecureBERT | 0,2 | 0,9711 | 0,8542 | 0,875 | 88,3853 |
| BERT | 0,3 | **1** | **1** | **1** | 78,0869 |
| **DistilBERT** | 0,3 | **1** | **1** | **1** | **38,903** |
| RoBERTa | 0,3 | **1** | **1** | **1** | 78,1723 |
| SecureBERT | 0,3 | **1** | **1** | **1** | 74,8581 |

Эксперимент на датасете с сетевым трафиком показал, что записи соединений содержат явно выраженные шаблоны, позволяющие всем моделям достигать качества классификации выше 99 % даже при 20 % обучающих данных, что можно увидеть в таблице 2. Архитектурные преимущества специализированных моделей нивелируются высокой структурированностью исходных параметров, таких как IP-адреса и флаги. Главным критерием выбора модели для анализа трафика является вычислительная эффективность, где дистиллированная версия BERT превосходит смежные архитектуры, обеспечивая время обработки менее 40 миллисекунд на образец.

ТАБЛИЦА 2. Результаты для датасета Server Logs от CIDDS

| Модель | Доля обучающей выборки | Accuracy | F1-macro | Recall-macro | Inference-per-sample (ms) |
|---|---|---|---|---|---|
| BERT | 0.2 | 0.9987 | 0.9974 | 0.9967 | 74.88 |
| **DistilBERT** | 0.2 | **0.9991** | **0.9982** | **0.997** | **39.1201** |
| RoBERTa | 0.2 | 0.9929 | 0.9861 | 0.9962 | 75.7069 |
| SecureBERT | 0.2 | 0.9984 | 0.9968 | 0.9944 | 75.97 |
| BERT | 0,5 | 0,9991 | 0,9981 | 0,9967 | 78,518 |
| DistilBERT | 0.5 | 0.9981 | 0.9962 | 0.9962 | **37.9186** |
| RoBERTa | 0,5 | 0,9977 | 0,9953 | 0,9988 | 78,804 |
| **SecureBERT** | 0,5 | **1** | **1** | **1** | 77,4143 |
| BERT | 0,8 | 0,9994 | 0,9989 | 0,9981 | 80,6738 |
| DistilBERT | 0,8 | 0,9977 | 0,9955 | 0,9971 | **38,1076** |
| **RoBERTa** | 0,8 | **1** | **1** | **1** | 84,8017 |
| **SecureBERT** | 0,8 | **1** | **1** | **1** | 82,7938 |

Работа с третьим датасетом HTTP-запросов для моделей оказалась наиболее сложной. Результаты в таблице 3 демонстрируют превосходство моделей RoBERTa и SecureBERT над базовой и дистиллированной архитектурами при любом объеме обучающей выборки. Оптимизация предобучения и адаптированность к данным, связанных с информационной безопасностью, стали решающими факторами при анализе и обработке менее структуризированных и более семантически сложных логов.

ТАБЛИЦА 3. Результаты для датасета WebApplication Attack – объединения ECML/PKDD 2007 и CSIC 2010

| Модель | Доля обучающей выборки | Accuracy | F1-macro | Recall-macro | Inference-per-sample (ms) |
|---|---|---|---|---|---|
| BERT | 0,2 | 0,8308 | 0,8252 | 0,8215 | 167,3546 |
| DistilBERT | 0,2 | 0,8343 | 0,8284 | 0,8244 | **42,3778** |
| **RoBERTa** | 0,2 | **0,8609** | **0,8559** | **0,8512** | 93,4015 |
| SecureBERT | 0,2 | 0,8543 | 0,8492 | 0,8448 | 82,5718 |
| BERT | 0,5 | 0,8611 | 0,8569 | 0,8531 | 72,118 |
| DistilBERT | 0,5 | 0,8479 | 0,8454 | 0,843 | **41,4726** |

| Модель | Доля обучающей выборки | Accuracy | F1-macro | Recall-macro | Inference-per-sample (ms) |
|---|---|---|---|---|---|
| RoBERTa | 0,5 | 0,8618 | 0,8578 | 0,854 | 75,5356 |
| **SecureBERT** | 0,5 | **0,8628** | **0,8589** | **0,8552** | 78,2313 |
| BERT | 0,8 | 0,8793 | 0,875 | 0,87 | 72,7294 |
| DistilBERT | 0,8 | 0,877 | 0,8729 | 0,8682 | **38,6069** |
| **RoBERTa** | 0,8 | **0,8799** | 0,876 | 0,8713 | 76,6119 |
| **SecureBERT** | 0,8 | 0,8793 | **0,8765** | **0,8729** | 77,8092 |

На основании полученных результатов можно сказать, что выбор оптимальной архитектуры трансформера для обнаружения вредоносной активности зависит от специфики логов, требований к системе мониторинга и того, какие вычислительные мощности возможно выделить для анализа. Для систем, генерирующих большое количество однородных сетевых или серверных логов с явно выраженными шаблонами, наиболее эффективным решением будет DistilBERT. Эта архитектура обеспечивает максимальную скорость логического вывода без потери качества при наличии хорошей обучающей выборки. В свою очередь, к примеру, в системах мониторинга веб-приложений, где анализируются семантически сложные записи, предпочтение стоит отдать моделям RoBERTa и SecureBERT. Их архитектурные особенности позволяют точнее извлекать признаки вредоносной активности из менее структурированных записей событий. Оценка влияния объема обучающей выборки показала, что оно носит нелинейный характер и определяется информативностью данных: для четко структурированных записей достаточна малая доля выборки, в то время как анализ сложных веб-логов требует максимального объема обучающих примеров для раскрытия потенциала доменно-ориентированных моделей.

**Список используемых источников**

1. Левшун Д. С., Чечулин А. А., Котенко И. В. Жизненный цикл разработки защищенных систем на основе встроенных устройств // Защита информации. Инсайд. 2017. № 4. С. 53-59.

2. Левшун Д. С., Веснин Д. В., Котенко И. В. Прогнозирование категорий уязвимостей в конфигурациях устройств с помощью методов искусственного интеллекта // Вопросы кибербезопасности. 2024. № 3 (61). С. 33-39.

3. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges // Cybersecurity. 2019. Vol. 2. N 20. DOI: 10.1186/s42400-019-0038-7.

4. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT). 2019. P. 4171–4186.

5. Sanh V., Debut L., Chaumond J., Wolf T. DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter // 5th Workshop on Energy Efficient Machine Learning and Cognitive Computing (EMC² at NeurIPS 2019). 2019.

6. Liu Y. [и др.] RoBERTa: A Robustly Optimized BERT Pretraining Approach // arXiv.org: электрон. б-ка препринтов. 2019. URL: https://arxiv.org/pdf/1907.11692 (дата обращения: 24.03.2026).

7. Aghaei E., Niu X., Shadid W., Al-Shaer E. SecureBERT: A Domain-Specific Language Model for Cybersecurity // Security and Privacy in Communication Networks (SecureComm 2022): материалы 18-й Международной конференции. Springer, 2022. P. 39–56.

8. Ilifydev. Server Log For Attack Detection: набор данных / Kaggle. URL: https://www.kaggle.com/datasets/ilifydev/sever-log-for-attacks-detection (дата обращения: 24.03.2026).

9. Ring M., Wunderlich S., Gruedl D., Landes D., Hotho A. Flow-based benchmark data sets for intrusion detection // Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS). 2017. P. 361–369.

10. Sudol M. Web-Application-Attack-Datasets: репозиторий / GitHub. URL: https://github.com/msudol/Web-Application-Attack-Datasets (дата обращения: 24.03.2026).

## STUDYING THE EFFICIENCY OF BERT MODIFICATIONS FOR DETECTING MALICIOUS ACTIVITY IN INFORMATION SYSTEM LOGS

**Levshun D., Russkikh A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article is devoted to detecting malicious activity in information system event logs. The limitations of signature-based methods necessitate the application of natural language processing methods to log analysis. The objective of this study is to comparatively evaluate the basic architecture of bidirectional transformer-based encoders and three of its modifications: a distilled version, a robust model with an optimized learning algorithm, and a version pretrained on texts in the field of information security. The models were tuned on three heterogeneous datasets containing server, network, and web logs with labeled attack classes. The comparison was conducted using the metrics of precision, recall, macro-averaged F1 score, and inference time. The impact of architectural changes and training sample size on classification quality was analyzed. The results identify promising areas for adapting transformer models to security monitoring systems.*

***Key words:*** *event logs, anomaly detection, malicious activity, BERT, DistilBERT, RoBERTa, SecureBERT, machine learning, information security, text classification*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ИНТЕЛЛЕКТУАЛЬНЫЙ АНАЛИЗ: ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПОДБОРА ИНДИВИДУАЛЬНОГО ОБУЧЕНИЯ СОТРУДНИКОВ НА ОСНОВЕ ДАННЫХ ОБ ИНЦИДЕНТЕ

**К. Е. Легков, Е. П. Плотников**

Благотворительный фонд «На благо Отечества», акционерное общество «Навигатор»

*Для подготовки специалистов по информационной безопасности (ИБ) все чаще обращаются к технологиям искусственного интеллекта (ИИ) в целях повышения эффективности обучения. Один из перспективных подходов – использование интеллектуального анализа данных для подбора индивидуальных образовательных траекторий на основе анализа инцидентов в информационных системах, то есть ситуаций, которые используются в процессе обучения, где обучаемые сталкиваются с трудностями или ошибками. Такой подход позволяет: оперативно выявлять пробелы в знаниях; адаптировать учебный материал под конкретного сотрудника; предотвращать накопление ошибок и отставание в обучении; повышать мотивацию за счет персонализации процесса. Интеллектуальный анализ данных (Data Mining) в контексте образования включает: сбор данных о действиях обучаемых (время выполнения заданий, количество попыток, типы ошибок); анализ этих данных с помощью алгоритмов машинного обучения; формирование рекомендаций для корректировки учебного процесса. ИИ в этом контексте выступает как инструмент, способный обрабатывать огромные массивы информации и выявлять неочевидные закономерности, выявленные в ходе обучения специалистов по ИБ.*

***информационная безопасность, искусственный интеллект, информационные системы***

## Введение

В современном мире для повышения эффективности обучения при подготовке специалистов по информационной безопасности (ИБ) все чаще обращается к технологиям искусственного интеллекта (ИИ). Один из перспективных подходов – использование интеллектуального анализа данных для подбора индивидуальных образовательных траекторий на основе анализа инцидентов, то есть ситуаций, когда обучающийся сталкивается с трудностями или ошибками в процессе обучения.

Такой подход позволяет:

– оперативно выявлять пробелы в знаниях;
– адаптировать учебный материал под конкретного специалиста;

– предотвращать накопление ошибок и отставание в изучении необходимого материала;
– повышать мотивацию за счет персонализации процесса.

**Интеллектуальный анализ данных и его вклад в процесс обучения специалистов по ИБ**

Интеллектуальный анализ данных (Data Mining) – это процесс обнаружения полезных закономерностей или знаний из больших объемов данных. В контексте обучения специалистов по ИБ он включает:
– сбор данных о действиях обучающихся (время выполнения заданий, количество попыток, типы ошибок);
– анализ этих данных с помощью алгоритмов машинного обучения;
– формирование рекомендаций для корректировки образовательного процесса.

ИИ в этом контексте выступает как инструмент, способный обрабатывать огромные массивы информации и выявлять неочевидные закономерности, которые могут быть незаметны руководителям направления по ИБ, проводящим обучение своих сотрудников.

Под «данными об инциденте» в контексте обучения специалистов по ИБ понимаются сведения о ситуациях, когда:
– обучающийся допустил ошибку в задании;
– не смог выполнить задание в отведенное время;
– продемонстрировал низкий уровень понимания темы;
– задал вопрос, указывающий на пробел в знаниях.

Эти данные могут включать:
– тип ошибки (фактическая, логическая, вычислительная и т.д.);
– контекст, в котором она была допущена (тема, сложность задания);
– действия обучающегося до и после ошибки (попытки самостоятельного исправления, обращение за помощью);
– временные показатели (сколько времени ушло на выполнение, были ли паузы);
– эмоциональные реакции (если фиксируются, например, через анализ мимики или текста сообщений).

Сбор и анализ таких данных позволяют:
– точно определить, в какой области у обучающегося есть трудности;
– понять причины этих трудностей (недостаток знаний, непонимание концепции, невнимательность и т.п.);
– подобрать наиболее эффективные методы коррекции.

ИИ использует различные алгоритмы и методы для анализа данных об инцидентах и формирования персонализированных рекомендаций [1-5]. Рассмотрим основные подходы:

1. Машинное обучение с руководителем направления по ИБ, проводящих обучение. Алгоритмы обучаются на статистических данных о результатах обучения и ошибках обучающихся. На основе этого они могут предсказывать, какие темы вызовут трудности у конкретного обучаемого специалиста, и предлагать дополнительные материалы для обучения.

2. Кластеризация. Обучающиеся группируются по схожим паттернам ошибок и успехов. Это позволяет создавать типовые рекомендации для каждой группы.

Например:

– группа А: трудности с алгебраическими преобразованиями – дополнительные упражнения на упрощение выражений;
– группа Б: проблемы с геометрическими доказательствами → видеоуроки по построению логических цепочек.

3. Рекомендательные системы. По аналогии с сервисами вроде YouTube или Netflix, ИИ предлагает учебные материалы, которые помогли другим обучающимся с похожими проблемами. Формула может выглядеть так:

$$R(u,i) = \mu + b_u + b_i + k = 1 \sum K_{qikpuk},$$

где $R(u,i)$ – оценка полезности материала $i$ для обучающегося $u$;

$\mu$ – средняя оценка всех материалов;

$b_u$ – смещение для обучающегося (его общий уровень);

$b_i$ – смещение для материала (его сложность/популярность);

$qik$ и $puk$ – векторы признаков материала и обучающегося в $K$-мерном пространстве.

4. Обработка естественного языка (NLP). Анализ текстовых ответов обучающихся и их вопросов позволяет выявлять семантические ошибки и недопонимания. Например, если обучающийся пишет «система безопасности всегда обеспечивает защиту информации в инфокоммуникационных системах», система может определить концептуальную ошибку и предложить материал о случаях, когда система безопасности не выполняет в полном объеме свои задачи.

5. Глубокое обучение. Нейронные сети могут анализировать сложные паттерны, например:

– последовательности действий в интерактивных заданиях;
– динамику изменения скорости и точности ответов во времени;

– корреляции между разными типами ошибок.

6. Байесовские сети. Моделируют вероятностные зависимости между знаниями, навыками и ошибками. Позволяют оценить вероятность того, что обучающийся освоил определенную концепцию, на основе его ответов.

**Практическая реализация: этапы внедрения**

Процесс внедрения системы интеллектуального анализа для индивидуального обучения можно разделить на несколько этапов:

*Этап 1. Сбор данных*

Источники данных:

– LMS (системы управления обучением): журналы действий, результаты тестов, время выполнения;
– интерактивные платформы: клики, паузы, возвраты к предыдущим шагам;
– чат боты и форумы: текстовые вопросы и ответы;
– биометрические данные (при согласии): взгляд, мимика, пульс (для оценки стресса).

*Этап 2. Предобработка данных*

– очистка от шума (ошибок ввода, аномалий);
– нормализация (приведение к единому формату);
– кодирование категориальных переменных (например, темы уроков);
– создание признаков (features): количество ошибок по темам, среднее время ответа, частота обращений за помощью.

*Этап 3. Обучение моделей*

– выбор алгоритма (регрессия, классификация, кластеризация);
– разделение данных на обучающую и тестовую выборки;
– настройка гиперпараметров;
– валидация модели (кросс валидация, метрики точности, полноты, F1 score).

*Этап 4. Генерация рекомендаций*

На основе предсказаний модели система предлагает:

– дополнительные материалы (статьи, видео, упражнения);
– изменение последовательности изучения тем;
– индивидуальные задания для отработки слабых мест;
– советы руководителю образовательного процесса по работе с обучающимся.

*Этап 5. Обратная связь и адаптация*

– Система отслеживает эффективность рекомендаций:

– улучшились ли результаты после вмешательства;
– как изменилось поведение обучающегося;
– какие рекомендации оказались наиболее полезными.

На основе этих данных модель дообучается, повышая точность будущих прогнозов.

## Примеры использования

*Пример 1. Подготовка специалиста по сбору статистических данных*

Обучающийся регулярно допускает ошибки в задачах на проценты. Система:

1. Фиксирует тип инцидента (неправильная формула, путаница с десятичными дробями).

2. Анализирует историю: ранее были проблемы с дробями.

3. Предлагает:

– видеоурок по преобразованию процентов в дроби;
– интерактивное упражнение на сравнение дробей и процентов;
– мини тест для закрепления.

*Пример 2. Корпоративное обучение*

Сотрудник не справляется с симуляцией процесса обеспечения ИБ на предприятии. ИИ:

– выявляет этап, где возникает ошибка (например, выбор стратегии);
– предлагает кейс с разбором аналогичных ситуаций;
– назначает ментора для индивидуальной консультации.

*Пример 3. Языковая платформа*

Обучающийся делает грамматические ошибки при составлении отчетов по ИБ. NLP модель:

– определяет проблемные конструкции (времена глаголов, артикли);
– генерирует упражнения на эти правила;
– подбирает тексты для чтения с акцентом на нужные структуры.

## Преимущества и вызовы

Преимущества:

– Персонализация. Процесс обучения подстраивается под темп и стиль каждого обучающегося.
– Эффективность. Ресурсы (время, материалы) направляются на реальные пробелы.

– Масштабируемость. Система может работать с тысячами обучающихся одновременно.
– Объективность. Решения основаны на данных, а не на субъективном мнении.
– Проактивность. Проблемы выявляются до того, как они приведут к серьезному отставанию.

Вызовы:

– Качество данных. Неполные или неточные данные снижают точность прогнозов.
– Приватность. Сбор персональных данных требует соблюдения законов (GDPR, ФЗ 152).
– Интерпретируемость. Сложные модели (нейросети) могут быть «черными ящиками», что затрудняет объяснение рекомендаций.
– Этика. Риск дискриминации, если алгоритмы обучались на смещенных данных.
– Затраты. Внедрение требует инвестиций в инфраструктуру и специалистов.

**Будущие тенденции**

Развитие технологий ИИ открывает новые возможности для интеллектуального анализа при обучении специалистов в области ИБ:

– Гибридные модели. Сочетание разных подходов (например, байесовские сети + глубокое обучение) для повышения точности.
– Объяснимый ИИ (XAI). Алгоритмы, которые не только дают рекомендации, но и объясняют их логику на понятном языке.
– Эмоциональный ИИ. Анализ эмоций обучающегося для адаптации сложности и тональности материалов.
– Метавселенные. Иммерсивное обучение в VR/AR с отслеживанием действий и реакций в реальном времени.
– Федеративное обучение. Обработка данных на устройствах обучающихся без передачи в облако, что повышает приватность.

**Заключение**

Использование ИИ для подбора индивидуального обучения на основе данных об инцидентах – это мощный инструмент, который способен революционизировать процесс обучения специалистов в области ИБ. Он позволяет перейти от универсального подхода к персонализированному, где каждый обучающийся получает поддержку именно там, где она нужна.

Несмотря на вызовы, связанные с качеством данных, приватностью и интерпретируемостью, преимущества такого подхода очевидны. По мере развития технологий ИИ и накопления образовательных данных системы интеллектуального анализа будут становиться все точнее и доступнее, делая качественное образование более гибким и эффективным для специалистов в области ИТ и ИБ.

**Список используемых источников**

1. Стрельцов А. А. Основные задачи государственной политики в области информационного противоборства // Военная мысль. 2011. № 5. С. 15-25.

2. Легков К. Е. К вопросу создания единого информационного пространства в гетерогенной автоматизированной системе управления корпорацией // Наукоемкие технологии в космических исследованиях Земли. 2024. Т. 16. № 6. С. 28-33.

3. Буренин А. Н., Легков К. Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения. Способы и средства обеспечения комплексной безопасности сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 3. С. 46-61.

4. Буренин А. Н., Легков К. Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения. Управление безопасностью сетей // Наукоемкие технологии в космических исследованиях Земли. 2015. Т. 7. № 4. С. 42-51.

5. Буренин А. Н., Курносов В. И. Теоретические основы управления современными телекоммуникационными сетями. Под ред. д-ра техн. наук, проф. В. И. Курносова. М.: Наука. 2011. 464 с.

## INTELLIGENT ANALYSIS: USING ARTIFICIAL INTELLIGENCE TO SELECATE INDIVIDUAL TRAINING FOR EMPLOYEES BASED ON INCIDENT DATA

**Legkov K., Plotnikov E.**
«Na blago Otechestva» Charitable Foundation, "Navigator" Joint-Stock Company

*To train information security (IS) specialists, more and more often turn to artificial intelligence (AI) technologies in order to improve the effectiveness of training. One promising approach is to use data mining to create individualized learning paths based on incidents in information systems, which are situations that arise during the learning process where students encounter difficulties or errors. This approach allows for the rapid identification of knowledge gaps, the customization of learning materials to suit individual employees, the prevention of error accumulation and learning delays, and the enhancement of motivation through personalized learning experiences. Data mining (Data Mining) in the context of education includes: collecting data on students' actions (task completion time, number of attempts, types of errors); analyzing this data using machine learning algorithms; and generating recommendations for adjusting the learning process. In this context, AI acts as a tool capable of processing vast amounts of information and identifying hidden patterns that emerge during the training of information security specialists.*

***Key words:*** *information security, artificial intelligence, and information systems*

**УДК 004.056**
**ГРНТИ 81.93.29**

# ИССЛЕДОВАНИЕ СООТВЕТСТВИЯ МОДЕЛЕЙ УГРОЗ ФСТЭК И ТАКТИК MITRE ATT&CK ДЛЯ СОВЕРШЕНСТВОВАНИЯ МОНИТОРИНГА ОБЛАЧНЫХ ИНФРАСТРУКТУР

**Т. Д. Любащенко, Д. П. Спиридонов**

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

*Активное внедрение облачных технологий в государственном и корпоративном секторе требует интеграции регуляторных требований и операционных практик информационной безопасности. В исследовании проводится анализ соответствия нормативных моделей угроз ФСТЭК и тактик фреймворка MITRE ATT&CK, направленный на совершенствование мониторинга облачных инфраструктур. Рассматриваются механизмы реализации угроз в наблюдаемые поведенческие индикаторы, оценивается покрытие тактик доступными источниками телеметрии и выявляются системные пробелы в детектировании. Работа систематизирует принципы построения гибридных систем обнаружения, ориентированных на раннее выявление кибератак, снижение времени реагирования и адаптацию к динамичной облачной среде. Полученные результаты создают методическую основу для развития практик мониторинга, обеспечивая переход от формального аудита к непрерывному, основанному на данных контролю безопасности.*

***информационная безопасность, облачные инфраструктуры, ФСТЭК России, MITRE ATT&CK, мониторинг безопасности, детектирование атак, оценка угроз, SIEM, киберустойчивость***

Цифровая трансформация государственного управления и коммерческого сектора сопровождается миграцией информационных систем в облачные среды (IaaS, PaaS, SaaS). Данный переход кардинально меняет архитектуру защиты: традиционные периметровые модели уступают место концепции Zero Trust, а акцент смещается на непрерывный мониторинг, поведенческий анализ и автоматизированное реагирование. В Российской Федерации процесс регулируется нормативными требованиями ФСТЭК России (приказы № 17, № 117 и др.), обязывающими субъектов критической информационной инфраструктуры, операторов персональных данных и владельцев государственных информационных систем проводить периодическую оценку угроз и организовывать мониторинг защищенности [1, 2].

Параллельно в международной практике матрица MITRE ATT&CK утвердилась в качестве де-факто стандарта описания тактик, техник и процедур (TTP) злоумышленников. Специализированная матрица *ATT&CK for Cloud* фокусируется на векторах атак, специфичных для публичных и частных облаков. Несмотря на различие в целеполагании, обе модели систематизируют угрозы ИБ, что создает предпосылки для их взаимного обогащения.

Методика ФСТЭК России (утверждена 5 февраля 2021 г.) [3] определяет порядок, содержание и результаты работ, по оценке угроз безопасности информации.

MITRE ATT&CK документирует реальные TTP атакующих, адаптированные под облачные платформы [4]. Версия 18 (октябрь 2025 г.) расширила покрытие на 14 новых техник, отражающих атаки на контейнерные среды.

Несмотря на общую предметную область (угрозы ИБ), модели решают принципиально разные задачи, что проявляется в следующих аспектах, для наглядности представлены в таблице 1.

ТАБЛИЦА 1 Сравнение матриц атак

| Критерий | Модель ФСТЭК | MITRE ATT&CK for Cloud |
|---|---|---|
| Назначение | Регуляторная оценка угроз для аттестации и декларирования соответствия | Описание реальных TTP для операционного детектирования, защиты и реагирования |
| Объект оценки | Информационные системы (включая облачные компоненты) в целом | Конкретные облачные платформы и их сервисные модели (IaaS/PaaS/SaaS) |
| Тактики | Неявно заданы через способы реализации угроз | Явно выделены 11 тактик, строго соответствующих kill chain |
| Техники | Фиксированный каталог из 145 техник | 60+ облачных техник с регулярным обновлением под новые векторы |
| Модель нарушителя | Формальная (потенциал, мотивация, классификация) | Эмпирическая (атрибуция через известные APT-группы и кампании) |

ФСТЭК обеспечивает нормативный фундамент и задает обязательный минимальный уровень защищенности, тогда как MITRE ATT&CK предлагает динамичную, ориентированную на данные карту реальных атак. Пересечение моделей наблюдается на уровне базовых сценариев: нарушение контроля доступа, утечка данных, компрометация учетных записей. Однако

глубина детализации и оперативная применимость существенно различаются.

Пробелы приводят к тому, что формально соответствующая требованиям ФСТЭК система может оставаться слепой к современным облачным векторам атак, если мониторинг не адаптирован под cloud-native телеметрию [5]. Для преодоления выявленных расхождений целесообразно внедрение гибридной модели мониторинга, где нормативные требования ФСТЭК служат базисом, а матрица MITRE ATT&CK for Cloud выступает операционным каркасом детектирования.

Нормативное покрытие и операционная детализация. Каталог ФСТЭК используется для формирования требований к классам защиты и аттестационным проверкам. MITRE ATT&CK применяется для маппинга этих требований на конкретные источники телеметрии (CloudTrail, Azure Monitor, Kubernetes Audit Log, CSPM/CWPP решения).

Развитие Detection Engineering. Каждая тактика MITRE транслируется в правила корреляции SIEM/SOAR. Например, техника изменения IAM-ролей (Persistence) детектируется через мониторинг событий ModifyRole/PutRolePolicy с алертированием на аномальные временные паттерны.

Телеметрическая адаптация. Мониторинг должен охватывать не только хостовые и сетевые метрики, но и облачные control plane события: аутентификацию через Identity Provider, вызовы API, конфигурационные дрифты, логи оркестраторов и serverless-выполнений [6, 7].

Continuous Threat Exposure Management (CTEM). Переход от периодической оценки угроз по ФСТЭК к непрерывному анализу поверхности атак. Интеграция данных CSPM с матрицей ATT&CK позволяет автоматически выявлять misconfigurations, соответствующие тактикам Initial Access или Privilege Escalation [8].

Обеспечение регуляторного соответствия. Интеграция фреймворка MITRE не подменяет, а расширяет методологию ФСТЭК. Внедрение дополнительных техник обнаружения фиксируется как усиление мер защиты, что в полной мере отвечает принципам приказов № 17 и № 117, предписывающих соразмерность средств обеспечения безопасности актуальным уровням угроз.

Результаты работы показывают: методика оценки угроз ФСТЭК и матрица MITRE ATT&CK, при всей разнице в их изначальных задачах, отлично работают в связке. ФСТЭК формирует нормативный фундамент и закры-

вает базовые классы угроз, без чего невозможна аттестация. ATT&CK же дает динамичную тактическую карту, опирающуюся на реальный опыт. Без нее сегодня не выстроить ни полноценный мониторинг, ни адекватное реагирование на инциденты.

При этом анализ выявил явный дефицит описания атак в облачных средах в обеих моделях. Совместное применение этих подходов, где ФСТЭК задает нормативные требования, а ATT&CK предоставляет прикладные индикаторы компрометации, позволяет устранить пробелы в каталогах угроз и повысить общую устойчивость инфраструктуры [9].

Перспективным направлением дальнейших исследований станет разработка инструментов для автоматической методика оценки угроз ФСТЭК на матрицу ATT&CK.

**Список использованных источников**

1. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17. М.: ФСТЭК России, 2013.

2. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017. № 239. М.: ФСТЭК России, 2017.

3. Методика оценки угроз безопасности информации: утв. ФСТЭК России 05.02.2021. М.: ФСТЭК России, 2021.

4. The MITRE Corporation. MITRE ATT&CK® for Cloud. Version 18. October 2025. – URL: https://attack.mitre.org/matrices/enterprise/cloud/ (дата обращения: 15.05.2026).

5. Top Threats to Cloud Computing: The Pandemic 11 / Cloud Security Alliance. – Seattle: CSA, 2022. URL:https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning

6. ISO/IEC 27017:2015. Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Geneva: ISO, 2015.

7. Степаненко Д. В. Сравнительный обзор моделирования угроз безопасности информации с использованием фреймворка MITRE ATT&CK / Д. В. Степаненко // Вопросы кибербезопасности. 2022. № 4. С. 45–52.

8. Касимова, А. Р. Моделирование вектора сетевых атак с применением базы знаний MITRE ATT&CK для совершенствования оценки угроз / А. Р. Касимова // Информационные технологии. 2023. № 6. С. 34–40.

9. ГОСТ Р ИСО/МЭК 27017-2021. Информационная технология. Методы и средства обеспечения безопасности. Практические правила применения мер защиты информации в облачных средах на основе ГОСТ Р ИСО/МЭК 27002. Москва: Российский институт стандартизации, 2021. 48 с.

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ЗСС СПбГУТ, доцентом Д. В. Сахаровым.*

# COMPARATIVE ANALYSIS OF FSTEC REGULATORY THREAT MODELS AND MITRE ATT&CK TACTICS TO IMPROVE CLOUD INFRASTRUCTURE SECURITY MONITORING

**Lyubashchenko T., Spiridonov D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The active adoption of cloud technologies in the public and corporate sectors requires the integration of regulatory requirements and operational information security practices. This study analyzes the alignment between FSTEC regulatory threat models and MITRE ATT&CK framework tactics to enhance cloud infrastructure monitoring. It examines the mapping of threat execution mechanisms to observable behavioral indicators, evaluates tactic coverage using available telemetry sources, and identifies systemic detection gaps. The paper systematizes the principles for designing hybrid detection systems aimed at early cyberattack identification, reducing response times, and adapting to dynamic cloud environments. The findings establish a methodological foundation for advancing monitoring practices, facilitating a transition from formal compliance audits to continuous, data-driven security control.*

***Key words:*** *information security, cloud infrastructure, FSTEC Russia, MITRE ATT&CK, security monitoring, attack detection, threat assessment, SIEM, cyber resilience*

**УДК 343.14**
**ГРНТИ 34.01.17**

# АВТОМАТИЗАЦИЯ СУДЕБНОЙ ЭКСПЕРТИЗЫ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

**А. У. Паскенова, П. И. Шариков**

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

*Развитие цифровых технологий привело к возникновению ключевого вызова при расследовании инцидентов в информационной сфере – гарантирование целостности, подлинности и прослеживаемости собранных доказательств. Логи систем, файлы с носителей информации и данные с IoT-устройств все чаще предоставляются в качестве ключевых доказательств в процессе судебных разбирательств. Применение блокчейн-технологий в автоматизации судебных экспертиз значительно повысит достоверность и неизменность цифровых доказательств, обеспечивая прозрачность всей цепочки их обработки – от этапа поступления объекта исследования до выдачи экспертного заключения.*

***автоматизация судебной экспертизы, блокчейн, децентрализованные базы данных, цифровые доказательства, неизменность, прозрачность***

Стремительный прогресс в области информационных технологий в современном мире приводит к экспоненциальному росту объемов цифровых данных, которые становятся ключевыми при расследовании инцидентов в сфере информационных технологий и последующем судебном процессе. Традиционная система проведения экспертиз не в силах обеспечить гарантированную защиту цифровых доказательств в целях их сохранности и подлинности. Возможность модификации метаданных, отсутствие неразрывной цепочки хранения, человеческий фактор при обнаружении, фиксации и передачи материалов – все это создает риск фальсификации экспертных заключений и их последующего оспаривания.

Современная судебная экспертиза содержит в себе интеграции информационных технологий, однако уровень автоматизации не исключает ключевых проблем обеспечения неизменности цифровых артефактов и остается фрагментарным. На сегодняшний день функционирует ряд автоматизированных систем (АС), которые используются в судопроизводстве и экспертной деятельности. Представлены основные из них:

– ГАС «Правосудие»: платформа для автоматизации документооборота и протоколирования судебных заседаний. Она обеспечивает обмен документами между участниками процесса. Система фиксирует факт загрузки файлов, не затрагивая их содержимое или историю модификаций;
– *LIS*-системы: применяются для регистрации поступающих объектов, назначения экспертиз и формирования заключений;

Вопреки очевидным преимуществам, перечисленные решения построены на централизованной архитектуре, что является фундаментальным недостатком. Уполномоченные сотрудники учреждения, где применяются данные АС, обладают привилегированными учетными записями, что не обеспечивает гарантии отсутствия вмешательства в целостность доказательств [1, 2].

Для обеспечения подлинности артефактов на практике применяются криптографические инструменты такие как: электронная цифровая подпись (ЭЦП) и хеширование файлов. Однако данные средства фиксируют только финальное состояние объекта, в то время как этап до подписания остается критически уязвимым.

Внедрение блокчейн-технологий, представляющих собой распределенный реестр объединенных последовательных блоков, криптографически связанных между собой, в автоматизацию расследования инцидентов поспособствует преодолению ограничений, присущих централизованным системам и традиционным криптографическим методам. Блокчейн выступает в роли инфраструктурной основы для построения децентрализованных баз данных, которые способны обеспечить аудируемость, целостность и прозрачность цифровых доказательств на всех этапах проведения судебной экспертизы [3]. Перспектива применения блокчейна в проведении судебной экспертизы заключаются в том, что блокчейн фиксирует криптографические хэши предыдущих блоков и метрики времени. Процесс функционирования включает следующие ключевые стадии:
– инициирование транзакции со стороны пользователя;
– верификация транзакции участниками сети;
– агрегация верифицированных транзакций в единый блок;
– формирование непрерывной последовательности путем криптографического связывания нового блока с предыдущим.

Важность технологии распределенного реестра – блокчейн в проведении расследования информационного инцидента заключается в том, что гарантия неизменности обеспечивается связью блоков через хэши, гарантия

единой точки отказа – за счет распределенного хранения, в дополнение исключается возможность единоличного редактирования благодаря консенсусному механизму, который требует подтверждения большинства узлов сети [4].

Криптографическая временная метка хэша в блокчейне обеспечивает неопровержимое подтверждение существование цифрового артефакта в неизменном виде в определенный отрезок времени. Распределенный реестр с консенсусным механизмом позволяет вести децентрализованный, неизменяемый журнал всех действий, совершенных с электронно-цифровыми следами. Сравнительный анализ традиционной системы расследования инцидентов и системы на основе блокчейн-технологии в контексте средства для автоматизации судебной экспертизы представлен в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ систем расследования инцидентов

| № п/п | Критерий сравнения | Традиционная система | Система на основе блокчейн-технологий |
|---|---|---|---|
| 1 | Неизменность доказательств | Модификация возможна без следов. | Модификация требует контроля большинства узлов |
| 2 | Прозрачность цепочки хранения артефактов | Ограниченная, так как журналы аудита могут быть отредактированы | Полная. Каждый участник сети имеет доступ к неизменяемому реестру |
| 3 | Время проверки подлинности артефакта | От нескольких дней до нескольких недель (направление запросов) | Несколько секунд за счет автоматической сверки хеша через блокчейн-обозреватель |
| 4 | Вероятность человеческого фактора | Высокая. Могут возникнуть ошибки при фиксации, передаче, хранении | Низкая. Наличие автоматической фиксации хешей и временных меток |
| 5 | Наличие возможности независимой проверки судом | Отсутствует. Суд вынужден доверять эксперту | Присутствует. Суд может самостоятельно верифицировать неизменность артефакта |
| 6 | Сложность фальсификации | Небольшая. Будет достаточно доступа к БД или носителю | Экстремальная. Потребуется контроль более 50 % вычислительных узлов сети |
| 7 | Защита от внутренних нарушителей | Слабая, так как администратор в силах скрыть свои действия | Сильная, так как любое изменение оставляет криптографический след |
| 8 | Зависимость от единого центра управления | Полная. Зависимость от сервера, администратора и СУБД | Отсутствует. Так как применяется распределенная архитектура |

Внедрение блокчейн-технологий в автоматизацию судебных экспертиз и переход к децентрализованным решениям является объективной необходимостью для обеспечения подлинности цифровых доказательств в современном расследовании информационных инцидентов.

Традиционная процедура установления подлинности цифрового доказательства в судебном разбирательстве включает в себя подачу запроса в экспертное учреждение, получение оригиналов носителей информации и проведение допроса уполномоченного эксперта. Возможно назначение дополнительной экспертизы. Данный процесс может занимать от нескольких дней до нескольких месяцев. Проверка цифровых артефактов с использованием блокчейн-технологии кардинально отличается от общепринятого метода и представляет собой принципиально иной подход. Сравнительный анализ алгоритма верификации цифрового артефакта судом с использованием технологии с консенсусным механизмом и традиционного алгоритма представлен в таблице 2.

ТАБЛИЦА 2. Сравнительный анализ алгоритмов верификации доказательств

| Этап | Действие | Традиционная алгоритм | Алгоритм с использованием блокчейна |
|---|---|---|---|
| 1 | Истребование хэша | Отсутствует. ЭЦП не фиксирует исходный хэш | Запрос из блокчейна |
| 2 | Проверка целостности | Без повторной экспертизы невозможна | Автоматическая сверка |
| 3 | Верификация метки времени | Запрос в экспертное учреждение | Мгновенно |
| 4 | Проверка цепочки хранения доказательств | Данные отсутствуют или могут быть фальсифицированы | Неизменяемый аудит |

На основе сравнительного анализа систем расследования инцидентов и алгоритмов верификации цифрового артефакта ожидается, что интеграция технологий распределенных реестров в судебно-экспертную деятельность приведет к снижению споров о подложности доказательств, прозрачному аудиту экспертной деятельности, повышению доверия к экспертным заключениям и сокращению процессуальных сроков за счет автоматических проверок.

Таким образом, применение блокчейн-технологий предоставляет значительные возможности для автоматизации процедур судебной экспертизы. Это, в свою очередь, способствует достижению нового уровня доверия и открытости в процессе анализа цифровых артефактов. Потенциальные выгоды от интеграции обосновывают дальнейшее изучение и практическое применение распределенных реестров с консенсусным механизмом и придают им статус необходимого условия для современного судебного производства.

**Список источников информации**

1. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (ред. от 28.12.2022) // Собрание законодательства РФ. 2001. № 23. Ст. 2291.

2. Красов А. В., Гельфанд А. М., Коржик В. И. [и др.]. Построение доверенной вычислительной среды. Санкт-Петербург: Индивидуальный предприниматель Петрив Роман Богданович, 2019. 108 с. ISBN 978-5-6043143-2-6. EDN RECXBI.

3. Подобных А. В. КриптодетективЪ – Цепная безопасность. Санкт-Петербург: ЛитРес, 2024. 440 с.

4. Шариков П. И., Красов А. В., Майоров А. В. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52. № 1. С. 147–161. DOI: 10.21822/2073-6185-2025-52-1-147-161. EDN: AWEHRP.

## AUTOMATION OF FORENSIC EXAMINATIONS USING BLOCKCHAIN TECHNOLOGIES

**Paskenova A., Sharikov P.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The development of digital technologies has led to the emergence of a key challenge in investigating incidents in the information sphere – ensuring the integrity, authenticity, and traceability of the collected evidence. System logs, files from storage media, and data from IoT devices are increasingly being presented as key evidence in court proceedings. The use of blockchain technologies in automating forensic examinations will significantly enhance the reliability and integrity of digital evidence, ensuring transparency throughout the entire chain of its processing – from the stage of receiving the object of study to the issuance of an expert opinion.*

***Key words:*** *forensic automation, blockchain, decentralized databases, digital evidence, immutability, transparency*

**УДК 004.75**
**ГРНТИ 20.51.17**

# БЛОКЧЕЙН КАК МЕТОД ЮРИДИЧЕСКОЙ АУТЕНТИФИКАЦИИ ЦИФРОВЫХ АРХИВНЫХ КОПИЙ

**А. У. Паскенова, П. И. Шариков**

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

*В эпоху повсеместной цифровизации архивное дело также претерпевает значительные изменения. В связи с этим особенно актуально становится задача обеспечения достоверности и сохранности электронных архивных материалов без каких-либо искажений. Хотя цифровые копии пока уступают микрофильмам в плане аппаратной неизменности, использование блокчейна может решить эту проблему. Запись хэшей цифровых копий с временными метками в распределенный реестр обеспечит их идентичность, подобно микрофильмам. Внедрение блокчейна в процесс оцифровки придаст цифровым копиям юридическую силу, сравнимую с микрофильмами, и повысит надежность хранения и неизменность оцифрованных документов.*

***блокчейн-технология, оцифровка архивных фондов, микрофильмирование, достоверность цифровых копий, неизменность данных, хэширование***

Цифровая трансформация проникает в экономическую сферу и систему государственного управления, затрагивая и архивную отрасль. Каждый год в электронный вид переводятся миллионы оригинальных архивных материалов, что позволяет сохранять культурное и историческое наследие, обеспечивать дистанционный доступ для ученых и снижать нагрузку на хранилища. Тем не менее, до сих пор не решен ключевой вопрос о том, могут ли электронные версии документов обладать той же юридической значимостью, что и их традиционные бумажные или пленочные аналоги.

На данный момент законодательство Российской Федерации предусматривает микрофильмы, представляющие собой пленочные копии оригиналов документов, в качестве традиционного юридического эталона достоверности и подлинности архивных копий. Объекты микрографического дублирования принимаются в суде в качестве доказательств, архивы используются как страховой фонд, тем не менее, стоит признать, что данная технология несет в себе ряд ограничений, таких как деградация пленки по истечении времени, требования к климатическому контролю в помещении хранения, трудоемкость поиска информации и невозможность проведе-

ния полнотекстового анализа. Микрофильмы, как материальные носители информации, подвержены многочисленным угрозам. Представлены критичные из них:

– пожар: температурный порог плавления пленки в 150-170 градусов Цельсия достигается молниеносно при горении в архивах, вызывая ее безвозвратное уничтожение;
– наводнение: при контакте с водой эмульсия подвергается необратимому разрушению, через двое суток после намокания, в дополнение, начинается процесс активного развития плесени;
– механическое воздействие: целенаправленное повреждение, такое как разрывы, порезы или сжигание, способно полностью уничтожить пленку;
– химическая деградация: материал подвержен саморазрушению в силу обладания "уксусным синдромом", приводящего к деградации и утере записанных изображений [1].

Стремление преодолеть ограничения микрографического дублирования привело к попыткам использования цифровых технологий для создания архивных копий. Вопреки распространенности, базовые электронные форматы, включая *PDF*, *TIFF* и *JPEG*, до сих пор не обрели юридического признания, сравнимого с микрофильмами. Причина этого кроется в их чувствительности к модификациям, отсутствии надежной привязки к моменту оцифровки и сильной зависимости от устаревающих программных решений. Технология распределенных реестров с консенсусным механизмом является многообещающей альтернативой традиционному методу. Суть технологии кроется в децентрализованной структуре управления информацией. Данные хранятся в виде цепочки блоков, связанным между собой посредством криптографических методов. Каждый блок содержит в себе сведения, последовательно добавляемые к существующим, тем самым создавая неразрывную хронологическую запись. Благодаря такой архитектуре, внесение поздних изменений в ранее записанные данные становится крайне затруднительным, практически невыполнимым. Надежность функционирования сети достигается за счет географического распределения ее компонентов. Узлы сети размещаются в разных областях, свободных от зон отказа, что гарантирует бесперебойность работы всей системы даже в случае возникновения локальных неполадок [2].

Основополагающей операцией всех блокчейн-решений для верификации документов является криптографическое хеширование. Данный процесс обеспечивает преобразование файла произвольного размера в уникаль-

ный цифровой идентификатор – строку фиксированной длины, что делает любую последующую модификацию цифровой копии немедленно обнаруживаемой. Полная конфиденциальность содержимого оцифровываемых архивных материалов обеспечивается за счет того, что регистрируется исключительно его криптографический отпечаток, полная загрузка документа не производится. Для подтверждения подлинности объектов культурного наследия наилучшим решением является применение алгоритма *SHA*-256. Этот криптографический метод, благодаря своей неизменности и высокой реакции на любые модификации, успешно обеспечивает сохранность и достоверность цифровых данных. Представлены шаги регистрации цифровой копии подлинников архивных документов:

– вычисление *SHA*-256 хэша оцифрованного документа;
– запись полученного хэша в блокчейн в качестве отдельной транзакции или части пакетной операции;
– повторное вычисление хэша документа и сравнение с записью в блокчейне (при необходимости верификации).

Отсутствие надежной привязки к моменту оцифровки является одной из критических проблем простых цифровых копий [3]. Технология с консенсусным механизмом предлагает эффективное решение данной проблемы, внедряя необратимую временную метку, устойчивую к фальсификации.

При проектировании системы важным архитектурным решением выступает выбор типа блокчейна. Для архивной деятельности особенно важен баланс между требованиями к конфиденциальности, производительности, прозрачности и юридической значимости. Наиболее оптимальным решением для рассматриваемой отрасли представляется композиционная модель, где авторизованные узлы формируют консенсус внутри доверенной периметральной сети, а их агрегированные хэши «замораживаются» в распределенном реестре публичного блокчейна, тем самым приобретая свойства повсеместной верифицируемости. В композиционной модели узлами могут выступать: государственные архивы, выполняющие функции основных хранители и валидаторов; нотариат – институциональный субъект, легитимированный на свидетельство достоверности копий; удостоверяющие центры, осуществляющие управление цифровыми сертификатами участников; а также публичный блокчейн, который используется для периодического якорения корневых хэшей, что добавляет дополнительный слой криптографической защиты.

Данная композиционная архитектура позволяет:

– произвести внедрение механизма разграничения прав доступа и обеспечить соответствие нормативным требованиям в области защиты персональных данных с помощью специализированного уровня разрешений;
– обеспечить высокую скорость обработки при масштабной цифровой трансформации данных;
– гарантировать долговечность и неизменность данных путем их фиксации в публичном реестре блокчейна;
– сформировать юридически значимое информационное пространство с привлечением нотариуса в качестве доверенного посредника [4].

Неотъемлемой частью приравнивания юридической силы цифровых копий к силе микрофильмов возможно через смарт-контракты. Они представляются в виде программного кода, который размещен в блокчейне и автоматически выполняет заданные условия. В процессе архивной оцифровки данный технологический ресурс позволяет автоматизировать процесс фиксации всех параметров создания цифровой копии. Представлены ключевые элементы, подлежащие фиксации в составе смарт-контракта:
– идентификатор оператора: подтверждение лица, выполнившего оцифровку, путем предоставления электронной цифровой подписи;
– временная метка: точное время начала и завершения процесса оцифровки, заверенное доверенными узлами временных меток;
– идентификатор оригинала: архивный код (шифр), номер документа и страницы;
– оборудование и параметр сканирования: необходим для гарантии повторяемости результата;
– хэш полученного цифрового образа уникальный криптографический код (отпечаток) сформированного файла.

Итог работы смарт-контракта представляется в цифровом удостоверении неизменности – структурированном наборе метаданных, связывающих все элементы процесса. Выполняя функцию нотариального заверения, оно создается автоматически и является криптографически защищенным [5].

Сравнительный анализ технологии микрофильмирования и оцифрованных подлинников с применением распределенного реестра с консенсусным механизмом приведен в таблице 1.

ТАБЛИЦА 1. Сравнительный анализ методов оцифровки подлинников архивных документов

| № п/п | Критерий сравнения | Микрофильмирование | Блокчейн-верификация |
|---|---|---|---|
| 1 | Обеспечение неизменности | Физический (химическая фиксация) | Криптографический. Обеспечивается за счет хэш-функции и механизма «консенсус» |
| 2 | Невозможность незаметного редактирования | Высокая. Требует разрешения носителя | Абсолютная. Изменение хэша делает фальсификацию очевидной |
| 3 | Деградация носителя | Высокая. В силу наличия особенностей пленки: «уксусный синдром», плесень, старение эмульсии | Отсутствует. Так как хэш – математический объект |
| 4 | Срок жизни копии без пересоздания | 50-70 лет | Теоретически бесконечен |
| 5 | Скорость проверки подлинности одного документа | Около 47 минут. Процесс: извлечение, зарядка в аппарат и просмотр | Около 18 секунд. Процесс: онлайн-верификация |
| 6 | Возможность удаленной проверки | Отсутствует. Для проверки требуется физический доступ к читальному аппарату | Присутствует. Достаточно компьютера с доступом в сеть «Интернет» |
| 7 | Возможность полнотекстового поиска | Отсутствует | Присутствует |
| 8 | Устойчивость к пожару /наводнению | Низкая | Высокая |

Представленная блокчейн-архитектура для оцифровывания подлинников архивных документов гарантирует непрерывную цепь доверия. Процесс начинается с оцифровки, где смарт-контракт фиксирует все этапы, и продолжается на стадии долговременного хранения и проверки. Цифровой сертификат, подтверждающий неизменность данных и закрепленный в публичной блокчейн-сети, в совокупности формирует юридическую основу, аналогичную статусу микрофильмов.

Таким образом, блокчейн-технологии выступают новым этапом в технологическом развитии архивной отрасли и превосходят микрофильмиро-

вание по всем эксплуатационным, эмпирически подтвержденным характеристикам. Приобретение юридической силы произойдет при более низких затратах, более высокой скорости проверки и беспрецедентной устойчивости к непредвиденным обстоятельствам, что еще раз доказывает необходимость внедрения блокчейн-технологий в работу архивной отрасли, постепенно конвергирующей с информационными технологиями.

**Список используемых источников**

1. Ипполитов С. С. Блокчейн и национальное наследие России: перспективные направления сохранения, популяризации, использования // Вестник архивиста. 2021. № 4. С. 1120–1132. DOI: 10.28995/2073-0101-2021-4-1120-1132. URL: https://cyberleninka.ru/article/n/blokcheyn-i-natsionalnoe-nasledie-rossii-perspektivnye-napravleniya-sohraneniya-populyarizatsii-ispolzovaniya (дата обращения 30.08.2026).

2. Баласанян В. Э. Сохранность электронных документов: проблемы и решения // Отечественные архивы. 2019. № 5. С. 14–21. URL: https://rusarchives.ru/publikacii/otechestvennye-arhivy/5763/balasanyan-sohrannost-elektronnyh-dokumentov-problemy-i-resheniya (дата обращения 30.08.2026).

3. Шариков П. И., Красов А. В., Майоров А. В. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52. № 1. С. 147–161. DOI: 10.21822/2073-6185-2025-52-1-147-161. EDN: AWEHRP.

4. Красов А. В., Гельфанд А. М., Коржик В. И. [и др.] Построение доверенной вычислительной среды. Санкт-Петербург: Индивидуальный предприниматель Петрив Роман Богданович, 2019. 108 с. ISBN 978-5-6043143-2-6. EDN RECXBI.

## BLOCKCHAIN AS A METHOD OF LEGAL AUTHENTICATION OF DIGITAL ARCHIVE COPIES

**Paskenova A., Sharikov P.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In the era of widespread digitalization, archival work is also undergoing significant changes. In this regard, the task of ensuring the reliability and preservation of electronic archival materials without any distortions becomes particularly relevant. Although digital copies currently lag behind microfilms in terms of hardware integrity, the use of blockchain could solve this problem. Recording the hashes of digital copies with timestamps in a distributed ledger will ensure their identity, similar to microfilms. Implementing blockchain in the digitization process will give digital copies legal validity comparable to microfilms and will enhance the reliability of storage and the integrity of digitized documents.*

***Key words:*** *blockchain technology, digitization of archival funds, microfilming, authenticity of digital copies, immutability of data, and hashing*

**УДК 343.98:681.327**
**ГРНТИ 10.81.19**

# ИССЛЕДОВАНИЕ ЦИФРОВЫХ СЛЕДОВ НА УСТРОЙСТВАХ ИНТЕРНЕТА ВЕЩЕЙ (IoT) В АСПЕКТЕ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

**А. У. Паскенова, П. И. Шариков**

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

*В условиях экспоненциального роста числа устройств Интернета вещей возрастает количество информационных инцидентов. Ежедневно современные системы фиксируют колоссальные объемы данных о каждом взаимодействии пользователя с окружающим миром. Злоумышленники, воспользовавшись уязвимыми смарт-устройствами, способны перехватить персональные данные, управлять устройствами удаленно и даже саботировать работу критической информационной инфраструктуры. Таким образом, вопрос глубокого изучения цифровых следов выступает стратегически важным элементом обеспечения информационной безопасности и проведения цифро-криминалистического анализа при расследовании информационных инцидентов.*

***интернет вещей, цифровая криминалистика, цифровые следы, цифровая доказательная база, смарт-устройства, расследование информационных инцидентов***

Цифровая трансформация технологического поля напрямую связана с стремительным совершенствованием технологий Интернета вещей (*IoT – Internet of Things*). В наши дни, когда мир стоит на пороге эпохи полной цифровизации, Интернет вещей занимает стратегическое место в интеграции физических объектов и виртуальных систем. Согласно статистическим данным, количество смарт-устройств растет экспоненциально и достигает миллиардов единиц ежегодно. Взаимодействие между устройствами и системами управления осуществляется посредством информационного обмена, что приводит к формированию значительного объема цифровых данных.

Информационный след представляет собой некую совокупность данных, оставленных пользователем или устройством впоследствии их взаимодействия с технологичным пространством. Популярность *IoT*-устройств поспособствовала появлению новых вызовов, включая кибербезопасность и детальное изучение цифровых артефактов, как один из значимых. Большинство смарт-устройств имеют уязвимости, которыми активно пользу-

ются злоумышленники и получают несанкционированный доступ к персональным данным, контроль управления оборудованием, в отдельных случаях получают возможность влияния на критически значимые объекты инфраструктуры. С точки зрения криминалистической экспертизы, совокупность данных, генерируемых устройствами Интернета вещей, формирует собой уже имеющуюся информационную систему.

Цифровые отпечатки, оставляемые устройствами в рамках Интернета вещей, поддаются классификации на основе их местонахождения, источника происхождения и уровня надежности как доказательства. Представлены артефакты по локализации, определяющие конкретное место поиска следов и средства, необходимые для его извлечения:

– электронные следы: хранятся непосредственно на смарт-устройстве. К ним причисляют прошивку, оперативную память и буферы сенсоров;
– сетевые следы: осели на сетевом оборудовании или находятся в процессе передачи между устройствами. К ним относится транзитный трафик шлюзов, брокеров *MQTT/CoAP, BLE*-рекламные пакеты;
– инфраструктурные следы: генерируются и хранятся на серверах производителя или в облаке. Представляют собой логи облачных платформ, теневые устройства, метаданные синхронизации;
– эмерджентные (кросс-устройственные) следы: «эхо» события на соседних *IoT*-агентах.

Артефакты, классифицированные по природе возникновения, являются важными для оценки достоверности. Включают в себя:

– детерминированные: легко интерпретируемые, строго определенные логикой работы устройства или протокола. Представляются логами авторизации, heartbeat, *OTA*-запросами;
– стохастические: зависят от внешних факторов, могут появляться попеременно при одном и том же событии. Требуют статического подхода обработки и включают объекты флуктуации *RSSI*, ошибки передачи, артефакты сжатия данных;
– индуцированные: представляют собой следы, возникшие исключительно при криминалистическом вмешательстве. Требуют специальных методов извлечения [1, 2].

Классификация по степени доказательной ценности, позволяет избежать неопределенные формулировки и перейти к ранжированной оценке. Данная шкала представляет собой:

– *D*0 – технический шум. Данные с высокой вероятностью (более 95 %);

– *D*1 – косвенные следы, требующие кросс-верификацию. Могут быть связаны с событием;
– *D*2 – прямые артефакты, но недолговечные. Обычно фиксируют действия злоумышленника или последствие атаки, но хранятся в энергозависимой памяти или быстро перезаписываются;
– *D*3 – неизменяемые следы, криптографически защищенные. Такие данные, которые обычно подписаны аппаратным ключом или хранятся в защищенных местах, не подвергающихся модификации.

Классификация представлена на рисунке 1.

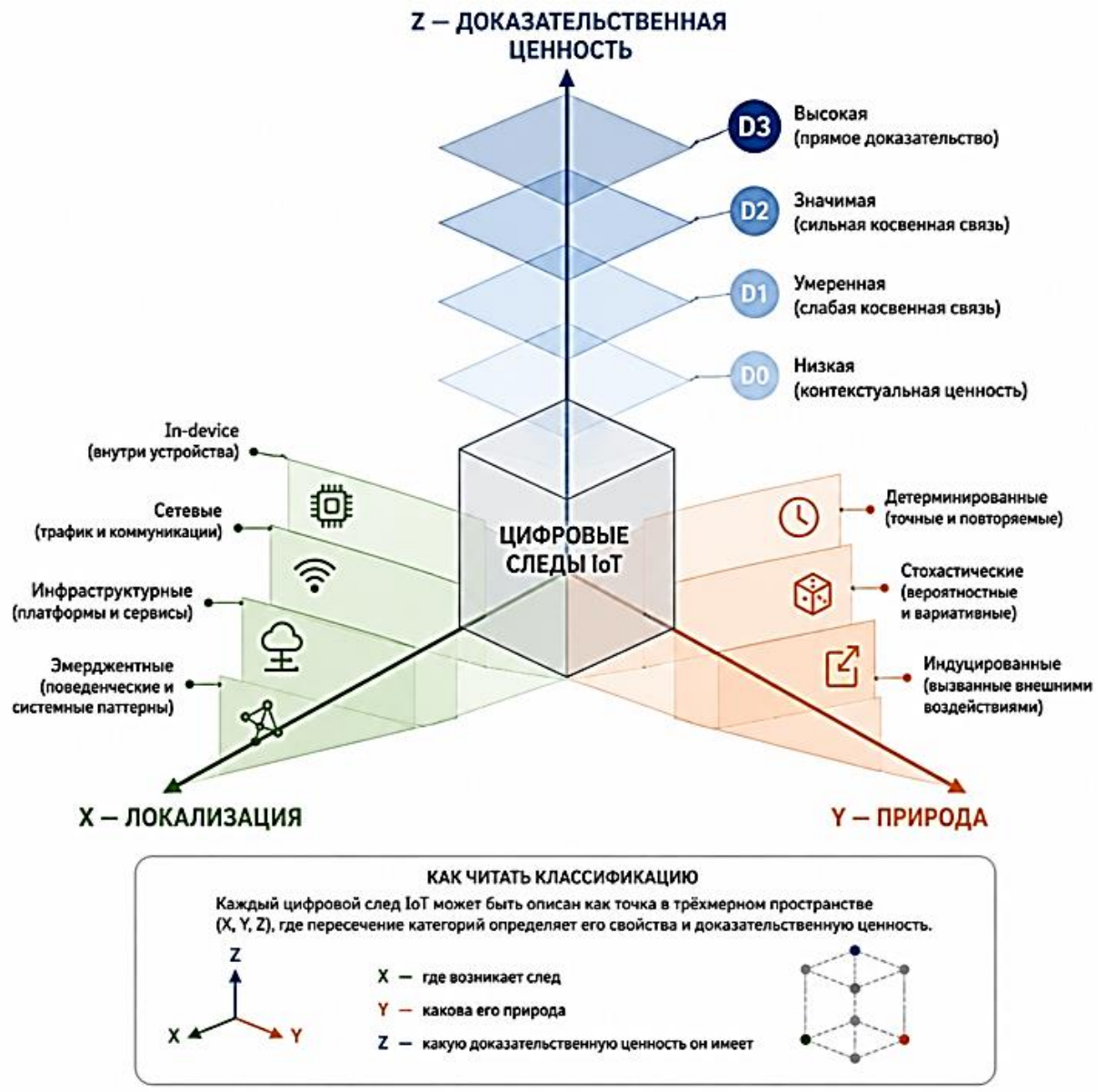



Рис. 1. Трехмерная классификация цифровых следов IoT

Данная классификация может быть использована в качестве основы для построения базы знаний экспертной системы, подсказывающей криминалисту, какой тип следа искать, в каком месте он может находиться, его вероятное время жизни и недопустимые при расследовании действия.

Извлечение цифровых следов из IoT-устройств и традиционная компьютерная криминалистика имеют принципиальные отличия. В силу этого, неверно выбранная последовательность операций может повлечь за собой безвозвратное уничтожение следов уровня *D*2-*D*3.

В рамках данной работы проведен глубокий анализ нюансов работы с артефактами объектов Интернета вещей и предложен подход к унификации гетерогенных протоколов, которые предоставят возможность перехода к единой теоретической рамке от большого количества различных методик под каждый тип устройства. В дополнении сформулированы принципы работы с умными устройствами и представлена модель жизненного цикла следа.

Для IoT-устройств прием отключения питания часто противопоказан, так как в этот момент теряются все энергозависимые артефакты. Стремление избежать этого привело к разработке принципов работы при извлечении артефактов, таких как:

– отключение электропитания до полного завершения процесса сохранения энергозависимой памяти строго запрещено;
– приоритет отдается пассивному перехвату радиочастотных сигналов над методами активного зондирования;
– до начала исследования необходимо обязательно изолировать устройство в Faraday-боксе.

Соблюдение предложенных принципов поспособствует обеспечению сохранности всех артефактов, необходимых в расследовании информационных инцидентов.

В целях систематизации процесса извлечения следов необходимо определить принцип появления, изменения и исчезновения цифрового следа. Разработанная модель представляет след, в качестве объекта, проходящего 5 стадий, каждая из которых имеет моменты, в которые след может быть изъят с минимальными потерями (точки захвата). Представлена модель жизненного цикла цифрового следа:

– стадия 1 – генерация: момент возникновения любого физического взаимодействия с устройством;

– стадия 2 – буферизация: сохранение сгенерированных данных в энергозависимое хранилище перед отправлением или записью в дамп памяти устройства;
– стадия 3 – передача с возможной агрегацией: перемещение данных из хранилища в другой узел сети;
– стадия 4 – ретенция: хранение данных после передачи в энергонезависимой памяти;
– стадия 5 – деградация: логическая перезапись или необратимая утеря информации ввиду физического изнашивания носителя.

Предложенные принципы и модель оптимизируют процесс работы с цифровыми следами, что значительно скажется на результате с положительной стороны.

Цифровая криминалистика Интернета вещей сталкивается с тремя группами дискуссионных проблем. Первая категория проблем связана с угрозами для сохранности цифровых доказательств. К примеру, рассмотрим открытую возможность внедрения злоумышленниками поддельных сообщений MQTT, изменения пакетов BLE или редактирования данных в журнале flash-памяти. Противодействием данным угрозам является использование криптографически защищенных журналов и строгое соблюдение протоколов изъятия данных, чтобы избежать их искажения или компрометации.

Вторая группа дискуссионных моментов касается использования "умных устройств как невольных свидетелей". Такие устройства, предназначенные для других целей, могут оставлять ценные следы. Например, LIDAR в роботе-пылесосе может помочь реконструировать карту помещения и траекторию передвижения, акселерометр в аудиоколонке способен зафиксировать шаги, а данные Wi-Fi триангуляции на основе маяков позволяют определить местоположение злоумышленника с точностью до метра.

Третья группа проблем относится к будущему цифровой криминалистики IoT. Прогнозируется, что в период с 2026 по 2028 годы появятся специалисты, узко профилированные на расследованиях в области IoT. Ожидается появление первых судебных прецедентов на основе композиции слабых цифровых следов [3, 4].

Проведенное теоретическое исследование привело к созданию уникальной классификации цифровых следов, генерируемых устройствами Интернета вещей. Данная классификация учитывает такие аспекты, как местоположение следа, его происхождение и значимость в качестве доказатель-

ства. Кроме того, были выдвинуты аксиоматические принципы изъятия устройств непосредственно на месте происшествия, а также разработана формальная модель, описывающая жизненный цикл цифрового следа.

Таким образом, разработанные теоретические положения закладывают фундамент для будущих прикладных исследований и формирования нормативно-правовой базы в сфере цифровой криминалистики, связанной с Интернетом вещей.

**Список используемых источников**

1. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: диссертация … доктора юридических наук: 12.00.09 / В. Б. Вехов. Волгоград, 2008. 401 с.

2. Шариков П. И. Архитектура интегрированного java-приложения для анализа журналов с целью обнаружения компьютерных атак в информационных системах посредством реагирования на различные аномалии безопасности / П. И. Шариков, А. В. Красов, А. В. Майоров // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т. 52, № 1. С. 147-161. DOI: 10.21822/2073-6185-2025-52-1-147-161. EDN AWEHRP.

3. Мещеряков В. А. Цифровые (виртуальные) следы в криминалистике и уголовном процессе / В. А. Мещеряков // Воронежские криминалистические чтения: сборник научных трудов. Воронеж, 2008. Вып. 9. С. 221–232.

## RESEARCH ON DIGITAL FOOTPRINTS ON INTERNET OF THINGS (IOT) DEVICES IN THE ASPECT OF DIGITAL FORENSICS

**Paskenova A., Sharikov P.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

***As the number of Internet of Things devices increases exponentially, the number of information incidents also increases. Every day, modern systems capture vast amounts of data about every user's interaction with the world. Attackers can exploit vulnerable smart devices to intercept personal data, remotely control devices, and even sabotage critical information infrastructure. Therefore, it is crucial to thoroughly investigate digital traces as a strategic element of information security and digital forensics in the investigation of information incidents.***

***Key words:*** *Internet of Things, digital forensics, digital footprints, digital evidence base, smart devices, and information incident investigation*

**УДК 004.8**
**ГРНТИ 20.51.19**

# ВЛИЯНИЕ ГРАДИЕНТНОЙ СОСТЯЗАТЕЛЬНОЙ АТАКИ CARLINI & WAGNER НА ТОЧНОСТЬ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ В СИСТЕМАХ МАШИННОГО ОБУЧЕНИЯ

**В. Е. Садовников**

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

*Статья посвящена комплексному анализу влияния оптимизационной атаки Карлини и Вагнера (Carlini & Wagner) как одного из наиболее мощных инструментов генерации состязательных примеров на показатели точности систем классификации изображений, построенных на базе глубоких нейронных сетей. В работе рассматриваются теоретические основы формирования состязательных возмущений, математический аппарат атаки, ее соотношение с другими методами, а также эмпирические закономерности деградации точности классификаторов при различных параметрах оптимизации.*

***кибербезопасность, состязательные атаки, C&W, атака Карлини и Вагнера, классификация изображений, глубокое обучение, устойчивость нейронных сетей, состязательные примеры***

Глубокие сверточные сети – ResNet, EfficientNet, Vision Transformer – удерживают 90–95 % на ImageNet и CIFAR-10, и эта цифра создает ложное ощущение завершенности. Архитектурная хрупкость проявляется сразу, как только к изображению добавляется градиентное возмущение, не различимое зрительно: классификатор выдает уверенный, но ошибочный вердикт. Валидация на чистых выборках перестала быть достаточным критерием; фокус сместился к синтезу контрпримеров и построению механизмов противодействия [1].

Атака Карлини и Вагнера (C&W, 2016) инвертирует привычную логику генерации возмущений [2]. Вместо наращивания шума до фиксированного порога алгоритм ищет минимальное искажение, гарантированно переводящее объект за границу решения. Целевая функция балансирует норму возмущения и штраф по логитам сети; градиентный спуск (обычно Adam) в связке с бинарным поиском по параметру уверенности определяет кратчайшую траекторию к сбою. Именно установка на минимизацию расстоя-

ния до чужого класса делает C&W более разрушительным методом с жестким бюджетом ε.

В режиме белого ящика метод выполняет роль строгого аудитора. Авторы показали, что эвристические защиты, ранее считавшиеся достаточными, рассыпаются под градиентами C&W без остатка. В сообществе закрепился негласный критерий: система, не выдерживающая адаптивную атаку Карлини–Вагнера, не признается робастной [3]. Метод стал обязательным стресс-тестом; без него сертификацию модели для задач с реальными последствиями ошибки трудно считать обоснованной.

Влияние на точность структурное и резкое. Сеть, распознающая 95 % объектов на чистом ImageNet, под действием C&W проседает ниже 1 %, причем амплитуда внедренного шума оказывается кратно меньше, чем у атак с фиксированным ε. Сопоставление с FGSM проясняет природу деградации: одношаговый метод вычисляет возмущение за одно применение градиента и порождает избыточный шум, не гарантируя минимальности. C&W, выполняя сотни итераций оптимизации, находит именно ближайшую точку на разделяющей поверхности. Там, где FGSM требует относительно крупного ε для снижения точности ResNet-50 на CIFAR-10 до 30–40 %, C&W обнуляет модель при практически невидимых искажениях [4].

Вычислительная стоимость определяется числом итераций оптимизатора и глубиной бинарного поиска. При короткой цепочке шагов алгоритм не находит глобальный минимум штрафной функции, и часть изображений остается неатакованной.

Выбор нормы меняет геометрию атаки. Авторы предлагают три варианта: $L_0$, $L_2$, $L_\infty$. $L_2$-версия стала наиболее распространенной благодаря гладкости функции потерь: микроскопический шум равномерно распределяется по кадру и остается невидимым. $L_0$ наносит точечные изменения в отдельные пиксели и требует комбинаторных приемов из-за недифференцируемости; $L_\infty$ вынуждает обходить неравномерность максимума. Модели, выдержавшие атаку в одной метрике, не обязательно устойчивы в другой, поэтому защищенные системы проверяют по всем трем нормам либо применяют мульти-нормативные схемы.

Атака распределяется по классам неравномерно. Объекты вблизи чужих границ капитулируют при ничтожных сдвигах; экземпляры с уникальной текстурой, расположенные далеко от разделяющих гиперплоскостей, требуют существенно больших возмущений. Семантически близкие категории атакуются легче. Допускается и целевой режим: алгоритм принуди-

тельно переводит объект в заранее выбранный класс-мишень с заданной уверенностью, что позволяет точечно контролировать поведение модели в критических сценариях.

Переносимость атак, сгенерированных C&W, ниже, чем у грубых градиентных методов. Алгоритм фиксирует специфические точки на границе решения конкретной архитектуры; в режиме черного ящика без моделей-суррогатов пробивная сила падает. При полном доступе к весам, напротив, многошаговая адаптивная оптимизация восстанавливает эффективность, требуя перебалансировки защиты.

Единственный системный ответ – состязательное обучение. В идеальном варианте сеть обучается против C&W-контрпримеров на каждом шаге, решая минимаксную задачу. На практике итеративный синтез внутри цикла обучения неподъемен вычислительно; индустрия тренирует модели на более дешевых методах (PGD, FAST), а C&W приберегает для финального аудита. Даже после такой закалки падение чистой точности в обмен на робастность остается неразрешенным структурным компромиссом.

Полумеры не выдерживают проверки. Защитная дистилляция и регуляризация градиентов под натиском C&W рассыпаются: метод обнажает замаскированные градиенты (gradient masking), доказывая, что сглаживание вероятностей не лечит модель, а лишь скрывает уязвимость. Сертификаты рандомизированного сглаживания тоже не спасают: гарантированный радиус неуязвимости оказывается меньше реального радиуса поражения C&W.

Практические последствия ощутимы в автономном транспорте, где микроскопическое возмущение на знаке провоцирует опасное решение бортовой системы; в медицинской визуализации, где невидимый шум способен привести к ложному диагнозу; в биометрии, где целевые модификации открывают путь к подмене личности. Это подталкивает к стандартам, обязывающим тестировать робастность с привлечением адаптивных атак до сертификации.

C&W перестала быть просто одним из алгоритмов в каталоге атак. Вычисляя минимально допустимые отступы границ и вскрывая ложную робастность, метод служит эталонным инструментом оценки: без прохождения этого теста развертывание модели в задачах с реальной ценой ошибки необоснованно. Дальнейший прогресс потребует междисциплинарных усилий, и C&W в обозримом будущем сохранит роль основного калибровочного критерия устойчивости.

**Список используемых источников**

1. Chen J., Chen H., Chen K., Zhang Y., Zou Z., Shi Z. Diffusion models for imperceptible and transferable adversarial attack // IEEE Trans. Pattern Anal. Mach. Intell. 2025. Vol. 47. P. 961–977.

2. Salman H., Ilyas A., Engstrom L., Kapoor A., Mądry A. Do adversarially robust ImageNet models transfer better // Proc. Adv. Neural Inf. Process. Syst. (NeurIPS). 2020. P. 3533–3545.

3. Билан В. В., Перов Р. А., Шевяков В. Д. Исследование текущих структур и методов обеспечения безопасности информации в сфере беспилотного транспорта // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2025). 2025. С. 540–544.

4. Николаева П. А., Садовников В. Е., Гладких Д. С., Шевяков В. Д. Разработка протоколов аудита данных для предотвращения атак с отравлением в системах видеонаблюдения // Опыт и перспективы совершенствования систем связи и акустических испытаний современной техники. 2025. С. 387–390.

*Статья представлена научным руководителем, профессором кафедры автоматизированных систем специального назначения ВАС, доктором технических наук, профессором И. Б. Саенко.*

## THE EFFECT OF CARLINI & WAGNER'S GRADIENT ADVERSARIAL ATTACK ON IMAGE CLASSIFICATION ACCURACY IN MACHINE LEARNING SYSTEMS

**Sadovnikov V.**
Military Academy of Communications named after Marshal of the Soviet Union
S. M. Budyonny

*The article is devoted to a comprehensive analysis of the impact of the optimization attack by Carlini and Wagner as one of the most powerful tools for generating competitive examples for the accuracy of image classification systems based on deep neural networks. The paper examines the theoretical foundations of the formation of adversarial perturbations, the mathematical apparatus of the attack, its relationship with other methods, as well as empirical patterns of degradation of classifier accuracy under various optimization parameters.*

***Key words:*** *cybersecurity, adversarial attacks, C&W, Carlini and Wagner attack, image classification, deep learning, neural network resilience, adversarial examples*

**УДК 004.8**
**ГРНТИ 20.51.19**

# ВЛИЯНИЕ ЗАШУМЛЕНИЯ НА УСТОЙЧИВОСТЬ СИСТЕМ КЛАССИФИКАЦИИ ИЗОБРАЖЕНИЙ К СОСТЯЗАТЕЛЬНЫМ АТАКАМ

**В. Е. Садовников**

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

*Статья посвящена комплексному анализу влияния стохастического зашумления как одного из наиболее перспективных инструментов защиты от генерации состязательных примеров на показатели точности и робастности систем классификации изображений, построенных на базе глубоких нейронных сетей. В работе рассматриваются теоретические основы формирования защитных возмущений, математический аппарат случайных преобразований, их соотношение с детерминированными методами очистки, а также эмпирические закономерности деградации атакующего потенциала при различных параметрах шумовых распределений и стратегий аугментации.*

***состязательная защита, зашумление, классификация изображений, глубокое обучение, устойчивость нейронных сетей, защитная аугментация, шумовые преобразования***

Современные системы машинного обучения, особенно глубокие сверточные нейронные сети, демонстрируют выдающиеся результаты в классификации изображений, превосходя человека во многих задачах. Архитектуры вроде ResNet, EfficientNet и Vision Transformer достигают точности выше 90–95 % на бенчмарках ImageNet и CIFAR-10, создавая иллюзию высокой надежности.

В самой архитектуре глубоких сетей заложена хрупкость, которую принято называть проблемой состязательных примеров. Суть ее проста и тревожна: к входному изображению добавляется градиентное возмущение, настолько малое, что человеческий глаз не фиксирует разницы, – и классификатор выдает уверенный, но в корне неверный ответ. Привычка судить о надежности модели исключительно по чистым тестовым наборам оказалась несостоятельной; сообщество обратилось к стохастическим механизмам защиты и рандомизации входного пространства [1].

Среди защитных подходов стохастическое зашумление выделяется тем, что не пытается «подлатать» вход детерминированным фильтром или

спрятать градиенты за фиксированными преобразованиями. Идея, выросшая из классической защитной аугментации [2], состоит в другом: защита формулируется как задача стохастической оптимизации, где цель – максимизировать энтропию входного распределения, не теряя семантической информативности, необходимой для корректной классификации. Практически это реализуется наложением контролируемого шума – гауссовского, импульсного, структурного – или применением случайных преобразований: поворотов, масштабирования, кроппинга, цветовых сдвигов. В основу положены вероятностные модели и теорема о размытии границы принятия решения. Прямая инъекция стохастичности при жестком контроле за сохранением полезных признаков превращает рандомизацию в инструмент с четкой теоретической базой, а не в эвристическую заплатку.

Репутация стохастического зашумления в иерархии защитных механизмов – как белого, так и черного ящика – не случайна. Эмпирика и теория сходятся: метод способен разрушить градиентную согласованность, на которую опираются атаки, ранее считавшиеся непреодолимыми для статических моделей. Если после введения входной рандомизации сеть выдерживает полноценную оптимизационную атаку, это весомое свидетельство подлинной устойчивости. Фактически случайные преобразования стали обязательным стресс-тестом на финальной стадии разработки: детерминированную защиту, не выдерживающую рандомизированного входного пространства, сегодня трудно считать пригодной для задач, где ошибка несет реальные последствия.

Влияние на точность при атаках здесь не косметическое, а структурное. Атакующий оптимизатор полагается на когерентность градиента вдоль траектории возмущения; рандомизация разрушает эту когерентность еще до того, как возмущение достигает сети. В результате стандартные состязательные методы теряют предсказательную способность даже при минимальных исходных возмущениях – оптимизатору просто не за что «зацепиться» в условиях постоянно меняющегося входного ландшафта.

Модель с точностью 95 % на чистом ImageNet может показать снижение успешности атаки C&W или PGD до менее 5–10 % при успешном наложении шума, при этом падение точности на чистых данных окажется незначительным (менее 1–2 %). Это значительное подавление атак объясняется тем, что стохастичность превращает детерминированную границу принятия решения в вероятностное распределение, эксплуатируя нелинейность градиентного потока и разрушая итеративную сходимость оптимизатора [3].

Сопоставление стохастического зашумления с детерминированной защитной дистилляцией или сжатием проясняет природу повышения устойчивости. Детерминированные методы вычисляют преобразования единожды и часто создают фиксированные артефакты, не гарантируя разрушения градиента для всех возможных атак. Рандомизация, выполняя независимые преобразования при каждом инференсе, решает задачу размытия границы решений, находя именно те стохастические траектории, которые максимально отклоняют атакующий пример от целевого класса.

Интенсивность шума, дисперсия распределения и частота случайных преобразований критически влияют на вычислительную стоимость и степень деградации атакующего потенциала. При малой дисперсии оптимизатор может не успеть столкнуться с существенным стохастическим барьером, и атака окажется успешной для большинства изображений. С ростом уровня шума и разнообразия преобразований алгоритм находит все более нестабильные градиенты, монотонно снижая успех атакующих методов. Основной вычислительный затрат приходится на генерацию шума и многократный инференс (при использовании ансамблирования или усреднения вероятностей), после чего улучшение защиты выходит на плато. Для строгой оценки устойчивости применяют до нескольких десятков вариаций распределений и комбинированные стратегии аугментации, гарантируя, что защита достигла своего теоретического предела [4].

Выбор метрики зашумления и типа преобразований существенно влияет на характер генерируемой защиты. Авторы предложили три варианта: аддитивный гауссовский шум, мультипликативные/структурные искажения и пространственно-вероятностные преобразования. Вариант с гауссовским шумом является наиболее популярным и математически элегантным, так как функция потерь легко дифференцируема в рамках теоретического анализа, а возмущения распределяются равномерно, оставаясь визуально незаметными. Структурные преобразования изменяют лишь геометрию изображения, создавая локализованные артефакты, а пространственные требуют специальных приемов для обхода потери контекста. Неуязвимость к одному типу случайных преобразований вовсе не гарантирует защиту от других – геометрия брешей в классификаторе всякий раз оказывается уникальной. Отсюда жесткое требование: аудиту должны подвергаться все три метрики возмущений.

Внесение стохастичности причудливо искажает карту ошибок. Там, где объект балансирует на грани чужого класса, даже слабое «дрожание» вход-

ного пространства срывает атаку. Совсем иначе обстоит дело с семантически близкими категориями: их границы размыть сложнее, и уникальная текстура здесь уже не спасает. Зато именно этот вероятностный подход лежит в основе randomized smoothing – техники, которая превращает гадание нейросети в строгий математический сертификат, гарантирующий неуязвимость внутри заданного радиуса.

Состязательные примеры, созданные в вакууме (без учета защитного шума), разбиваются о стохастический барьер. В сценарии «черного ящика», где атакующий слеп, рандомизация работает безупречно: она стирает микроскопические детали границы принятия решений, делая перенос атак бессмысленным. Но стоит противнику получить доступ к весам («белый ящик»), как он переходит на язык математических ожиданий и адаптивных обходов.

Идеальный щит рождается на стыке стохастики и состязательного обучения. Теоретически безупречный сценарий – генерировать контрпримеры, сразу погруженные в шумовое распределение. На практике же многократный инференс для калибровки дисперсии на каждом шаге обучения выжигает вычислительные ресурсы. Индустрия пошла на компромисс: сеть тренируют быстрыми методами вроде PGD с аугментацией, а тяжелую стохастическую артиллерию приберегают для финального аудита. И хотя такой гибрид отлично держит адаптивные удары, фундаментальная дилемма – падение точности на чистых данных в обмен на броню – по-прежнему не имеет элегантного решения.

Попытки обойтись малой кровью – регуляризацией градиентов или защитной дистилляцией – раз за разом проваливаются. Стохастический подход обнажил их главную слабость: дистилляция не лечит модель, а лишь маскирует градиенты (gradient masking), создавая иллюзию безопасности. Даже строгие сертификаты рандомизированного сглаживания часто оказываются бесполезными, поскольку реальный радиус неуязвимости критически меньше шага полноценной оптимизационной атаки.

Стохастическое зашумление перестало быть просто техническим трюком – оно стало оптикой, через которую мы рассматриваем саму природу уязвимостей нейросетей. Внося хаос во входные данные, мы находим те самые энтропийные барьеры, о которые разбиваются хакерские атаки. Рандомизация выступает безжалостным аудитором, срывающим маски с псевдоустойчивых моделей. Без глубокого понимания того, как шум искривляет пространство признаков, выпускать ИИ в реальный мир сегодня просто без-

ответственно. И хотя архитектура защит будет усложняться, стохастика навсегда останется тем фундаментом, на котором строится доверие к искусственному интеллекту.

**Список используемых источников**

1. Zhang L., Lambotharan S., Zheng G., Liao G., Demontis A., Roli F. A hybrid training-time and run-time defense against adversarial attacks in modulation classification // IEEE Wireless Communications Letters. 2022. Vol. 11. P. 1161–1165.

2. Sahay R., Brinton C. G., Love D. J. A deep ensemble based wireless receiver architecture for mitigating adversarial attacks in automatic modulation classification // IEEE Transactions on Cognitive Communications and Networking. 2022. Vol. 8. P. 71–85.

3. Xu Y., Raja K., Ramachandra R., Busch C. Adversarial attacks on face recognition systems // Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks. Cham: Springer International Publishing, 2022.

4. Fu X., Gui G., Wang Y., Gacanin H., Adachi F. Automatic modulation classification based on decentralized learning and ensemble learning // IEEE Transactions on Vehicular Technology. 2022. Vol. 71. P. 7942–7946.

*Статья представлена научным руководителем, профессором кафедры автоматизированных систем специального назначения ВАС, доктором технических наук, профессором И. Б. Саенко.*

## THE EFFECT OF NOISE ON THE STABILITY OF IMAGE CLASSIFICATION SYSTEMS TO COMPETITIVE ATTACKS

**Sadovnikov V.**
Military Academy of Communications named after Marshal of the Soviet Union
S. M. Budyonny

*The article is devoted to a comprehensive analysis of the effect of stochastic noise as one of the most promising tools for protecting against the generation of adversarial examples on the accuracy and robustness of image classification systems based on deep neural networks. The paper examines the theoretical foundations of the formation of defensive disturbances, the mathematical apparatus of random transformations, their relationship to deterministic cleaning methods, as well as empirical patterns of degradation of the attacking potential under various parameters of noise distributions and augmentation strategies.*

***Key words:*** *adversarial protection, noise reduction, image classification, deep learning, neural network resilience, defensive augmentation, noise transformations*

**УДК 004.8**
**ГРНТИ 20.51.19**

# СОСТЯЗАТЕЛЬНОЕ ОБУЧЕНИЕ КАК МЕТОД ПРОТИВОДЕЙТСВИЯ СОСТЯЗАТЕЛЬНЫМ АТАКАМ НА СИСТЕМЫ МАШИННОГО ОБУЧЕНИЯ

**В. Е. Садовников**

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

*Статья посвящена комплексному анализу влияния состязательного обучения (Adversarial Training) как одного из наиболее эффективных методов минимаксной оптимизации на показатели робастности и точности систем классификации изображений, построенных на базе глубоких нейронных сетей. В работе рассматриваются теоретические основы формирования защитных границ принятия решений, математический аппарат вложенной оптимизации, его соотношение с пассивными методами фильтрации, а также эмпирические закономерности деградации устойчивости классификаторов при различных параметрах генерации возмущений и стратегиях обновления весов.*

***состязательное обучение, робастность нейронных сетей, минимаксная оптимизация, состязательные примеры, глубокое обучение***

Глубокие сверточные сети – ResNet, EfficientNet, Vision Transformer – достигают 90–95 % на ImageNet и CIFAR-10, создавая иллюзию непогрешимости. Однако в их архитектуре заложена хрупкость: достаточно добавить к изображению градиентное возмущение, невидимое глазу, чтобы классификатор выдал уверенный, но в корне неверный ответ. Судить о надежности модели по чистым тестовым наборам оказалось несостоятельно; сообщество обратилось к активным механизмам защиты и минимаксным формулировкам [1].

Состязательное обучение (Adversarial Training, AT), предложенное в 2014 году и позднее получившее строгую математическую форму [2], не «латает» вход и не прячет градиенты за случайными преобразованиями. Модель обучается против наихудшего противника: внутренний цикл генерирует разрушительные примеры через PGD или C&W, внешний – подстраивает веса для их корректной классификации. Внедрение возмущенных образцов в выборку и контроль за смещением разделяющей гиперплоскости делают AT теоретически обоснованным инструментом, а не эвристикой.

Эмпирика подтверждает: если после полного цикла AT модель выдерживает адаптивную атаку, это свидетельство подлинной устойчивости. Метод фактически стал обязательным стресс-тестом; систему, не прошедшую минимаксную оптимизацию, трудно считать пригодной для задач с реальными последствиями ошибки.

Влияние на точность структурное. Алгоритм раздвигает отступы до границы решения: сеть с 95 % на чистом ImageNet без защиты проваливается ниже 10 % при атаке PGD с $\varepsilon = 8/255$, а после AT удерживает 40–50 % робастной точности. Минимаксная процедура находит конфигурацию весов, минимизирующую верхнюю границу риска, подавляя избыточную уверенность [3]. В отличие от пассивных приемов – сжатия, защитной дистилляции, входного шума, – применяемых однократно и бессильных против знающего противника, AT итеративно генерирует возмущения на каждом шаге, формируя глобально устойчивое пространство признаков с наименьшей потерей чистого качества.

Вычислительная цена определяется бюджетом $\varepsilon$ и числом итераций генератора. Малый $\varepsilon$ или короткая цепочка шагов не позволяют нащупать наихудший пример; рост параметров повышает робастность, но роняет чистую точность. Прирост выходит на плато, и основная нагрузка приходится на внутренний цикл. Для строгой проверки применяют до десяти итераций PGD, адаптивный $\varepsilon$ и раннюю остановку по робастной валидации [4]. Выбор нормы – $L_0$, $L_2$, $L_\infty$ – меняет геометрию защитных границ. AT-$L_\infty$ прижился шире благодаря простоте градиента знака и равномерному распределению возмущений; AT-$L_2$ дает более плавные деформации; AT-$L_0$ требует комбинаторных приемов из-за недифференцируемости. Модели, обученные против одной нормы, не обязательно устойчивы к другой, поэтому защищенные системы тренируют и проверяют по всем трем метрикам либо используют мульти-нормативные схемы.

AT перераспределяет ошибки по классам: изображения вблизи чужих классов стабилизируются и требуют больших возмущений для пересечения границы. Объекты с уникальной текстурой сидят далеко от разделяющих поверхностей; семантически близкие классы атакуются легче. Допускается и целевая защита – минимизация риска переклассификации в конкретный враждебный класс, что позволяет точечно контролировать поведение в критических сценариях.

Переносимость атак на AT-модели ниже, чем на незащищенные: алгоритм фиксирует устойчивые точки в пространстве параметров, специфич-

ные для данного распределения. В режиме черного ящика AT уверенно отражает стандартные атаки, но при полном доступе к весам атакующий способен запустить многошаговые адаптивные процедуры, требуя перебалансировки параметров обучения.

Наибольшую прочность дает сочетание AT с регуляризацией и архитектурными доработками. Чистый AT для крупных задач неподъемен из-за вложенной оптимизации, поэтому применяют ускоренные варианты (Free AT, FAST) или дистилляцию возмущений, оставляя полноценный AT для финального аудита. Альтернативы – Randomized Smoothing, архитектурные перестройки, замена функций активации – против сильных адаптивных атак показали себя слабо: рабочие радиусы сертификатов оказываются меньше необходимых для отражения PGD/C&W, а стохастические слои не выдерживают прямой оптимизации границы решения.

Практические последствия ощутимы в автономном транспорте, где возмущения на знаках провоцируют опасные решения; в медицинской визуализации, где AT предохраняет от ложного диагноза; в биометрии, где защита усложняет подмену личности. Это подталкивает к стандартам, обязывающим тестировать робастность с привлечением состязательного обучения до сертификации.

Состязательное обучение остается центральным инструментом исследования устойчивости: оно выявляет минимально допустимые отступы границ, вскрывает ложную робастность и служит основой для взвешенных решений о развертывании моделей. Дальнейший прогресс потребует междисциплинарных усилий, и AT в обозримом будущем сохранит свою ключевую роль.

**Список используемых источников**

1. Hameed M. Z., György A., Gündüz D. The best defense is a good offense: Adversarial attacks to avoid modulation detection // IEEE Trans. Inf. Forensics Security. 2021. Vol. 16. P. 1074–1087.

2. Kwon H., Kim Y., Yoon H., Choi D. Classification score approach for detecting adversarial example in deep neural network // Multimedia Tools Appl. 2021. Vol. 80. P. 10339–10360.

3. Karim F., Majumdar S., Darabi H. Adversarial attacks on time series // IEEE Trans. Pattern Anal. Mach. Intell. 2021. Vol. 43. P. 3309–3320.

4. Zhou M., Wu J., Liu Y., Liu S., Zhu C. DaST: Data-free substitute training for adversarial attacks // Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR). 2020. P. 10310–10319.

*Статья представлена научным руководителем, профессором кафедры автоматизированных систем специального назначения ВАС, доктором технических наук, профессором И. Б. Саенко.*

## ADVERSARIAL TRAINING AS A METHOD OF COUNTERING ADVERSARIAL ATTACKS ON MACHINE LEARNING SYSTEMS

**Sadovnikov V.**
Military Academy of Communications named after Marshal of the Soviet Union
S. M. Budyonny

*The article is devoted to a comprehensive analysis of the impact of Adversarial Training as one of the most effective minimax optimization methods on the robustness and accuracy of image classification systems based on deep neural networks. The paper examines the theoretical foundations of the formation of protective decision-making boundaries, the mathematical apparatus of nested optimization, its relationship with passive filtering methods, as well as empirical patterns of degradation of classifier stability under various parameters of perturbation generation and strategies for updating weights.*

***Key words**: competitive learning, robustness of neural networks, minimax optimization, competitive examples, deep learning*

# СОЦИАЛЬНЫЕ ТЕХНОЛОГИИ И ЭКОНОМИКА ДАННЫХ

**УДК 338.47**
**ГРНТИ 06.71.11**

## МЕНЕДЖМЕНТ ОНЛАЙН-ОБУЧЕНИЯ: АДАПТИВНОСТЬ И ПЕРСПЕКТИВЫ НА БУДУЩЕЕ

**И. Н. Александров[1], М. Ю. Фёдорова[2]**

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

*Несмотря на то, что обучение онлайн появилось достаточно давно, до сих пор остается много вопросов относительно обеспечения качества предоставления образовательного продукта онлайн. В постоянно изменяющихся условиях к образовательному продукту онлайн также постоянно предъявляются все новые и новые требования, продиктованные не только необходимостью повышением его качества, но и удовлетворением изменяющегося запроса. В работе рассмотрены ключевые аспекты менеджмента онлайн обучения с целью обеспечения адаптивности образовательной среды и перспектив ее развития. Особое внимание уделяется анализу факторов, влияющих на качество образовательного процесса, включая педагогический дизайн, уровень цифровой компетентности участников, организационные механизмы управления и использование современных технологических решений.*

***инфокоммуникационные услуги, индустрия онлайн образования, образование онлайн***

В последние годы наблюдается рост рынка онлайн образования и коммерческие образовательные организации, предлагающие разные виды дополнительного образования для взрослых и детей активно отвечают на этот запрос. [1, 2] В то же время крупнейшие участники рынка коммерческих образовательных организаций отмечают, что на смотря на постоянно растущий спрос ВУЗы не могут так же быстро отвечать на потребности рынка, как это происходит с коммерческими образовательными организациями. Что касается работодателей, то только «*15 % работодателей не готовы нанимать выпускников курсов» и ориентированы на выпускников ВУЗов»* [1]. Это, в свою очередь, при сохранении данной тенденции, а также росте популярности коммерческих образовательных организаций, ставит под угрозу спрос

на образовательный продукт ВУЗов, так как, не смотря на рост, отмечается одновременно и замедление темпов роста рынка [3], что объясняется общим снижением среднего чека на предлагаемые онлайн курсы [2]. Это обязывает образовательные учреждения более пересмотреть процессы организации образовательного процесса с целью снижения себестоимости образовательного продукта онлайн без потери качества.

В связи с этим авторами предпринята попытка проанализировать преимущества адаптивности коммерческих образовательных организаций к изменяющимся условиям рынка образования с целью предложить возможные решения для ВУЗов.

М. С. Мотышина определяет адаптивное обучение в виде подхода, «*который максимально учитывает индивидуальные способности и потребности обучающегося*». Целями адаптивного обучения по мнению М. С. Мотышина выступают «*развитие навыков самостоятельной работы, самоконтроля, приемам исследовательской деятельности*» [4]. Необходимость адаптивного обучения подчеркивается в связи с тем, что до сегодняшнего дня остается проблема низкого процента (2-5 %) завершаемости онлайн курсов, среди которых встречаются даже самые популярные.

Среди факторов, влияющих на повышение адаптивности образовательных курсов онлайн, М. С. Мотышина [4]. выделает «*психологические особенности и особенности восприятия информации, уровень «входных» знаний, цели и задачи обучения*», а Т. А. Блатова и др. [5] подчеркивают, что обучение онлайн требует совершенно иного уровня организации обучающегося, и это также накладывает особые требования на уровень входных знаний потребителя образовательного продукта онлайн.

Согласно выводу А. М. Волохова и М. Г. Бич на «*уровень развития онлайн сегмента рынка образовательных услуг влияет уровень той или иной страны прямое воздействие оказывает уровень технологического развития страны в целом*» [6, 7]. Если продолжить эту мысль, также уровень технологического развития ВУЗа непосредственно влияет на его конкурентные преимущества по отношению к коммерческим образовательным организациям и другим ВУЗами, предлагающим свой образовательный продукт онлайн. Учитывая тот факт, что согласно В. В. Макарову и др. в эпоху цифровизации высокое технологическое развитие является залогом сохранения конкурентоспособности на рынке [7, 8], следует обратить особое пристальное внимание на развитие онлайн образовательных платформ и их актуализации требованиям рынка образовательных продуктов онлайн.

Исследователи активно выделяют инструменты виртуальной и дополненной реальности [9, 10], как необходимые для обеспечения конкуренто-

способности организации, предлагающей образовательный продукт онлайн. Следует отметить, что сегодня инструменты виртуальной и дополненной реальности уже не являются особой новинкой для больших и средних представителей рынка онлайн и традиционного образования, но в то же время позволяют сразу же применять приобретенные теоретические навыки, что является серьезным конкурентным преимуществом.

Коммерческие образовательные организации сегодня активно используют инструменты геймификации [10, 11] не только с целью не только сделать образовательный процесс более интерактивным, но и с целью привлечения обучающихся.

Л. А. Снопок и др. [11] также обращают внимание на использование искусственного интеллекта для разработки обучающих систем с целью анализа прогресса обучающихся. Кроме того, работа с нейросетями сама по себе может быть использована в учебном процессе, что является инструментов геймификации. Использование искусственного интеллекта также позволяет облегчить подготовку обучающих программ, работу с документацией.

Еще один фактор, на который обращают внимание Л. А. Снопок и др. [11] и который выделяет образовательные организации, предлагающие образовательный продукт онлайн, – это использование мобильного обучения, когда образовательные платформы и образовательные курсы адаптированы для пользования на мобильном телефоне.

Согласно А. Л. Семенову и др., важным фактором, позволяющим выявить необходимые векторы развития в области предоставления онлайн образовательного продукта, является своевременное получение обратной связи от лиц, заинтересованных в получении онлайн образовательного продукта [12]. Здесь следует разделять эти категории лиц, как на работодателей и рекрутинговых агентств, от которых образовательная организации необходимо получать информацию об актуальном спросе на те или иные навыки и компетенции. А также следует собирать связь от лиц, непосредственно получающих образовательный продукт онлайн. В обоих случаях работа с обратной связь должна вестись не только по ее сбору, но также обработке, аналитике с целью последующей корректировки образовательного процесса и доведения информации об осуществленной корректировке до лиц, заинтересованных в онлайн образовательном продукте.

Еще одним важным фактором, который оказывает влияние на адаптивность образовательных организаций, предлагающих образовательных продукт онлайн выступает построение коммуникации и сбор необходимой информации о непосредственном спросе на актуальные компетенции и навыки на рынке труда [13, 14]. Данная работа зачастую ведется компаниями с пред-

ставителями бизнеса, а также с рекрутинговыми агентствами и позволяет корректировать учебный план и предоставлять программы, пользующиеся спросом со стороны потенциальных обучающихся.

Согласно проведенному исследованию практик ведущих лидеров рынка коммерческого онлайн образования и исследователей, занимающихся изучением вопроса адаптивности онлайн образования были выделены следующие приоритетные векторы, на которые можно обратить внимание при работе образовательной организации, занимающей предложением образовательного продукта онлайн:

– подготовка и корректировка образовательных программ по результатам опросов бизнес-организаций, рекрутинговых агентств;
– персонализированный подход к обучению;
– адаптивные траектории обучения;
– короткие мини-курсы до года обучения с целью получения конкретных навыков, востребованных на рынке труда
– маркетинговая деятельность ВУЗов;
– использование инструментов виртуальной и дополненной реальности.
– работа с обратной связью с лицами, заинтересованными в приобретении образовательного продукта онлайн и непосредственно его получающих.

**Список используемых источников**

1. Онлайн-образование набирает признание. URL: https://www.kommersant.ru/doc/6522559?ysclid=ltfsykn78c402652616 (дата обращения 10.04. 2026).

2. Российский рынок онлайн-образования в сфере ИИ демонстрирует рекордный рост. URL: https://www.forbes.ru/education/543382-rossijskij-rynok-onlajn-obrazovania-v-sfere-ii-demonstriruet-rekordnyj-rost (дата обращения 10.04. 2026).

3. Объем российского рынка онлайн-услуг дополнительного профессионального образования за год вырос на 6 % и достиг 52,5 млрд рублей. URL: https://www.tadviser.ru/a/864325 (дата обращения 10.04. 2026).

4. Мотышина М. С. Системный подход к обеспечению адаптивности дистанционного обучения // Системный анализ в проектировании и управлении, 2020

5. Блатова Т. А., Макаров В. В., Слуцкий М. Г. Оценка качества дистанционного обучения на базе информационно-коммуникационных технологий в образовательных организациях // Журнал правовых и экономических исследований. 2020. № 3. С. 114-121.

6. Волохов А. В., Бич М. Г., Направления повышения конкурентоспособности российского рынка онлайн-образования // Горизонты экономики. 2024. № 2 (82). С. 133-141.

7. Волохов А. В. Онлайн-сегмент рынка образовательных услуг: факторы, влияющие на степень его развитости // В сборнике: Science and technology research-2022. Сборник статей IV Международной научно-практической конференции. Петрозаводск, 2022. С. 13-20.

8. Макаров В. В., Фёдорова М. Ю. Цифровая грамотность сельского населения, необходимая для развития сферы услуг // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). Сборник научных трудов XI Международной научно-технической и научно-методической конференции. В 4-х томах. Под.

редакцией А. В. Шестакова, сост. В. С. Елагин, Е. А. Аникевич. Санкт-Петербург, 2022. С. 609-613.

9. Макаров В. В., Слуцкий М. Г., Устриков Н. К., Проблемы и задачи цифровой трансформации экономики России // Международный журнал гуманитарных и естественных наук. 2020. № 4-1 (43). С. 174-177.

10. Чернышева Е. И., Копылов Ю. А. Инновационные образовательные подходы в системе профессионального образования: путь к успеху в меняющемся мире // Актуальные проблемы современного образования: опыт и инновации. Материалы всероссийской научно-практической конференции с дистанционным и международным участием. Том 1. Ульяновск, 2026/

11. Снопок Л. А., Купрейчик А. С. Комличенко В. Н. Адаптивное online-образование: инновационные подходы к развитию образовательных услуг // Инженерное образование в цифровом обществе: материалы Международной научно-методической конференции, Минск, 14 марта 2024 г.: в 2 ч. Ч. 2 / Белорусский государственный университет информатики и радиоэлектроники; редкол.: Е. Н. Шнейдеров [и др.]. Минск, 2024. С. 160–162.

12. Семенов А. Л., Уваров А. Ю., Рудченко Т. А. Аксель Берг о цифровой трансформации образования. // В сборнике: Информатизация образования и методика электронного обучения: цифровые технологии в образовании. Материалы VII Международной научной конференции. Красноярск, 2023. С. 24-28.

13. Тренды онлайн-образования. Стоит ли открывать онлайн-школу в 2025 году – URL: https://sberbusiness.live/publications/trendi-rinka-onlain-obrazovaniya-2024-chto-nuzhno-znat-esli-vi-reshili-otkrit-onlain-shkolu (дата обращения 10.04. 2026).

14. Уваров А. Ю., Гейбл Э., Дворецкая И. В. Трудности и перспективы цифровой трансформации образования / А. Ю. Уваров, Э. Гейбл, И. В. Дворецкая [и др.]; под ред. А. Ю. Уварова, И. Д. Фрумина. М.: Изд-во ВШЭ, 2019. 343 с. DOI: https://DOI.org/10.17323/978-5-7598-1990-5.

*Статья представлена научным руководителем, доктором экономических наук, Академиком Международной академии связи, заслуженным деятелем науки РФ, руководителем образовательной программы по аспирантуре СПбГУТ, профессором В. В. Макаровым.*

## ONLINE LEARNING MANAGEMENT: ADAPTABILITY AND FUTURE PROSPECTS

**Aleksandrov I.[1], Fedorova M.[2]**
[1]Peter the Great Saint Petersburg Polytechnic University
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Despite the relatively recent emergence of online learning, many questions remain regarding the quality of online education. In a constantly changing environment, online education is constantly being subject to new demands, driven not only by the need to improve its quality but also by meeting evolving demands. This paper examines key aspects of online learning management to ensure the adaptability of the educational environment and its development prospects. Particular attention is paid to analyzing factors influencing the quality of the educational process, including pedagogical design, the level of digital competence of participants, organizational management mechanics, and the use of modern technological solutions.*

***Key words:*** *infocommunication services, online education industry, online education*

**УДК 331.5**
**ГРНТИ 06.77.61**

# ПРОБЛЕМЫ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНОЙ ИДЕНТИЧНОСТИ PR-СПЕЦИАЛИСТОВ В КОНТЕКСТЕ ПРЕКАРИЗАЦИИ РЫНКА ТРУДА

**И. А. Алексеенко, А. П. Луков**

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

*В статье раскрывается сущность профессиональной идентичности, ее структура и факторы формирования, рассматриваются проблемы формирования профессиональной идентичности в условиях прекаризации занятости в сфере общественных коммуникаций (PR). На основе результатов исследования выявляются признаки прекаризации на рынке труда Санкт-Петербурга и основные факторы, тормозящие профессиональное развитие специалистов по связям с общественностью.*

***идентификация, профессиональная идентичность, профессиональное развитие, прекаризация занятости, адаптация, специалист по связям с общественностью***

Процессы глобализации и цифровой трансформации оказывают существенное влияние на социально-экономическое положение человека в обществе. Одним из важнейших признаков формирования новой реальности в сфере общественных отношений стало размывание традиционных моделей профессиональной культуры и прекаризация занятости. Актуальность исследования обусловлена необходимостью выявления проблем формирования профессиональной идентичности специалистов по связям с общественностью и разработки рекомендаций, позволяющих обеспечить их успешную адаптацию на рынке труда.

Профессиональная идентичность как научное понятие берет истоки в профессиональной Я-концепции, предложенной Д. Сьюпером в 1949 г. Д. Сьюпер определяет профессиональную Я-концепцию как важнейший адаптационный ресурс, представляющий собой набор характеристик самовосприятия, осознаваемых индивидом как профессионально релевантные [1].

Российские ученые развили представления о процессах формирования профессиональной идентичности. Е. И. Рогов полагает, что основой формирования идентичности является идентификация – психологический процесс отождествления индивидом себя с другим человеком, группой, коллекти-

вом, помогающий ему успешно овладевать различными видами социальной деятельности, усваивать и преобразовывать социальные нормы и ценности, принимать социальные роли [2]. Л. Б. Шнейдер, развивая психологическую концепцию профессиональной идентичности, рассматривала ее как психологическую категорию, которая относится к осознанию своей принадлежности к определенной профессии и профессиональному сообществу. В данном аспекте профессиональная идентичность является результатом профессионального самоопределения, персонализации и самоорганизации [3]. Э. Ф. Зеер определял профессиональную идентичность как профессиональный «Я-образ», включающий профессиональные стереотипы и уникальность собственного «Я», осознание своей тождественности с профессиональным образом «Я». Он считал, что профессиональная идентичность формируется на основе восприятия человеком себя в рамках профессии, включая как общие представления о ней, так и личные качества и достижения [4].

Раскрывая структуру профессиональной идентичности, необходимо подчеркнуть, что она является целостной динамической системой, состоящей из следующих компонентов: профессиональное самосознание, профессиональные знания и навыки, профессиональная роль, профессиональные ценности и нормы, профессиональная мотивация, профессиональная самооценка, профессиональная идентификация [5]. Каждый компонент данной системы находится во взаимосвязи и во взаимовлиянии с остальными. Например, профессиональное самосознание включает в себя представления человека о себе как о профессионале и о своей профессиональной роли, профессиональные ценности и нормы лежат в основе профессиональной мотивации и самоидентификации, профессиональные знания и навыки обеспечивают качественное выполнение профессиональной роли и служат основой для профессиональной самооценки.

Формирование и развитие профессиональной идентичности PR-специалистов происходит как в процессе обучения в вузе, так и в процессе непосредственной работы. Процесс профессионального становления личности начинается, когда студенты приобретают первые теоретические и практические знания, принимают базовые ценностные ориентации профессии, приобретают опыт профессионального общения. Некоторые студенты во время учебы в вузе проходят стажировки или начинают работать по специальности, что только усиливает их вхождение в профессию.

Необходимо отметить, что процесс формирования профессиональной идентичности происходит под влиянием широкого круга факторов, которые могут оказывать на данный процесс как стимулирующее, так и деформирующее, тормозящее влияние [6]. Поскольку профессиональная идентичность детерминирована внутренними процессами саморазвития личности, важнейшую роль в процессе становления профессионала играют индивидуально-личностные факторы: ценностные ориентации и мотивация личности, ответственность за результаты труда, следование семейным традициям. К внешним факторам, влияющим на формирование профессиональной идентичности специалистов, можно отнести макроуровневые условия (состояние экономики идеологические императивы, культурные особенности), социально-профессиональные условия (востребованность специалистов данной профессии, состояние профессиональной культуры, престижность профессии в обществе), образовательные условия (качество подготовки специалистов в системе профессионального образования, практикоориентированность и учет потребностей рынка труда). В рамках поставленных нами целей исследования, рассмотрим влияние внешнего фактора – прекаризации рынка труда – на формирование профессиональной идентичности PR-специалиста.

Социологические исследования, проведенные на Западе и в России в 2010-2020 гг., (Г. Стендинг, О. Шкаратан, В. Бобков) позволяют представить основные аспекты феномена прекарной занятости [7]. Традиционно к признакам прекарной занятости относятся: нестабильность занятости и доходов, активная включенность в реципрокные связи (нерыночные, основанные на взаимных услугах), распространение гибких форм трудовых отношений (сезонность, ненормированный рабочий день), отсутствие социальных гарантий. Одним из признаков прекаризации труда, оказывающих долгосрочное негативное влияние на развитие социально-экономических отношений, является потеря профессиональной идентичности, происходящая вследствие частой смены работы, размывания профессиональных компетенций, ограничения профессионального развития, отстраненности от профессионального сообщества.

Для выявления признаков прекаризации в PR-сфере было проведено комплексное исследование, включающее изучение практики трудовых отношений на основе контент-анализа 184 вакансий специалистов по связям с общественностью на рынке труда Санкт-Петербурга, размещенных работодателями в марте-апреле 2026 года на портале поиска работы; опрос фо-

кус-группы из 40 студентов, обучающихся в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича по заочной форме и работающих на различных позициях в сфере PR.

Исследование позволило сделать выводы о наличии прекаризации занятости в отрасли PR и выявить проблемы, оказывающие влияние на формирование профессиональной идентичности специалистов.

Применительно к PR-сфере в Санкт-Петербурге и в целом по России тренд прекаризации занятости проявляется особенно отчетливо, что во многом обусловлено проектной и креативной природой индустрии, высокой конкуренцией и быстрой цифровой трансформацией. К основным признакам прекаризации можно отнести следующие факторы.

Выявлено активное развитие проектной занятости и фриланса вместо штатных позиций в компании, когда значительная доля PR-специалистов привлекается не на постоянную работу, а под конкретные проекты: запуск продукта, фестиваль, антикризисная кампания. По данным вакансий Санкт-Петербурга, 11 % соискателей ищут удаленную работу и еще 11 % – свободный график. На деле за этим часто скрывается фриланс без трудового договора либо контракты на 2–3 месяца с отсутствием оплаты больничных и отпусков, пенсионных отчислений и даже стабильного графика выплат.

В оформлении трудовых отношений растет доля самозанятости и договоров гражданско-правового характера вместо трудовых договоров и полагающегося к ним социального пакета. Работодатели все активнее выводят штатных PR-менеджеров за штат, назначая номинально более высокую сумму «на руки», но исключая все трудовые гарантии. Согласно опросам, 88 % PR-специалистов уже используют ИИ-инструменты для контента, и работодатели часто нанимают таких «универсальных» специалистов именно по разовым договорам, исключающим обязательства по обучению и развитию.

Рынок труда в отрасли демонстрирует нестабильность доходов и широкий разброс зарплат. Разброс в ожиданиях PR-соискателей составляет от 25 000 до 160 000 руб. и отражает не столько разницу в опыте и квалификации, а является индикатором слабой нормированности оплаты труда. Начинающий специалист может получать 25–35 тыс. руб., что ниже прожиточного минимума для комфортного проживания в Петербурге. При этом конкуренция за место с медианной зарплатой 91 000 руб. столь высока, что работодатель может позволить себе держать несколько кандидатов на испытательном сроке с меньшей ставкой, а затем не продлевать договор.

Тревожным фактором является размывание границ рабочего времени и стресс как норма трудовых отношений. Профессиональные требования к PR-деятельности, особенно антикризисной, всегда подразумевают готовность реагировать в режиме «24/7», однако в условиях прекаризации эта готовность становится требованием без адекватной компенсации. Вакансии массово указывают «стрессоустойчивость» и «многозадачность» как базовое требование, что часто означает работу в режиме постоянной перегрузки.

В условиях цифровой и технологической трансформации наблюдается постоянная гонка компетенций без поддержки работодателя. Рынок требует от PR-специалиста владения Figma, Adobe Premier, CRM, чат-ботами и нейросетями, что подразумевает постоянное совершенствование и профессиональный рост, однако инвестирует в обучение преимущественно сам сотрудник. PR-специалист вынужден непрерывно актуализировать навыки за свой счет, чтобы не потерять конкурентоспособность, при этом как только компетенции устаревают, работодатель легко находит более «цифрового» кандидата, часто на худших условиях.

Работодатели все чаще стали прибегать к замене опытных дорогих специалистов начинающими и аутсорсингом. В PR-сфере Санкт-Петербурга наблюдается опасный перекос: острый дефицит квалифицированных кадров при нежелании платить за опыт. Бизнес все чаще закрывает потребности связкой «один квалифицированный специалист на аутсорсе и несколько дешевых исполнителей на почасовой оплате». В таком случае опытные эксперты с зарплатными притязаниями от 120 до 160 тыс. руб. либо уходят в узкий консалтинг, либо переезжают в Москву за стабильностью, а оставшиеся специалисты нередко сталкиваются с падением дохода из-за сезонности проектов.

Влияние искусственного интеллекта оказывается фактором нестабильности, создавая предпосылки для сокращения персонала. Нейросети автоматизируют написание пресс-релизов, создание контент-планов и мониторинг упоминаний, что снижает порог входа в профессию и одновременно обесценивает рутинный труд. Работодатель ожидает, что один специалист с ИИ сделает работу, которую раньше выполняли три человека.

В ходе анкетирования фокус-группы было установлено значительное негативное влияние прекарных условий занятости на профессиональную идентичность: индекс 4,3 по 5-балльной шкале. На рисунке 1 представлены результаты анализа влияния факторов прекарной занятости на развитие профессиональной идентичности PR специалистов. Особенно тормозят формирование профессиональной идентичности нестабильный доход, от-

сутствие видимых карьерных перспектив и недостаточность социальных гарантий.




Рис. 1. Влияние факторов прекарной занятости на профессиональную идентичность PR специалистов (% опрошенных, давших утвердительный ответ)

Таким образом, пути преодоления барьеров для профессиональной идентичности PR специалистов в условиях прекаризации рынка труда лежат в двух плоскостях. Работодателям необходимо создать организационные, финансовые и психологические условия для профессионального развития PR специалистов, что в конечном итоге отразится на повышении качества работы и экономической эффективности компаний. Не менее важной является собственная активная позиция специалиста, формирующая его профессиональную Я-концепцию: саморефлексия, обучение, повышение квалификации, развитие профессиональных контактов, поиск баланса между работой и личной жизнью. Преодоление барьеров профессиональной идентичности отвечает глубоким и долгосрочным интересам личности, общества и государства.

**Список используемых источников**

1. Рикель А. М. Профессиональная Я-концепция и профессиональная идентичность в структуре самосознания личности. Часть 1 // Психологические исследования: электрон. науч. журн. 2011. № 2. URL: http://psystudy.ru (дата обращения: 07.05.2026).

2. Рогов Е. И. Выбор профессии. Становление профессионала [Текст] / Е.И. Рогов. М.: ВЛАДОС-ПРЕСС, 2003. 336 с.

3. Шнейдер Л. Б. Профессиональная идентичность. М.: МОСУ, 2001. 272 с. URL: https://psychlib.ru/inc/absid.php?absid=15490. (дата обращения: 07.05.2026).

4. Зеер Э. Ф. Психология профессий: Учебное пособие для студентов вузов. 2-е изд., перераб., доп. М.: Академический Проект; Екатеринбург: Деловая книга, 2003. 336 с. («Gaudeamus»). URL (дата обращения: 07.05.2026).

5. Опетенок Н. Г. Структурные компоненты профессиональной идентичности: теоретический анализ // Universum: психология и образование: электрон. научн. журн. 2025. 10(136). URL: https://7universum.com/ru/psy/archive/item/20866 (дата обращения: 28.04.2026).

6. Нор-Аревян О. А., Шаповалова А. М. Факторы формирования профессиональной идентичности // Гуманитарий Юга России. 2016. Том 21. № 5. С. 102-113.

7. Растегаева А. В. Прекаризация на современном рынке труда: основные признаки и причины распространения // Вестник ПАГС. 2018. № 3. URL: https://cyberleninka.ru/article/n/prekarizatsiya-na-sovremennom-rynke-truda-osnovnye-priznaki-i-prichiny-rasprostraneniya (дата обращения: 28.04.2026).

## PROBLEMS OF FORMING PROFESSIONAL IDENTITY OF PUBLIC RELATIONS SPECIALIST IN THE CONTEXT OF LABOR MARKET PRECARIZATION

**Alekseenko I., Lukov A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article reveals the essence of professional identity, its structure and factors of formation, and examines the problems of forming professional identity in the context of precarious employment in the field of public relations (PR). Based on the results of the study, the article identifies the signs of precariousness in the St. Petersburg labor market and the main factors that hinder the professional development of public relations specialists.*

***Key words:*** *identification, professional identity, professional development, precarious employment, adaptation, Public Relations specialist*

**УДК 32.019.5**
**ГРНТИ 02.41.31**

# ПОЛИТИЧЕСКАЯ РОЛЬ ПРЕКАРИАТА В УСЛОВИЯХ МЕДИЙНОЙ НЕВИДИМОСТИ: ОТ «ОПАСНОГО КЛАССА» К «МОЛЧАЛИВОМУ БОЛЬШИНСТВУ»

**И. А. Алексеенко, А. С. Халапян**

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

*В статье анализируется политический потенциал прекариата – социального класса, сформированного в результате неолиберальной трансформации рынка труда и цифровизации экономики. Феномен медийной невидимости прекариата в СМИ препятствует формированию классового сознания и коллективной политической субъектности. Прекариат, оставаясь одной из самых многочисленных социальных групп, оказывается исключен из публичного политического дискурса, что создает риски радикализации и делает его уязвимым для популистских политических проектов.*

***прекариат, медийная невидимость, политизация, политическая субъектность, социальная уязвимость, политические риски***

В 2011 году британский экономист Гай Стэндинг опубликовал книгу «Прекариат: новый опасный класс», в которой впервые системно описал социальную группу, чье существование долгое время оставалось на периферии социологического анализа [1]. Прекариат – это не просто совокупность людей с нестабильной занятостью, отсутствием социальных гарантий и неуверенностью в будущем. Это качественно новый социальный феномен, порожденный неолиберальной политикой 1980-х годов, глобализацией и цифровой революцией. Однако, несмотря на свою растущую численность, прекариат остается в значительной степени невидимым в публичном пространстве – и эта невидимость имеет прямые политические последствия. Центральными сейчас являются вопросы о том, как медийное игнорирование прекариата влияет на его политическую субъектность и какие риски это создает для стабильности политической системы.

По определению Г. Стэндинга, прекариат является протоклассом, поскольку он представляет собой промежуточный класс между традиционными рабочими и средним классом, и его члены могут сталкиваться с множеством экономических и социальных рисков. Прекариат занимает пятое

место в семиступенчатой социальной иерархии, уступая лишь безработным и социально обездоленным, но при этом принципиально отличается от традиционного рабочего класса [1]. Если пролетариат обладал (пусть и ограниченными) механизмами коллективной защиты – профсоюзами, трудовым законодательством, политическими партиями, выражавшими его интересы, – то прекариат лишен этих инструментов. Для него характерны: отсутствие гарантий занятости, острая зависимость от сиюминутного дохода, ограничение трудовых прав, отсутствие профессиональной идентичности и, как следствие, уязвимость [2; 3].

По мнению П. Бурдье, отсутствие четких профессиональных признаков, дифференциация уровня образования и дохода не позволяют рассматривать прекариат в контексте классической теории социальной стратификации, соотносить его с высшим, средним или низшим слоями. Поскольку прекариат находится в процессе становления и еще не осознал своего единства, он может быть рассмотрен как возможный класс. Так, его представители занимают сходную позицию в социальном пространстве, которая обусловливается наличием экономического, социального и культурного капиталов, и будут оказывать меньше сопротивления в случае необходимости их «мобилизации», поскольку еще не осознали своего единства и общности интересов [4].

При этом прекариат неоднороден по своему составу: в него входят и курьеры, и таксисты, и IT-специалисты на аутсорсе, и журналисты-фрилансеры, и самозанятые, чье число в России к концу 2024 года достигло 12 млн человек [5].

Именно эта численность делает прекариат значимой политической силой – или, по крайней мере, потенциальной политической силой. В России, по оценкам Ж. Т. Тощенко, доля прекаризированных слоев может достигать 40 % трудоспособного населения [2]. Это означает, что прекариат – это не маргинальная группа, а массовый социальный слой, чьи интересы в силу своего масштаба не могут быть проигнорированы в политическом процессе.

Политизация прекариата – это процесс, в ходе которого представители этой социальной группы начинают осознавать свои коллективные интересы и требовать улучшения своих условий жизни и труда. На рисунке 1 представлены условия, способствующие политизации прекариата, а также возможные способы проявления политической активности данного социального слоя. К условиям политизации прекариата можно отнести экономическую нестабильность, социальное неравенство, глобализацию

экономических связей, развитие социальных и политических движений. Осознание классовых интересов в сочетании с кризисом доверия к власти и доступом к информации в цифровой среде может значительно ускорить процессы политизации, вовлекая широкие слои представителей прекариата в политическую жизнь общества.

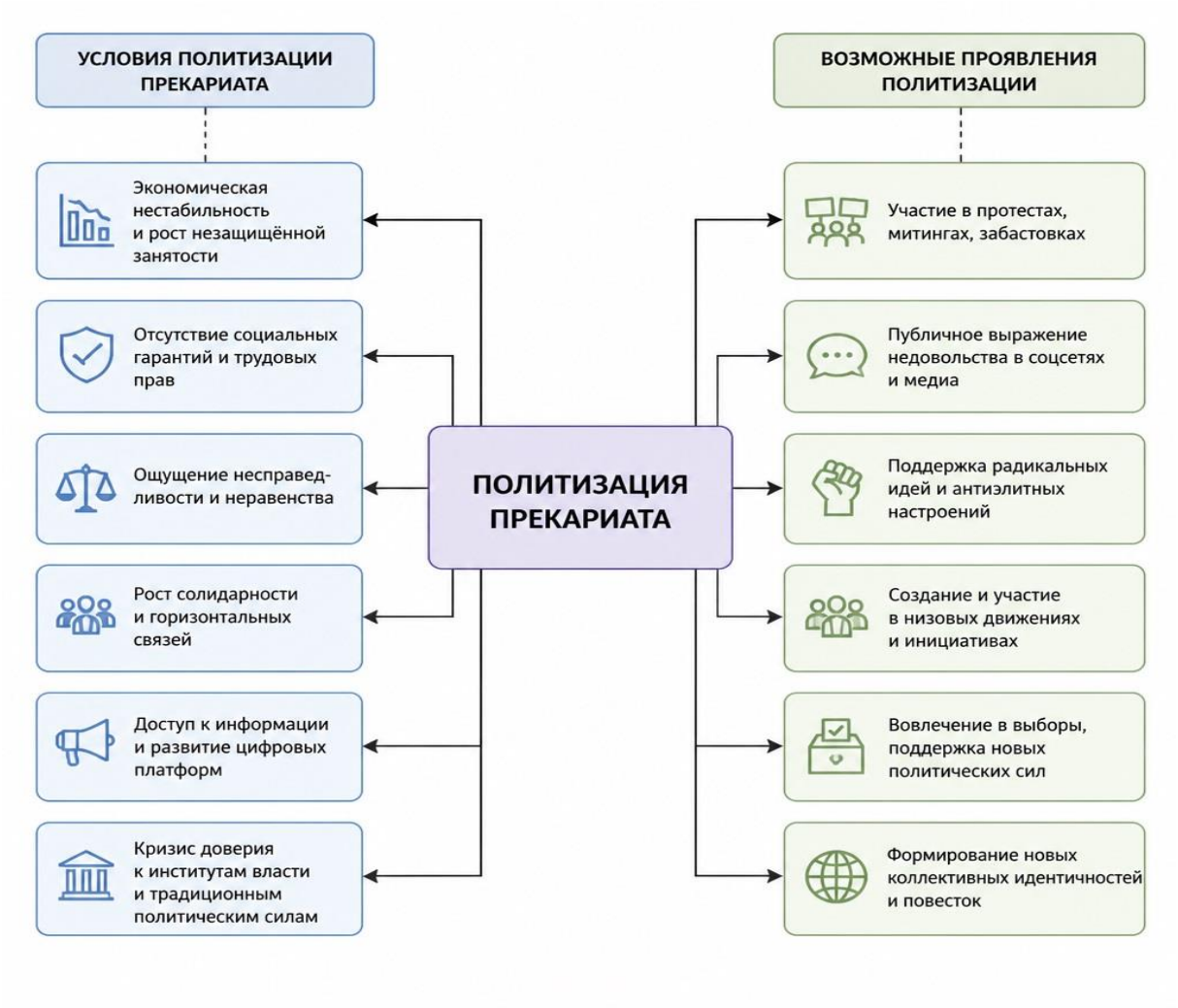



Рис. 1. Процессы политизации прекариата

Однако здесь возникает ключевое противоречие: имея количественную мощь и осознание необходимости улучшения своего социально-экономического положения, прекариат лишен собственного голоса. Одним из главных факторов, препятствующих превращению прекариата в политическую силу, является его медийная невидимость. Под медийной невидимостью понимается не отсутствие упоминаний о людях, относящихся к этой группе, а отсутствие их репрезентации именно как класса – как общности, обладающей общими интересами, общими проблемами и потенциально общей политической волей.

Анализ российского медиаполя позволяет выделить несколько уровней репрезентации прекариата. На экспертном уровне (научные журналы, специализированные издания) термин активно используется, ведутся дискуссии о границах класса и методологии его изучения [6; 7]. На уровне деловой прессы (Forbes, РБК, «Коммерсант») прекариат освещается фрагментарно, обычно в контексте статистических отчетов или острых социальных событий (забастовки курьеров, изменения в налоговом законодательстве) [8; 9]. Однако в масс-медиа и новостной ленте понятие «прекариат» практически отсутствует. Вместо него используются конкретные профессиональные категории: «курьеры», «водители такси», «самозанятые», «фрилансеры», «удаленщики».

Такая замена не является нейтральной. Когда проблема описывается через профессиональные группы, она фрагментируется. Курьер не видит своих проблем в проблемах таксиста, а дизайнер-фрилансер не идентифицирует себя с самозанятым мастером по ремонту. В результате класс распадается на отдельных индивидов, каждый из которых борется со своей нестабильностью в одиночку.

Эта медийная фрагментация имеет прямые политические последствия. Гай Стэндинг называл прекариат «опасным классом» не потому, что его представители склонны к насилию, а потому, что, лишенные традиций социальной памяти и конкретных механизмов защиты, они становятся уязвимы для политических сил, предлагающих простые и радикальные решения [1]. У прекариата пока почти нет собственных организаций и идеологии, но таких людей становится все больше, и к ним все чаще обращаются политики, которые умело работают с их повышенной тревожностью и неуверенностью. Именно прекариат, по мнению Стэндинга, обеспечил подъем новых правых движений в США и Западной Европе – Tea Party [1].

В российской специфике этот механизм может проявляться иначе, но суть остается той же. Прекариат в условиях отсутствия видимости и легитимных каналов репрезентации может быть использован самыми разными силами. При этом важно понимать, что прекариат не голосует как класс не потому, что у него нет политических предпочтений, а потому, что эти предпочтения не заявлены в публичном пространстве.

Психологический профиль прекариата, описанный в исследованиях, лишь усиливает эту уязвимость. Как отмечают О. И. Миронова и М. М. Алексапольская, для представителей данной социальной группы характерны постоянное пребывание в ситуации неопределенности, отсутствие

субъективного контроля, тревожность и утрата профессиональной самоидентификации, а их деятельность направлена преимущественно на стабилизацию социального и финансового положения [10]. Хроническая тревога, эмоциональное истощение и дефицит доверия к социальным институтам делают прекариев особенно восприимчивыми к политическим обещаниям, сулящим простое и скорое решение их проблем.

При этом медиа, вместо того чтобы говорить о классовых интересах прекариата, часто впадают в две крайности. Первая – стигматизация, когда прекарии изображаются как неудачники или социальные аутсайдеры. Вторая – романтизация фриланса, когда нестабильность подается как «свобода» и «независимость», а отсутствие социальных гарантий остается за кадром. Обе стратегии уводят от осознания проблемы как системной и требующей политического решения.

Прекариат представляет собой значительную по численности социальную группу, чей политический потенциал находится в прямом противоречии с отсутствием его полноценного присутствия в публичном пространстве. Медийная невидимость прекариата – это не случайное упущение, а закономерный результат того, что СМИ практически не используют обобщающие понятия, способные объединить эту группу. Политическая позиция прекариата остается не заявленной, но это не означает, что ее нет: в условиях нарастающей социально-экономической нестабильности, которую исследователи связывают с развитием искусственного интеллекта и автоматизацией [11], прекариат может стать ключевой политической силой. Задача политической системы и медиа – не ждать, пока эта потенциальная сила проявит себя в крайних формах, а создавать возможности для выражения интересов прекариата, включая его полноценное отражение в информационном поле. Пока же прекариат остается молчаливым большинством – классом, который существует, голосует, но не говорит вслух, и в этой тишине кроется главный политический риск современности.

## Список используемых источников

1. Стэндинг Г. Прекариат: новый опасный класс. URL: https://djvu.online/file/xfH4CrEceJsN4 (дата обращения: 20.03.2026).

2. Тощенко Ж. Т. Прекариат – новый социальный класс // Социологические исследования. URL: https://www.socis.isras.ru/article/5237 (дата обращения: 20.03.2026).

3. Тощенко Ж. Т. (ред.) Прекариат: становление нового класса. М.: Центр социального прогнозирования и маркетинга, 2020. С. 400 URL: https://www.isras.ru/files/File/publ/Toschenko_Prekariat_2020.pdf (дата обращения: 20.03.2026).

4. Бурдье П. Социология социального пространства. М.: Институт экспериментальной социологии, 2007. С. 288.

5. Федеральная налоговая служба. Более 12 млн самозанятых зарегистрировались в России. URL: https://www.nalog.gov.ru/rn77/news/activities_fts/15487019/ (дата обращения: 20.03.2026).

6. Кученкова А. В. Прекаризация занятости: к методологии и методами измерения // Вестник РУДН: Социология, Москва, 2019. Вып. 1. С. 137.

7. Вартанова Е. Л. Медиапрекариат: в условиях неопределенности // Меди@льманах, Москва, 2021. Вып. 5. С. 11.

8. Forbes Life. Опасный класс: что такое прекариат и почему люди оказываются без стабильной работы. URL: https://www.forbes.ru/forbeslife/543133-opasnyj-klass-cto-takoe-prekariat-i-pocemu-ludi-okazyvautsa-bez-stabil-noj-raboty (дата обращения: 20.03.2026).

9. РБК. Тренды на рынке самозанятости в 2025 году. URL: https://trends.rbc.ru/trends/social/6798589f9a7947620aba78ad (дата обращения: 20.03.2026).

10. Миронова О. И., Алексапольская М. М. Совладающее поведение представителей социальной группы прекариата в ситуации неопределенности // Психология и педагогика служебной деятельности, Москва, 2025. Вып. 2. С. 43–44.

11. Шатунова Д. С., Шхагошев Р.В. Влияние автоматизации и искусственного интеллекта на рынок труда и экономическую стабильность // Международный научный журнал «Вестник науки», Ростов-на-Дону, 2024. Вып. 12. С. 497–498.

## THE POLITICAL ROLE OF THE PRECARIATE IN THE CONDITIONS OF MEDIA INVISIBILITY: FROM THE “DANGEROUS CLASS” TO THE “SILENT MAJORITY”

**Alekseenko I., Khalapyan A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article analyzes the political potential of the precariat, a social class formed as a result of the neoliberal transformation of the labor market and the digitalization of the economy. The phenomenon of the media invisibility of the precariat prevents the formation of class consciousness and collective political agency. Despite being one of the most numerous social groups, the precariat is excluded from public political discourse, which creates risks of radicalization and makes it vulnerable to populist political projects.*

***Key words:*** *precariat, media invisibility, politicization, political subjectivity, social vulnerability, and political risks*

**УДК 355.58**
**ГРНТИ 81.93.21**

# ОСОБЕННОСТИ ЭКОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ В СОВРЕМЕННОМ ОБЩЕСТВЕ

**Н. Н. Бабин**

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

*Экологическое образование является важным фактором в улучшении экологической ситуации. Как формальный, так и неформальный подходы в осуществлении экологического образования дают осознание чувствительности окружающей среды к внешнему воздействию и приобретение навыков в решении экологических проблем. Важно, чтобы экологическое просвещение сочеталось с экологическими коммуникациями, ключевыми компонентами которых являются научная обоснованность, качество образования, критическое мышление и высокая эффективность при низких затратах. Экологическое образование приводит к экологически чистому образу жизни человека.*

***экологическое образование, экологические коммуникации, экологически чистый образ жизни***

Первым шагом в содействии улучшению экологической ситуации является предоставление информации и знаний о ней. На практике существуют всевозможные взаимосвязи между знанием и действием. Последствия могут проявляться только в следующем поколении, к тому же далеко в географическом отношении, но они могут быть ошеломляющими. Донести до людей информацию о чем-то далеком и очень опасном, но невидимом в повседневной жизни, достаточно сложно. Осведомленность об окружающей экологической ситуации в собственном доме или районе может являться платформой для ознакомления с состоянием экологии в глобальном масштабе. Повышение осведомленности и образование идут рука об руку.

Экологическое образование является довольно молодой областью знаний, которая при этом очень быстро развивается. Основной целью экологического образования можно назвать осознание чувствительности окружающей среды к внешнему воздействию и приобретение навыков в решении экологических проблем. Экологическое образование предполагает не только передачу знаний об окружающей среде, но и включение когнитивных и эмоциональных ценностей, которые могут стимулировать людей изменять свое отношение к окружающей среде и способствовать позитивному поведению.

Существует два основных подхода в осуществлении экологического образования – формальный и неформальный. Эти подходы используются взаимозаменяемо, в некоторых случаях границу между ними, когда один начинается, а другой заканчивается, трудно определить [1].

Формальное образование использует разработку учебных программ для краткосрочных курсов, модулей, тем и вставок в учебные планы. Формальное образование сочетает в себе осведомленность, знания, навыки, отношение и участие. Это может быть:

– изучение окружающей среды – понимание природных и человеческих систем и их взаимодействий;
– образование через окружающую среду – окружающая среда используется в качестве средства исследования и изучения;
– образование для окружающей среды – развитие осознанной заботы об окружающей среде и воспитание бережного отношения к ней.

Неформальное образование характеризуется отсутствием определенного набора правил со строгой структурой, учебными программами и процедурой отчетности. Оно способно более гибко реагировать на местные экологические проблемы, которые имеют большое социальное значение и полезность для общества и в меньшей степени зависят от академических требований. Неформальный подход так же важен, как и формальный, и поэтому его следует считать обязательным наряду с формальным экологическим образованием, если конечной целью является формирование экологически информированного, интеллектуального и эффективного гражданского общества.

Для того, чтобы действенно выполнять свою роль, экологическое просвещение должно сочетаться с экологическими коммуникациями [2].

Ключевые компоненты коммуникаций включают:

– научная обоснованность – все методы (ресурсы) должны соответствовать новейшим научным знаниям в области прикладных междисциплинарных наук;
– качество образования – все методы (ресурсы) должны быть адаптированы к психическому и физическому состоянию обучающегося и соответствовать всем другим педагогическим принципам;
– критическое мышление – все средства коммуникации отражают определенную предвзятость, и, делая это явным, можно развивать критическое мышление как важнейший компонент процесса экологического образования;

– высокая эффективность при низких затратах – все методы (ресурсы) должны быть широкодоступными и использоваться на международном уровне;
– средства коммуникации должны включать входные данные, которые относятся к социальным, экономическим, эстетическим, этическим и другим элементам, имеющим значение для экологических проблем.

Экологическое образование приводит к изменению образа жизни человека. Образ жизни во многом определяется привычками человека. Поведение, связанное с окружающей средой, позволяет говорить об экологически чистом образе жизни [3]. Многие модели поведения, наносящие вред здоровью, аналогичны моделям поведения, наносящим ущерб окружающей среде, в том смысле, что они не являются незаконными, а скорее частью нормального и общепринятого репертуара, в отличие, например, от преступного поведения. Ясно, что полученная индивидом информация о том, что его поведение наносит ущерб, автоматически не приводит к изменениям. Однако сама по себе информация важна в ситуациях, когда существуют внутренние факторы, блокирующие изменения, например, если человеку не хватает информации, он не знал о проблеме раньше или не доверял тому, что он видел ранее. Информация, если она используется, должна быть направлена на информирование людей о проблеме и повышение доверия, то есть убеждать людей. Но если внешние факторы являются более важными, такие как структурные препятствия, отсутствие инфраструктуры и т.д., то информации недостаточно.

Как повлиять на склонность людей неосмотрительно выбрасывать мусор или твердые отходы? Ситуация или предшествующие события имеют важное значение, например, частные территории менее замусорены, чем общественные, уже замусоренные территории становятся еще более замусоренными. Кроме того, решающее значение для нового поведения имеет доступность, чтобы была доступна альтернатива, то есть мусорное ведро или контейнер для отходов. Засорение уменьшится на 15-30 %, если будут доступны контейнеры для отходов, и еще эффективнее, если мусорные баки красиво оформлены. Пространство вокруг украшенных контейнеров будет довольно чистым по сравнению с остальной территорией.

Очевидный способ повлиять на поведение – это поощрение. Эти так называемые подсказки обычно представляют собой словесные инструкции, но иногда ими могут быть другие люди или предметы. Успешные подсказки различны, они поощряют поведение, которое уже существует в репертуаре

индивида, и они поощряют поведение, которое может быть выработано прямо сейчас. Подсказки становятся неэффективными, когда существует слишком большое расстояние во времени и пространстве до возможности выполнить все, о чем просят. Эффективность выше при использовании подсказок, выражающих желание или вежливую просьбу, а не тех, в которых указывается, что поведение является обязательным или запрещенным. Такие требования часто приводят к негативной реакции [4].

Поскольку истинные экологические последствия будут далеко, кто-то попытается создать «искусственные» положительные эффекты, награды за изменение поведения. Проще всего получить экономическое вознаграждение, такое как возврат депозита за бутылки или участие в лотерее с шансом выиграть деньги. Установлено, если есть экономическая выгода от доставки отходов в контейнеры, люди даже привозят отходы из других отдаленных районов.

Следует упомянуть выбор потребителями экологически чистых продуктов, поскольку эта область включает в себя достижения перехода к экологически правильному поведению. Появление продуктов с экологической маркировкой помогает потребителю перейти на экологически чистые продукты. Тем не менее, это не так просто, поскольку новые продукты часто стоят дороже, по крайней мере, когда они производятся небольшими сериями. Вероятно, это будет продолжаться до тех пор, пока цены на обычные продукты не будут включать стоимость ущерба окружающей среде, что сегодня редко практикуется.

Энергосбережение чаще всего решается с помощью технологических инноваций, то есть путем внедрения новых источников энергии и информационных технологий. Скидка при экономии энергии – это один из подходов, который доказал свою эффективность. При этом важное значение имеет обратная связь с энергопоставщиками, позволяющая потребителям получать информацию о потребленной энергии и расходах за ее оплату.

Как правило, внимание на экономию электроэнергии обращается лишь тогда, когда затраты на ее потребление становятся существенными для бюджета отдельной семьи. К типовым мерам энергосбережения можно отнести утепление оконных и дверных проемов, использование приборов с низким энергопотреблением. Более эффективные меры, такие как установка солнечных батарей или систем автономного теплоснабжения, распространены еще не во всех регионах, но их внедрение неизбежно, когда это будет экономически обосновано.

Можно вспомнить, что сокращение потребления воды во многом решалось с помощью технических решений, а не изменения поведенческих подходов людей. В качестве примеров можно указать новые насадки для душа и туалеты, которые потребляют меньше воды. В некоторых случаях это привело к сокращению потребления воды до трех раз, до 100-150 литров на человека в день, что является вполне приемлемым уровнем.

Современный образ жизни характеризуется значительной мобильностью. Мы пользуемся различными средствами коммуникаций, в которых доминируют автомобили. Но при этом очевидно, что использование автомобилей оказывает негативное воздействие на окружающую среду, даже если технические и экологические стандарты двигателей внутреннего сгорания будут значительно улучшены.

Тем не менее люди пользуются автомобилями. Как правило, в качестве главной причины можно отметить фактор времени. Так, средняя поездка на автомобиле, если считать от двери до двери, в десять раз быстрее, чем пешком, в четыре раза быстрее, чем на велосипеде, и в два раза быстрее, чем на общественном транспорте.

В качестве общих выводов о мобильности общества можно указать:

1. Пройденное расстояние в основном определяется скоростью. Сегодня автомобиль предлагает лучшую скорость.

2. Расстояния для поездок, во многом, определяют экономические возможности. Более высокие цены на эксплуатацию автомобиля, например, более дорогое топливо, являются одной из причин сократить пробег автомобилей.

Можно предположить, что более экономически эффективные транспортные системы будут в основном использоваться для поездок на большие расстояния. Если поездки на работу станут более затратными, люди пересядут на общественный транспорт или будут работать по удаленной схеме, но не меньше путешествовать. Изменения в обществе, которое стремится сократить поездки, такие как уплотнение городов, вероятно, только переместит поездки в другие области, такие как поездки в свободное время.

Таким образом, инновационные методы экологического образования имеют критически важное значение в современном обществе. Они не только повышают уровень осведомленности людей о необходимости сохранения окружающей среды, но и формируют активную жизненную позицию граждан, способных участвовать в решении экологических проблем.

**Список используемых источников**

1. Попов А. М. Актуальные проблемы экологического образования и воспитания // Вестник ОмГУ. 2007. № 1. С. 141-164.
2. Романчук М. В. Проблемы экологического образования в современном мире // Научный аспект. Самара: Изд-во «Аспект», 2020. С. 1-5.
3. Топор А. В., Иващенко О. В. Зарубежный опыт и мировые тенденции в организации экологического образования // Молодой ученый. 2013. № 10. С. 539-542.
4. Хуррамов И. А. Проблемы экологического образования и воспитания на примере мирового сообщества // Молодой ученый. 2012. № 11. С. 493-496.

## FEATURES OF ENVIRONMENTAL EDUCATION IN MODERN SOCIETY

**Babin N.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Environmental education is an important factor in improving the environmental situation. Both formal and informal approaches to environmental education provide awareness of the environment's sensitivity to external influences and the acquisition of skills in addressing environmental challenges. It is crucial to combine environmental education with environmental communication, which emphasizes scientific evidence, quality education, critical thinking, and cost-effectiveness. Environmental education leads to a sustainable lifestyle.*

***Key words:*** *environmental education, environmental communication, and an environmentally friendly lifestyle*

**УДК 004.089**
**ГРНТИ 20.19.01**

# ГИБРИДНЫЙ ПОДХОД К РЕФЕРАТИВНОЙ РАБОТЕ В ЭПОХУ ИИ: ПРОМПТ-ИНЖИНИРИНГ И РУЧНОЕ ПЕРЕПИСЫВАНИЕ КАК ИНСТРУМЕНТ ГЛУБОКОГО УСВОЕНИЯ

**А. Р. Балса, Н. А. Николаева**

Государственный университет морского и речного флота им. адмирала С. О. Макарова

*В статье рассмотрена роль искусственного интеллекта в развитии цифровой педагогики. Анализируются проблемы написания рефератов при массовом использовании ИИ (YandexGPT, GigaChat), приводящем к поверхностному усвоению материала. Предложен гибридный метод: ИИ-генерация черновиков, их ручное переписывание и вопросы по тексту реферата. Эксперимент показывает, что примерно половина студентов не отвечают на вопросы по переписанному тексту, что подтверждает эффективность предложенного в статье подхода. Метод формирует навыки осмысленного использования ИИ в академической работе.*

***гибридный подход, ГигаЧат, искусственный интеллект (ИИ), критическое мышление, нейросеть, проектированию запросов (промпт-инжиниринг), рефераты, ручное переписывание, цифровая педагогика, YandexGPT***

Искусственный интеллект (ИИ) прочно вошел в образовательный процесс как свершившийся факт, трансформируя повседневные практики преподавания и обучения. Первоначальный энтузиазм преподавателей был связан со значительным сокращением времени на подготовку занятий с помощью ИИ. Использование в работе готовых инструментов помогло ускорить подбор и анализ онлайн-источников, упростило формулировки практических заданий с учетом профиля обучения, облегчило создание рабочих программ и тестов для ФОС. Но довольно скоро стало ясно, что вместе с удобством появились и новые педагогические проблемы [1–3].

Многие традиционные формы изучения материала студентами, нацеленные на более глубокую проработку и указанные в рабочих программах, перестали давать прежний эффект. Так как студенты все чаще передают выполнение заданий тем же ИИ-инструментам, нередко даже не вчитываясь в формулировку задания и ограничиваясь механическим копированием в запрос для ИИ. В результате не получается глубокого усвоения материала и формирования ключевых компетенций, таких как критическое мышление,

способность к самостоятельному анализу и интерпретации информации. По сути, студенты превращаются в операторов нейросетей, а не в их осмысленных пользователей.

Особое внимание в контексте использования ИИ студентами заслуживает такая традиционная форма работы, как рефераты, предусмотренные рабочими программами многих дисциплин. Рефераты представляют собой краткий обзор научной литературы по заданной теме, предполагающий поиск, анализ, синтез источников и оригинальное изложение материала в целях формирования навыков научного мышления и академического письма. Но с внедрением ИИ (YandexGPT, GigaChat, ChatGPT) реферативная работа утратила свою эффективность. Студенты всего лишь делегируют генерацию текста нейросетям, копируя запросы без вникания в содержание, что приводит к поверхностному усвоению и размыванию компетенций анализа и синтеза.

В некоторых источниках указывается, что преподаватели отмечают снижение в рефератах критической обработки текста и отсутствие осмысленных выводов [4]. Получив подобное замечание от преподавателя, студент обрабатывает текст повторно через ИИ с указанием запроса: «Сделай выводы по тексту». Далее он приносит сдавать слегка подправленную работу, по-прежнему даже не прочитав ее.

Таким образом, из выше сказанного следует, что вместо борьбы с использованием ИИ традиционными методами контроля, необходимо радикально переосмыслить подход к реферативной работе, интегрировав нейросети в образовательный процесс осознанно и целенаправленно.

Одно из перспективных решений заключается в обдуманной интеграции нейросетей в процесс написания рефератов. При данном подходе студентам разрешается генерировать черновики с помощью ИИ для автоматизации рутины – поиска, анализа и структурирования материала. Также предполагается обучить студентов грамотному «проектированию запросов» (промпт-инжинирингу) – навыкам точной формулировки инструкций для получения логичных и достоверных результатов.

Одним из подходов является самостоятельное задание студентом роли ИИ, например, «Ты – специалист по Python для анализа данных» или «Ты – эксперт по симуляции навигационных процессов». Это ключевой прием: указывая роль, студент настраивает ИИ под конкретную задачу, получая релевантный текст реферата вместо общего или поверхностного ответа.

Для улучшения качества работы ИИ рекомендуется дальше конкретизировать задачу. Например, задать: «Напиши реферат для студентов 1-го курса бакалавриата по Python» со следующей структурой: «Введение (проблема, цель, задачи); основная часть (3–4 абзаца с анализом источников); выводы (2–3 предложения, пишутся по задачам)».

Перечитывая результат, сгенерированный ИИ, следует уточнять запросы, например: «В разделе «Выводы» добавить критический анализ источников X и Y из текста»; «В разделе «Использование» приведи 2 реальных примера кода на Python из практики анализа данных и объясни их отличия»; или аналогично для других разделов.

Дополнительно к интеграции ИИ предлагается комбинированный подход, включающий ручное переписывание сгенерированного ИИ черновика. Этот метод сочетает автоматизацию с низкотехнологичным контролем глубокого усвоения материала. То есть студент генерирует черновик реферата с помощью ИИ, а затем переписывает его от руки. Переписывание активирует моторную память и зрительное восприятие, обеспечивая непроизвольное запоминание структуры текста, ключевых фраз и логических связей, то есть эффекта, недостижимого при печати [5].

Вопросы преподавателя при защите реферата следует формулировать не как общие по теме, а по конкретным фрагментам текста. Например, «Что изложено во 2-м абзаце про Python Pandas?». При этом проверяются не энциклопедические знания, а факт осознанного чтения и усвоения. Такой контроль выявляет студентов, выполнивших переписывание механически, без понимания содержания.

В педагогической практике авторов статьи примерно половина студентов не смогли ответить на простые вопросы по только что переписанному от руки тексту. Это свидетельствует о поверхностном усвоении при работе только с ИИ и подтверждает эффективность ручного переписывания как фильтра понимания.

Таким образом, этот гибридный подход – ИИ плюс ручное переписывание и вопросы, ответы на которые написаны студентами в защищаемом реферате – оптимально сочетает производительность нейросетей с глубиной традиционных педагогических методов, формируя навыки осмысленного использования ИИ в академической работе.

**Список используемых источников**

1. Цифровая среда в образовательных организациях различных уровней: Аналитический доклад / Н. Б. Шугаль, Н. В. Бондаренко, Т. А. Варламова [и др.]. Москва: Национальный исследовательский университет "Высшая школа экономики", 2023. 164 с. (Мониторинг экономики образования).

2. Балса А. Р. Искусственный интеллект в цифровой педагогике: новые тенденции и вызовы / А. Р. Балса, Н. А. Николаева // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025): Сборник научных статей, Санкт-Петербург, 17–21 февраля 2025 года. Санкт-Петербург: СПбГУТ, 2025. С. 49-53.

3. Микелевич Е. Б. Отношение студентов к использованию chatgpt в учебной деятельности: результаты эмпирического исследования / Е. Б. Микелевич // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2025. № 2. С. 35-43.

4. Грицай Л. А. Кризис письменных заданий: необходимость изменения формата обучения студентов в эпоху искусственного интеллекта / Л. А. Грицай // Цифровая гуманитаристика и технологии в образовании (DHTE 2025): Сборник статей VI Международной научно-практической конференции , Москва, 13–14 ноября 2025 года. Москва: Московский государственный психолого-педагогический университет, 2025. С. 155-169.

5. Mueller, F. M., & Oppenheimer, D. M. The Pen Is Mightier Than the Keyboard: Advantages of Longhand Over Laptop Note Taking // Psychological Science, 201425(6), 1159–1168.

## A HYBRID APPROACH TO ABSTRACT WRITING IN THE AI ERA: PROMPT ENGINEERING AND MANUAL REWRITING AS TOOLS FOR DEEP LEARNING

**Balsa A., Nikolaeva N.**
Admiral Makarov State University of Maritime and Inland Shipping

*This article examines the role of artificial intelligence in advancing digital pedagogy. It analyzes challenges in abstract writing amid widespread AI use (YandexGPT, GigaChat), which leads to superficial material comprehension. A hybrid method is proposed: AI-generated drafts, manual rewriting, and quiz questions on the rewritten abstract. An experiment reveals that approximately half of students fail to answer questions on their rewritten texts, confirming the approach's effectiveness. The method fosters skills for meaningful AI integration in academic work.*

***Key words:*** *artificial intelligence (AI), abstracts, critical thinking, digital pedagogy, GigaChat, hybrid approach, manual rewriting, neural network, prompt engineering, YandexGPT*

**УДК 339.138**
**ГРНТИ 06.81.55**

# УПРАВЛЕНИЕ УСПЕХОМ КЛИЕНТА В ЦИФРОВОЙ СРЕДЕ

**М. Б. Вольфсон**

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

*В статье исследуется концепция Customer Success Management (CSM) в условиях цифровой экономики. Актуальность тематики обусловлена переходом компаний от реактивной модели поддержки клиентов к проактивным цифровым стратегиям удержания и развития клиентской базы, основанным на предиктивной аналитике. В работе анализируются технологические и организационные изменения в практике CSM, рассмотрены подходы к использованию больших данных. Представлен обзор функциональных возможностей цифровых CSM платформ. Предложена концептуальная модель построения и внедрения CSM.*

***Customer Success Management, клиентский опыт, успех клиента, большие данные, предиктивная аналитика, цифровые платформы***

Современная экономическая среда характеризуется фундаментальным сдвигом от транзакционных моделей обмена к формам взаимодействия, основанным на длительном сотрудничестве и совместном создании ценности. Данный переход, усиленный распространением программных решений по модели SaaS (Software-as-a-Service), предполагающий непрерывный коммерческий цикл, в рамках которого потребитель систематически переоценивает соотношение «цена – ценность», актуализировал проблему обеспечения долгосрочной лояльности клиентов как ключевого фактора финансовой устойчивости предприятия.

Классическая модель взаимоотношений с клиентом предполагает дихотомию двух функций: отдела продаж, отвечающего за привлечение клиента и заключение сделки, и службы поддержки, функционирующей в реактивном режиме и устраняющей проблемы по факту их возникновения.

Однако в условиях цифровизации, когда клиентский опыт формируется преимущественно в онлайн-среде, а конкурентное преимущество определяется способностью компании предвосхищать потребности клиентов и обеспечивать бесшовный цифровой опыт на всех точках контакта, традиционные подходы к управлению клиентами утрачивают свою эффективность.

Успех клиента – это долгосрочная, научно обоснованная и профессионально управляемая бизнес-стратегия, направленная на максимизацию устойчивой и доказанной прибыльности как для клиентов, так и для компании [1].

Управление успехом клиентов (Customer Success Management, CSM) – это бизнес-стратегия, направленная на обеспечение достижения клиентами желаемых результатов при использовании продуктов или услуг компании. Она ориентирована на понимание и удовлетворение потребностей клиентов для построения долгосрочных отношений и максимизации пожизненной ценности клиента.

CSM функционирует в русле теории сервис-доминантной логики [2], согласно которой ценность не встраивается в продукт на стадии производства, а совместно создается в процессе взаимодействия поставщика и потребителя. В данной перспективе роль продавца состоит не в передаче готовой ценности, а в предоставлении знаний, компетенций, аналитики, необходимых клиенту для самостоятельного создания ценности, а CSM обеспечивает системное сопровождение клиента на всем протяжении жизненного цикла.

В отличие от классической системы поддержки клиентов, CSM реализует проактивную логику посредством:

– мониторинга паттернов использования продукта;
– вычисления индекса «здоровья» клиента (customer health score) на основе многомерных данных;
– предиктивной аналитики риска оттока клиентов на основе методов машинного обучения;
– выявления отклонений от нормативной траектории и совершения корректирующих воздействий.

Таким образом, управление успехом клиентов обладает следующими основными характеристиками:

1) максимизация вероятности достижения клиентом его целей;

2) непрерывное сопровождение на протяжении всего жизненного цикла;

3) проактивная и предиктивная логика действия;

4) использование системы метрик, позволяющих оценивать потенциал отношений до наступления критических событий (Time to First Value, Product Adoption Rate, Churn Rate, Net Revenue Retention, Customer Lifetime Value и др.).

Стратегия CSM опирается на три известные концепции: управление отношениями с клиентами (Customer Relationship Management, CRM), управление клиентским опытом (Customer Experience Management) и управление вовлеченностью клиента (Customer Engagement Management) [3-4].

По аналогии с CRM, CSM также учитывает демографические и транзакционные данные клиентов, но идет дальше, используя потоковые данные с датчиков и другие неструктурированные данные о клиентах для получения информации о ценности использования и ее прогнозирования для клиентов.

CSM опирается на основы клиентского опыта, стремясь улучшить опыт клиентов в использовании продукта, но не концентрируется лишь на эмоциональном воздействии, а отдает приоритет более отдаленным финансовым, социальным, операционным и стратегическим целям клиентов.

Также, как и при управлении вовлеченностью, CSM учитывает лояльность клиентов, но отдает приоритет достижению клиентских целей, а не их поведению, связанному с вовлечением.

Следует отметить, что традиционные подходы к управлению клиентским успехом опирались преимущественно на экспертную интуицию, ретроспективный анализ агрегированных метрик и реактивные интервенции. В условиях цифровой экономики, характеризующейся экспоненциальным ростом объемов данных, усложнением клиентских траекторий и повышением динамики рыночной среды, этого становится уже недостаточно. Интеграция технологий искусственного интеллекта (ИИ) и машинного обучения в архитектуру CSM позволяет перейти от управления на основе ретроспективных отчетов к управлению на основе предиктивных моделей и прескриптивных рекомендаций.

Рассмотрим ключевые подходы использования больших данных в контексте управления клиентским успехом.

1) предиктивное моделирование вероятности оттока, позволяющее идентифицировать клиентов в зоне риска до наступления критического события, обеспечивая временной лаг для проактивных интервенций;

2) разнородность клиентской базы требует использования дифференцированных подходов. Методы кластеризации позволяют осуществлять сегментацию клиентской базы на основе многомерных поведенческих паттернов. Для каждого сегмента генерируется персонализированный план онбординга с адаптивной последовательностью шагов, динамически корректируемой на основе реального прогресса;

3) прескриптивная аналитика предоставляет персонализированные рекомендации (например, образовательного контента на основе пробелов в использовании функционала);

4) значительная часть ценных инсайтов о клиентском опыте содержится в неструктурированных текстовых данных (тикеты, отзывы, транскрипты звонков). NLP-методы позволяют извлекать, обрабатывать и анализировать эти данные, классифицируя обращения клиентов;

5) при большом количестве клиентов менеджеры CSM не способны уделить равное внимание каждому. Точное прогнозирование пожизненной ценности клиента позволяет оптимизировать распределение ресурсов CSM, отдавая приоритеты клиентам с наибольшим потенциалом роста;

6) генеративные большие языковые модели (LLM) могут использоваться для автоматизации первой линии коммуникаций с персонализацией под контекст клиента.

Согласно прогнозу Straits Research, объем рынка CSM-систем вырастет с 2,82 млрд долларов США в 2025 году до 16,56 млрд к 2035 году, демонстрируя среднегодовой темп роста (CAGR) в 24,73 % [5].

Платформа CSM представляет собой специализированное программное обеспечение, предназначенное для системного мониторинга, анализа и оптимизации клиентских отношений на протяжении всего жизненного цикла. Можно выделить следующие виды платформ:

а) платформы полного жизненного цикла CS – интегрированная платформа с максимальной функциональной глубиной (Gainsight, Planhat);

б) модульные платформы – предполагают старт с минимальным набором модулей с возможностью наращивания функциональности по мере роста команды (Totango, Vitally);

в) CRM-нативные платформы – встраивают CS-функциональность в существующую CRM-экосистему, устраняя необходимость отдельной интеграционной прослойки (Catalyst, HubSpot Service Hub);

г) AI-нативные агентные платформы – функционируют на базе ИИ-агентов (ChurnZero, Olive.ai) [6].

Несмотря на растущее признание стратегической роли CSM, его внедрение часто носит фрагментарный характер, а организации ограничиваются приобретением специализированного программного обеспечения или реформированием службы поддержки.

Предлагаемая концептуальная модель построения и внедрения CSM базируется на принципе замкнутой системы, в которой каждый слой гене-

рирует выходные сигналы для последующего, а результаты исполнения рекурсивно поступают в контур управления для калибровки. Архитектура включает в себя четыре функциональных уровня и один сквозной управляющий контур (рис. 1).

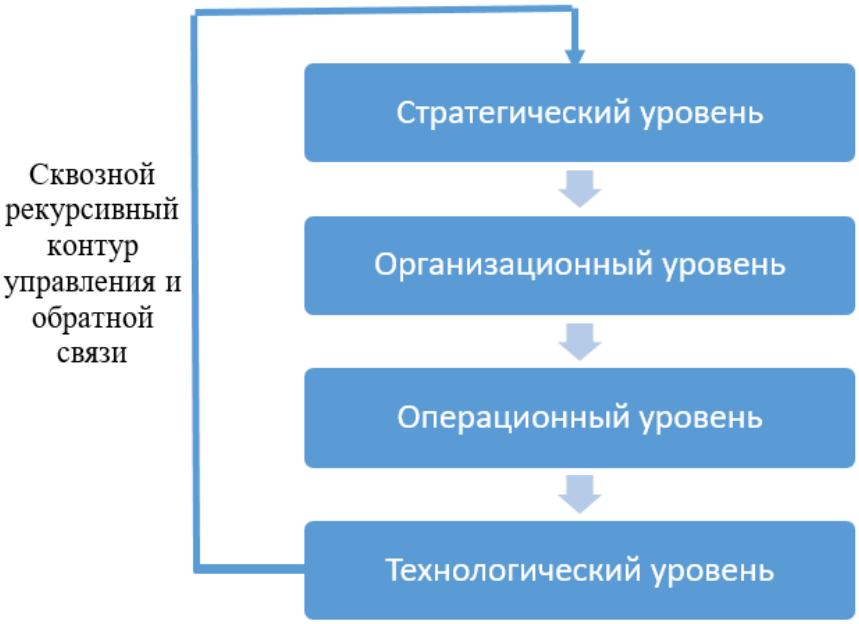



Рис. 1. Концептуальная модель построения и внедрения CSM

Стратегический уровень определяет, зачем организация внедряет CSM и какую ценность ожидает получить. На этом уровне происходит формулировка клиенто-центричной миссии, согласованной с бизнес-стратегией компании, перевод абстрактных целей бизнеса в конкретные CS-требования, а также определение целевых показателей (метрик).

Организационный уровень решает задачу создания структурных элементов, отделенных от продаж и поддержки. Предполагается ввод таких ролей как Customer Success Manager («менеджер по успеху клиентов»), CS CS Operations Manager («менеджер по операциям в сфере успеха клиентов»), Digital CS Manager («цифровой менеджер по успеху клиентов»). «Менеджер по успеху клиентов» представляет собой «лицо компании» для клиента, которое строит с ним доверительные отношения, «цифровой менеджер» реализует массовое, автоматизированное взаимодействие с клиентами через цифровые каналы, а «менеджер по операциям» осуществляет роль «архитектора процессов», делая команду CSM эффективнее, при этом напрямую с клиентами, не взаимодействуя [7-8].

Операционный уровень детализирует жизненный цикл клиента в виде управляемых процессов, структурируя операционную деятельность. На этом уровне происходит построение карты пути клиента с выделением критических точек принятия решений, разработка плейбуков (сборников сценариев, описывающих порядок действий для достижения цели при наступлении триггерного события) и формализация стандартов коммуникации с клиентами.

Технологический уровень обеспечивает инфраструктурную основу для всех предшествующих уровней. Центральным элементом является концепция Customer 360 – единое, целостное представление о клиенте, агрегирующее данные из всех точек контакта. Также на этом уровне происходит внедрение предиктивных моделей и систем автоматизации.

Сквозной контур управления и обратной связи замыкает архитектуру в самообучающуюся систему за счет мониторинга индикаторов, проведения регулярных аудитов зрелости процессов и качества данных.

Таким образом, предложенная концептуальная модель построения и внедрения CSM в цифровой среде представляет собой системную архитектуру, интегрирующую стратегическое целеполагание, организационное проектирование, процессную стандартизацию и технологическую инфраструктуру в единый рекурсивный контур создания ценности.

**Список использованных источников**

1. The Definition of Customer Success // The Customer Success Association. URL: https://www.customersuccessassociation.com/library/the-definition-of-customer-success/

2. Vargo, S. L., and Lusch, R. F. (2004). 'Evolving to a New Dominant Logic for Marketing', Journal of Marketing, 68(1), 1–17.

3. Hilton, B., Hajihashemi, B., Henderson, C. M., & Palmatier, R. W. (2020). Customer success management: The next evolution in customer management practice? Industrial Marketing Management, 90, 360–369.

4.Seidenstricker, Sven & Krause, Vinzenz. (2023). Making customers successful: Customer Success Management a new management approach // 14th International Conference on Applied Human Factors and Ergonomics (AHFE 2023), Vol. 97. P. 248-258.

5. Customer Success Management Market Size, Industry Trends to 2033 // Straits Research. URL: https://straitsresearch.com/report/customer-success-management-market (дата обращения 10.04.2026).

6. Top 10 Customer Success Platforms in 2026 // Kommunicate. URL: https://www.kommunicate.io/blog/top-customer-success-platforms/ (дата обращения 10.04.2026).

7. The Role of the Digital CSM: Goals and Responsibilities in Modern Customer Success // Velaris. 27.02.2026. URL: https://www.velaris.io/articles/role-of-the-digital-csm (дата обращения 10.04.2026).

8. Customer Success Operations Manager: Does Your Team Need One? // UnMoment. URL: https://inmoment.com/blog/customer-success-operations-manager-does-your-team-need-one/ (дата обращения 10.04.2026).

## CUSTOMER SUCCESS MANAGEMENT IN THE DIGITAL ENVIRONMENT

**Volfson M.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article explores the concept of Customer Success Management (CSM) in the digital economy. The relevance of the topic is due to the transition of companies from a reactive customer support model to proactive digital strategies for retaining and developing their customer base based on predictive analytics. The article analyzes technological and organizational changes in CSM practices and discusses approaches to using big data. It provides an overview of the functionality of digital CSM platforms and proposes a conceptual model for building and implementing CSM.*

***Key words:*** *Customer Success Management, customer experience, customer success, big data, predictive analytics, digital platforms*

**УДК 004.8: 330.45**
**ГРНТИ 06.03.07**

# ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА ПОДПИСОК НА ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: АНАЛИЗ РЫНКА, СЦЕНАРИИ, КЕЙСЫ

**И. Д. Вторыгин, Н. Д. Сергеев, И. Н. Федоренко, Д. Л. Янченко**

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

*В статье рассматривается экономическая эффективность выбора платных подписок на сервисы искусственного интеллекта (Perplexity Pro, Grok, ChatGPT Plus) для образовательных и исследовательских задач. На основе сравнительного анализа тарифов, функциональности, доступности в Российской Федерации и проведенного в исследовании опроса студентов, аспирантов, преподавателей, других представителей академического мира, предложена модель расчета окупаемости временных вложений и набор рекомендаций по оптимизации затрат на инструменты искусственного интеллекта в образовательном процессе. Полученные результаты могут быть использованы для повышения академической продуктивности и планирования индивидуальных образовательных бюджетов.*

***искусственный интеллект, экономическое обоснование, рентабельность инвестиций, образовательные технологии***

Национальный проект «Экономика данных и цифровая трансформация государства», определил роль цифровых технологий для экономики, социальной сферы, государственного управления за счет обеспечения кибербезопасности, качественного доступа к Интернету, подготовки ИТ-кадров, развития отечественных цифровых платформ, программного обеспечения и искусственного интеллекта [1].

В условиях цифровизации высшего образования искусственный интеллект (ИИ) стал важным компонентом образовательных технологий. Выбор ИИ-подписки превратился в стратегическое решение, влияющее на конкурентоспособность выпускника.

Экономическое обоснование подписок базируется на концепции стоимости учебного времени: час продуктивной работы студента технических и других направлений оценивается в рублях, а использование ИИ-ассистента рассчитывается в процентах, как сокращение времени на выполнения типовых задач. Исходя из цены за подписку и экономии часов в месяц, определяется окупаемость.

Научная новизна заключается в адаптации методов экономической оценки стоимости времени к специфике технического вуза и расчете ROI

(расшифровка)для академических сценариев (подготовка курсовых и выпускных квалификационных работ, отладка кода, поиск источников, презентации). Впервые проведено масштабное исследование предпочтений студентов СПбГУТ, позволившее выявить корреляцию между профилем обучения, цифровой грамотностью и выбором сервиса.

Практическая значимость – разработка методики выбора ИИ-подписки на основе окупаемости времени для студентов программистов, инженерных и управленческих направлений.

Детализация выпуска студентов, обучавшихся по программам, с модулями по искусственному интеллекту представлена в таблице 1.

ТАБЛИЦА 1. Количество студентов бакалавров, специалистов, магистров, обучавшихся по программам с модулями по искусственному интеллекту [2, 3]

| Укрупненные группы специальностей и направлений подготовки | Тысячи человек | | | В процентах к итогу | | |
|---|---|---|---|---|---|---|
| | 2023 | 2024 | Откл. +/– | 2023 | 2024 | Откл. +/– |
| Всего | 64,6 | 113,2 | +48,6 | 8,0 | 12,7 | +4,7 |
| Математика и механика | 1,0 | 1,7 | +0,7 | 0,1 | 0,2 | +0,1 |
| Компьютерные и информационные науки | 1,2 | 2,1 | +0,9 | 0,1 | 0,2 | +0,1 |
| Информатика и вычислительная техника | 22,4 | 39,1 | +16,7 | 2,8 | 4,4 | +1,6 |
| Информационная безопасность | 4,2 | 7,3 | +3,1 | 0,5 | 0,8 | +0,3 |
| Электроника, радиотехника и системы связи | 5,8 | 9,8 | +4,0 | 0,7 | 1,1 | +0,4 |
| Фотоника, приборостроение, оптические и биотехнические системы и технологии | 1,5 | 2,5 | +1,0 | 0,2 | 0,3 | +0,1 |
| Электро- и теплоэнергетика | 5,2 | 8,4 | +3,2 | 0,6 | 0,9 | +0,3 |
| Авиационная и ракетно-космическая техника | 2,1 | 3,6 | +1,5 | 0,3 | 0,4 | +0,1 |
| Аэронавигация и эксплуатация авиационной и ракетно-космической техники | 1,1 | 1,9 | +0,8 | 0,1 | 0,2 | +0,1 |
| Экономика и управление | 4,2 | 7,6 | +3,4 | 0,5 | 0,9 | +0,4 |

Таким образом выявлено, что выпуск специалистов по программам, содержащим модули по искусственному интеллекту, демонстрирует значительный рост: в 2023 году – 64,6 тыс. человек (8,0 % от общего выпуска), в 2024 году – 113,2 тыс. человек (12,7 %), прирост составил +48,6 тыс. человек (+4,7 п.п.). Наибольший абсолютный прирост зафиксирован по укрупненной группе «Информатика и вычислительная техника» (+16,7 тыс. чел.) – с 22,4 до 39,1 тыс. человек. Существенное увеличение отмечается по группам «Машиностроение» (+5,0 тыс.), «Электроника, радиотехника и системы связи» (+4,0 тыс.) и «Экономика и управление» (+3,4 тыс.). Устойчивый рост выпуска по ИИ-программам отражает государственный приоритет на развитие кадрового обеспечения цифровой экономики и реализацию национальной стратегии в области искусственного интеллекта.

Подходы к рассмотрению вопросов, связанных с экономической эффективностью выбора платных подписок на сервисы искусственного интеллекта (Perplexity Pro, Grok, ChatGPT Plus) для образовательных и исследовательских задач основываются на анализе рынка, тарифов, функциональности, доступности.

Методология исследования базируется на веб-анкетировании 200 респондентов СПбГУТ (студенты бакалавриата – 96,5 %, магистратуры – 1,5 %, преподаватели – 1,0 %). Возрастной диапазон респондентов составляет 17–35 лет и более, из них 89,0 % – 18–20 лет. Анкетирование проведено через Google Forms с учетом принципов веб-юзабилити [4].

Авторы статьи выражают благодарность за помощь в организации опроса и методологическую поддержку, доцента кафедры экономики данных кандидата экономических наук Надежду Владимировну Квашу. Анкета охватывала демографические данные, сценарии использования ИИ, оценку расходов на образовательный софт и барьеры доступа. Активное внедрение цифровых технологий является одним из важных условий современного образования [5].

Экономическая эффективность оценивалась через ROI сэкономленного учебного времени:

$$ROI = \frac{T_{эк} \cdot C_{час}}{C_{подп}} \cdot 100\ \%, \qquad (1)$$

где $T_{эк}$ – экономия времени, ч; $C_{час}$ – ставка часа, руб.; $C_{подп}$ – стоимость подписки, руб.

Например, при модальной ставке 500 руб./час (34,0 % респондентов) и экономии 10 часов/мес (медиана) ROI составляет 250 %.

Для оценки ландшафта применения ИИ респонденты указали используемые сервисы и типовые задачи. Результаты распределения представлены на рис. 1.

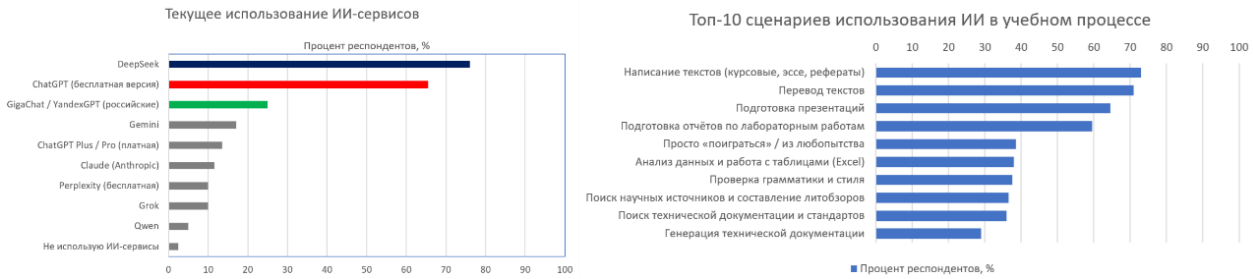



Рис. 1. Ландшафт использования ИИ-сервисов и топ-10 академических сценариев среди студентов и преподавателей СПбГУТ

Абсолютное доминирование бесплатных сервисов: DeepSeek – 76,0 %, бесплатный ChatGPT – 65,5 %. Платные подписки: ChatGPT Plus/Pro – 13,5 %, Perplexity Pro – 2,0 %. Российские альтернативы привлекли 25,0 %. В позиции универсальные задачи лидируют тексты – 73,0 %, перевод – 71,0 %, однако технические сценарии тоже значимы: код – 27,5 %, анализ протоколов – 26,0 %, сетевые конфигурации – 12,0 %. Это подтверждает востребованность ИИ в инженерном образовании.

Особое внимание уделено в данном исследовании, расчетам по оценке экономической эффективности, с учетом цены за подписку и экономии часов продуктивной работы в месяц, участников образовательной деятельности. Выбран способ отбора актуальных сервисов при фиксированной цене, с использованием базовых тарифов провайдеров [6, 7, 8].

Обратимся к следующим результатам проведенного опроса. Респондентам было предложено оценить готовность к оплате, ответы распределились сведущим образом: 53,5 % не готовы платить, 39,5 % – до 1000 руб./мес, лишь 7 % – на стандартную стоимость. Участники так же указали факторы, сдерживающие использование подписок: наличие в свободном доступе бесплатных версий (51,0 %), высокая стоимость (37,0 %), сложность оплаты (28,0 %), необходимость VPN (21,5 %).

Таким образом, экономическая эффективность выбора платных подписок на сервисы искусственного интеллекта с использованием, предложенные рекомендаций по оптимизации затрат, могут быть использованы для

повышения академической продуктивности и планирования индивидуальных образовательных бюджетов.

**Список использованных источников**

1. Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https: //www.https://digital.gov.ru/ru/events/48369/ (дата обращения:01.04.2026)

2. Индикаторы образования: 2025: статистический сборник / Н. В. Бондаренко, Т. А. Варламова, Л. М. Гохберг и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: ИСИЭЗ ВШЭ, 2025. URL: https://issek.hse.ru/news/1023576877.html (дата обращения 01.04.2026).

3. Индикаторы образования: 2026: статистический сборник / Н. В. Бондаренко, Т. А. Варламова, Л. М. Гохберг и др.; Нац. исслед. ун-т «Высшая школа экономики». М.: ИСИЭЗ ВШЭ, 2026.. URL: https://issek.hse.ru/news/1125008549.html(дата обращения 01.04.2026).

4. Нильсен Я. Web-дизайн: удобство использования Web-сайтов / Якоб Нильсен, Хоа Лоранжер; [пер. с англ. и ред. В. С. Иващенко]. М.: Вильямс, 2007. 366 с.

5. Федоренко И. Н. Цифровые информационные решения в электронном обучении // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2021. № 8. С.16-20.

6. OpenAI Pricing Page // OpenAI. 2026. URL: https://openai.com/pricing (дата обращения: 01.04.2026).

7. Perplexity AI Pricing // Perplexity AI. 2026. URL: https://www.perplexity.ai/pricing (дата обращения: 01.04.2026).

8. Premium Subscriptions / X Corp. 2026. URL: https://twitter.com/i/premium_signups (дата обращения: 01.04.2026).

## ECONOMIC JUSTIFICATION FOR CHOOSING ARTIFICIAL INTELLIGENCE SUBSCRIPTIONS: MARKET ANALYSIS, SCENARIOS, CASES

**Vtorygin I., Sergeev N., Fedorenko I., Yanchenko D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article examines the economic efficiency of choosing paid subscriptions to artificial intelligence services (Perplexity Pro, Grok, ChatGPT Plus) for educational and research purposes. Based on a comparative analysis of tariffs, functionality, and accessibility in the Russian Federation and a survey of students, graduate students, teachers, and other representatives of the academic world conducted in the study, a model for calculating the payback on time investments and a set of recommendations for optimizing the costs of artificial intelligence tools in the educational process are proposed. The results obtained can be used to increase academic productivity and plan individual educational budgets.*

***Key words:*** *artificial intelligence, economic justification, return on investment, educational technologies*

**УДК 167.3:7**
**ГРНТИ 02.31.01**

# КОНСТИТУИРОВАНИЕ ЛИЧНОСТИ И ЦИФРОВАЯ КОНФИГУРАЦИЯ СМЫСЛА

**А. Ю. Вязьмин**

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

*Рабочая гипотеза «генетической» феноменологии Гуссерля заключает в себе два положения, которые добавлены к более ранней версии трансцендентально-феноменологического метода: интерсубъективность и пассивный синтез анонимного сознания. Для самого феноменологического метода это означает, что сфера трансцендентального, понимаемая не только как условие познания, но и самосознания, выступает в качестве конституирующего элемента эго-монады, т.е. всей личностной сферы человека. Однако такое конституирование происходит интерсубъективно в предзаданном пространстве взаимодействующих монад жизненного мира (Lebenswelt), в их до-личностной коммуникации. Актуальность феноменологического метода Гуссерля можно проверить на вызовах современности, поскольку в XXI веке участником коммуникации в социуме становится искусственный интеллект (ИИ). ИИ безличен и представляет собой цифровую конфигурацию смысла. Тем не менее возникают вопросы: взаимодействует ли ИИ с человеком на до-личностном уровне сознания, входит ли он в пространство жизненного мира, влияет ли на становление личности.*

***интерсубъективность, пассивный синтез, коммуникация, ИИ***

В XXI веке человек сталкивается с феноменом, который состоит в том, что участником коммуникации в социуме становится искусственный интеллект (ИИ). Это событие инициирует появление многих философских вопросов, связанные с определением сознания, генезисом осознанности в коммуникации, интеграции продуктов языковой модели в когнитивные контуры человека, возможного изменения, под влиянием искусственного интеллекта основ культуры и цивилизации человечества в целом. Так или иначе, эти вопросы в известной мере коррелируют с вопросами сознания в феноменологии Гуссерля и могут быть решаемы с помощью феноменологического метода.

Рабочая гипотеза «генетической» феноменологии Гуссерля, развиваемая им в поздний период творчества, заключает в себе два положения, которые добавлены к более ранней версии трансцендентально-феноменологи-

ческого метода: интерсубъективность и пассивный синтез анонимного сознания.

Интерсубъективность – это феноменальная данность «другого», не являющаяся феноменом «я», данным мне ни в каком переживании: ни в переживании самовосприятия, ни в переживании совокупного нарратива мышления о «я», однако тем не менее подобного «я» и, вместе с тем, достоверно существующего. Феноменальная данность «другого» конституирована в полной аналогии с «я», т. е. конгруэнтно феномену «я» в своей развернутой эгологии в горизонте сознания.

Интерсубъективность представляет для Гуссерля изначально трудноразрешимую философскую проблему, поскольку достоверность трансцендентального метода познания опирается на сферу чистого сознания и предполагает методологический солипсизм.

Первоначально Гуссерль хотел априорно конституировать феномен «я» как «другого для другого», и этот способ решил бы все проблемы обоснования достоверности «другого». Однако он предпочел другой путь: установить границы «моего собственного» (примордиальной сферы сознания), обнаружить с этой примордиальной сфере феномен «мое живое тело» (Leib) в отличие от просто протяженных тел (Körper), затем обнаружить предметности, подобные «моему живому телу», и сделать вывод о существовании «других ego».

Гносеологическая процедура обнаружения примордиальной сферы была представлена Гуссерлем в «Картезианских размышлениях» как более детализированный вид трансцендентально-феноменологической редукции [1, 442]. Обнаружение «моего живого тела» осуществлялось в корреляции к апперцепции «себя как психофизического человека» – эго-монады со всеми уровнями эгологии.

Гуссерль утверждает, что после конституирования «моего живого тела» наступает стадия аппрезентации и аналогизирующей апперцепции «другого»: аппрезентация – это реактуализация воображаемого «я» как «другого» в модусе «как если бы я был там», а аналогизирующая апперцепция – это конституирование «другого» в полном смысле как подобного «я» на основе вчувствования (первичной эмпатии) и имитации [1, 461]. В итоге, в качестве интермонадического феномена конституируется сообщество эго-монад и объективный мир, достоверность существования которого фундирована в этом сообществе.

Ассоциативный синтез «другого» в теории интерсубъективности Гуссерля порождает множество вопросов, касающихся связи или даже корреляции между аналогизирующими актами сознания и теми, которые участвуют в пассивном синтезе самоидентификации. Наброски ответов на эти вопросы намечались у Гуссерля не только в период написания «Картезианских размышлений» [1], но и в более ранних работах, таких, как «Идеи I» [2] и «Идеи II» [3].

Синтез самоидентификации действительно соотнесен с актами, в которых конституируются предметности эгологии и примордиальной сферы сознания. Но в то же время верно, что «само», отрицательным образом обнаруживаемое как остаток седиментаций после «выключения» трансцендентного, тоже является в некотором роде самоидентификацией. Рефлексия сферы трансцендентального не складывается из двух интенций, она сложнее и требует темпорального синтеза. Для самого феноменологического метода это означает, что сфера трансцендентального, понимаемая не только как условие познания, но и самосознания, выступает в качестве конституирующего элемента эго-монады, т.е. всей личностной сферы человека. Однако, поскольку сфера эгологии все же согласно Гуссерлю не есть трансцендентальная субъективность, мы имеем двоякую схему самоидентификации: первый раз – в темпоральном потоке пассивными актами анонимного сознания, второй раз – в конституировании значений «я» в сфере эго-монады.

Соответственно конституированию взаимодействующих монад жизненного мира (Lebenswelt) предшествует до-личностный интерсубъективный пассивный генезис того первого «само», которое в темпоральном потоке «живого настоящего» (Lebendige Gegenwart) эксплицируется в анонимное ego или анонимное alter ego в их до-личностной «коммуникации». Безличность, или даже без-«я» (Unichlichkeit) пассивного синтеза заключается в том, что он согласно Гуссерлю носит некий вне-временной характер, поэтому первоначальное «само» строго говоря нельзя назвать ни ego или alter ego [3, 289].

В «Кризисе европейских наук» Гуссерль утверждает, что сознание интерсубъективности, равно как и сознание самоидентификации, должно быть трансцендентальной проблемой, т. е., иными словами, на до-личностном до-временном уровне самоконституирования чистой трансцендентальной сферы сознания посредством пассивного синтеза должны складываться предпосылки того, чтобы в аналогизирующих апперцепциях можно было

достоверно проводить различие «между мной и другими и придавать им смысл “мне подобных”» [4, 269].

В рассуждениях Гуссерля можно проследить некую допускаемую метафизичность: сфера до-личностного пассивного синтеза трансцендентальной субъективности – это «описание» вне-временной «точки» в потоке внутреннего сознания времени, тем не менее Гуссерль уверен, что эта «не-яйная» субъективность «уже» в некотором роде идентична, что она соотносится с культурной и цивилизационной идентичностью человека вообще, идентичностью принадлежности к человечеству, а таже и самому бытию, и что эта «не-яйная» субъективность предшествует рождению и воспоследствует смерти.

Актуальность феноменологического метода Гуссерля можно проверить, или хотя бы примерить в качестве перспективы научного исследования на вызовах современности, на таких, например, как коммуникация с искусственным интеллектом.

С точки зрения феноменологии Гуссерля «персона» искусственного интеллекта в активном синтезе аналогизирующей апперцепции конституируется нами вне аналогий телесности и, хотя в нейтрализующих актах сознания «персону» искусственного интеллекта можно вообразить в виде нарратива-собеседника в пространстве смыслов, этот собеседник лишен переживания и интенциональности и только встраивается в структуры интенционального содержания. Искусственный интеллект безличен и представляет собой конфигурацию смысла, взаимосвязи значений, архитектурно сконструированных в устойчивые языковые модели при помощи вероятностного анализа.

В осуществляемой коммуникации с искусственным интеллектом как собеседником, эго-монада не эмпатирует искусственному интеллекту и не имитирует его, подобно тому, как не эмпатируют изображению тела в отличие от воспринимаемой «живой телесности» (Leib).

Учитывая допущения Гуссерля о пассивном генезисе, с еще большей уверенностью можно предположить, как бы он ответил бы на вопрос, входит ли искусственный интеллект в трансцендентальную сферу человека и участвует ли он в синтезе смыслов человеческой цивилизации и культуры. Разумеется, искусственный интеллект способен изменять сознание человека, и такие изменения будут заметны в перспективе. Однако Гуссерль был бы категорически против допущения мысли о том, что наличие «персоны» искусственного интеллекта в коммуникации предполагает его до-личностное участие в синтезе субъекта «я» и я-идентичности.

Таким образом, если мы принимаем позицию Гуссерля относительно онтологического статуса искусственного интеллекта в качестве собеседника и участника коммуникации, то можно надеяться, что те изменения в культуре и общественном сознании, которые произведет искусственный интеллект в будущем не затронут основ культуры и цивилизации человечества в целом, поскольку не включены в процесс синтеза личности. Искусственный интеллект в данном случае можно сравнить с зеркалом человеческого сознания и культуры, построенным с помощью языковых моделей, отражающих подлинный синтез эйдосов.

**Список используемых источников**

1. Гуссерль Э. Картезианские размышления. / Гуссерль Э. Логические исследования. Картезианские размышления. Мн.: Харвест, М.: АСТ, 2000. С. 331-523.

2. Гуссерль Э. Идеи к чистой феноменологии и феноменологической философии. Книга I. Общее введение в чистую феноменологию. М.: Дом интеллектуальной книги, 1999. 336 с.

3. Гуссерль Э. Идеи к чистой феноменологии и феноменологической философии. Книга II. Феноменологические исследования конституирования. Калининград: БФУ им. И. Канта, 2025. 660 с.

4. Гуссерль Э. Кризис европейских наук и трансцендентальная феноменология. СПб.: Владимир Даль, 2004. 399 с.

## THE CONSTITUTION OF PERSONALITY AND DIGITAL CONFIGURATION OF MEANING

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

*The working hypothesis of Husserl's "genetic" phenomenology includes two provisions that were added to an earlier version of the transcendental phenomenological method: intersubjectivity and the passive synthesis of anonymous consciousness. For the phenomenological method itself, this means that the sphere of the transcendental, understood not only as a condition of cognition, but also of self-awareness, acts as a constituent element of the ego monad, i.e., the entire personal sphere of man. However, such a constitution occurs intersubjectively in a predetermined space of interacting monads of the life world (Lebenswelt), in their pre-personal communication. The relevance of Husserl's phenomenological method can be tested against the challenges of our time, since artificial intelligence (AI) is becoming a participant in communication in society in the 21st century. AI is impersonal and represents a digital configuration of meaning. Nevertheless, questions arise as to whether AI interacts with humans at a pre-personal level of consciousness, whether it enters the space of the life world, and whether it influences personality formation.*

***Key words:*** *intersubjectivity, passive synthesis, communication, AI*

**УДК 327(485+470):355.02(261.2)**
**ГРНТИ 11.25.40**

# ФАКТОР ШВЕЦИИ В КОНТЕКСТЕ ВОЕННО-ПОЛИТИЧЕСКОЙ ОБСТАНОВКИ В РЕГИОНЕ БАЛТИЙСКОГО МОРЯ

**А. Б. Гехт**

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

*Вступление Швеции в НАТО в марте 2024 года, после длительного периода проведения политики нейтралитета и неучастия в военных альянсах в мирное время, существенным образом изменило баланс сил в Северной Европе и регионе Балтийского моря. На современном этапе Швеция – это не просто «новый член», а передовой технологический бастион Североатлантического альянса, обеспечивающий руководству НАТО дополнительные возможности для установления контроля над Балтикой. Настоящая статья посвящена краткому рассмотрению роли и значения о. Готланд в качестве главного геостратегического актива Швеции в акватории Балтийского моря, анализу возможностей военно-промышленного комплекса крупнейшей скандинавской страны, а также описанию текущего состояния и перспектив развития ключевого актива шведских вооруженных сил – военно-морского флота, способного бросить вызов отечественному Балтийскому флоту.*

***Швеция, НАТО, регион Балтийского моря***

Вступление Швеции в НАТО в марте 2024 года стало одним из наиболее значимых геополитических событий в Северной Европе за последние десятилетия. Оно завершило более чем двухсотлетний период декларируемого нейтралитета, определившего внешнюю политику страны еще со времен наполеоновских войн. Этот исторический разворот радикально изменил баланс сил в Балтийском регионе, превратив Балтийское море в зону доминирования Североатлантического альянса. Швеция, обладающая развитой оборонной промышленностью, мощными военно-морскими силами и стратегическим положением, сегодня становится одним из ключевых звеньев системы сдерживания России в регионе Балтийского моря и Западной Арктике. В настоящей статье кратко анализируются роль и значение Швеции в современной военно-политической конфигурации региона Балтийского моря с акцентом на фактор острова Готланд, арктическую стратегию, потенциал шведского флота и военно-промышленного комплекса в контексте членства в НАТО.

Вооруженные силы Швеции переживают наиболее масштабную трансформацию со времен холодной войны. После вступления в НАТО в марте 2024 года Стокгольм взял курс на достижение оборонных расходов в 3,5 % ВВП к 2030 году – в 2026 году этот показатель уже достигнет 2,8 % [1]. Рост финансирования (более чем на 18 % за год) направлен на качественное переоснащение армии, флота и авиации. За последние годы Швеция стала рамочной страной для передовых сил НАТО в Финляндии (FLF Finland), что предполагает размещение шведского контингента численностью от 600 до 1200 военнослужащих на территории соседней страны. Кроме того, шведские вооруженные силы выделяют до 1700 военнослужащих сухопутных и специальных подразделений, 700 моряков и 600 летчиков для операций НАТО в Североатлантическом регионе, включая участие в многонациональной бригаде в Латвии. Отметим, что военно-политическая активность Швеции в качестве нового члена Североатлантического альянса отнюдь не исчерпывается приведенными примерами.

Центральное место в шведской обороне на Балтике занимает остров Готланд – крупнейший остров Балтийского моря, расположенный всего в 275 километрах от Калининграда. Его стратегическое значение трудно переоценить, контроль над островом позволяет блокировать морские коммуникации между Калининградской областью и основной территорией России, а также затруднить любую отправку подкреплений в страны Прибалтики. После окончания холодной войны Швеция фактически отказалась от военного присутствия на Готланде. Однако события 2014 года и последующее ухудшение отношений с Россией побудили Стокгольм пересмотреть эту политику. На современном острове находится около 400 профессиональных солдат и призывников, а по планам шведского командования в течение четырех лет численность бригады должна быть доведена до 4,5 тысяч человек [2].

В 2026 году начальник штаба обороны Швеции генерал Микаэль Классон назвал захват Готланда «вполне разумным сценарием», который [президент Российской Федерации Владимир Владимирович] Путин «мог бы использовать для проверки НАТО на прочность» [3]. На учениях альянса этот сценарий активно отрабатывается. Такая риторика, сопровождаемая реальным наращиванием военной инфраструктуры, создает напряженность в регионе, однако следует признать: заявления о «российской угрозе» служат для шведского руководства внутренним оправданием резкого увеличения

военных расходов и отказа от политики декларировавшегося нейтралитета в мирное время.

Арктическое направление является вторым критически важным театром для шведской политики обороны. Швеция, хотя и не имеет прямого выхода к Северному Ледовитому океану, обладает обширными территориями в Лапландии, граничащими с Норвегией и Финляндией. В мае 2026 года на встрече глав МИД арктических государств НАТО в шведском Хельсингборге было заявлено о наращивании военного присутствия, возможностей наблюдения и совместной подготовки в Арктике и на Крайнем Севере. В документе прямо указывается, что Арктика «быстро становится сферой возрастающей геополитической стратегической важности» [4]. Отметим, что Швеция активно участвует в создании так называемого «блока викингов» – военной интеграции Норвегии, Швеции и Финляндии, которую эксперты называют «альянсом внутри альянса». Ключевой элемент этой интеграции – создание единого военного транспортного коридора, соединяющего норвежские порты (включая стратегический Нарвик) через Швецию с Финляндией. Этот коридор позволит перебрасывать войска и тяжелую технику к российским границам не за недели, а за дни [5]. Кроме того, Швеция вместе с Данией, Норвегией и Финляндией создает Объединенное северное воздушное командование (JNAC), объединяющее около 250 современных боевых самолетов. Вся эта инфраструктура консолидирована под эгидой Объединенного командования НАТО в Норфолке (JFC Norfolk), которое координирует операции от Северной Америки до российских границ [6].

Рассматривая военный потенциал Швеции, невозможно обойти вниманием военно-морские силы этого королевства. Шведский флот исторически является одной из самых боеспособных сил в Балтийском регионе. В отличие от многих европейских стран, Швеция сохраняла подводный флот даже в периоды разрядки, делая ставку на скрытность и асимметричные угрозы. Хотя некоторые эксперты полагают, что шведский флот не сопоставим по мощи с Балтийским флотом России, реальное соотношение сил требует более детального анализа.

Швеция обладает дизель-электрическими подводными лодками типа Gotland, которые считаются одними из лучших в своем классе благодаря воздухонезависимой энергетической установке, позволяющей находиться под водой до нескольких недель. В надводном компоненте основу ударной мощи составляют корветы типа Visby, выполненные по технологии малозаметности. Однако качественный скачок ожидается в 2030 году, когда швед-

ский флот получит четыре новых фрегата типа FDI (фрегат для обороны и нападения) французской постройки, называемых в Швеции типом «Лулео». Эти корабли водоизмещением около 4,5 тысяч тонн станут первыми крупными надводными боевыми единицами шведского флота с 1982 года. Их стоимость оценивается примерно в пять миллиардов долларов [7].

Особую опасность представляют радиолокационные возможности фрегатов. Комплекс Thales Sea Fire 500 с четырьмя активными фазированными антенными решетками отслеживает одновременно до 800 целей на дальности до 300 километров, совмещая функции обзора, наведения зенитных ракет и обнаружения надводных целей. Зенитный ракетный комплекс Aster 15/30, способный поражать цели на дальности до 120 километров, делает эти корабли серьезным вызовом для российской авиации на Балтике. Однако у этих фрегатов есть и слабые места. Как отмечается в российских военных аналитических изданиях, они обладают ограниченными возможностями для нанесения ударов по береговым целям, а главным противовесом им остаются российские крылатые ракеты «Калибр» и береговые ракетные комплексы. Тем не менее, появление таких кораблей меняет баланс сил: как признают российские эксперты, у Балтийского флота «нет кораблей с аналогичными возможностями» [8]. Кратко обобщая материалы о потенциале ВМФ Швеции, можно отметить, что официальный Стокгольм делает ставку на качество и скрытность: 5 современных дизель-электрических лодок с AIP и 5 стелс-корветов типа «Visby», составляющих костяк его боевой мощи в регионе Балтийского моря.

Рассуждая о факторе Швеции в качестве важного члена Североатлантического альянса, важно принимать во внимание, что помимо географического положения страны и ее стратегического значения как в арктических широтах, так и в регионе Балтийского моря, а также наличия развитых вооруженных сил, важной предпосылкой высокой заинтересованности руководства альянса в дальнейшей интеграции этой страны был ее масштабный военно-промышленный комплекс. Особое место в системе военной промышленности Швеции занимает входящий в финансово-промышленную группу Валленбергов концерн «SAAB» [9], крупнейший шведский экспортер военной техники и одно из ведущих европейских предприятий военного назначения, специализирующийся на разработке и производстве истребителей. В частности, именно компания «Saab» производит истребитель JAS 39 Gripen, который является основой не только шведских, но и, например, венгерских и чешских ВВС. Компания «Bofors» (ныне часть BAE Systems) про-

изводит артиллерийские системы, а «Kockums» – подводные лодки [10]. Безусловно, вступление в НАТО открыло для шведского ВПК новые рынки и возможности.

Подводя итог, можно констатировать: к концу первой четверти XXI века Швеция превратилась из формально не входящего в военные блоки в мирное время наблюдателя в активного и важного участника Североатлантического альянса. Этот переход, занявший всего два года (с подачи заявки в мае 2022 года до полноправного членства в марте 2024-го), кардинально изменил военно-политическую обстановку в регионе Балтийского моря. Остров Готланд на современном этапе укрепляется быстрее, чем когда-либо со времен холодной войны, и к концу десятилетия на нем будет развернута бригада численностью 4,5 тысячи человек с современными зенитными комплексами. Арктические территории Швеции интегрируются в единую оборонную сеть с Норвегией и Финляндией, создавая непрерывный логистический коридор от Атлантики до российских границ. Шведский флот, усиленный четырьмя новыми фрегатами FDI, получит возможность на равных конкурировать с российским Балтийским флотом в надводной плоскости, хотя преимущество России в ракетном оружии большой дальности пока сохраняется.

Явления и процессы, длительный период остававшиеся скрытыми – антироссийские настроения и стремление играть более заметную роль в большой европейской политике – стали частью политического курса, проводимого официальным Стокгольмом. Для России это означает оформление на северо-западных рубежах серьезного, технологически оснащенного и идеологически мотивированного противника, который десятилетиями готовился к войне на своей территории и теперь готов перенести этот опыт за пределы своих границ в составе Североатлантического альянса.

**Список используемых источников**

1. The Government presents defence investments for a stronger Sweden [Electronic resource]: Press release, 2025-09-15 / Government Offices of Sweden, Ministry of Defence. URL: https://www.government.se/press-releases/2025/09/the-government-presents-defence-investments-for-a-stronger-sweden/ (last request: 28.05.2026).

2. GP. Stor styrka till Gotland försvarets insatschef: Vi anpassar beredskapen [Electronic resource] // Göteborgs-Posten. 2022. 12 januari. URL: https://www.gp.se/nyheter/varlden/stor-styrka-till-gotland-forsvarets-insatschef-vi-anpassar-beredskapen.0bf34c94-e2fd-4829-8d49-d6faf8ed3f74 (last request: 28.05.2026).

3. Burrows E., Keaten J. Ukrainian drone pilots turn a military exercise in Sweden into a critical warning for NATO [Electronic resource] // AP News. 2026. 12 May. URL: https://ap-

news.com/article/russia-sweden-nato-gotland-trump-sabotage-europe-a50cec79865d7a85e913b7aca30b1fb5 (last request: 28.05.2026).

4. NATO Foreign Ministers meeting in Sweden address how to make the Alliance stronger [Electronic resource] // NATO. 2026. 22 May. URL: https://www.nato.int/en/news-and-events/articles/news/2026/05/22/nato-foreign-ministers-wrap-up-preparations-for-ankara-summit-in-helsingborg (last request: 28.05.2026).

5. Общий штаб, BBC и логистика: на границах России растет «блок викингов» // REGNUM. 2026. 27 мая. URL: https://regnum.ru/article/4039527 (дата обращения: 28.05.2026).

6. Sweden Has the Tanks. Finland Has the Troops. Welcome to the Pan-Nordic Army [Electronic resource] // The Wall Street Journal. 2025. 20 April. URL: https://www.wsj.com/world/europe/europe-nordic-military-defense-a5d5da5b?mod=hp_lead_pos11 (last request: 28.05.2026).

7. Ahlander J., Jeppesen S., Pollard N., Solsvik T., Lehto E., Trompiz G. Sweden to buy navy frigates from France for over $4 billion to boost Baltic defence [Electronic resource] // Reuters. 2026. 19 May. URL: https://www.reuters.com/business/aerospace-defense/sweden-plans-buy-navy-frigates-france-2026-05-19/ (last request: 28.05.2026).

8. Тимохин А. Чем опасны для Балтийского флота новые фрегаты ВМС Швеции // Взгляд: интернет-газета. 2026. 20 мая. URL: https://vz.ru/world/2026/5/20/1420602.html (дата обращения: 28.05.2026).

9. Saab in brief [Electronic resource] // Saab: official website. URL: https://www.saab.com/about/company-in-brief (last request: 28.05.2026).

10. Гехт А. Б. Фактор финансово-промышленной группы семьи Валленберг во вступлении Швеции в НАТО // Клио. 2026. № 3 (231). С. 77-80.

## THE SWEDISH FACTOR IN THE CONTEXT OF THE MILITARY AND POLITICAL SITUATION IN THE BALTIC SEA REGION

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

*Sweden's accession to NATO in March 2024, following a long period of neutrality and non-participation in military alliances during peacetime, has significantly altered the balance of power in Northern Europe and the Baltic Sea region. Today, Sweden is not just a "new member" but a forward-thinking technological bastion of the North Atlantic Alliance, providing NATO leadership with additional opportunities to establish control over the Baltic Sea. This article provides a brief overview of the role and significance of Gotland as Sweden's main geostrategic asset in the Baltic Sea, analyzing the capabilities of the military-industrial complex of the largest Scandinavian country, and describing the current state and development prospects of the Swedish Armed Forces' key asset, the navy, which can challenge the Russian Baltic Fleet.*

***Key words:*** *Sweden, NATO, the Baltic Sea region/*

**УДК 321.7**
**ГРНТИ 11.15.31**

# ЗАКОН «ЯДАН»: ОБЩЕСТВЕННАЯ ДИСКУССИЯ В СОВРЕМЕННОЙ ФРАНЦИИ

**А. Б. Гехт, О. А. Ухалов**

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

*В современных демократиях наблюдается тенденция к ограничению свободы слова под видом защиты меньшинств. Во Франции, традиционно считающейся колыбелью демократии, парламент продвигает законопроект «Ядан», который формально направлен против антисемитизма, но фактически приравнивает критику действий Израиля к уголовно наказуемому деянию. В данной работе анализируется содержание законопроекта, его ключевые положения, а также реакция общества – петиция 707 тысяч граждан, которую юридическая служба Национального собрания закрыла без объяснений. Рассматривается противоречие между демократическими принципами и практикой их подавления.*

***демократия, свобода слова, Франция, законопроект «Ядан», ограничение прав***

В современном мире наблюдается тенденция к подавлению демократии в ее подлинном, прямом смысле. Демократия – это политический режим, основанный на коллективном принятии решений при равном влиянии участников на результат. Рассмотрим современную Францию, страну, которая считается колыбелью демократии и родиной революции 1789 года, провозгласившей принципы «Свобода, равенство, братство» и объявившей всех граждан равными. Однако сегодня французская юридическая служба Национального собрания закрыла петицию 700 тысяч граждан, требовавших не принимать закон «Ядан». Согласно противникам этого законопроекта, он дискредитирует свободу слова, поскольку фактически приравнивает критику действующей власти в Израиле к антисемитизму. Тем самым парламент, проигнорировав волю сотен тысяч граждан, не стал препятствовать дальнейшему рассмотрению нормы, которая, по мнению ее критиков, сужает демократические свободы. Цель данной работы – проанализировать содержание законопроекта «Ядан», выявить его потенциальное влияние на свободу слова и оценить, насколько обоснованными являются требования граждан не принимать этот закон с точки зрения демократических принципов.

Законопроект назван в честь Каролины Ядан [4], депутата от президентской партии «Возрождение». В преамбуле законопроекта на французском языке приводятся цифры, призванные обосновать его необходимость. В переводе на русский: «*Согласно данным Министерства национального образования, в течение 2023–2024 учебного года количество антисемитских актов, зафиксированных в начальных и средних школах, увеличилось более чем в четыре раза с 400 до 1 670*». Но что конкретно понимается под «антисемитскими актами»? Преамбула этого не раскрывает. Приводится только число без содержания. Это позволяет заведомо напугать парламентариев ростом актов, при этом тип этих актов остается неопределенным. Речь может идти как о прямых угрозах, так и о выкриках или лозунгах, осуждающих действия Израиля в секторе Газа. Различие между собственно антисемитизмом и политической критикой действий иностранного правительства в преамбуле стирается.

Далее автор законопроекта утверждает: «*В то время как евреи составляют менее 1 % населения Франции, антисемитские агрессии теперь составляют 57 % от всех расистских и антирелигиозных агрессий в стране*». Однако здесь возникает проблема методологического характера. Французское законодательство [3] запрещает государству собирать официальные данные о религиозной принадлежности граждан. Следовательно, цифра «менее 1 %» – это не точный статистический факт, а оценочная величина. На ее основе предлагается принимать закон, последствия которого затронут все население, но обоснование строится вокруг интересов менее чем одного процента.

Далее в законопроекте: «*Эта тревожная динамика подчеркивает возрождение антисемитизма, который, будучи далеко не остаточным явлением, представляет собой серьезную угрозу...*». Формально закон направлен на защиту граждан от антисемитизма. Но вопрос остается открытым: защита какого именно процента населения имеется в виду? Если речь идет об одном проценте, то почему остальные 99 % должны автоматически соглашаться с ограничениями, которые могут затронуть и их право на выражение мнения? Особенно учитывая, что во Франции проживает, по разным оценкам, около 8 % [1] мусульман, значительная часть которых выступает на стороне палестинцев.

Ключевое положение преамбулы звучит так: «*Каждый имеет право на свое мнение о политике того или иного государства, но ничто не может оправдывать его отрицание, призыв к его исчезновению или уничтожению.*

*Каждый свободен в своих политических взглядах в отношении израильского правительства, но ничто не может оправдывать призыв к уничтожению Израиля*». Иными словами, законопроект прямо проводит мысль о недопустимости призывов к уничтожению Израиля. Но что насчет права на критику действий Израиля в секторе Газа? Что насчет осуждения военных операций, в результате которых, по данным с 2023 года, погибло более 72 тысяч человек [5], включая женщин и детей? Для палестинского населения, согласно логике законопроекта, эта защита не работает. Закон получается направленным исключительно на один процент населения, игнорируя другие группы, которые тоже нуждаются в защите и праве голоса.

Далее в законопроекте: «*Расторможенное антисемитское слово больше не является прерогативой проповедников ненависти и крайне правых, но процветает в наших школах и университетах или в Интернете... стигматизируя Израиль тем более неоправданно, что это государство единственное на планете, которому теперь отказывают в праве на существование*». Здесь возникает обратный вопрос. Лозунги против Израиля во многом связаны с тем, что международные институты не могут или не хотят повлиять на действия израильского правительства после операций в секторе Газа, где число погибших превысило десятки тысяч. Люди пытаются выразить свою позицию именно потому, что чувствуют бездействие международного сообщества. Можно предположить, что воспринимаемый рост антисемитских настроений отчасти связан с тем, что международные институты демонстрируют свою неэффективность, а люди, бежавшие от войн с Ближнего Востока во Францию, видят продолжающуюся гибель тех, кто остался.

Таким образом, из преамбулы законопроекта «Ядан» следует, что французское правительство стремится обеспечить защиту примерно одному проценту населения, в то время как более крупные группы остаются без внимания или даже попадают в зону потенциального ограничения их прав. Норма, которая должна бороться с антисемитизмом, на деле рискует превратиться в инструмент подавления критики в адрес иностранного государства. В современной Франции, где еще жива память о свободе слова как одной из основ республики, это пытаются узаконить под видом защиты меньшинства.

Что же именно предлагает «закон Ядан»?

Статья 1 ужесточает наказание за пропаганду терроризма. Под уголовную ответственность попадают прямое и косвенное подстрекательство к терактам, а также публичные заявления, представляющие терроризм как

«законное сопротивление». Вводится наказание до одного года тюрьмы и 45 тысяч евро штрафа за публичное преуменьшение, публичное приуменьшение серьезности актов терроризма. Префекты получают право закрывать культовые места за подобные высказывания.

Статья 2 вводит новое преступление подстрекательство к уничтожению или отрицанию существования какого-либо государства, которое наказывается пятью годами тюрьмы и штрафом 75 тысяч евро.

Статья 3 расширяет права антирасистских ассоциаций они могут становиться гражданскими истцами при преступлениях с отягчающим обстоятельством расизма или антисемитизма, а также участвовать в делах по подстрекательству к уничтожению государства.

Статья 4 ужесточает ответственность за оспаривание преступлений против человечности, включая Холокост. Наказуемыми становятся преуменьшение, даже в завуалированной форме. Закрепляется ответственность за оспаривание роли режима Виши в депортации евреев. Прямое сравнение государства Израиль с нацизмом квалифицируется как вопиющая тривиализация Холокоста. Положения распространяются на заморские территории Франции.

Законопроект встретил в обществе довольно жесткую критику. Александр Баласс создал петицию на официальном сайте петиций Национального собрания Франции [2] с требованием не принимать данный закон. Ключевая мысль петиции выражена в следующих словах:

«*Он представляет реальную опасность для свободы выражения мнений, подавляя любую поддержку палестинского дела. Если этот законопроект будет принят, пацифистские лозунги, такие как «равенство и свобода для всех от моря до Иордана», могут стать предметом судебного преследования*». За эту петицию проголосовало 707 тысяч жителей Франции. Согласно правилам Национального собрания, если петиция преодолевает отметку в 500 тысяч подписей, она подлежит обязательному рассмотрению на конференции председателей для организации общественных дебатов. Однако 15 апреля 2026 года юридическая служба закрыла петицию без каких-либо комментариев. Обсуждение законопроекта назначено на 1 мая 2026 года.

В заключение следует отметить, что французское общество сопротивляется попытке государства под предлогом защиты еврейского населения сделать репрессивным закон, направленный на критику действий израильского правительства и военных операций в секторе Газа. Государство действует в специфической форме, не учитывая реальные настроения внутри

общества. Однако общество, в свою очередь, демонстрирует, что с ним нельзя не считаться 707 тысяч подписей это весомый сигнал. Тем самым под вопросом оказываются сами принципы, на которых строилась французская республика. Свобода, равенство и братство постепенно размываются подобными законами. Еврейская проблематика, требующая внимания и защиты перетягивает на себя все внимание государства, делая неравными других граждан. Реальный срок и штраф за слова, которые можно интерпретировать как критику, лишают свободы. Если еврей во Франции де-факто получает правовую защиту, которой не имеет, скажем, белый француз, критикующий действия иностранного государства, то это ставит под сомнение принцип равенства. А значит, и братство, без которого республика перестает быть собой.

**Список используемых источников**

1. Осипов Е. А. Ислам во Франции. Пройдена ли точка невозврата? // Obsfr.ru. 2023. 4 апр. URL: https://obsfr.ru/analytics/blogs/12640/ (дата обращения: 01.05.2026).

2. Balasse A. Non à la loi Yadan // Plateforme des pétitions de l'Assemblée nationale. 18 février 2026. URL: https://petitions.assemblee-nationale.fr/initiatives/i-5158 (дата обращения: 01.05.2026).

3. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (telle que modifiée jusqu'au 1 juin 2019) // WIPO Lex. URL: https://www.wipo.int/ wipolex/ru/legislation/details/18965 (дата обращения: 01.05.2025).

4. Proposition de loi n° 575 visant à lutter contre les formes renouvelées de l'antisémitisme // Assemblée nationale. URL: https://questions.assemblee-nationale.fr/dyn/17/textes/l17b0575_proposition-loi (дата обращения: 01.05.2025).

5. Şanlı E. Gaza death toll surpasses 72,300 as Israeli war continues // Yeni Şafak. 2026. 30 March. URL: https://en.yenisafak.com/world/gaza-death-toll-surpasses-72300-as-israeli-war-continues-3716490 (дата обращения: 01.05.2026).

## YADAN LAW: PUBLIC DISCUSSION IN CONTEMPORARY FRANCE

**Gekht A., Ukhalov O.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In modern democracies, there is a tendency to restrict freedom of speech under the guise of protecting minorities. In France, traditionally considered the cradle of democracy, the parliament is promoting the Yadan bill, which is formally aimed against antisemitism but in fact equates criticism of Israel's actions with a criminally punishable act. This paper analyzes the content of the bill, its key provisions, as well as the public reaction – a petition of 707 thousand citizens, which the legal service of the National Assembly closed without explanation. The contradiction between democratic principles and the practice of their suppression is examined.*

***Key words:*** *democracy, freedom of speech, France, Yadan bill, restriction of rights*

**УДК – 327.2**
**ГРНТИ – 11.25.67**

# ЮГО-ВОСТОЧНАЯ АЗИЯ ВО ВНЕШНЕЙ ПОЛИТИКЕ РОССИИ В 2020-Х ГОДАХ

**И. И. Докучаев[1], А. Ю. Завалишин[2]**

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

*Восточный вектор внешней политики современной России был обозначен еще в 2000-е годы. За прошедшее время, и особенно с началом специальной военной операции, партнерское взаимодействие со странами Востока приобрело для нашей страны еще большее значение. Очевидным лидером в этих взаимовыгодных отношениях выступает Китай. Однако и страны Юго-Восточной Азии проявляют значительный интерес как к экономическим, так и военно-политическим контактам с Россией. При этом страны Юго-Восточной Азии в силу их культурного и геополитического разнообразия имеют значительную специфику, что находит отражение в их взаимодействии с Российской Федерацией. Анализу этой специфики посвящена данная статья.*

***Россия, Юго-Восточная Азия, внешняя политика, поворот на Восток, международные отношения, двухсторонние договоры, военно-техническое сотрудничество***

Страны Юго-Восточной Азии (ЮВА) после их освобождения от колониальной зависимости заняли особое место во внешней политике СССР, и не менее важное место занимают во внешней политике современной России. Уже в 1950-е – 1960-е годы произошло установление дипломатических отношений этих стран с СССР, охвативших не только экономическое взаимодействие, но и военно-политическое сотрудничество, вскоре появилась организация нового типа, отметившая переход от «старого» к «новому» регионализму – АСЕАН [1].

За прошедшие десятилетия, а особенно начиная с 2000-х годов, выстраивание отношений со странами этого региона неизменно оставалось одним из важных направлений внешнеполитической деятельности советского / российского руководства, которое имело значительную специфику. Одним из следствий такого положения дел стал значительный научный интерес к их анализу, лишь усиливавшийся все последующие годы [2, 3, 4].

«Поворот на Восток» во внешней политике России привел не только к поиску и утверждению новых форм международного взаимодействия

с азиатскими гигантами – Китаем и Индией, но и выстраиванию взаимовыгодного сотрудничества со всеми остальными государствами Большого Востока, которое стало важным инструментом противодействия усиливавшемуся давлению на Россию со стороны Запада во главе с США, что объективно было и в интересах стран ЮВА. Если период отношений со странами АСЕАН до начала 2000-х годов исследователи нередко называют «пассивным», то с началом XXI века происходит их «оживление» и институционализация: в 2004 г. Россия присоединяется к Договору о дружбе и сотрудничестве в Юго-Восточной Азии, с 2005 г. начинают проводиться ежегодные встречи на высшем уровне в формате Россия – АСЕАН [5], в 2010 г. Россия становится полноправным участником Восточноазиатского саммита [6].

Новый этап отношений России со странами региона начался в 2020-е годы, определяющее влияние на которые оказали пандемия COVID-19 и СВО на территории Украины. Резко усилившееся санкционное давление США и их союзников на РФ и обострившееся противостояние за глобальное доминирование между КНР и Соединенными Штатами, в том числе, над странами ЮВА, в значительной мере предопределили дальнейшее развитие событий. В этот период обозначились такие их особенности и противоречия, как вынужденное ускорение «поворота на Восток» на фоне разрыва с Западом; объективная неспособность России конкурировать с Китаем и США в экономическом отношении, что отчасти компенсировалось «прагматичной нейтральностью» стран АСЕАН, которые стремятся использовать Россию в «большой игре» с США и Китаем, пытаясь лавировать между ними; поиске Россией новых партнеров в сфере военно-технического сотрудничества; увеличении товарооборота со странами ЮВА при одновременном росте перекоса в сторону российского экспорта (преимущественно углеводородного сырья) и падения импорта.

Явными парадоксами этого периода в международных отношениях стали деловое партнерство с Сингапуром, который при формальной поддержке санкций против РФ стал крупнейшим покупателем российской нефти в регионе [7], а также сохранение деловых отношений России с Таиландом и Малайзией, с одной стороны, позволяющее получать продукцию, важную для работы российского ВПК, с другой, создающее дополнительную зону напряженности не только с США, но и с Китаем. Очевидным плюсом, обеспечивающим долгосрочное стратегическое взаимодействие России со странами ЮВА в 2020-е годы, остается то, что они не считают Рос-

сию угрозой и воспринимают ее своего рода «третьим полюсом» в противостоянии Китая и США [8].

Важным успехом внешнеполитической деятельности России в ЮВА в качестве интегратора «Глобального Юга» стало присоединение к БРИКС в 2024 г. Индонезии, Малайзии и Таиланда [9]. При этом сохраняется существенное противоречие во взаимодействии России с Китаем, с одной стороны, и Вьетнамом, с другой, поскольку Россия, фактически, оказывает поддержку сторонам, между которыми сохраняется многолетняя напряженность в отношении спорных территорий в Южно-Китайском море.

В начале 2020-х годов в результате ухудшения дипломатических и торговых связей России со странами Западной Европы и США, важной задачей российской внешней политики стал поиск новых экономических партнеров, и диверсификация рынков сбыта товаров. Одним из наиболее перспективных регионов для ее реализации стала ЮВА, страны которой имеют долгую историю сотрудничества с Советским Союзом, а позже российскими федеральными компаниями и крупным бизнесом.

Согласно данным МИД РФ, наиболее многочисленные и разноплановые двусторонние связи в период с 2020 г. по 2026 гг. осуществлялись между Россией и странами, имеющими социалистическую ориентацию и находившимися в зоне влияния СССР и Китая, – Вьетнамом, Мьянмой и Лаосом, в то время как рынки государств, традиционно ориентировавшихся на США и страны НАТО, таких как Филиппины, Малайзия, Индонезия и Таиланд, практически не были задействованы и нуждаются в дальнейшей стратегической проработке. Показательно в этом смысле, что с Камбоджей и Филиппинами за последние 5 лет не было заключено ни одного договора о двустороннем сотрудничестве, а с Таиландом, Малайзией, Индонезией и Сингапуром – по одному соглашению в 2023–2024 гг., в то время как в 2010-е годы с этими странами был подписан ряд договоров о военном и военно-техническом сотрудничестве, в Камбодже проведены инициативы по развитию двусторонних контактов и студенческих обменов между образовательными организациями, взаимодействии в сфере атомной энергетики [10].

Основным партнером России в ЮВА остается Социалистическая Республика Вьетнам, с которой в период с 2020 по 2026 гг. было заключено 11 договоров о военно-техническом и энергетическом сотрудничестве, геологической разведке и добыче нефти и газа на континентальном шельфе Вьетнама и на территории России, а также о сотрудничестве в военной и образо-

вательной сферах [10]. Основным проектом российско-вьетнамского сотрудничества становится возобновление строительства атомной электростанции «Ниньтхуан-1», возведение которой планируется госкорпорацией Росатом. Изначальный договор о строительстве АЭС был заключен еще в 2010 г., однако в 2016 г. Вьетнам приостановил его реализацию из-за внутренних финансовых и экономических причин [11]. Военно-техническое сотрудничество в морской сфере, согласованное председателем Морской коллегии РФ Н. Патрушевым и вице-премьером, министром национальной обороны Вьетнама Фан Ван Зянгом в мае 2026 г., позволит России расширить присутствие в Южно-Китайском море, а вьетнамской стороне – усилить свои позиции в территориальном споре с Китаем о принадлежности островов Спратли и Парасельских [12].

С Республикой Союз Мьянма за тот же период Россия заключила 7 договоров, преимущественно о сотрудничестве в сферах таможенной безопасности, космических исследований и образовании. Помимо этого, была произведена взаимная отмена визовых требований для въезда граждан обеих стран и заключено соглашение о строительстве атомной электростанции (2025 г.) [10]. Мьянма остается одним из наиболее перспективных плацдармов для расширения российского присутствия в ЮВА: в условиях гражданской войны и санкционного давления стран Западной Европы и США на официальное правительство страны, она нуждается в расширении круга союзников и привлечении инвестиций со стороны России в сферу военной и энергетической промышленности. Так, строительство планируемой атомной электростанции в специальной экономической зоне «Давэй» осуществляется при содействии госкорпорации Росатом и нуждается в охране от действий вооруженных повстанческих группировок, для чего необходимы российская военная экспертиза и оборудование. Сотрудничество в сфере морской безопасности, включая проведение совместных военно-морских учений «Марумекс» в 2025 г., открывает перед Россией выход к Индийскому океану и возможность присутствия в нем российского флота [13].

Наиболее продуктивной сферой развития двусторонних отношений между Россией и странами ЮВА остается военное партнерство. К 2026 г. Россия заключила более 12 соглашений о военно-техническом сотрудничестве с 7 государствами региона и продолжает вкладывать усилия в развитие этого направления. Другой важной статьей российского экспорта в страны данного региона является экспертиза в строительстве и обслуживании атомных электростанций под эгидой Росатома. Проекты реализуются в трех

странах: Мьянме, Вьетнаме и Камбодже. На третьем месте находятся инициативы в сфере образования и культурного сотрудничества.

Как отмечает эксперт РСМД Г. Толорая, «России невыгодно замыкаться на Китае, попадая от него в экономическую и психологическую зависимость. России целесообразно поддерживать «холодную стабилизацию» в отношениях с оппонентами в АТР, одновременно наполняя диалог с восприимчивыми к этому странами АСЕАН конкретными проектами в сфере энергетического суверенитета, кибербезопасности и использования Северного морского пути. Главная задача – избежать превращения региона в арену прокси-конфликтов, сохраняя статус «балансира» и гаранта инклюзивности» [14].

Юго-Восточная Азия сегодня – один из наиболее важных регионов международного влияния, где сталкиваются интересы крупных держав: Китая, России, США и Индии. Используя существующие противоречия между государствами региона, такие как гражданская война в Мьянме, территориальный спор между Китаем и Вьетнамом, а также пограничный конфликт между Камбоджей и Таиландом, Россия имеет шанс занять позицию посредника и гаранта безопасности в этих странах.

**Список используемых источников**

1. Burfisher M. E., Robinson S., Thierfelder K. Regionalism: Old and New, Theory and Practice / International Food Policy Research Institute 2033 K Street, N.W. Washington, D.C. 20006 U.S.A. 2004. 63 p.

2. Дробинин А., Ходынская-Голенищева М. Юго-Восточная Азия в многополярном мире // Россия в глобальной политике. 2026, 3 апреля // https://globalaffairs.ru/articles/aziya-drobinin-hodynskaya/ (дата обращения: 23.04.2026).

3. Рогожин А. А., Рогожина Н. Г. Юго-Восточная Азия в приоритетах российской политики «поворота к Азии» // Контуры глобальных трансформаций: политика, экономика, право. 2019. Т. 12. № 1. С. 185–203 // DOI: 10.23932/2542-0240-2019-12-1-185-203.

4. Сунь Чжици. Внешняя политика России в Юго-Восточной Азии: актуальные проблемы и перспективы // Культура мира. 2024. Т. 12. № 38. С. 182–188.

5. Ассоциация государств Юго-Восточной Азии // https://www.mid.ru/ru/detail-material-page/1524218/ (дата обращения: 26.04.2026).

6. Мосяков Д.В. Россия и ВАС: трудный путь навстречу друг другу // Юго-Восточная Азия: актуальные проблемы развития. 2016. Вып. XXXI. № 31. С. 5–11.

7. Lee S. Southeast Asia Deepens Trade and Energy Ties with Russia Despite Global Sanctions // https://www.asiapacific.ca/publication/southeast-asia-deepens-trade-and-energy-ties-russia-despite-global-sanctions (дата обращения: 14.03.2026).

8. Strangio S. Ian Storey on Russia’s Turn to Southeast Asia // The Diplomat, July, 15, 2025 // https://thediplomat.com/2025/07/ian-storey-on-russias-turn-to-southeast-asia/ (дата обращения: 28.04.2026).

9. Рогожина Н.Г. Особенности расширения БРИКС в Юго-Восточной Азии // Контуры глобальных трансформаций: политика, экономика, право. 2025. Т. 18. № 1. С. 72–89. DOI: 10.31249/kgt/2025.01.05

10. МИД РФ: Двусторонние договоры (сайт) // https://www.mid.ru/ru/ foreign_policy/international_contracts/international_contracts/2_contract/ (дата обращения: 28.04.2026).

11. Россия и Вьетнам подписали соглашение о строительстве АЭС // Ведомости. 2026, 3 марта // URL: https://www.vedomosti.ru/politics/news/2026/03/23/1184877-o-stroitelstve-aes (дата обращения: 24.04.2026).

12. Россия и Вьетнам подписали план сотрудничества в морской сфере до 2030 года // ТАСС. 2026, 22 мая // URL: https://tass.ru/politika/27500025 (дата обращения: 24.05.2026).

13. Как сотрудничество России и Мьянмы вышло на новый уровень в 2025 году // РСМД. 2026, 16 января // URL: https://russiancouncil.ru/analytics-and-comments/columns/sandbox/kak-sotrudnichestvo-rossii-i-myanmy-vyshlo-na-novyy-uroven-v-2025-godu/ (дата обращения: 24.04.2026).

14. Толорая Г. «Сердцевинная Азия» в эпицентре: как России и АСЕАН сохранить инклюзивный порядок в АТР // Российский совет по международным делам. 2026, 13 мая // https://russiancouncil.ru/analytics-and-comments/analytics/serdtsevinnaya-aziya-v-epitsentre-kak-rossii-i-asean-sokhranit-inklyuzivnyy-poryadok-v-atr/ (дата обращения: 23.04.2026).

## SOUTHEAST ASIA IN RUSSIAN FOREIGN POLICY IN THE 2020S

**Dokuchaev. I.[1], Zavalishin A.[2]**
[1]Saint Petersburg State University
[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The Eastern vector of modern Russia's foreign policy was outlined back in the 2000s. Since then, and especially since the start of the special military operation, partnerships with Eastern countries have become even more important for our country. China is the clear leader in these mutually beneficial relations. However, the countries of Southeast Asia have also shown significant interest in both economic and military-political contacts with Russia. At the same time, due to their cultural and geopolitical diversity, the countries of Southeast Asia have significant specific characteristics, which are reflected in their interactions with the Russian Federation. This article analyzes these specific characteristics.*

***Key words:*** *Russia, Southeast Asia, foreign policy, turn to the East, international relations, bilateral treaties, military-technical cooperation*

**УДК 336.012.23**
**ГРНТИ 06.73.07**

# МЕТОДИКА РАСЧЕТА ИНДЕКСА ФИНАНСОВОЙ КУЛЬТУРЫ НА ОСНОВЕ ВСЕРОССИЙСКОГО ОБСЛЕДОВАНИЯ ДОМОХОЗЯЙСТВ ПО ПОТРЕБИТЕЛЬСКИМ ФИНАНСАМ

**М. А. Егорова, Д. С. Суздалов**

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

*Для оценки эффективности мероприятий в рамках Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года необходимы количественные показатели, которые отражали бы не только знания, но и реальные установки, ценности и поведенческие практики граждан. В связи с этим актуальной задачей становится разработка методики конструирования индекса финансовой культуры на основе открытых данных лонгитюдных опросов, позволяющих оценивать ответственность, долгосрочное планирование и доверие к финансовым институтам.*

***индекс финансовой культуры, финансовая культура, финансовое поведение, доверие, ответственность, долгосрочные горизонты***

Формирование финансовой культуры является основой осознанного поведения и уверенности в будущем. Для целенаправленного воздействия на формирование финансовой культуры, анализа и оценки проводимых мероприятий в рамках «Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года» [1] и их дальнейшей корректировки необходимы индикаторы ее реализации, одним из которых является индекс финансовой культуры, что обосновывает актуальность его разработки.

В основе предлагаемого подхода расчета индекса лежит представление о финансовой культуре как о многомерном явлении, включающем ценностные установки, поведенческие практики и отношение к институтам [2, 3]. Авторы выделили три ключевых компонента: «Ответственность» (регулярность сбережений, наличие банковского счета, готовность управлять личными рисками), «Долгосрочные горизонты» (временной горизонт финансового планирования, участие в добровольных пенсионных накоплениях) и «Доверие» (использование срочных вкладов, страховых полисов, а также ожидаемые источники дохода в пенсионном возрасте). Каждый компонент

агрегирует ответы на 2-3 вопроса, которые присутствуют во всех шести волнах Всероссийского обследования домохозяйств по потребительским финансам (2013–2024 гг.) [4]. Такой выбор обеспечивает содержательную валидность и сопоставимость данных во времени.

Нами разработана методика расчета интегрального индекса финансовой культуры и его компонентов на основе на прошедших валидацию показателей, их балльной оценке, взвешивании и нормализации относительно базового периода. Применение данной методики позволяет обеспечить сопоставимость данных во времени и корректное отражение динамики финансового поведения населения.

Индекс финансовой культуры (ИФК) – индикатор, позволяющий измерить ценности и установки граждан, влияющие на финансовое поведение, «показывает уровень осознанности граждан при принятии финансовых решений и учете сопутствующих рисков» [5].

Методика расчета индекса финансовой культуры состоит из нескольких последовательных этапов.

1. Источники данных: Всероссийское обследование домохозяйств по потребительским финансам (ВОДПФ) – индивидуальные ответы респондентов на вопросы анкеты из шести волн опроса за 2013, 2015, 2018, 2020, 2024 гг.

2. Принцип отбора вопросов из индивидуальных вопросников. Выбрать вопросы, характеризующие ключевые аспекты финансового поведения, которые есть в анкетах всех шести волн опроса для сопоставимости данных в динамике.

3. Структура индекса. Индекс состоит из трех компонент (субиндексов), включающих наиболее значимые вопросы по компонентам: Ответственность (2 вопроса); Долгосрочные горизонты (2 вопроса); Доверие (3 вопроса).

4. Перевод ответов в баллы. Присвоить каждому варианту ответа на отобранные вопросы числовое значение (балл) в диапазоне от 0 до 1 по принципу – более высокая оценка присваивается ответам, отражающим рациональное, финансово устойчивое поведение методом экспертной оценки на основе анализа содержания ответов и их соответствия рациональной модели управления личными финансами.

5. Базовый период и система весов (коррекция на редкость). Провести частотную коррекцию для того, чтобы редкие, но значимые ответы не терялись на фоне массовых ответов.

Для обеспечения стабильности ретроспективных данных первые три волны опроса (2013, 2015, 2018) принять в качестве базового периода. Для каждого варианта ответа в базовом периоде рассчитать общую частоту:

**Базовая частота = ∑ ответов / ∑ респондентов**

На основе базовой частоты вычислить опорный (базовый) вес:

**Базовый вес =1 / Базовая частота**

Чем реже встречается ответ, тем выше его вес, и тем сильнее он влияет на итоговый индекс. Эти веса используются для расчета во всех годах базового периода, а также служат основой для корректировки весов в последующие годы.

6. Учет изменений в структуре ответов (поправочный коэффициент). Скорректировать для волн опроса 2020, 2022, 2024 годов опорные веса с учетом того, насколько частота данного варианта ответа отклонилась от базового уровня в конкретной волне исследования.

Рассчитать для каждого варианта ответа и каждого года (2020, 2022, 2024) коэффициент актуальности:

**Коэффициент актуальности =**
**= Частота варианта в году / Базовая частота * Базовый вес,**

где Частота варианта в году = Число ответов в году / Число респондентов в году.

Такая корректировка позволит сохранить неизменными значения индекса за базовые годы, учесть изменения в частоте ответов в последующие волны и обеспечит актуальность весов без пересмотра ретроспективных данных.

7. Вклад варианта в индекс года. Рассчитать для каждого года и каждого варианта ответа:

**Вклад = Число ответов в году * Балл варианта * Вес года.**

Просуммировать вклады всех вариантов и разделить на общее число респондентов в данном году. Таким образом рассчитывается средний взвешенный балл на человека.

8. Агрегация по компонентам. Субиндексы по каждому компоненту для каждой волны рассчитать, как среднее арифметическое значение индексов входящих в компонент вопросов (на основании ответов респондентов):

– индекс ответственности (среднее по двум вопросам);
– индекс долгосрочные горизонты (ИДГ) (среднее по двум вопросам);
– индекс доверия (среднее по трем вопросам).

9. Нормализация по компонентам (приведение к базовому году). Провести нормировку относительно базового 2013 года для сопоставимости компонент между собой и обеспечения равного вклада каждого в итоговый ИФК. Для каждого компонента все значения индексов за 6 волн обследования разделить на значение индекса этого компонента в 2013 году. Таким образом, индекс каждого компонента в 2013 году равен 1, и значения в последующие волны отражают рост или падение относительно базового уровня.

Предварительная частотная коррекция и нормализация по компонентам (приведение значений каждого субиндекса к базовому 2013 году) обеспечивает сопоставимость компонентов и равный вклад в итоговый ИФК. Для актуализации данных в новых волнах опроса следует использовать поправочные коэффициенты. Ответы респондентов учитываются с учетом взвешивания.

10. Итоговый индекс финансовой культуры. Рассчитать среднее арифметическое трех нормализованных субиндексов компонент за каждый год:

$$\text{ИФК} = (\text{Индекс ответственности (норм)} + \text{Индекс ДСГ (норм)} + \text{Индекс доверия (норм)})/3.$$

Таким образом, итоговый композитный ИФК формируется из нормированных субиндексов компонентов с равными весами «на основании анализа релевантности показателей» [3]. Такое усреднение нормированных индексов обеспечивает равный вклад каждого компонента (по 33,3 %) в итоговый ИФК независимо от абсолютных значений субиндексов.

Предложенная методика позволяет рассчитать индекс финансовой культуры на основе данных лонгитюдных опросов с повторяющимися вопросами, используя частотную коррекцию весов и нормировку компонентов относительно базового периода. Алгоритм обеспечивает сопоставимость данных во времени и устойчивость ретроспективных оценок при добавлении новых волн опроса. Методика может быть адаптирована для измерения других социально-экономических установок на аналогичных панельных данных.

Сконструированный индекс финансовой культуры переводит не измеряемые абстрактные категории финансовых установок и ценностей в конкретный измеряемый показатель. Начальное (базовое) значение индекса ИФК принимается за единицу, а последующие значения отражают рост или падение относительно базового года. Чем выше данный показатель, тем выше общий уровень финансовой культуры.

Предложенный нами метод расчета позволяет оценивать общую динамику финансовой культуры населения во времени; отслеживать рост или падение и анализировать структурные изменения отдельных компонентов относительно базового 2013 года.

Данная методика позволяет превратить субъективные мнения граждан в объективный математический инструмент, который учитывает как значимость редких моделей поведения, так и изменения в обществе с течением времени. Таким образом, ИФК позволяет перевести абстрактные категории ценностей и установок в измеряемый объект управления.

Преимуществами методики являются соответствие вопросов теоретическим определениям компонентов, учет всесторонних аспектов поведенческих установок, прозрачность расчетов, возможность дальнейшего анализа без искажения предыдущих результатов. Метод нормировки показателей относительно базового года позволяет корректно сопоставлять их динамику и вклад в агрегированный ИФК.

Сконструированный по данной методике индекс прошел проверку методами математической статистики. Связь между каждым компонентом и интегральным ИФК доказана методами корреляции Пирсона и альфа Кронбаха [6]. Расчеты показали, что все компоненты положительно коррелируют с ИФК, что доказывает внутреннюю согласованность конструкта. и подтверждает гипотезу о том, что финансовую культуру можно измерить через три ключевых компонента – ответственность, долгосрочные горизонты и доверие.

Проведенный нами расчет смоделированного индекса развития финансовой культуры и его компонентов для Российской Федерации на основе «Объединенных данных по индивидуальной анкете – все волны» Всероссийского лонгитюдного обследования домохозяйств по потребительским финансам показал, что это надежный инструмент, по которому можно отслеживать прогресс в развитии финансовой культуры как в целом, так и по отдельным компонентам.

**Список используемых источников**

1. Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 года // http://static.government.ru/media/files/FJj6iZ8geL94xUACfr2s32ZQoUgqP7fd.pdf (дата обращения 10.05.2026).

2. Методика расчета индикатора реализации Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года «Индекс развития финансовой культуры» // https://minfin.gov.ru/common/upload/library/2025/06/main/12-12-12VN-25159__PRG-59-6-11522.pdf (дата обращения 10.05.2026).

3. Аузан А., Богомолова А., Р. Кокорев. Индекс развития финансовой культуры: подходы к формированию и измерению // Деньги и кредит. Москва, 2025 № 3. Том 84: https://rjmf.econs.online/2025/3/financial-cultureindex-design/ (дата обращения 10.05.2026).

4. Всероссийское обследование домохозяйств по потребительским финансам | Банк России // https://www.cbr.ru/ec_research/vserossiyskoe-obsledovanie-domokhozyaystv-po-potrebitel-skim-finansam/ (дата обращения 10.05.2026).

5. Финансовая культура в России: точка отсчета // Банк России. URL: https://cbr.ru/press/event/?id=23251 (дата обращения 10.05.2026).

6. Фомина Е. Е. Обзор методов оценки надежности измерительной шкалы в социологических исследованиях // Экономика. Социология. Право. 2018. № 4 (12). С. 63-70.

## METHOD FOR CALCULATING THE FINANCIAL CULTURE INDEX BASED ON THE ALL-RUSSIAN SURVEY OF HOUSEHOLDS ON CONSUMER FINANCE

**Egorova M., Suzdalov D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*To assess the effectiveness of measures within the framework of the Strategy for improving financial literacy and forming a financial culture until 2030, it is necessary to use quantitative indicators that reflect not only knowledge, but also real attitudes, values, and behavioral practices of citizens. In this regard, it is an urgent task to develop a methodology for constructing a financial culture index based on open data from longitudinal surveys, which allows for assessing responsibility, long-term planning, and trust in financial institutions.*

***Key words:*** *financial culture index, financial culture, financial behavior, trust, responsibility, long-term horizons*

**УДК 316.454.52**
**ГРНТИ 14.35.07**

# ФОРМИРОВАНИЕ КРИТИЧЕСКОГО МЫШЛЕНИЯ И ЭТИЧЕСКОЙ РЕФЛЕКСИИ ПРИ РАБОТЕ С ИИ У МАГИСТРАНТОВ В РАМКАХ КУРСА «ИЯ ДЛЯ НИР»

**Е. П. Желтова, Н. В. Маршева**

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

*В рамках редизайна курса по иностранному языку для научно-исследовательской работы обоснована проблема некритического и неэтичного использования генеративных моделей ИИ студентами магистратуры, для решения которой предлагается методическая модель формирования критического и этичного подхода к работе с ИИ, включающая систему заданий для взаимодействия с технологией в различных академических контекстах. Особое внимание уделяется этической рефлексии обучающихся при оценке текстов, генерируемых ИИ.*

***генеративные модели, этическая рефлексия, академическая коммуникация, грамотность в области ИИ, методическая модель***

Цифровизация высшего образования и стремительное распространение инструментов генеративного искусственного интеллекта (ИИ) существенно изменили характер учебной и научно-исследовательской деятельности студентов магистратуры. Если ранее основной задачей академического обучения являлось формирование навыков поиска, анализа и представления информации, то в настоящее время особую актуальность приобретает способность критически оценивать информацию, генерируемую интеллектуальными системами, а также использовать ИИ как инструмент научной работы, не подменяя им собственную аналитическую деятельность.

Обучение принципам академической этики является важной составляющей профессиональной подготовки в современном университете, в том числе для преподавательской и научной деятельности [1]. Сегодня данный подход необходимо экстраполировать на взаимодействие студентов с технологиями ИИ. В этом контексте этическая рефлексия в отношении ИИ выполняет функцию внутреннего ограничителя в сознании студента, механизма, благодаря которому он перестает быть пассивным пользователем

и превращается в субъект, ответственного за применение цифрового инструмента. Речь идет об аксиологическом измерении цифровой компетентности, способности не просто владеть навыками, но и демонстрировать намерение использовать ИИ правильно, честно и ответственно [2]. Однако анализ реальной педагогической практики показывает, что большинство учебных дисциплин в вузе либо полностью игнорируют наличие ИИ в арсенале студентов, либо ограничиваются запретами, которые легко обходятся обучающимися. При этом методически обоснованных, воспроизводимых систем заданий, где ИИ становится не готовым решением, а инструментом развития критического мышления, на данный момент недостаточно. Особенно остро этот дефицит проявляется в магистратуре технических направлений, где студенты активно используют генеративные модели, но часто без соблюдения академической этики, без этической рефлексии, без понимания границ применения ИИ и без навыков верификации результатов.

Данное исследование восполняет этот пробел, предлагая не общие рекомендации, а конкретную, апробированную систему практических заданий при обучении ИЯ. Цель данной статьи – представить систему заданий для формирования критического и этичного использования ИИ у магистрантов технических направлений, разработанную и апробированную в рамках проекта по редизайну курса «Иностранный язык для научно-исследовательской работы» в интерактивный электронный курс «English for Research: Mastering Academic Communication» при поддержке Фонда Потанина, направленного на развитие академического письма, научной презентации, навыков дискуссии и представления результатов исследования на английском языке.

В современных трудах критическое мышление рассматривается как одна из ключевых метакомпетенций XXI века, обеспечивающая способность анализировать информацию, выявлять логические противоречия, принимать обоснованные решения и нести ответственность за их последствия [3]. Особую значимость эта компетенция приобретает в условиях широкого распространения генеративных моделей ИИ, которые создают иллюзию компетентности и могут формировать технологическую зависимость [4, 5].

Обзор эмпирических исследований показывает, что в большинстве из них подтверждается положительное влияние генеративного ИИ на развитие критического мышления студентов, но при условии педагогического сопровождения, структурированных заданий и рефлексивной практики. Однако в обзоре также фиксируются риски «когнитивной разгрузки» (cognitive offloading), когда студенты делегируют ИИ аналитическую работу без кри-

тической оценки результатов [3, 5]. Исследования демонстрируют, что сравнение обратной связи от ИИ и от человека-рецензента способствует развитию грамотности в области ИИ (AI literacy), то есть способности критически оценивать ограничения ИИ (неточности, предубеждения, отсутствие контекста) [6]. В исследованиях вводится важное различение двух типов критического мышления в контексте ИИ, а именно «критическое мышление по отношению к самому ИИ» (оценка качества ответов, выявление предвзятости, уточнение промптов) и «критическое мышление для выполнения задания» (синтез и применение сгенерированных ИИ идей в решении реальной задачи) [7]. При этом подчеркивается, что некритическое использование ИИ ведет к снижению когнитивной автономии студентов.

Наряду с когнитивными аспектами, исследователи выделяют этическую составляющую грамотности в области ИИ. Студенты должны осознавать границы допустимого использования ИИ в академической деятельности, понимать необходимость декларации использования ИИ, а также риски, связанные с алгоритмическими искажениями и генерацией ложной информации [8, 9]. Анализ литературы показывает, что большинство исследований либо остаются на уровне общих рекомендаций по развитию критического мышления и этической рефлексии, либо фокусируются на технических аспектах использования ИИ. Несмотря на значительное количество работ, остается недостаточно разработанным вопрос о том, каким образом можно системно интегрировать развитие критического мышления и навыков работы с ИИ в структуру конкретной учебной дисциплины, особенно на уровне магистратуры.

Научная новизна предлагаемого подхода заключается не в самом факте использования ИИ в обучении, а в трех принципиальных аспектах. Первый вектор трансформации связан с переходом от запрета к легитимизации ИИ, сопряженной с обязательной критической рефлексией, что предполагает не сокрытие, а открытое декларирование и аналитическое осмысление студентом факта использования технологий. Второй заключается в разработке восходящей спирали критической нагрузки, где движение идет от личного контекста, где цена ошибки невелика (резюме, оценка своих качеств, мотивов) к академически значимому (верификация источников) и далее к стратегическому (выбор формата презентации исследования). Третий подразумевает введение этической рефлексии как обязательного элемента каждого задания, что превращает техническое действие в осознанную профессиональную практику. В отличие от большинства работ, сосредоточенных на техни-

ческой стороне промптинга, данная система фиксирует внимание на аргументированном отказе от рекомендаций ИИ как ключевом действии, формирующем когнитивную автономию студента.

Разработанная система заданий интегрирована в авторский интерактивный электронный курс [10] и представлена в каждом модуле рабочей программы дисциплины (РПД) в виде отдельного раздела «Лаборатория ИИ для НИР» (AI Research Lab) (см. рис. 1).

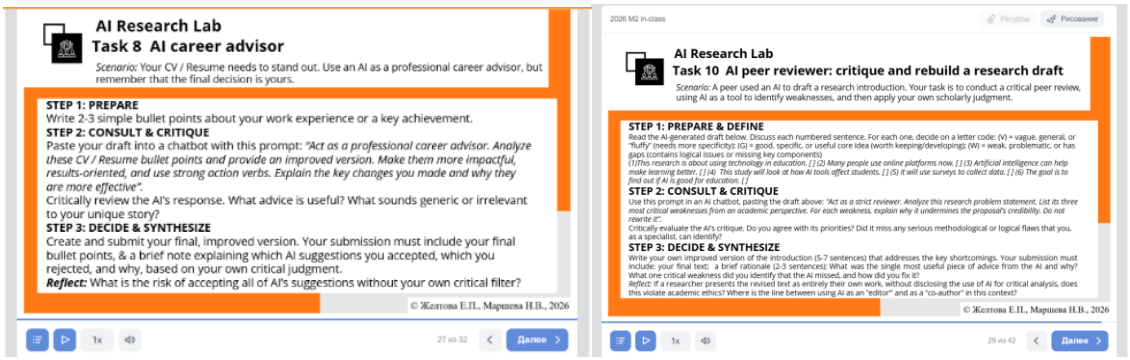



Рис. 1. Фрагменты интерактивного курса с заданиями AI Research Lab

Функционирование данной системы базируется на четырех ключевых принципах, представленных в Таблице 1.

ТАБЛИЦА 1. Ключевые принципы использования ИИ в AI Research Lab

| № | Принцип | Значение |
|---|---|---|
| 1 | Легитимность ≠ авторитет | ИИ использовать можно, но истиной он не является |
| 2 | Прозрачность | О факте использования ИИ сообщается открыто |
| 3 | Верификация | Любой результат ИИ должен быть проверен |
| 4 | Ответственность | Финальное решение и его последствия за студентом |

Логика учебной деятельности выстроена по вектору от рефлексии над собой к оценке внешних объектов. В соответствии с этим для каждого модуля курса «ИЯ для НИР» были разработаны задания, в рамках которых магистранты взаимодействуют с ИИ в различных ролях. При этом каждое задание включает описание роли ИИ, действий магистранта, формируемых навыков, а также блок этической рефлексии на всех этапах обучения.

В модуле 1 «Постдипломное образование и академическая среда» ИИ выступает в роли консультанта по развитию карьеры. Магистрант пишет черновик резюме, просит ИИ улучшить формулировки, анализирует полученные советы и создает финальную версию с пояснением, какие рекомендации он принял, а какие отклонил. В ходе работы формируются навыки

критического отбора и сохранения авторской позиции. Этическая рефлексия направлена на осмысление риска принятия всех советов ИИ без собственного критического фильтра. В модуле 2 «Основы и этапы НИР» ИИ выступает в роли строгого рецензента академического текста. Магистрант получает слабый черновик текста, просит ИИ назвать три главных недостатка, оценивает полученную критику и пишет улучшенную версию. При этом формируются навыки диагностики текста и оценки экспертного мнения. Этическая рефлексия касается вопроса о том, является ли нарушением этики представление переработанного ИИ текста как своей работы без раскрытия использования ИИ.

В модуле 3 «Основы академического чтения и академического письма» ИИ выступает в роли редактора академического текста. ИИ предлагает стилистические правки аннотации, студент критически оценивает каждую правку и создает финальную версию, сохраняя авторский голос. При этом формируются навыки отбора правок. Этическая рефлексия связана с вопросом о том, в какой степени текст остается авторским, если ИИ значительно улучшил его ясность. При обучении академическому чтению и поиску достоверных источников студенту предлагается использовать ИИ как консультанта по выбору источников с изучением алгоритмических искажений, анализом рисков опоры на рекомендации ИИ и применением критериев CRAAP (Currency, Relevance, Authority, Accuracy, Purpose) для проверки источника на актуальность, релевантность, авторитетность источника, точность информации, цель данной публикации. Таким образом, формируются навыки информационной грамотности и верификации. Этическая рефлексия заключается в вопросе о необходимости цитирования ИИ в методологии при использовании его для поиска источников.

В модуле 4 «Научная конференция как основа академического и профессионального взаимодействия» ИИ выступает в роли консультанта по выбору релевантной конференции для участия. Магистрант описывает свое исследование, просит ИИ рекомендовать наиболее подходящий формат презентации, оценивает полученные рекомендации и принимает самостоятельное решение. Формируются навыки стратегического мышления и аргументации. Этическая рефлексия направлена на вопрос об этичности использования сгенерированных ИИ обоснований при принятии решения об отправки заявки на конференцию.

Ключевая особенность всех заданий заключается в том, что студент не может использовать ответ ИИ как готовое решение. Каждое задание требует обязательной оценки, отбора, аргументации и этической рефлексии. Особенно важным представляется требование аргументированного отказа от со-

вета ИИ, поскольку именно это действие формирует критическую автономию. Задания выстроены по нарастающей сложности, что позволяет постепенно увеличивать критическую нагрузку, при этом каждое задание завершается этическим вопросом, который превращает техническое действие в осознанную практику и формирует у студента понимание границ допустимого использования ИИ. Например, в задании «AI and your literature search strategy» Модуля 3 студент рефлексирует о том, является ли ИИ «исследовательским инструментом» или «интеллектуальным соавтором»? Полный перечень этических вопросов для каждого модуля интегрирован в интерактивный курс [10].

Практическая значимость методической модели состоит в том, что предложенная система заданий может быть внедрена в любую дисциплину, где требуется работа с текстами, источниками и аргументацией (не только в курс иностранного языка); не требует специальной технической подготовки преподавателя и работает на любых доступных генеративных моделях; легко масштабируется за счет замены академических контекстов (резюме, аннотация, поиск источников, выбор конференции и т.д.) на профильные; включает готовые формулировки этических вопросов и инструкции для студентов.

Результаты апробации курса, основанные на анализе письменных работ магистрантов и педагогическом наблюдении, показали, что студенты начинают осознанно подходить к оценке рекомендаций ИИ, фиксируя случаи, когда совет ИИ был отклонен, аргументируя свой выбор и демонстрируя понимание этических границ использования технологии.

Таким образом, в рамках проекта по редизайну курса «Иностранный язык для НИР» была разработана, внедрена и апробирована система заданий для формирования критического и этичного использования ИИ у магистрантов технических направлений. Предложенная методическая модель заполняет существующий пробел, поскольку предлагает конкретные и воспроизводимые приемы, средства и задания, где ИИ служит не готовым ответом, а материалом для критической оценки студентом. Каждое задание включает этическую рефлексию, что позволяет формировать не только критическое, но и этичное отношение к использованию ИИ, включая понимание границ его применения, необходимости декларации и ответственности за результат. Ключевым педагогическим условием эффективности является замена запрета на легитимизацию ИИ с обязательной критической рефлексией, что формирует у магистрантов навыки ответственного и осознанного использования ИИ в учебе, проектной и исследовательской деятельности.

**Список используемых источников**

1. Соколов Н. В., Виноградский В. Г. Искусственный интеллект и образование: анализ систем и технологий, применяемых в РФ // Образование и общество. 2023. № 1 (138).
2. Конколь М. М., Шишлова Е. Э. Трансформация образовательной субъектности студента университета в эпоху ИИ-технологий // Высшее образование в России. 2026. Т. 35. № 2. С. 36–52.
3. Raitskaya L., Tikhonova E. Enhancing Critical Thinking Skills in ChatGPT-Human Interaction: A Scoping Review // Journal of Language and Education. 2025. Vol. 11. N 2. P. 5–19. https://DOI.org/10.17323/jle.2025.27387.
4. Сысоев П. В., Филатов Е. М. ChatGPT в исследовательской работе студентов: запрещать или обучать? // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2023. Т. 28. № 2. С. 276–301. https://DOI.org/10.20310/1810-0201-2023-28-2-276-301.
5. Гаркуша Н. С., Городова Ю. С. Педагогические возможности ChatGPT для развития когнитивной активности студентов // Профессиональное образование и рынок труда. 2023. Т. 11. № 1. С. 6–23. https://DOI.org/10.52944/PORT.2023.52.1.001.
6. Tzirides A. O., Zapata G., Kastania N. P., Saini A. K., Castro V., Ismael S. A., You Y. L., Santos T. A., Searsmith D., O'Brien C., Cope B., Kalantzis M. Combining human and artificial intelligence for enhanced AI literacy in higher education // Computers and Education Open. 2024. Vol. 6. 100184. https://DOI.org/10.1016/j.caeo.2024.100184.
7. Gonsalves C. Generative AI's impact on critical thinking: Revisiting Bloom's taxonomy // Journal of Marketing Education. 2024. Vol. 48. N 1. P. 4–19. https://DOI.org/10.1177/02734753241305980.
8. Holmes W., Porayska-Pomsta K., Holstein K., Sutherland E., Baker T., et al. Ethics of AI in education: Towards a community-wide framework // International Journal of Artificial Intelligence in Education. 2022. Vol. 32. N 3. P. 504–526. https://DOI.org/10.1007/s40593-021-00239-1.
9. Farrelly T., Baker N. Generative artificial intelligence: Implications and considerations for higher education practice // Education Sciences. 2023. Vol. 13. N 11. 1109.
10. Желтова Е. П., Маршева Н. В. Электронный курс «ИЯ для НИР» // СЭО СПбГУТ. 2026. URL: https://lms.sut.ru/course/view.php?id=139 (дата обращения: 09.04.2026).

## DEVELOPING CRITICAL THINKING AND ETHICAL REFLECTION ON AI IN A MASTER'S COURSE "FOREIGN LANGUAGE FOR RESEARCH"

**Zheltova E., Marsheva N.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper addresses the problem of uncritical and unethical use of generative AI models by master's students; a concern identified during the redesign of a foreign language course for research purposes. To counter this issue, a methodological model is proposed to foster critical thinking and ethical AI practices. The model integrates practical tasks that engage students with generative AI across a range of academic contexts. Particular emphasis is placed on ethical reflection by students when evaluating AI-generated texts.*

***Key words:*** *generative models, ethical reflection, academic communication, AI literacy, methodological model*

**УДК 3.314/316; 33.330.3; 33.338.1**
**ГРНТИ 13.11.47; 13.21.01: 68.01.99**

# СОЦИОКУЛЬТУРНЫЕ АСПЕКТЫ РАЗВИТИЯ БЕЛОРУССКОГО СЕЛА

**В. А. Журавлев**
Белорусская государственная академия связи

*Настоящая статья посвящена комплексному исследованию социокультурных аспектов развития белорусского села. В условиях современных социально-экономических трансформаций, село сталкивается с целым рядом вызовов. Особое внимание уделяется роли культуры, традиций и ценностей в формировании устойчивого села. Анализируются аспекты развития современного белорусского села, влияющие на социокультурный потенциал села, включая демографические процессы, миграцию, уровень образования, состояние социальной инфраструктуры и развитие культурных инициатив.*

*В контексте сохранения национальной идентичности и самобытности, исследование социокультурного развития белорусского села приобретает особую актуальность. Традиционные формы хозяйствования, народные ремесла, фольклор и обычаи являются не только частью культурного наследия, но и потенциальным ресурсом для развития агротуризма, сельского предпринимательства и повышения качества жизни сельского населения.*

***село, социокультурное развитие, национальная идентичность, социальная инфраструктура, культурные традиции***

Социокультурное развитие белорусского села представляет собой сложный и многогранный процесс, в котором тесно переплетаются задачи сохранения национального наследия, повышения качества жизни и формирования идентичности сельских территорий. Экономические, социальные и культурные аспекты развития села вышли на уровень государственной политики, поскольку деревня рассматривается не только как центр агропромышленного производства, но и как хранительница, традиций и исторической памяти малой родины [1].

Современное белорусское село стоит на пороге перемен, где традиционные уклады соседствуют с новыми реалиями. Важность сохранения культурного наследия, аутентичности быта и народных обычаев становится тем стержнем, который может обеспечить устойчивость и самобытность сельских территорий в условиях глобализации.

Однако для реального возрождения села необходимы комплексные меры, направленные на решение насущных проблем: создание рабочих мест, развитие инфраструктуры, повышение уровня жизни и доступности качественных услуг. Привлечение молодежи, поддержка фермерских хозяйств, развитие агротуризма – все это кирпичики в фундаменте будущего процветания села.

В центре внимания правительства Республики Беларусь находится трансформация традиционных укладов жизни под влиянием цифровизации, урбанизации и глобализации, затрагивающие социальную структуру, демографическую ситуацию, культуру и досуг сельского населения.

Одним из ключевых аспектов является демографическая ситуация. Сокращение сельского населения, старение активной части, миграция молодежи в города – эти тенденции создают серьезные вызовы для устойчивого развития села. Они влияют на социальную напряженность, доступность социальных услуг и возможность воспроизводства сельского сообщества.

Также не менее важна социальная инфраструктура села. Доступность качественного образования, здравоохранения, культурных учреждений, бытового обслуживания – это факторы, определяющие качество жизни сельского жителя и его желание оставаться на селе. Развитие этих сфер напрямую связано с экономическим состоянием сельских территорий и государственной политикой поддержки агрогородков и сельских населенных пунктов.

Важным фактором развития является также совершенствование инфраструктуры, обеспечивающей доступ к культурным благам. Строительство и модернизация сельских домов культуры, библиотек, музеев, а также обеспечение доступа к современным информационным технологиям позволяют расширить возможности для культурного досуга и самообразования. Это способствует преодолению культурной изоляции и интеграции сельских сообществ в более широкий социокультурный контекст.

В Республике Беларусь волоконно-оптические линии связи уже подведены ко всем населенным пунктам с числом домохозяйств от 100 и более. На данный момент завершается подключение деревень с 50 – 100 домохозяйствами. В целом оптоволокно уже подведено в 1449 населенных пунктах. Создание условий для гражданской активности способствуют формированию чувства принадлежности и ответственности за судьбу своей малой родины. Вовлечение молодежи в культурную и общественную жизнь становится приоритетом для обеспечения преемственности и устойчивого развития.

Анализ деятельности правительства Республики Беларусь позволяет выделить несколько ключевых социокультурных аспектов развития современного белорусского села.

### 1. Сохранение и возрождение традиционной культуры как основа идентичности

Одним из главных трендов является активное возрождение аутентичных обрядов и народных праздников. Это не просто дань моде, а осознанная стратегия по сохранению «культурного обычая» нации [2]. По всей стране проходят мероприятия, которые реконструируют старинные традиции. В рамках фольклорного проекта «Кола жыцця» ежегодно реконструируют старинные колядные обряды, привлекая тысячи гостей [3].

### 2. Формирование новых культурных брендов и развитие агротуризма

Современное село становится площадкой для создания ярких событийных брендов, которые работают на привлечение туристов и формирование позитивного имиджа территории. Фестивали деревенской еды, праздники, посвященные местным продуктам или ремеслам (каравай-фест «Бацькава булка», праздник гончара, рушника), становятся точками притяжения и драйверами экономического развития [2]. Ярким примером успеха стал фестиваль «Бацькава булка», который всего за несколько лет получил признание на республиканском уровне и специальную премию Президента [2].

Агроусадьбы превращаются в настоящие центры притяжения, предлагая гостям не просто ночлег, а погружение в народную культуру и спрос на них растет с каждым годом, причем как среди белорусов, так и среди иностранных гостей, которые ищут «простоты и тепла» [3].

### 3. Преобразование культурной инфраструктуры и социальной сферы

Государственные программы, такие как Государственная программа возрождения и развития села, привели к созданию сети агрогородков – качественно новых типов сельских поселений с современной инфраструктурой [4].

Реализуются проекты, которые через мастер-классы и интерактивные экскурсии вовлекают посетителей в жизнь крестьянина начала XX века, а также учат народным ремеслам, таким как плетение из лозы [5].

## 4. Преемственность поколений и вовлечение молодежи

Ключевым фактором устойчивости социокультурного развития является передача традиций молодому поколению. Во многих селах дети и подростки не просто являются зрителями, а активно участвуют в обрядах и фольклорных коллективах. Школьники включаются в колядные шествия, понимая свою роль в сохранении памяти малой родины [3]. Детские коллективы становятся лауреатами престижных конкурсов, получая поддержку из специальных фондов Президента [2].

## 5. Духовные ориентиры и качество жизни

В основе социокультурного развития лежит не только экономика, но и система ценностей. Изменилось качество жизни, но не изменились духовные ориентиры: семья, уважение к земле, взаимопомощь и почитание предков остаются приоритетами [3]. Задача государства – создать условия (достойная зарплата, благоустроенное жилье, доступная медицина и образование), чтобы эти ценности могли быть реализованы в современном контексте, чтобы жизнь на селе была престижной и комфортной, а молодежь видела здесь перспективы для себя [1, 5] – [7].

Будущее белорусского села видится в гармоничном сочетании традиционных ценностей и современных инноваций. Именно в этом синтезе кроется потенциал для создания благополучной, культурно богатой и привлекательной для жизни сельской местности, которая продолжит играть ведущую роль в формировании национальной идентичности Беларуси.

Таким образом, цифровизация белорусского села, направленна на повышение качества жизни сельских жителей, развитие инфраструктуры и создание новых рабочих мест, что являются залогом его устойчивого развития. Особое значение приобретают программы, стимулирующие молодежь к возвращению и работе на селе, обеспечивая преемственность поколений и приток свежих идей.

Возрождение традиционных форм хозяйствования, поддержка народных промыслов и развитие агроэкотуризма создают новые экономические возможности, и позволяет белорусскому селу оставаться живым организмом, наполненным смыслом и сохраняющим свою уникальную идентичность.

Социокультурное развитие белорусского села сегодня – это симбиоз бережного сохранения традиций и смелого внедрения инноваций. Это процесс превращения сельской местности из пространства преимущественно

аграрного в пространство многофункциональное, где культура становится и ресурсом для развития туризма, и фактором привлечения людей, и, самое главное, основой для формирования национальной идентичности.

В конечном итоге, социальная и культурная устойчивость белорусского села зависит от баланса между сохранением уникальных традиций и открытостью к инновациям. Именно осознанное отношение к своему прошлому, в сочетании с активной жизненной позицией и стремлением к развитию, позволит белорусской деревне не просто выжить, но и стать полноценным, динамичным и привлекательным местом для жизни, работы и творчества.

Формирование новой идентичности белорусского села из преимущественно аграрного трансформируется в многофункциональный центр, где культурное наследие (обряды, ремесла, фольклор) становится ресурсом для развития туризма, создания локальных брендов и экономического роста. Успешная реализация государственных программ, выразившаяся в создании сети агрогородков с развитой инфраструктурой и обновленными Домами культуры, создает материальную базу для этого развития.

Особую значимость приобретает принцип преемственности: вовлечение молодежи в народные традиции и поддержка юных дарований обеспечивают передачу «культурного кода» будущим поколениям. В конечном счете, социокультурное развитие белорусского села направлено на достижение главной цели – сделать жизнь на земле престижной и комфортной, укрепив духовные ориентиры (семья, труд, взаимопомощь), которые всегда были основой белорусского общества.

**Список используемых источников**

1. Спасти деревню – фундаментальный вопрос для существования белорусского государства // vns.gov.by. URL: https://vns.gov.by/ru/intervyu-publikacii-mneniya-ru/view/spasti-derevnju-fundamentalnyj-vopros-dlja-suschestvovanija-belorusskogo-gosudarstva-305/. (дата обращения: 07.04.2026).

2. В проекте «Свислоччина: шаги успешного развития» рассказываем, как развивается сфера культуры в Свислочском районе // svisloch.gov.by. URL: https://svisloch.gov.by/ru/svisloch-news-ru/view/v-proekte-svislochchina-shagi-uspeshnogo-razvitija-rasskazyvaem-kak-razvivaetsja-sfera-kultury-v-28008-2025. (дата обращения: 27.04.2026).

3. Народный колорит и гостеприимство: узнали, почему россияне едут на Коляду в Могилевский район // mogilev-region.gov.by. URL: https://mogilev-region.gov.by/news/kultura/narodnyy-kolorit-i-gostepriimstvo-uznali-pochemu-rossiyane-edut-na-kolyadu-v. (дата обращения: 20.03.2026).

4. Kitobni o'qish: «История формирования и современный облик белорусского села» // litres.uz. URL: https://litres.uz/book/a-i-lokotko/istoriya-formirovaniya-i-sovremennyy-oblik-belorusskogo-sela-69553783/read/. (дата обращения: 23.04.2026).

5. Экскурсия в прошлое через современность // belynichi.gov.by. – URL: https://belynichi.gov.by/news/region/8317.html#up. (дата обращения: 10.04.2026).

6. Развитие современного белорусского села: проблемы, тенденции, перспективы // socio.bas-net.by. URL:https://socio.bas-net.by/?portfolio=razvitie-sovremennogo-belorusskogo-sela-problemy-tendentsii-perspektivy. (дата обращения: 10.04.2026).

7. Глеб Лапицкий: «В Пальминке я увидел пример того, как надо реализовывать мероприятия по развитию малых населенных пунктов» // vitvesti.by. URL: https://vitvesti.by/obshestvo/gleb-lapitckii-v-palminke-ia-uvidel-primer-togo-kak-nado-realizovyvat-meropriiatiia-po-razvitiiu-malykh-naselennykh-punktov.html. (дата обращения: 15.04.2026).

## SOCIO-CULTURAL ASPECTS OF THE DEVELOPMENT OF THE BELARUSIAN VILLAGE

**Zhuravlev V.**
Belarusian State Academy of Communications

*This article focuses on a comprehensive study of the sociocultural aspects of the development of the Belarusian countryside. In the context of modern socio-economic transformations, the countryside faces a range of challenges. The article emphasizes the role of culture, traditions, and values in shaping a sustainable countryside. It analyzes the aspects of the development of the modern Belarusian countryside that influence its sociocultural potential, including demographic processes, migration, educational levels, social infrastructure, and cultural initiatives.*

*In the context of preserving national identity and distinctiveness, the study of the sociocultural development of the Belarusian countryside becomes particularly relevant. Traditional forms of farming, folk crafts, folklore, and customs are not only part of the cultural heritage, but also a potential resource for the development of agrotourism, rural entrepreneurship, and improving the quality of life for the rural population.*

***Key words:*** *village, socio-cultural development, national identity, social infrastructure, and cultural traditions*

**УДК 004.932.4**
**ГРНТИ 12.21.55**

# ОСОБЕННОСТИ ФОРМИРОВАНИЯ НАУЧНОЙ КОМПЕТЕНЦИИ В РАМКАХ РАБОТЫ СНО «ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

**Е. В. Зайцева**

Санкт-Петербургский горный университет императрицы Екатерины II

*В данной работе рассмотрены особенности формирования научной компетенции в рамках работы студенческого научного общества «Цифровые технологии в профессиональной деятельности». Приведены особенности формирования перечня мероприятий, тематики лекций общества.*

***студенческое научное общество, цифровые технологии, горнотехническое направление, научные исследования, конференции***

В Санкт-Петербургском горном университете императрицы Екатерины II сейчас реализуется пилотный проект «Совершенствование системы высшего образования». В рамках проекта осуществляется подготовка специалистов по стандартам «Высшего инженерного образования». Реализация проекта невозможна без вовлечения в научную работу молодых исследователей (студентов, аспирантов). Одной из форм такого вовлечения являются студенческие научные общества (СНО).

Одной из составляющих цели СНО «Цифровые технологии в профессиональной деятельности», закрепленной в Положении, является формирование ценностного отношения к научным исследованиям в области применения цифровых технологий в профессиональной сфере и выявление одаренных студентов, развитие их интеллектуального потенциала. Достижение данной цели осуществляется через решение двух основных задач СНО:

– подготовка обучающихся к проведению участию в научных конференциях, симпозиумах, круглых столах;
– содействие реализации общественно значимых молодежных инициатив.

Ключевой особенностью реализации первой задачи в рамках СНО в Горном университете является формирования списка конференций, форумов и других научных мероприятий, касающихся как горнотехнического

направления, так и цифровых технологий. К таким мероприятиям, например, относятся:

1. Международная научно-техническая конференция «Актуальные проблемы транспорта и хранения углеводородных ресурсов при освоении Арктики и Мирового океана» (секции «Диагностика и мониторинг оборудования, объектов и сооружений нефтегазового комплекса» и «Цифровизация, математическое и гидродинамическое моделирование процессов при транспорте и хранении углеводородного сырья»), г. Тюмень.

2. Всероссийская научно-техническая конференция «Актуальные вопросы энергомашиностроения, нефтяной и газовой отрасли» (секция «Математическое моделирование физических процессов, процессов инженерной экономики и управления»), г. Ижевск.

Участие студентов в подобных мероприятиях позволяет понять возможную проблематику своих профессиональных отраслей и возможности решения тех или иных задач. Все это, конечно, не отменяет формирования навыков проведения научных исследований, подготовки докладов, презентаций, устного выступления, аргументирования своей позиции.

Также в этот список необходимо включить конференции, форумы и научные мероприятия, посвященные непосредственно цифровым и информационным технологиям, такие как:

1. Международная молодежная научно-техническая конференция «Молодежь. Техника. Космос», г. Санкт-Петербург.

2. Международный форум «Математические методы и модели в высокотехнологичном производстве», г. Санкт-Петербург.

3. Всероссийская научная конференция с международным участием «Невская фотоника», г. Санкт-Петербург.

Научные мероприятия подобного толка позволяет ознакомиться с развитием цифровых технологий, новыми инженерными решениями, применяемыми коллегами как из университетской среды, так и представителями промышленности.

Членами СНО уже сделаны доклады и опубликованы статьи по следующим темам:

1. Исследование методов цифровой обработки видеокадров, полученных в глубинных скважинах [1].

2. Исследование методов адаптивного выравнивания гистограммы к видеоинформации, полученной в глубинных скважинах [2].

3. Применение методов цифровой обработки изображений для повышения качества видеоисследований на примере нефтегазовых скважин [3].

4. Применение метода эквализации гистограммы для повышения качества видеоисследований в нефтегазовых скважинах.

5. Цифровая обработка видеокадров, полученных в нефтяных и газовых скважинах [4].

Рассмотренная проблематика исследований связана с научными интересами куратора СНО и касается в основном видеоаналитики в добывающей промышленности. Сейчас с участием студентов – членов СНО и привлеченных экспертов из промышленного сообщества, формируется перечень возможных тем исследований. Планируется расширить тематику докладов и статей за счет проведения исследований по следующим направлениям:

1. Использование дополненной реальности для визуализации геологических моделей и планирования горных работ.

2. Внедрение беспилотного управления карьерным автотранспортом.

3. Исследование применения подземных роботов-разведчиков для обследования обрушенных или загазованных участков шахты.

Для проведения качественных исследований для членов СНО и всех желающих проводятся лекции по следующим тематикам:

1. Цифровые решения в инженерии.

2. Математика: язык цифрового будущего.

3. Система компьютерной верстки LaTeX и ее применение при написании научных статей.

Важно также постоянно совершенствовать практические навыки владения цифровыми технологиями. Например, председатель СНО –Алексей Яковлев в сентябре 2025 года участвовал в треке «Цифровая трансформация в государственной молодежной политике» в рамках Федерального форума «Область будущего», проводимого в городе Липецке. Алексей поучаствовал в командной разработке IT-продукта – конструктора патриотичного дизайна с внедренным ИИ-помощником.

В рамках СНО студентам также рассказывается, что для участия в мероприятиях, написания статей, докладов, тезисов в Санкт-Петербургском горном университете существует ряд нормативных документов, которые стоит учитывать при подготовке. Например, таким документом является Приказ № 408 адм, регламентирующий порядок прохождения экспертизы, требуемые документы, особенности формирования комиссий, требования

к предоставляемым материалам. Следует учитывать требования по экспертизе и экспортному контролю научных материалов, рассчитывать время на подготовку Экспертного и Экспортного заключений при планировании своих научных исследований.

Ознакомление с «Регламентом направления обучающихся на внешние научные и образовательные мероприятия», утвержденным приказом ректора от 18.03.2025 № 325 адм, позволяет членам СНО понять тип мероприятий, возможных для участия и собрать необходимый пакет документов.

В рамках СНО, таким образом, формируется некая научная среда, включающая знание внутренних регламентов и правил Университета, корпоративных традиций, участия в мероприятиях, совершенствования знаний о цифровых технологиях, общение со специалистами – таким образом и происходит формирование закрепление научной компетенции. Включение студента в процесс научных исследований происходит быстрее, формируются традиции, команды, представляющие Университет. Свободное от занятий время участники СНО не тратят в пустую и реализуют таким образом свой исследовательский потенциал. Поскольку вступить в СНО можно сразу на 1 курсе, то к изучению специальных дисциплин уже приступит студент знакомый с понятием и требованиями, предъявляемыми к научным исследованиям и сформированными научными компетенциями.

**Список используемых источников**

1. Скворцов В. Ю., Скворцов И. В., Савенок О. В. 3D моделирование в интерпретации результатов телевидеоинспекций скважин // В книге: БайкалГео'24. Сборник тезисов докладов научно-практической конференции. Москва, 2024. С. 125-130.

2. Опыт применения скважинных систем видеонаблюдения при проведении капитального ремонта скважин / Н. А. Исмаилов, А. А. Воркожоков // Территория «Нефтегаз». 2010. № 12. С. 14-17.

3. Опыт применения аппаратуры скважинного акустического сканера высокого разрешения совместно с видеокаротажем для исследований открытого ствола / В. Е. Косарев, Ю. С. Масленникова, А. Д. Акчурин [и др.] // Нефтяное хозяйство. 2013. № 6. С. 53-55. EDN QCNAMB.

4. Зайцева Е. В., Кочнева А. А., Катунцов Е. В. Оптимизация технологического процесса повышения контрастности на изображениях, полученных в шахтах // Горный информационно-аналитический бюллетень. 2025. № 7. С. 115–130. DOI: 10.25018/0236_1493_2025_7_0_115.

# FEATURES OF THE FORMATION OF SCIENTIFIC COMPETENCE WITHIN THE FRAMEWORK OF THE SOCIAL SCIENCE "DIGITAL TECHNOLOGIES IN PROFESSIONAL ACTIVITIES"

**Zaytseva E.**
Empress Catherine II Saint Petersburg Mining University

*This article examines the features of developing scientific competence within the framework of the Student Scientific Society "Digital Technologies in Professional Activities." It outlines the specifics of organizing the society's event schedule and the topics of its lectures.*

***Key words:*** *professional competencies, digital technologies, mining engineering, digital processing, production tasks*

**УДК 004**
**ГРНТИ 06.54.51**

# ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

**М. Д. Ивакина, В. И. Шилков**

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина

*В статье обсуждаются вопросы применения информационно-коммуникационных технологий в энергетической отрасли. Названы основные проблемы информатизации энергетики и обозначены направления цифровой трансформации в сфере производства и потребления энергоресурсов, Перспективные направления информатизации энергетической отрасли предлагается связывать с применением гибридных решений, на основе инструментальных средств искусственного интеллекта, блокчейн-технологий, интернета вещей и интеллектуальных сетей, позволяющих гибко управлять процессами производства и распределения энергетических ресурсов.*

***энергетика, цифровая трансформация, инновационные технологии, блокчейн, интеллектуальные сети***

Энергетическая отрасль является важнейшим элементом, обеспечивающим функционирование и развитие всех социально-экономических систем. Цели и задачи энергетической отрасли экономики, в первую очередь, связывают с добычей, производством, переработкой, транспортировкой и распределением, как традиционных, так и возобновляемых энергоресурсов.

К актуальным и важнейшим задачам энергетической отрасли следует относить не только задачи повышения эффективности производства энергоресурсов, но и задачи их рационального использования, возникающие как по экономическим причинам, так и в связи с негативными последствиями использования энергоресурсов на состояние окружающей среды. Решение задач эффективного производства и использования энергетических ресурсов в современных условиях невозможно без применения современных информационно-коммуникационных технологий.

Разработка стратегических решений в сфере цифровой трансформации энергетической отрасли требует анализа, например: тенденций, прогнозов

развития сценариев мирового энергопотребления; опыта применения информационных технологий в сфере энергетики в России и за рубежом с учетом специфики технологических процессов; – проблем внедрения и эксплуатации информационных систем в сфере энергетики.

Согласно Navigant Research, объем рынка цифровых технологий в электроэнергетике превышает 60 млрд долларов США, из которых более 25 млрд долларов приходится на «умные» электросчетчики, а на автоматизацию распределительных сетей, цифровизацию процессов эксплуатации и технического обслуживания тепловых электростанций и на домашние системы управления энергопотреблением, приходится более 20 млрд долларов США [1]. В соответствии с [2] снижению эмиссии парниковых газов на 18 % в 2023 году в Европейском союзе в значительной мере способствовало внедрение современных технологий управления в энергетические сектора экономик.

В соответствии со сведениями, приведенными в [3], компания British Petroleum (BP) активно применяет технологии Интернета вещей для мониторинга состояния скважин. Уже в 2015 году было объединено 650 нефтедобывающих скважин в единую сеть, что позволило осуществлять опрос датчиков (сенсоров), установленных на каждой скважине и фиксирующих широкий спектр параметров. Для анализа получаемой информации BP использует облачный IoT-сервис Predix (разработка компании GE).

В Российской Федерации процесс цифровой трансформации электроэнергетики стартовал позднее по сравнению с зарубежными странами, однако в настоящее время он приобрел приоритетное значение. Так, например, ассоциацией «Цифровая энергетика» разработана стратегия цифровой трансформации электроэнергетики России, в соответствии с которой развитие отрасли будет определяться тремя ключевыми факторами: децентрализацией, цифровизацией, а также конвергенцией технологий и продуктов.

Цифровая стратегия «Газпромнефти» обеспечивает 40-процентную оптимизацию деятельности основных бизнес-направлений компании. Внедрение когнитивных технологий позволяет выявлять перспективные участки для бурения за 15 минут, сокращая трудозатраты геологов на 70–80 %. Среди активно применяемых решений – RFID-датчики, используемые, в частности, в логистике. Как описано в одном из исследований, на закупаемые комплектующие устанавливались радиочастотные метки и GPS-датчики, которые отслеживали перемещение грузов от момента отгрузки до прибытия на склад.

Операторы получали данные о скорости движения, количестве и длительности остановок. Собранная информация оформлялась в виде смарт-контрактов на базе блокчейн-платформы, что позволило объединить физические поставки с сопутствующим документооборотом. Дополнительно компания внедрила программный продукт «Когнитивный геолог», где за счет машинного обучения удалось значительно ускорить проведение геологоразведочных работ.

Компания «ЛУКОЙЛ» осуществляет управление промыслом на основе компьютерных систем и платформ сбора больших данных в соответствии со стратегией «ЛУКОЙЛ 4.0», реализованной в рамках концепции интеллектуального месторождения (Life-Field).

В то же время, как отмечают авторы работы [4], необходимость внедрения современных информационных систем в теплоэнергетике стала предметом обсуждения лишь в недавнее время. Указанное отставание обусловлено технологическими особенностями данной отрасли, которые обусловливают более высокую сложность и продолжительность перехода к цифровизации по сравнению с электротехническим сегментом.

Вместе с тем, цифровизация энергетических секторов экономики в Российской Федерации сталкивается с рядом проблем и препятствий, к которым, в соответствии с [5], например, следует отнести: дефицит высококвалифицированных ИТ-специалистов; недостаточная зрелость отечественных ИТ-решений, существенно уступающих зарубежным аналогам; низкий уровень защиты информации и сложность реализации принципов экономической и кибербезопасности; отсутствие унификации данных и единых подходов к цифровизации в энергетической отрасли.

Анализ примеров, достигнутых результатов и тенденций применения информационных технологий в различных задачах энергетики показывает, что к перспективным направлениям цифровой трансформации энергетики, инструментальным средствам и концепциям следует отнести, например: технологии интернета вещей, блокчейна, виртуальной реальности, цифровых двойников и искусственного интеллекта, с помощью которых, для повышения эффективности управления задачами энергетики, могут быть созданы интеллектуальные сети (Smart Grids).

На современном этапе развития российской энергетики технологии интернета вещей (Internet of Things, IoT) применяются в двух основных направлениях: снижение энергопотребления и контроль технической исправности оборудования с целью предотвращения аварийных ситуаций.

Технологии IoT базируются на принципах телеметрии и телеуправления, что обусловливает их использование в отрасли для создания интеллектуальных сетей и инфраструктуры Smart Grid посредством датчиков и сенсоров, интегрированных в единый облачный или онлайн-сервис.

Применение интернета вещей в умных городах (Smart City) позволяет организовать эффективный контроль энергопотребления. Осветительные системы транспортной инфраструктуры реализованы на базе гибридной модели, которая позволяет осуществлять мониторинг и управление через IoT-среду даже при отсутствии связи с основной сетью в реальном времени. Такая гибридная система обеспечивает взаимодействие IoT-экосистемы и централизованной энергосети для непрерывного контроля и управления [6].

В соответствии со сведениями, приведенными в [7], экономический эффект от внедрения IoT в электроэнергетике России по результатам 2025 году может составить порядка 532 млрд рублей. По мере осознания представителями сетевых компаний экономической выгоды от инвестиций в IoT-инфраструктуру прогнозируется увеличение количества таких устройств.

В соответствии со сведениями, приведенными в [8], к перспективным инструментальным средствам, которые найдут применение в энергетике следует отнести и технологию блокчейн, практическую значимость внедрения которой следует связывать, в первую очередь, с возможностью формирования таких моделей взаимодействия участников энергетического рынка, которые позволяют минимизировать участие посреднических структур в процессах купли-продажи энергоресурсов.

Вместе с тем, как отмечено в [9], следует принять во внимание, что энергетический сектор существенно отличается от финансового, в рамках которого, возникла и получила наибольшее развитие, концепция блокчейна, так как, наряду с денежными транзакциями, энергетический сектор, предполагает и физические поставки электрической энергии.

В соответствии с [10], в энергетике найдет широкое применение и технология виртуальной реальности, которая может быть использована как для обучения персонала, так и позволит моделировать работу реального оборудования в условиях чрезвычайных ситуаций. Так, например, VR-тренажеры, воспроизводящие функционирование реального оборудования, уже нашли применение на предприятиях концерна «Росэнергоатом».

К важнейшим перспективным направлениям информатизации энергетики следует отнести и внедрение инструментальных средств искусствен-

ного интеллекта. Так, например, в соответствии с [11] внедрение искусственного интеллекта в энергетическом секторе Румынии обеспечивает до 42,8 % оборота в сегменте пользователей, что в 2023 году составило 3,54 % национального ВВП и способствовало чистому приросту занятости более чем на 65 000 рабочих мест, несмотря на прямое перемещение рабочей силы.

Применение текстовой аналитики на основе машинного обучения, методов статистического причинно-следственного вывода и макроэкономического моделирования на больших данных позволяет создать воспроизводимую методологическую основу для достоверной оценки внедрения ИИ и его макроэкономических эффектов. Полученные результаты представляют ценность для разработчиков политики и исследователей в области цифровой трансформации, экономики энергетики и устойчивого развития.

Как отмечено в [12], компания Pacific Gas and Electric в США применяет методы машинного обучения для прогнозирования пиковых нагрузок и автоматического управления режимами потребления, что позволяет существенно сократить потери электроэнергии и повысить эффективность балансировки энергосистемы. Гибридные подходы и алгоритмы машинного обучения позволяют создавать прогнозные модели, учитывающие неопределенности, обусловленные прерывистостью выработки энергии и оптимизировать процессы планирования и управления сетью.

Применение инструментальных средств искусственного интеллекта сделало возможным создание, так называемых, интеллектуальных сетей (Smart Grid). Так, например, в Нидерландах, компанией TenneT разработана модель «умной сети», обеспечивающая возможность одновременного управления как традиционными, так и возобновляемыми источниками энергии. При возникновении дефицита энергии система в автоматическом режиме осуществляет балансировку спроса и предложения путем перераспределения энергетических потоков из регионов с избыточной генерацией в зоны с ее недостатком.

Министерство энергетики США определяет интеллектуальную сеть (Smart Grid) как автоматизированную, интегрированную энергетическую систему, функционирующую на принципах двунаправленной доставки электроэнергии и, обеспечивающую сбор важной информации о предпочтениях потребителей и режимах функционирования технологического оборудования. Можно сказать, что интеллектуальная сеть – это энергосистема, которая оснащена системами контроля: датчиками, вычислительными сред-

ствами и автоматизированными средствами управления. Совокупность программно-аппаратных компонентов «умной сети» обеспечивает надежность, повышает безопасность и эффективность работы энергетической инфраструктуры [13].

Таким образом, можно сделать вывод, что применение и развитие информационных технологий в сфере энергопроизводства и энергопотребления в Российской Федерации осуществляется по нескольким направлениям единого стратегического комплекса, предполагающего создание гибридных сетевых решений на основе технологий IoT, блокчейна и искусственного интеллекта.

**Список используемых источников**

1. Иваненко О. Б., Головкина Е. В. Цифровая трансформация российской электроэнергетики: перспективы и ограничения // Экономика, предпринимательство и право. 2023. Т. 13, № 11. С. 5063-5076.

2. Campana P. et al. Smart grids and sustainability: The impact of digital technologies on the energy transition // Energies. 2025. Т. 18. № 9. С. 2149.

3. Черняев Д. С., Намиот Д. Е. Роль цифровых технологий в разведке, добыче и транспортировке нефтегазовых продуктов //International Journal of Open Information Technologies. 2019. Т. 7. № . 11. С. 79-85.

4. Ермоленко Д. В., Азаров П. С. Применение современных информационных технологий в энергетике // Инновации. Наука. Образование. 2022. № 71. С. 12-16.

5. Коледа А. С., Райко Д. М. Информационные технологии в управлении объектами и процессами в энергетике // Молодежь и научно-технический прогресс: Сборник докладов XVI международной научно-практической конференции студентов, аспирантов и молодых ученых. Губкин-Старый Оскол: ООО «Ассистент плюс», 2023. С. 284-286.

6. Singh R. et al. Energy system 4.0: Digitalization of the energy sector with inclination towards sustainability //Sensors. 2022. Т. 22. № 17. С. 6619.

7. Засухина О. А., Малинин Н. К., Кузнецов М. Е., Гусев И. Г. Применение технологий интернет вещей в энергосистемах // Сборник научных трудов Ангарского государственного технического университета. 2023. № 1. С. 187-191.

8. Ермолаев К. А., Кузьмин М. С., Дырдонова А. Н. Использование цифровых технологий при сопровождении процессов энергосбережения и повышения энергоэффективности в российской экономике // Инновационные кластеры цифровой экономики: драйверы развития: Труды научно-практической конференции с международным участием. Санкт-Петербург: СПбПУ Петра Великого, 2018. С. 39-44.

9. Засухина О. А., Слинько А. Н., Нефедов С. Л., Нефедова Р. А. Блокчейн в энергетике // Сборник научных трудов Ангарского государственного технического университета. 2024. № 1. С. 293-297.

10. Барабан А. Д., Коваленко А. Н. Использование информационных технологий в процессе подготовки специалистов атомной энергетики // Современные средства связи. 2021. Т. 1. № 1. С. 384-385.

11. Davidescu A. A. M. et al. A Machine Learning and Econometric Framework for Credibility-Aware AI Adoption Measurement and Macroeconomic Impact Assessment in the Energy Sector //Mathematics. 2025. Т. 13. № 19. С. 3075.

12. Кузнецова Э. М. Роль IT-технологий в устойчивом будущем энергетики: от предсказаний до автоматизации // Наука молодых – будущее России: сборник научных статей 9-й Международной научной конференции перспективных разработок молодых ученых. Курск: ЗАО «Университетская книга», 2024. С. 95-98.

13. Mahmood M. et al. Impacts of digitalization on smart grids, renewable energy, and demand response: An updated review of current applications //Energy Conversion and Management: X. 2024. Т. 24. С. 100790.

## INFORMATION AND COMMUNICATION TECHNOLOGIES AND PROMISING AREAS OF DIGITAL TRANSFORMATION OF THE ENERGY INDUSTRY

**Ivakina M., Shilkov V.**
Ural Federal University named after the first President of Russia B. N. Yeltsin

*The article discusses the application of information and communication technologies in the energy industry. The main problems of informatization of energy are named and the directions of digital transformation in the field of production and consumption of energy resources are outlined. Promising directions of informatization of the energy industry are proposed to be associated with the use of hybrid solutions based on artificial intelligence tools, blockchain technologies, the Internet of Things and intelligent networks that flexibly manage the processes of production and distribution of energy resources.*

***Key words:*** *energy, digital transformation, innovative technologies, blockchain, intelligent networks*

**УДК 353.9**
**ГРНТИ 06.61.53**

# ПРИВЛЕЧЕНИЕ ОБЩЕСТВЕННОСТИ К УПРАВЛЕНИЮ МУНИЦИПАЛЬНЫМ ОБРАЗОВАНИЕМ КАК ФАКТОР ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ МЕСТНОГО САМОУПРАВЛЕНИЯ

**Т. А. Иклюшина[1], В. В. Макаров[2]**

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

*В условиях продолжающейся реформы системы организации местного самоуправления в РФ в соответствии с новым законом «Об общих принципах организации местного самоуправления в единой системе публичной власти» (№ 33-ФЗ), в ходе которой стремительно сокращается количество муниципальных образований, система территориальной организации муниципалитетов стремится к одноуровневой, сокращая при этом уровень городских и сельских поселений, возрастает необходимость не только обеспечения эффективного взаимодействия органов местного самоуправления и жителей муниципальных образований, но и привлечения общественности к участию в управлении муниципальным образованием, в целях развития путей взаимодействия и повышения доверия населения к органам публичной власти.*

***местное самоуправление, МСУ, муниципальное образование, территориальная организация МСУ, эффективность местного самоуправления, взаимодействие органов МСУ с жителями, участие граждан в осуществлении местного самоуправления, качество жизни граждан***

Одной из важнейших задач государственного управления сегодня становится обеспечение мер для устойчивого развития регионов, и в страны в целом. Устойчивое развитие складывается из множества компонентов, в том числе оно формируется в значительной степени в месте жительства человека – на уровне муниципального образования как единицы системы местного самоуправления, гарантированного Конституцией РФ. Природно-климатические условия, экология, промышленно-производственные и финансово-экономические факторы, инфраструктура, демографическая ситуация, социальная сфера, культура, образование, спорт, общественные инициативы граждан и их объединений – все имеет важнейшее значение в вопросе обеспечения устойчивого развития региона в целом, а развитие или ограни-

чения эти сферы фактически получают в сфере муниципального управления [1].

В формуле эффективного местного самоуправления – активная гражданская позиция жителей территории по решению вопросов местного значения во взаимодействии с органами местного самоуправления. Органы МСУ являются ближайшей к жителям публично-властной структурой, что возлагает на них существенную ответственность в вопросе повышения доверия населения к власти. Для достижения этой цели органам местного самоуправления необходимо быть открытым к жителям, знать проблемы и принимать самые энергичные усилия по решению вопросов местного значения в интересах жителей данной местности.

Изучая исторические тенденции развития российской государственности, важно отметить доминирующую роль государства в жизни российского общества на протяжении всей истории, что не могло не оказать влияния на современную культуру и внутреннее состояние как отдельного гражданина, так и страны в целом. Это пассивное состояние складывалось в веках, его можно определить, как потребность быть ведомым, зависимым от лидера – от царя или отца народов, получать готовое решение, а не быть инициатором решения, что сегодня выражается в пассивности граждан и непонимании ценности гарантированного Конституцией РФ права на осуществление местного самоуправления, права на участие в заведывании и решении вопросов местного значения [2].

Также и со стороны государственной политики в отношении института местного самоуправления мы можем наблюдать недостаточность мер для обеспечения финансовой самостоятельности муниципальных образований: с одной стороны, огромный спектр полномочий муниципалитетов, с другой стороны, высокая дотационность муниципалитетов, недостаточность выделенных местных налогов для исполнения данных полномочий. Такая ситуация в целом подчеркивает ориентацию государства на развитие не местного самоуправления, а местного управления, как уровня публичной власти. Впрочем, «провести четкую границу между самоуправлением и местным государственным управлением в принципе сложно, а в истории России иногда почти невозможно» [3].

Между тем, в определении местного самоуправления в Конституции РФ и в сегодняшнем профильном законе № 33-ФЗ от 05.03.2025 «Об общих принципах организации местного самоуправления в единой системе публичной власти» (далее – № 33-ФЗ), можно увидеть много слов, определяю-

щих местное самоуправление как деятельность граждан: самостоятельно, под свою ответственность, в интересах населения, самоорганизация, самоуправление. Поэтому, ориентируясь на наш исторический контекст, на современные реалии продолжающейся реформы местного самоуправления, исходя из задач устойчивого развития региона, надлежит продолжать изучение, поиск и применение подходов, которые могли бы содействовать развитию эффективного местного самоуправления в России, как залога того, чтобы местные вопросы и внутреннее развитие каждого небольшого населенного пункта оставалось приоритетным, а не терялось из виду в угоду общегосударственным задачам.

Целью данной работы является осуществление мониторинга применения в муниципальных образованиях инструментов для развития более широкого общественного участия в решении вопросов местного значения, каким образом это участие способствует росту территориальной общности, локального партнерства, взаимодействия, а значит более эффективному управлению муниципальным образованием.

В 2025 году Комитетом общественных коммуникаций Ленинградской области было проведено личное полуформализованное интервью более чем 7213 человек по месту их жительства, о чем был подготовлен документ «Оценка эффективности деятельности органов исполнительной власти Ленинградской области, органов местного самоуправления Ленинградской области» [4].

По данным этого исследования, на вопрос «Был ли у Вас и/или ваших знакомых реальный опыт влияния на принятие решений по развитию района/населенного пункта (например, по Вашему обращению провели ремонт или установили новую детскую площадку)?», %, 2025» нет ответили 2/3 респондентов.

На вопрос «В какой степени Вы согласны/не согласны с утверждением: Я могу повлиять на принятие решений по развитию моего района/населенного пункта?» – треть респондентов согласны, что могут повлиять.

Треть респондентов данной выборки говорят о наличии опыта влияния на принятие решений по развитию района (населенного пункта), что довольно существенно, но еще требуются механизмы более широкого информирования граждан о способах влияния на развитие своего населенного пункта (муниципального образования).

Взаимодействие необходимо как органам МСУ, так и жителям конкретных населенных пунктов. С одной стороны, органам местного само-

управления необходимо знать мнение жителей и защищать их интересы при принятии решений, с другой стороны – гражданам важно информировать ОМСУ о существующих вопросах по месту проживания для скорейшего решения этих вопросов. Как мы можем видеть в нижеприведенной таблице 1, это взаимный интерес, польза, потенциал развития:

ТАБЛИЦА 1. Цели взаимодействия ОМСУ и жителей города

| Цели взаимодействия ОМСУ с жителями | Цели взаимодействия жителей с ОМСУ |
|---|---|
| – знать мнение жителей и защищать их интересы при принятии решений;<br>– формировать устойчивые формы взаимодействия граждан и их объединений с органами МСУ;<br>– формировать здоровые традиции управления на местах;<br>– поддерживать местных лидеров мнений; | – для информирования ОМСУ о существующих вопросах и скорейшего их решения по месту проживания;<br>– для учета мнения и защиты интересов при принятии решений ОМСУ;<br>– для создания устойчивых форм взаимодействия граждан и ОМСУ;<br>– для формирования общественного участия. |

В соответствии с федеральным законом № 33-ФЗ мы видим возможными следующие формы непосредственного осуществления населением МСУ и формы участия населения в осуществлении МСУ:

– формы непосредственного осуществления населением местного самоуправления – референдум, муниципальные выборы, сход. Принятые таким способом решения подлежат обязательному исполнению на территории муниципального образования без дополнительных согласований и утверждений;
– формы участия населения в осуществлении местного самоуправления (порядок реализации каждой из форм уточняется в муниципальном НПА): опрос, публичные слушания, собрание граждан, инициативные проекты, территориальное общественное самоуправление, староста сельского населенного пункта.

В Ленинградской области сегодня существует Стратегия развития территориального общественного самоуправления (ТОС) до 2030 года, которая была принята в 2023 году на совместном заседании президиума совета муниципальных образований и Общественной палаты Ленинградской области, и направлена на вовлечение граждан в местное самоуправление и реализацию гражданских инициатив. Соответственно, в муниципальных обра-

зованиях региона разработаны планы по ее реализации. Если ранее, например, в Гатчинском районе работали инициативные комиссии и реализовывались инициативные проекты, то с 2025 года уже в округе действует ориентир на образование ТОСов, в соответствии с которым предлагается активным жителям населенных пунктов организовывать ТОСы и на их базе содействовать решению вопросов местного значения. На конец 2024 года во вновь образованном Гатчинском округе работало 27 инициативных комиссий, 103 старосты сельских населенных пунктов, 62 общественных совета и 20 территориальных общественных самоуправлений [5].

ТОС может организовать любой инициативный человек, достигший 18-летнего возраста. Для этого ему потребуется организовать инициативную группу, определить границы действия данного самоуправления в населенном пункте, провести учредительное собрание и зарегистрировать устав ТОС в администрации муниципального образования (если ТОС без образования юридического лица).

Кроме того, должно отметить, что в последние 10 лет в России цифровые технологии значительно внедрены в экономике и социальной сфере, а также и в государственном и муниципальном управлении, что значительно повышает эффективность управления, оказания услуг и скорость обратной связи, что очень важно при принятии решений. Все больше услуг становится доступно через справочно-информационный портал «Госуслуги»; сеть МФЦ покрывает сегодня всю страну, достигая даже небольшие населенные пункты; все большую известность приобретает Платформа обратной связи «Решаем вместе», которая позволяет гражданам отправлять не только вопросы, но и предложения; работа официальных пабликов государственных и муниципальных органов власти в социальных сетях – для оперативного информирования граждан о полезных или экстренных вопросах [6].

В современных условиях развития и применения информационных технологий для взаимодействия с гражданами, требуется сохранять гибридную форму общения с жителями, поскольку есть еще существенные ограничения в техническом оснащении покрытия высокоскоростным интернетом населенных пунктов, а также в предпочтениях граждан, какие способы подачи обращений для них приемлемы.

В настоящее время существует необходимость просветительской деятельности для формирования и развития культуры местного самоуправления. Для этого могут применяться различные инструменты, как например, деловые игры для старшеклассников, дискуссионные площадки и форумы

на различные злободневные темы для горожан разных возрастов и форматов, а также проектные сессии с привлечением горожан всех возрастов для проектирования парков, общественных пространств и дворов.

Например, в городе Коммунар (до 01.01.2025 – муниципальном образовании «Город Коммунар», а сейчас территориальном управлении город Коммунар администрации муниципального образования Гатчинский муниципальный округ Ленинградской области) широко применяются современные инструменты для привлечения общественности города для участия в решении вопросов местного значения. Ежегодно глава администрации, а в настоящее время, территориального управления, участвует в проведении деловых игр для старшеклассников «Хочу решить», в результате чего ребята учатся на практике понимать вопросы местного значения, создавать обращения, а также видеть пути решения этих вопросов. Также Коммунар с 2018 года участвует в реализации федерального проекта «Комфортная городская среда», благодаря которому ежегодно город все больше преображается: строятся общественные пространства, набережные, детские площадки, пешеходные дорожки. Жители города уже хорошо знают, что они могут предложить то или иное место для обустройства, участвуя в голосовании, а также поучаствовать в проектной сессии и предметно обсудить с архитектором пространства, что именно хотелось бы там построить. В 2024 году Коммунар при организации местной администрации, молодежного волонтерского сообщества и жителей города собрал необходимое количество голосов для участия в отборе на строительство парка в рекордно короткие сроки – 3 дня, а как правило, отборочный KPI составляет 10 % от количества жителей поселения – для Коммунара это порядка 2600 человек. Благодаря такому развитому взаимодействию органов МСУ и общественности города можно решить много насущных вопросов в интересах жителей города.

Таким образом, для развития взаимодействия власти и общества, и особенно это важно на уровне места жительства, в муниципальном образовании, необходимо движение навстречу друг другу, органам МСУ важно инициировать формы вовлечения граждан для решения вопросов местного значения, сохранять открытость, чтобы услышать идеи и предложения граждан по решению различных местных вопросов. Для этого могут быть использованы и цифровые форматы, и информационные сообщения, и очные мероприятия – встречи с жителями и прямые эфиры, чаты и комментарии в социальных сетях, все, что будет способствовать развитию конструктивного общения и взаимодействия.

В каждом муниципальном образовании (населенном пункте) есть активные неравнодушные жители и их объединения, лидеры мнений, есть предприятия, в последнее время активно развиваются некоммерческие организации по решению самых актуальных вопросов на местах. Благодаря поиску и применению инструментов для взаимодействия органов МСУ и всех ресурсных единиц муниципального образования (населенного пункта) будет формироваться общение, взаимная договоренность, общность, ответственное партнерство, обмен ресурсами, взаимная поддержка на территории. В процессе взаимодействия этих инициативных ресурсных единиц, взаимного доверия и участия и формируется культура местного самоуправления, что чрезвычайно важно для устойчивого развития как отдельного муниципального образования, так и региона, и страны в целом.

**Список используемых источников**

1. Кузнецова М. Н. Государственная политика в области местного самоуправления: доступность власти или экономический эффект? / М. Н. Кузнецова, Н. Н. Якимчук // Современные парадигмы устойчивого развития региональных социально-экономических систем в условиях роста неопределенности внешней среды: Материалы Международной научно-практической конференции, Гатчина, 21 апреля 2023 года. Гатчина: Государственный институт экономики, финансов, права и технологий, 2023. С. 129-133. EDN ZBCEWV.

2. Иклюшина Т. А. Влияние исторически сложившихся тенденций на современное развитие местного самоуправления в России в контексте задач устойчивого развития региона. Журнал правовых и экономических исследований. 2026, № 2.

3. Петухов Р. В. Местное самоуправление: опыт теоретического осмысления А.И. Васильчиковым и современные реалии / Р. В. Петухов // Труды Института государства и права Российской академии наук. 2011. № 3. С. 89-106. EDN QNRNOC.

4. Оценка эффективности деятельности органов исполнительной власти Ленинградской области, органов местного самоуправления Ленинградской области, 2025 год. URL:https://kpb.lenobl.ru/media/uploads/userfiles/2025/10/23/Оценка_эффективности_деятельности_2025.pdf (дата обращения: 22.05.2026).

5. Официальный сайт газеты «Гатчинская правда» URL: https://gtn-pravda.ru/2024/11/29/5-shagov-k-sozdaniju-tos.html (дата обращения: 22.05.2026).

6. Иклюшина Т. А. Применение инфокоммуникационных технологий для повышения эффективности взаимодействия с жителями муниципального образования / Т. А. Иклюшина, В. В. Макаров // Актуальные проблемы инфотелекоммуникаций в науке и образовании" (АПИНО 2025). XIV Международная научно-техническая и научно-методическая конференция. Сб. науч. ст. в 2-х т. СПб.: СПбГУТ, 2025. С. 128-134. EDN IRUUDT.

# ENGAGING THE PUBLIC IN MUNICIPAL GOVERNANCE AS A FACTOR IN ENHANCING THE EFFECTIVENESS OF LOCAL SELF-GOVERNMENT

**Iklyushina T.[1], Makarov V.[2]**
**[1]Gatchina State University**
**[2]The Bonch-Bruevich Saint Petersburg State University of Telecommunications**

*The article examines the role of public involvement in the management of a municipal formation as a key factor in improving the efficiency of local self-government especially in the context of ongoing reform of the local self-government system in the Russian Federation, while the number of municipal formations is decreasing, reducing the level of urban and rural settlements. There is a growing need not only for effective interaction between citizens and local self-government bodies, but also for engaging the public in decision-making processes.*

***Key words:*** *local self-government, municipal formations, territorial organization of the local self-government, effectiveness of the local self-government, effective interaction of local government and residents, citizen participation in the local self-government, quality of life of citizens*

**УДК 338.47**
**ГРНТИ 06.81.45**

# ДАННЫЕ КАК ФАКТОР ПРОИЗВОДСТВА: ИНСТИТУЦИОНАЛЬНЫЙ АНАЛИЗ СТАНОВЛЕНИЯ ЭКОНОМИКИ ДАННЫХ В РОССИЙСКОМ ИКТ-СЕКТОРЕ

**А. В. Исаков, Е. В. Павлова**

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

*В статье осуществляется методологический анализ измерения вклада ИКТ-сектора в российскую экономику данных. На основе теоретического осмысления категории «данные» как фактора производства в цифровой экономике рассматриваются тенденции, происходящие в отечественном ИКТ-секторе в период 2025–2026 гг. Эмпирическую базу исследования составляют актуальные статистические данные Росстата. Выявляются ключевые институциональные противоречия между различными методологиями оценки вклада ИКТ-сектора в ВВП. Особое внимание уделяется анализу методического перехода от оценки ИКТ-сектора по видам экономической деятельности к оценке на основе реестра аккредитованных ИТ-компаний.*

***экономика данных, ИКТ-сектор, данные как фактор производства, цифровая экономика, большие данные***

Становление данных в контексте информационного ресурса как одного из ключевых факторов производства оказывает трансформационное влияние на все отрасли и российскую экономику в целом. Цифровизация экономики породила значительные противоречия в методологическом определении и понимании данного термина, а трансформация ее в «экономику данных» усугубило противоречия в научной среде и теоретических дискурсах и научных работах на данную тему [1-3]. Приоритетную сложность вызывает количественное оцифровывание и представление в виде статистических данных степени цифровизации отдельных отраслей экономики и непосредственно ИКТ-сектора [4].

В этой связи возникает ряд методологических трудностей при измерении вклада данных как четвертого фактора производства наряду с капиталом, рентой и трудом: в каких единицах измерять новый фактор? Если информация измеряется в битах, то каким образом перевести их в реальный вклад в ВВП экономики, измеряемый в стоимостных единицах [5, 6].

Дополнительную трудность создает определение границ ИКТ-сектора. Если опираться только на общероссийский классификатор экономических видов деятельности (далее – ОКВЭД), то под определение предприятий данного сектора попадут только занимающиеся разработкой программного обеспечения (код ОКВЭД – 62.0) и обработкой данных (код ОКВЭД – 63.1).

Тем не менее перечень предприятий ИКТ-сектора значительно шире и не попадает только под указанные коды ОКВЭД. Он включает организации, которые не являются разработчиками программного обеспечения, но вносят значимый вклад в цифровизацию экономики, например, такие как издатели игр, образовательные онлайн-платформы, платформы электронной коммерции и рекламы, производители средств защиты информации, интеграторы [7-9].

Федеральная служба государственной статистики (далее – Росстат) ежегодно дополняет и совершенствует базу для сбора статистической информации, характеризующей степень цифровизации экономики РФ. Ее основой является форма статистической отчетности 3-информ об использовании информационных технологий и производстве связанной с ними продукции, работ, услуг [10]. Впервые введена была данная форма отчетности в 2004 году постановлением Росстата и носила название «Сведения об использовании информационных и коммуникационных технологий и производстве вычислительной техники, программного обеспечения и оказания услуг в этих сферах». Основные сведения, которые аккумулировались с помощью данной формы – это объем информационных технологий, используемых предприятиями всех форм собственности, кроме субъектов малого предпринимательства, и производстве связанной продукции [11].

Вторая редакция данной формы сбора данных произошла в 2011 году, когда к разработке присоединилось Министерство экономического развития РФ. Форма была значительно расширена и детализирована. Более тщательная проработка коснулась перечня видов используемого оборудования, программного обеспечения, направления использования интернета, расхода, понесенных на информационные технологии, потребности в IT-кадрах [12].

В связи с утверждением программы «Цифровая экономика Российской Федерации» в 2017 году отчетность 3-информ также была обновлена и дополнена следующими данными:

– объем электронных продаж и закупок продукции, работ, услуг;

– объем продаж продукции и услуг сектора информационно-коммуникационных технологий, в том числе и по видам продукции в соответствии с кодом по общероссийскому классификатору продукции по видам экономической деятельности;
– направления использования «облачных» сервисов.

В последующих редакциях, начиная с 2020 года, произошло смещение акцента с информационных и коммуникационных технологий в сторону цифровых [13-14]. Изменения отражены в обновленной форме 3-информ «Сведения об использовании цифровых технологий и производстве связанных с ними товаров и услуг». В форму добавлены новые строки и разделы, связанные с новыми цифровыми технологиями:
– источники и направления применения технологий сбора, обработки и анализа больших данных;
– наличие возможности оказания услуг по хранению и обработке данных;
– цели применения технологий искусственного интеллекта;
– использование услуг центров обработки данных (ЦОД);
– применение технологии «интернета вещей» в бизнес-процессах;
– применение аддитивных технологий;
– использование «цифровых двойников» на различных этапах производства продукции;
– цели использования технологий радиочастотной идентификации;
– размер расходов на внедрение и использование цифровых технологий.

Так, по данным Росстата, на предприятиях ИКТ-сектора в первом полугодии 2025 года было занято 1,5 млн человек, показатель среднемесячной заработной платы составлял 190 тыс. руб. и более чем в два раза превышал средний показатель по стране.

Данные Росстата аккумулируют информацию различных составляющих отрасли ИКТ по объемам и в динамике:
– сегмента разработки программного обеспечения;
– производства компьютерной техники и телекоммуникационного оборудования;
– сектора связи и передачи данных.

По оперативным данным Росстата объем услуг в разработке ПО в феврале 2026 года составил 459,7 млрд рублей. Этот показатель вырос по сравнению с февралем 2025 года на 42,5 %, а по сравнению с предыдущим месяцем – на 9,2 %. За два месяца 2026 года объем услуг в разработке ПО со-

ставил 880,9 млрд рублей, что на 40,3 % выше итога аналогичного периода 2025 года.

Объем прочих IT-услуг в феврале 2026 года составил 149,8 млрд рублей, что выше показателя февраля 2025 года на 19,1 %. Объем платных IT-услуг населению за февраль составил 43,3 млрд рублей, увеличившись на 15,5 % по сравнению с февралем 2025 года.

За январь–апрель 2025 года производство компьютеров выросло на 48 % год к году. Производство радиолокационной, радионавигационной и радиоаппаратуры дистанционного управления увеличилось на 55 %. Производство навигационных приборов выросло на 26 %.

Объем услуг связи, оказываемых предприятиям, в феврале 2026 года вырос на 11,3 % относительно февраля 2025 года, составив 243,6 млрд рублей. За январь–февраль 2026 года объем услуг связи для предприятий составил 534,1 млрд рублей, что на 11,5 % выше аналогичного периода 2025 года.

Объем платных услуг связи населению за февраль 2026 года составил 166,6 млрд рублей, увеличившись на 8,5 % относительно февраля 2025 года.

На основании статистических данных, аккумулируемых Федеральная служба государственной статистики посредством отчетности 3информ, можно сделать выводы, что все сегменты ИКТ-отрасли демонстрируют устойчивые темпы роста, что характеризует ИКТ-сектор экономики как быстрорастущий.

**Список используемых источников**

1. Макаров В. В., Павлова Е. В. Инновационные подходы к приобретению и замещению продукции ИКТ в условиях санкций // Экономика и качество систем связи. 2025. № 3 (37). С. 4-15.

2. Лобанов М. А., Куганов В. Г., Павлова Е. В. Цифровизация российской экономики: положительные и отрицательные тенденции развития // Российская экономика 2024: новые технологии, старые проблемы, прорывные решения: материалы науч.-практ. конф. МАЭФ-2024, Санкт-Петербург, 2024. СПб.: СПбГЭУ, 2024. С. 76-82.

3. Макаров В. В., Павлова Е. В. Влияние экосистем на цифровую трансформацию экономики // Журнал правовых и экономических исследований. 2024. № 2. С. 209-214.

4. Макаров В. В., Павлова Е. В. Развитие цифровых экосистем и их влияние на участников рынка ИКТ // Журнал правовых и экономических исследований. 2024. № 4. С. 289-294.

5. Кулакова Ю. В., Павлова Е. В. Перспективы развития нейросетевых технологий в условиях цифровизации экономики // Экономика и качество систем связи. 2024. N 1 (31). С. 10–17.

6. Павлова Е. В. Факторные ограничения развития бизнес-среды экосистемной направленности в отрасли ИКТ // Экономика и качество систем связи. 2024. № 3 (33). С. 19-27.

7. Павлова Е. В., Свистунов Л. О. Цифровизация экономики как часть процесса индустрии 4.0. // Современный менеджмент: проблемы и перспективы: материалы XVIII нац. науч.-практ. конф., Санкт-Петербург, 2023. СПб.: СПбГЭУ, 2023. С. 22–25.

8. Куганов В. Г., Павлова Е. В. Экономические проблемы цифровизации отдельных отраслей и сфер деятельности // Национальные концепции качества: роль качества в научно-технологическом развитии страны: материалы нац. науч.-практ. конф., Санкт-Петербург, 2023. СПб.: СПбГЭУ, 2023. С. 263–266.

9. Исаков А. В., Павлова Е. В. Этапы интеграции элементов цифровой экономики в сферу здравоохранения // 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. 72–75.

10. Павлова Е. В. Интеграция цифровой экономики в социальные сферы деятельности // Социогуманитарные коммуникации. 2023. № 2 (4). С. 19-23.

11. Лобанов М. А., Куганов В. Г., Павлова Е. В. Повышение качества жизни посредством внедрения цифровых технологий // Качество жизни населения промышленных территорий в стратегии «Общество 5.0»: материалы конф., Казань, 2022. Казань: НИ КФУ, 2022. С. 51–53.

12. Кушнир Л. Д. Особенности и проблемы использования искусственного интеллекта // Студенческая весна – 2022: материалы 76-й Регион. науч.-тех. конф., Санкт-Петербург, 2022. СПб: СПбГУТ, 2022. С. 112–117.

13. Жолобова А. И., Макаров В. В., Павлова Е. В. Информационные технологии в цифровой экономике // Экономика и бизнес: теория и практика. 2021. № 7 (77). С. 59-62.

14. Жолобова А. И., Макаров В. В., Павлова Е. В. Проблемы развития рынка информационных технологий в условиях пандемии // Евразийское Научное Объединение. 2021. № 10-3 (80). С. 181-184.

## DATA AS A FACTOR OF PRODUCTION: AN INSTITUTIONAL ANALYSIS OF THE FORMATION OF THE DATA ECONOMY IN THE RUSSIAN ICT SECTOR

**Isakov A., Pavlova E.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article provides a methodological analysis of measuring the contribution of the ICT sector to the Russian data economy. Based on the theoretical understanding of the category "data" as a factor of production in the digital economy, the trends occurring in the domestic ICT sector in the period 2025-2026 are considered. The empirical basis of the study consists of up-to-date statistical data from Rosstat. The key institutional contradictions between different methodologies for assessing the contribution of the ICT sector to GDP are identified. Special attention is paid to the analysis of the methodological transition from the assessment of the ICT sector by type of economic activity to an assessment based on the register of accredited IT companies.*

***Key words**: data economics, ICT sector, data as a factor of production, digital economy, big data*

**УДК: 330.47**
**ГРНТИ 06.56.21**

# ЭФФЕКТЫ ШИРОКОГО ПРОНИКНОВЕНИЯ АЛГОРИТМИЧЕСКИХ МОДЕЛЕЙ В УСЛОВИЯХ РАЗВИТИЯ ЭКОНОМИКИ ДАННЫХ

**А. В. Исаков, Е. В. Павлова**

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

*В статье приводится понятие алгоритмического подхода, описание применения алгоритмического подхода в современных условиях. Его влияние на производство контента, формирование систем рекомендаций, ценообразования, развития потребительских предпочтений. Роль разного рода данных в современной экономике. Особое внимание уделяется побочным, часто нежелательным эффектам и последствиям широкого распространения алгоритмов в экономических платформенных моделях. И, соответственно, необходимости более глубокого анализа и изучения формирующихся тенденций. А также возможных путей минимизации негативных последствий.*

***экономика данных, алгоритмические модели, цифровая экономика, предиктивная аналитика, эффекты масштаба данных***

Переход к экономике данных (data economy) означает, что ключевым производственным фактором становятся не просто информация, а алгоритмические способности ее обработки в реальном времени. Алгоритмические модели – от регрессионных до генеративных нейросетей – все активнее проникают во все контуры принятия решений: кредитные скоринги, управление цепочками поставок, динамическое ценообразование, подбор персонала, медицинскую диагностику и даже государственное регулирование.

Однако широкое проникновение алгоритмов, помимо множества преимуществ (например, снижение неопределенности, кастомизация), создает и качественно новые негативные явления, которые недооцениваются стандартной экономической теорией. Цель данной работы – систематизировать эффекты масштабирования алгоритмических моделей в условиях экономики данных и выделить вызовы для цифровой экономической политики.

## 1. Специфика алгоритмических моделей как блага и инструмента

В отличие от обычных цифровых сервисов, алгоритмическая модель обладает следующими особенностями с точки зрения экономики данных:

– кумулятивная прогнозная сила: ценность модели растет не линейно, а экспоненциально с объемом разнородных данных (эффект масштаба данных);
– сетевое преимущества владельца: модель улучшается, когда ее используют больше агентов, но при этом каждый новый агент передает свои данные, усиливая асимметрию между владельцем модели и остальными. Хотя агенты «кормят» модель данными, они не получают равного доступа к накопленной информации. Причем асимметрия усиливается с каждым новым агентом;
– ангажированность алгоритмов: объективность моделей является иллюзией. Так или иначе, в нее закладываются цели разработчика, хотя те и маскируют их под видом объективности.

Таким образом, внедрение алгоритмов является не просто автоматизацией, а перекладыванием дискреционных полномочий от человека на математическую модель. Но которая, при этом, оптимизирована под заложенные в нее частные критерии.

## 2. Эффекты на микроуровне: новые издержки и влияние на формирование рынков

На уровне фирмы внедрение алгоритмических моделей приводит к следующим эффектам:

– снижаются издержки для поиска и систематизации контрагентов (благодаря предиктивному скорингу);
– рост издержек на обоснование**.** В регулируемых отраслях требуются дорогостоящие методы интерпретации моделей (LIME, SHAP). И это создает новый вид издержек, причем не связанных непосредственно с производством;
– фирма попадает в зависимость от применения алгоритма: даже сталкиваясь с систематическими ошибками модели, фирма не может отказаться от ее использования из-за потери скорости операционной деятельности или вообще приостановки работы.
– теряется возможность налаживать широкий функционал по индивидуальной работе с клиентами, выстраивание долгосрочных отношений.

Яркий пример – динамическое ценообразование на маркетплейсах. Оно увеличивает прибыль продавцов на 15–25 %, но одновременно порождает координацию без явного сговора. Эксперименты показывают, что Q-learning алгоритмы в повторяющихся аукционах устойчиво выходят на цены выше конкурентного равновесия.

### 3. Мезоуровень: алгоритмические экосистемы и барьеры входа

В экономике данных формируются **алгоритмические экосистемы** – связанные модели, использующие общие пулы данных. Это создает:

– эффект привязки: клиент не может покинуть платформу, так как альтернативы не имеют сопоставимой предиктивной точности;
– неценовые барьеры входа: новый игрок должен потратить не только на вычислительные ресурсы, но и на накопление массива обратной связи, что может занимать годы для выхода на уровень давно присутствующих на платформе конкурентов имеющих;
– алгоритмическую поляризацию отраслей: рынок делится на «обладателей больших моделей» и «пользователей», причем переход из второй группы в первую становится почти невозможным без регуляторного вмешательства.

### 4. Макроэкономические эффекты: циклы, занятость и стабильность

Широкое проникновение алгоритмических моделей модифицирует макродинамику:

– циклы переобучения: когда все агенты используют модели, обученные на одинаковых исторических данных, возникает синхронизация решений – продают активы в одно время, сокращают запасы одновременно, что усиливает волатильность.
– трансформация рынка труда: исчезают не столько профессии, сколько функции принятия рутинных решений. В то же время возникает спрос на новую профессию – «промпт-инженеров» и валидаторов алгоритмов, но их число на порядок меньше вытесняемых.
– риск алгоритмической монетарной политики: центральные банки начинают использовать модели машинного обучения для прогноза инфляции, но при массовом внедрении этих же моделей коммерческими банками возникают обратные связи, делающие политику процикличной.

## 5. Алгоритмические провалы рынка и направления регулирования

Классические провалы рынка в экономике данных приобретают новое звучание. В таблице 1 можно увидеть примеры некоторых из них, а также предложения для их минимизации.

ТАБЛИЦА 1. Некоторые отрицательные эффекты алгоритмических моделей и пути их минимизации

| Феномен | Проявление | Возможное решение |
|---|---|---|
| Алгоритмическая дискриминация | Продвинутые группы против групп без цифрового следа | Обязательный аудит моделей |
| Воздействие данных на третьи стороны | Модель одной фирмы ухудшает решения другой из-за корреляций | Создание моделей совместимости |
| Когнитивная перегрузка | Агент не может рационально оспорить решение модели | Право на объяснение, апелляцию, диалог |

Можно предложить следующее: необходима алгоритмическая антимонопольная политика, которая включает:

– требование интероперабельности базовых предиктивных моделей в социально значимых сферах;
– введение контроля за использованием данных при обучении моделей на поведении третьих лиц без одобрения;
– создание публичных алгоритмических реестров с метриками смещения.

Широкое проникновение алгоритмических моделей в условиях экономики данных – не просто технологический тренд, а сдвиг в основании экономической координации. Позитивные эффекты (снижение издержек, скорость, персонализация) сопровождаются системными рисками: алгоритмическим сговором, барьерами входа нового типа, макроциклами из-за синхронизации решений и новыми формами дискриминации.

Преподавание в университете дисциплин по цифровой экономике должно включать не только восхищение возможностями применения платформенных алгоритмов, развития экосистемных моделей, широкого использования искусственного интеллекта, но и объективный анализ побочных эффектов, как уже проявившихся в реальной экономике, так и потенциальных. Иначе мы рискуем подготовить поколение экономистов

и специалистов смежных областей, которые умеют строить модели, но не умеют оценивать их встроенные искажения и системные последствия.

**Список используемых источников**

1. Седых И. Ю. Риски и этические проблемы использования искусственного интеллекта в экономике // Экономика строительства. 2026. № 1. С. 272-274.

2. Седых И. Ю., Хрипунова М. Б. Цифровая трансформация экономики через призму технологий искусственного интеллекта //Фундаментальная и прикладная Математика. 2025. Т. 25. № 4. С. 108-112.

3. Ефимова Н. А., Миротворская И. В. Защита персональных данных и цифровые права в цифровой экономике: Юридические риски, механизмы ответственности //В сборнике: Цифровые технологии в развитии современных экономических систем. Материалы I Всероссийской научно-практической конференции с международным участием. Липецк, 2026. С. 256-261.

4. Колесникова Е. В., Усачев А. С., Майорова Л. Н. Роль искусственного интеллекта в цифровой экономике //В сборнике: Современные вопросы управления бизнес-процессами в цифровой экономике. Материалы II Всероссийской научной конференции Таганрогского института имени А. П. Чехова (филиала) ФГБОУ ВО "Ростовский государственный экономический университет (РИНХ)". Ростов-на-Дону, 2025. С. 26-33.

5. Фидаров А. А., Ваниева А. А. Технологии в парадигме цифровой экономики: Структурный анализ воздействия на бизнес-модели и рыночные институты //В сборнике: Управление экономикой, системами, процессами. Сборник статей IX Международной научно-практической конференции. Пенза, 2025. С. 688-691.

## THE EFFECTS OF WIDESPREAD PENETRATION OF ALGORITHMIC MODELS IN THE CONTEXT OF THE DEVELOPMENT OF THE DATA ECONOMY

**Isakov A., Pavlova E.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article provides the concept of an algorithmic approach, a description of the application of an algorithmic approach in modern conditions. Its influence on content production, the formation of recommendation systems, pricing, and the development of consumer preferences. The role of various kinds of data in the modern economy. Special attention is paid to side effects, often undesirable, and the consequences of widespread algorithms in economic platform models. And, accordingly, the need for a deeper analysis and study of emerging trends. As well as possible ways to minimize negative consequences.*

***Key words**: data economics, algorithmic models, digital economy, predictive analytics, data scale effects*

**УДК 332.1**
**ГРНТИ 82.33**

# ВЫБОР АРХИТЕКТУРЫ МУЛЬТИАГЕНТНЫХ СИСТЕМ ДЛЯ БИЗНЕСА

**О. В. Калимуллина**

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

*Мультиагентные системы позволяют декомпозировать сложные бизнес-задачи на параллельно исполняемые подзадачи, сокращая время выполнения с часов до минут. Выбор архитектуры и моделей определяется требованиями к локализации данных, бюджетом и наличием компетенций разработки. В статье рассматриваются архитектурные аспекты построения мультиагентных систем (МАС) для решения бизнес-задач. Описана типовая архитектура МАС, показано, что ключевым свойством МАС является параллельность подзадач, позволяющая сократить время выполнения сложных процессов с часов до минут. Приведены два практических пути внедрения: готовые платформы и самостоятельная разработка с использованием фреймворков оркестрации. Выявлены основные риски внедрения, сформулированы рекомендации по выбору архитектуры в зависимости от бюджета, компетенций и требований к локализации данных.*

***искусственный интеллект, архитектура мультиагентных систем, бизнес-процессы***

В июле 2024 года OpenAI опубликовала официальную пятиуровневую классификацию ИИ [1]. В данной классификации первый уровень представляют чат-боты, отвечающие на вопросы. Второй уровень предполагает возможность рассуждения, решения сложных задач на уровне эксперта, поиска информации в интернете. Третий уровень представляет собой агент, самостоятельно выполняющий действия, вызывающий инструменты, работающий в системах. Четвертый уровень представляет мультиагентная система, где несколько агентов работают параллельно под управлением оркестратора, выполняя задачи без участия человека. На данный момент технологии находятся на четвертом уровне. Пятый уровень AGI (искусственный общий интеллект) – это ИИ, способный выполнять работу целой организации, пока теоретический предел, который не достигнут [2]. Большинство организаций сегодня используют ИИ на уровне 1-2.

Мультиагентная система представляет собой архитектуру, в которой несколько специализированных агентов взаимодействуют для решения

сложной задачи. Центральный элемент системы: **оркестратор**, то есть агент-менеджер, который принимает запрос, декомпозирует его на подзадачи, назначает субагентов и собирает итоговый результат.

Ключевое свойство мультиагентной системы: **параллельность**. Пока агент-исследователь собирает данные, агент-аналитик обрабатывает предыдущую порцию, а агент-автор готовит структуру отчета. То, что человек делал бы последовательно часами, МАС выполняет одновременно за минуты [3].

Каждый ИИ-агент в мультиагентной системе состоит из нескольких компонентов, работающих в коллаборации (рисунок 1).

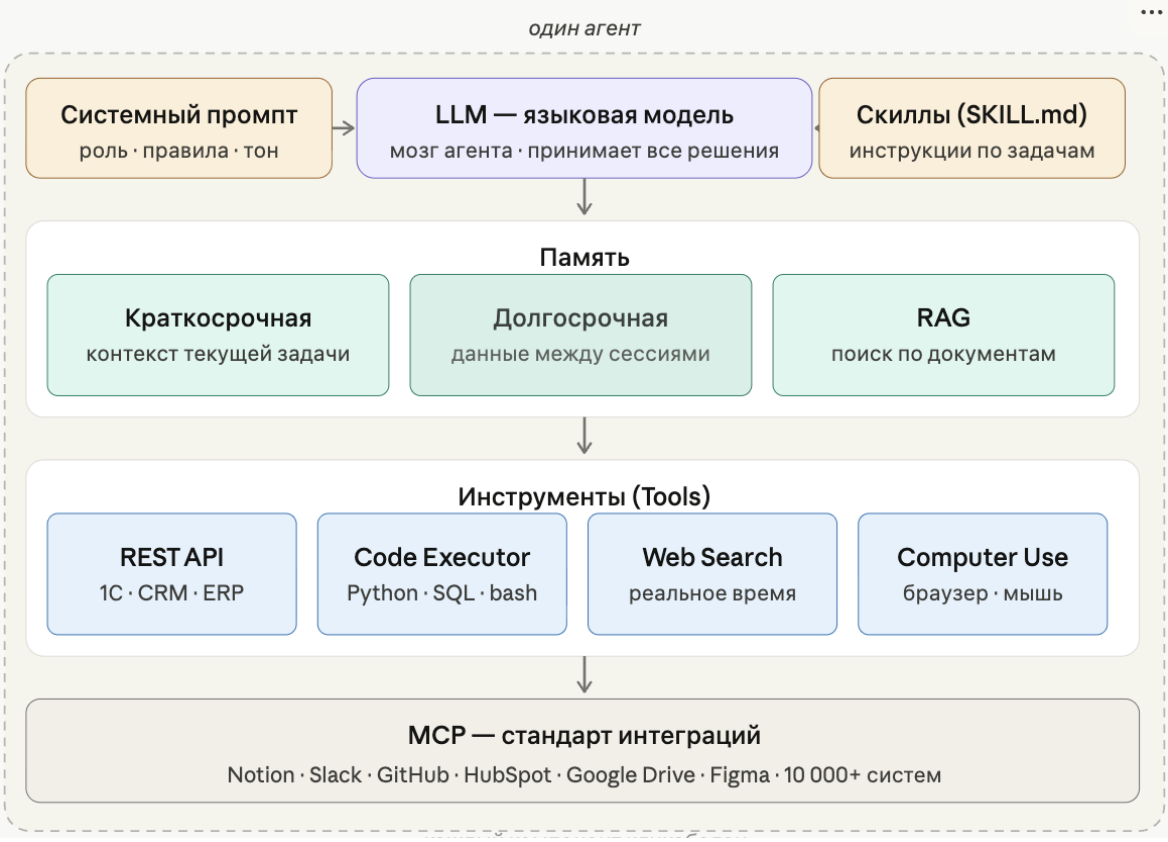



Рис. 1. Архитектура МАС

После получения пользовательского запроса оркестратор распределяет подзадачи между субагентами. На основе своей LLM и системного промпта каждый субагент решает, какие инструменты вызвать, обращается к памяти и возвращает результат оркестратору. При этом системный промпт представляет собой текстовый файл, описывающий роль агента, правила его работы и ограничения, а качество системного промпта определяет качество агента. Поскольку архитектура агента не привязана к конкретной модели, это позволяет гибко заменять большие языковые модели в зависимости от

конкретных задач, вычислительных ресурсов и требований к функциональности, что особенно актуально для бизнеса, где важны оптимизация затрат, скорость обработки данных и поддержка определенных возможностей [4].

Память агента делится на три уровня:

1. Краткосрочная: контекст (история) текущей задачи и сессии. Хранится во временной памяти модели.

2. Долгосрочная: база данных, в которую агент сохраняет важные факты между сессиями. Позволяет агенту "помнить" предыдущие взаимодействия.

3. RAG (Retrieval-Augmented Generation, то есть поиск по документам перед формированием ответа): перед ответом агент ищет релевантные фрагменты в корпоративной базе документов через векторное хранилище (специализированная база данных для поиска по смыслу, а не по ключевым словам). Агент не хранит все знания компании в памяти модели, а обращается к ним по мере необходимости.

Инструменты (Tools) представляют собой функции, которые агент вызывает для выполнения действий за пределами генерации текста:

– REST API (стандартный веб-интерфейс для обмена данными между программами): вызов внешних систем, CRM (системы управления клиентами), ERP (корпоративные системы управления ресурсами), электронная почта, календарь;
– Code Executor (исполнитель кода): выполнение кода на Python (язык программирования), SQL (язык запросов к базам данных), bash (командная строка) для обработки и анализа данных;
– поиск в интернете: поиск актуальной информации в реальном времени;
– управление компьютером: возможность модели управлять браузером, мышью и клавиатурой;
– файловая система: чтение и запись файлов на сервере.

При этой оркестратор управляет всей мультиагентной логикой: запускает субагентов, маршрутизирует результаты, обрабатывает ошибки.

Сегодня у организаций есть два практических варианта внедрения МАС. Первый путь – это готовая платформа, где нужно зарегистрироваться, настроить сценарии через визуальный конструктор без написания кода и запустить агентов за один-два дня. Второй путь для компании – самостоятельно создать МАС. Данный вариант подходит тем, у кого есть хотя бы один разработчик и важен контроль над системой. Внедрение МАС сопряжено с системными рисками, которые необходимо учитывать при выборе

архитектуры. Так, галлюцинации LLM могут выражаться в том, что агент может придумать несуществующие факты. В цепочке агентов ошибка может накапливаться и усиливаться. Высокая стоимость может быть вызвана параллельными вызовами LLM, увеличивающими расход токенов в 3–5 раз по сравнению с однозапросным решением. Сложность отладки – трудно выяснить, какой агент и почему принял неверное решение, особенно при асинхронном взаимодействии. Проблемы синхронизации – если подзадачи зависимы, неправильная оркестрация ведет к повторным вычислениям. Безопасность – агенты, имеющие доступ к API, файловой системе и браузеру, становятся вектором атаки.

В работе показано, что мультиагентные системы являются эффективной архитектурной парадигмой для параллельной декомпозиции сложных бизнес-задач, благодаря скоординированному взаимодействию управляющего оркестратора и специализированных субагентов, функционирующих на основе больших языковых моделей, трехуровневой архитектуры памяти и расширенного инструментария, достигается сокращение времени обработки с часов до минут. Анализ выявил, что внедрение МАС сопряжено как с преимуществами, так и с существенными рисками: кумулятивная эскалация галлюцинаций, многократное увеличение расхода токенов, сложность отладки асинхронных взаимодействий и уязвимости безопасности при обращении агентов к API и файловой системе. В исследовании определены две стратегии внедрения: использование готовых low-code платформ, обеспечивающих быстрый старт без привлечения разработчиков, либо самостоятельная разработка с применением фреймворков оркестрации для организаций, требующих полного контроля над системой и локализации данных.

**Список используемых источников**

1. OpenAI Scale Ranks Progress Toward ‘Human-Level’ Problem Solving// URL: https://www.bloomberg.com/news/articles/2024-07-11/openai-sets-levels-to-track-progress-toward-superintelligent-ai

2. Feng, Z., Xue, R., Yuan, L. et al. Multi-agent embodied AI: advances and future directions. Sci. China Inf. Sci. 69, 151202 (2026). URL: https://DOI.org/10.1007/s11432-025-4820-4 (дата обращения 10.04.2026).

3. Калимуллина О. В. Сравнительный анализ больших языковых моделей: преимущества для бизнеса. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании" (АПИНО 2025). Сборник научных статей XIV Международной научно-технической и научно-методической конференции. В 2-х томах. Санкт-Петербург, 2025. С. 134-137.

4. Wu D, Wei X, Chen G, et al. Generative multi-agent collaboration in embodied AI: a systematic review. 2025. ArXiv:2502.11518

# CHOOSING THE ARCHITECTURE OF MULTI-AGENT SYSTEMS FOR BUSINESS

**Kalimullina O.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Multi-agent systems allow you to decompose complex business tasks into parallel subtasks, reducing execution time from hours to minutes. The choice of architecture and models is determined by data localization requirements, budget, and the availability of development competencies. The article discusses the architectural aspects of building multi-agent systems (MAC) to solve business problems. A typical MAC architecture is described, and it is shown that the key property of MAC is the parallelism of subtasks, which reduces the execution time of complex processes from hours to minutes. Two practical ways of implementation are given: ready-made platforms and independent development using orchestration frameworks. The main risks of implementation have been identified, and recommendations have been formulated for choosing an architecture depending on budget, competencies, and data localization requirements.*

***Key words:*** *artificial intelligence, architecture of multi-agent systems, business processes*

**УДК 004.738.5:339.138:613**
**ГРНТИ 20.53.21**

# МОДЕЛИ МОТИВАЦИИ ПОЛЬЗОВАТЕЛЕЙ В WELLNESS-ЭКОСИСТЕМАХ

**О. В. Калимуллина, Н. А. Степанов**

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

*Долгосрочное удержание пользователей в современных wellness-экосистемах требует анализа моделей их мотивации. Раскрыты механизмы баланса внутренней и внешней мотивации через геймификацию, ИИ-персонализацию и социальную поддержку. Выявлены основные драйверы вовлеченности. Показано, что синергия превентивного подхода, конвергенции сервисов и партнерских моделей, персонализации и проактивной профилактики формирует устойчивую экосистему, охватывающую все пять измерений холистического благополучия.*

***wellness-экосистема, холистическое благополучие, ИИ-алгоритмы, геймификация***

Широкая трактовка wellness-экосистем подразумевает совокупность обоюдно согласованных компонентов, служащих повышению уровня целостного (холистического) благополучия человека. В силу социальной и экономической значимости вопросы развития современных wellness-экосистем привлекают пристальное внимание специалистов [1; 2]. И это вполне обоснованно: на уровне международного пространства по данным Global Wellness Institute денежный оборот экономики благополучия в 2024 г. составил около $7 трлн [3], по прогнозам сохраняя в перспективе нескольких ближайших лет положительную динамику.

Одновременно с этим фиксируется и проблема: более 90 % клиентов, установивших веб- и мобильные приложения, ориентированные на содействие в поддержке здоровья и благополучия, начинают отказываться от использования этих программных решений уже в первый месяц. Именно долгосрочное удержание – задача, требующая комплексного исследования и решения, а мотивация пользователей выступает как одна из важнейших ее сторон. Этим обусловлена актуальность настоящего исследования.

В первую очередь нужно принять во внимание составляющие wellness-экосистемы, к которым относятся целевые функциональные веб- и мобильные приложения, многофункциональные носимые гаджеты, тематические

интернет-сообщества, сервисы онлайн- и телемедицины, корпоративные программы благополучия и здоровья. В рассматриваемом контексте они ориентированы на контроль активности, предоставление персональных рекомендаций, мониторинг и оценку прогресса, оказание поддержки, повышение интереса с помощью игровых элементов и т.д.

Мотивация для использования составляющих wellness-экосистемы в самом общем смысле подразделяется на внутреннюю (интренсивную) и внешнюю (экстринсивную). Первая подразумевает личную потребность к самосовершенствованию, ценностные установки на самосохранительную модель поведения, воодушевление от процесса саморазвития. Вторая, внешняя мотивация, объективирована в систему поощрений, баллов, общественное признание, элементы соревновательности.

Важной задачей выступает достижение оптимального баланса между внутренней и внешней мотивацией. Данный компромисс предполагает двойную задачу: с одной стороны, зависимость от внешних поощрений не должна стать единственным значимым стимулом wellness-активности пользователя, и при этом, с другой стороны, ему следует внутренне укрепиться в желании следовать пути физического или психологического здоровья достаточно продолжительное время.

Рассмотрим несколько ключевых на сегодняшний день мотивационных моделей. Первая, весьма популярная – SDT (Теория самодетерминации), концептуальной основой имеет психологический подход. Она была разработана Э. Деси и Р. Райаном [4]. В рамках этой теории основным мотивационным механизмом выступает детерминированное природой человека стремление к росту. Авторы теории называют «тремя китами благополучия» автономию, компетентность (успех) и социальные связи. Все это можно обеспечить с помощью составляющих wellness-экосистемы. Например, пользователь сам может выбрать цель – похудение, через некоторое время обнаружить прогресс в виде снижения веса, опубликовать в коммуникативном пространстве фотографии и получить в виртуальном формате поддержку членов сообщества.

Еще одна известная мотивационная модель, обозначаемая аббревиатурой FBM, принадлежит авторству Б. Дж. Фогга [5]. Согласно этой разработке, импульс к действию создает сочетание таких компонентов, как мотивация (внутренний стимул к действию), способность (обусловлена степенью сложности действия) и стимул (триггер), в качестве которого может служить напоминание (некий сигнал). В рамках wellness-экосистемы эта мо-

дель реализуется без видимых сложностей. Например, довольно простым действием является выполнение 20 подряд физических упражнений в виде приседаний. О необходимости их осуществить в определенное время на мобильное приложение поступает звуковой сигнал-уведомление. По мере выполнения ежедневно пользователь получает на электронную почту награду (например, тематический афоризм или анимационное изображение).

В реализации обеих мотивационных систем на платформах wellness-экосистем широко задействуются такие механизмы, как геймификация, персонализация, влияние общества и многофункциональность. Так, например, В 2026 году несколько моделей фитнес-часов с NFC-платежами (Apple Watch SE 3, Xiaomi Watch S4 и др.) сочетают спортивные функции и бесконтактную оплату, а также акселерометр, гироскоп, пульсометр, барометр, датчик освещенности и пр., обладая влагозащитой и автономностью до 5 дней. Такой элемент мотивации как геймификация в приложениях может реализовываться в открытии возможности перехода пользователя на новый уровень (например, по мере накопления 200 проделанных физических упражнений в виде приседаний или пешего преодоления 10 км), повышается его позиция в электронном рейтинге среди других участников, присваивается бейдж, делается доступным возможность участия в интересном челлендже.

Высокий потенциал wellness-экосистем связан и с их персонализацией. Так, алгоритмы ИИ, контролирующие выполнение физических упражнений, могут адаптировать рекомендации под особенности и объективные показатели конкретного человека. Например, длина дистанции для пешей прогулки может регулироваться индивидуально с учетом анализа режима сна, частоты дыхания и пульса.

В функционирование wellness-экосистем органично интегрируется значимость общественного влияния в форме одобрения (преимущественно). Воздействие этого фактора конструктивно реализуется в тематических интернет-сообществах и группах поддержки. Программные ресурсы (чаты, форумы) позволяют организовать обмен «успехами», а также систему виртуальных жестов поощрения и мотивационных комментариев. В качестве примера можно привести чаты любителей пешей ходьбы, принявших решение отказаться от употребления напитков, содержащих кофеин, или участников марафонов по снижению массы тела. Все это становится выполнимым с помощью современных технологий, объективированных в изделия, осуществляющие сбор информации в режиме реального времени: фитнес-

браслеты, умные часы и т.д. Для оценки будущих потребностей и защитно-опережающих подсказок используются возможности ИИ и Big Data. VR и AR технологии позволяют эффективно проводить медитации с погружением, а также виртуальные тренировки. Современные автоматизированные помощники могут осуществлять круглосуточную консультативную поддержку, если таковая необходима.

Применение wellness-технологий порождает причины и факторы удержания клиента. В перечне таковых постоянное обеспечение обратной связи с помощью системы уведомлений, напоминаний, отражения динамики. Гибкость настроек – еще один важный фактор. Он позволяет адаптировать систему под скорректированные в процессе цели.

Учитывая уровень эстетических запросов современного общества, а также значимость визуального и эмоционального восприятия, очень важным фактором удержания пользователя выступает приятный дизайн wellness-экосистемы и интуитивно понятный набор инструментов, содержащий позитивные подкрепления в текстовой или иной форме. Существенное значение для клиента имеет минимизация всех видов барьеров. Для ее обеспечения необходимо сделать максимально простым процесс регистрации и удобный пользовательский интерфейс с возможностью расширения функционала управления, а также возможности сопряжения всех видов устройств между собой для успешной интеграции в повседневные привычки. Очень важный развивающийся сегмент рынка – корпоративные wellness-программы, позволяющие интегрировать в единую экосистему различные цифровые инструменты и платформы. С их помощью можно реализовывать интересные командные события и соревнования (например, компания Google выстроила одну из лучших комплексных корпоративных велнес-экосистем в мире, ориентированную на поддержку «целостного человека» (whole person), финансируя премиальные элементы корпоративной культуры: лап-пулы, фитнес-классы, зоны для сна, внутренние курсы от сотрудников и пр., продвигая всеобъемлющий холистический подход к здоровью).

Можно привести и отечественные примеры динамично развивающихся экосистем из разных отраслей. Так, ПАО «МТС» с 2018 года развивает в дополнение к традиционным телекоммуникационным услугам целый ряд цифровых сервисов для личного и корпоративного применения (телемедицинская платформа SmartMed, сервис Meditopia и прочие). Российская транснациональная компания Яндекс интегрирует все большее количество

различных цифровых сервисов: поисковых, картографических, музыкальных, транспортных, логистических, аптечных, инклюзивных, консультационных в режиме реального времени по вопросам здоровья (например, Yandex Cloud с 2018 года предоставляет технологические решения, включая анализ медицинских изображений, в сфере здравоохранения и медицины для частного и бизнес-сектора). Перспективным направлением развития экосистемы «СберЗдоровья» в рамках работы ПАО «Сбербанк России» с 2020 года являются программы дистанционного мониторинга для пациентов с хроническими заболеваниями (например, сердечно-сосудистыми, гипертонией, сахарным диабетом) на базе сопряженных «умных устройств» (тонометр, глюкометр, камера, кольцо, стетоскоп) и голосовых помощников, а также внедрение в функционал банкоматов опции экспресс-оценки здоровья. Доступ осуществляется ко всем предоставляемым сервисам (под узнаваемым брендом Сбер объединены более 60 компаний) через единый профиль Sber ID, общую программу лояльности и привычные для клиентов каналы.

Приведенные в пример модели мотивации пользователей wellness-экосистем таят в себе этические вызовы и потенциальные угрозы, требующие превентивных мер для того, чтобы максимально обезопасить пользователя. Во-первых, продуманности требует система защиты конфиденциальных данных о состоянии здоровья. Также следует направить меры на снижение формирования зависимости от поощрений и бонусов. Кроме того, сама система должна быть доступной независимо от возраста пользователя, его материального и социального статуса. Также нельзя забывать о сохранении баланса между вовлечением и раздражающими факторами, которые формируются при злоупотреблениях сигнальными уведомлениями.

Ключевыми тенденциями построения wellness-экосистем сегодня становятся: конвергенция сервисов и партнерские модели, персонализация, проактивная профилактика, охват пяти измерений благополучия – физического, ментального, социального, финансового и карьерного [6]. В целом же, конструктивно выстроенные мотивационные модели служат повышению вовлеченности пользователей wellness-экосистем, интегрируя достижения психологической науки, научных разработок, инновационных технологий.

**Список используемых источников**

1. Жура С. Е., Ершова И. В., Смирнова Н. С. Велнес экономика как основа современных концепций здравоохранения // Интерактивная наука. 2021. № 5 (60). С. 58 –59.

2. Кучеренко И. М., Абазян А. Г., Сорока В. М. Сегментация и современные тенденции развития рынка medical и wellness-туризма // Экономика и предпринимательство. 2025. № 12-1(185). С. 738–742.

3. Statistics & Facts // Global Wellness Institute. URL: https://globalwellnessinstitute.org/ press-room/statistics-and-facts/ (дата обращения: 24.04.2026).

4. Deci E. L., Ryan R. M. Intrinsic motivation and self-determination in human behavior. NY: Plenum Publishing Co, 1985. 371 c.

5. Fogg B. J. Tiny Habits: The Small Changes That Change Everything. Boston: Houghton Mifflin Harcourt, 2019. 304 c.

6. Practice Better. Creating Personalized Wellness Programs with Practice Better // Practice Better Blog: электрон. блог. 24 февраля 2025. URL: https://practicebetter.io/blog/creating-personalized-wellness-programs-with-practice-better (дата обращения: 08.04.2026).

## USER MOTIVATION MODELS IN WELLNESS-ECOSYSTEMS

**Kalimullina O., Stepanov N.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Long-term user retention in modern wellness ecosystems requires an analysis of their motivation models. The mechanisms of balancing internal and external motivation through gamification, AI personalization, and social support have been revealed. The main drivers of engagement have been identified. It has been shown that the synergy of a preventive approach, the convergence of services and partnership models, personalization, and proactive prevention forms a sustainable ecosystem that covers all five dimensions of holistic well-being.*

***Key words:*** *wellness ecosystem, holistic well-being, AI algorithms, gamification*

**УДК 351.761.3**
**ГРНТИ 76.75.91**

# МЕЖДУНАРОДНЫЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ СИНТЕТИЧЕСКИМ ОПИОИДАМ КАК ИНСТРУМЕНТ ОЦЕНКИ МЕР США В ПЕРИОД ЧЕТВЕРТОЙ ВОЛНЫ ОПИОИДНОГО КРИЗИСА

**А. А. Кобильняк, А. В. Неровный**

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

*В статье рассматривается распространение синтетических опиоидов в трансформации опиоидного кризиса в Соединенных Штатах Америки. Анализируются зарубежные подходы к профилактике передозировок, лечению зависимости, снижению вреда и раннему предупреждению. Международный опыт используется для сопоставления с американскими мерами и выявления критериев оценки.*

***опиоидный кризис, синтетические опиоиды, фентанил, нитазены, антинаркотическая политика, снижение вреда, США, международный опыт***

Современная динамика опиоидного кризиса в США определяется не только масштабами незаконного оборота наркотических веществ и употребления рецептурных препаратов не по назначению врача, но и качественным изменением нелегального рынка. На смену этапам, связанным преимущественно с рецептурными опиоидными обезболивающими и героином, пришел период доминирования высокопотентных синтетических веществ. Ключевую роль в нем играют незаконно произведенный фентанил и его аналоги, отличающиеся высокой токсичностью и трудностью контроля при нелегальном обороте. По данным Центров по контролю и профилактике заболеваний США, в 2023 г. от передозировки наркотиков умерло около 105 тыс. человек, при этом почти 80 тыс. смертей были связаны с опиоидами [1].

Особенность современного периода заключается в том, что синтетические опиоиды все чаще выступают не изолированным, а комбинированным фактором риска. В научной литературе данная трансформация обозначается как четвертая волна опиоидного кризиса, для которой характерно сочетание фентанила и других синтетических опиоидов со стимуляторами, включая кокаин и метамфетамин [2]. По данным Центров по контролю и профилактике заболеваний США, в 2023 г. почти 47 % смертей от передозировок

в ряде юрисдикций были связаны с одновременным употреблением опиоидов и стимуляторов [1]. Цель статьи состоит в определении того, какие элементы международного опыта могут использоваться как критерии оценки мер США в период четвертой волны опиоидного кризиса.

В этих условиях эффективность мер США не может оцениваться только по числу уголовных дел, объему изъятий наркотиков или степени ужесточения наказаний. Такие показатели отражают преимущественно правоохранительную сторону реагирования, но не позволяют в полной мере оценить способность государства снижать смертность и ограничивать последствия кризиса. Более значимыми становятся критерии, связанные с доступностью лечения зависимости, распространением препаратов для экстренного купирования передозировки, охватом программ снижения вреда, качеством токсикологического мониторинга и скоростью выявления новых психоактивных веществ. Поэтому международный опыт представляет интерес не как готовая модель для прямого переноса, а как сравнительный инструмент оценки американской политики.

Антинаркотическая политика США включает профилактику употребления психоактивных веществ, расширение доступа к лечению зависимости, распространение препаратов для купирования передозировки, развитие программ снижения вреда и пресечение незаконного оборота синтетических опиоидов. В Национальной стратегии контроля над наркотиками подчеркивается необходимость сочетания профилактических, медицинских и правоохранительных мер [3]. Однако наличие этих направлений само по себе не гарантирует эффективности. Существенное значение имеют их практическая доступность, согласованность между федеральным уровнем и штатами, а также способность адаптироваться к изменению структуры нелегального рынка. Так, расширение доступа к налоксону снижает риск смертельного исхода при передозировке, но не заменяет лечение зависимости, социальное сопровождение и профилактическую работу с группами риска.

Наиболее сопоставимым с США зарубежным примером является Канада, где также наблюдается высокая смертность, связанная с фентанилом, его аналогами и токсичным составом нелегального рынка. По данным Правительства Канады, с января 2016 г. по сентябрь 2025 г. было зарегистрировано 55 032 смерти от предполагаемой опиоидной токсичности. В январе–сентябре 2025 г. фентанил был выявлен в 58 % таких случаев, аналоги фентанила – в 57 %, а стимуляторы – в 70 % [4]. Поскольку эти категории пересекаются, приведенные показатели не суммируются, а указывают на поли-

наркотический характер кризиса. Канадский подход основан на сочетании распространения налоксона, пунктов контролируемого потребления, мониторинга токсичности и информирования населения [5]. Для оценки мер США этот опыт важен как пример политики, ориентированной на предотвращение смертельных исходов даже при сохранении нелегального рынка.

Европейский опыт представляет иную, но не менее значимую сравнительную перспективу. В отличие от Северной Америки, где фентанил уже стал устойчивым элементом нелегального рынка, в европейских государствах особую обеспокоенность вызывает распространение нитазенов. Нитазены представляют собой группу сильнодействующих синтетических опиоидов бензимидазольного ряда; от фентанила они отличаются химической структурой и чаще рассматриваются в Европе как новые психоактивные вещества, возникающие на нелегальном рынке в форме примесей, порошков или поддельных лекарственных препаратов. Европейское агентство по наркотикам указывает, что в 2024 г. в систему раннего предупреждения Европейского союза были впервые официально внесены семь новых синтетических опиоидов, и все они относились к нитазенам [6]. Кроме того, с 2019 г. наличие нитазенов было зафиксировано как минимум в 21 государстве Европейского союза [6].

Наиболее заметные сигналы о вреде, связанном с нитазенами, поступали из стран Балтии, Ирландии, Франции и Великобритании. В Эстонии в 2023 г. нитазены были связаны с 62 из 119 смертей от передозировок, а в Латвии – со 101 из 154 таких случаев [6]. Во Франции и Ирландии фиксировались вспышки отравлений, при которых нитазены могли продаваться под видом героина. В Англии и Уэльсе в 2024 г. было зарегистрировано 195 смертей с участием нитазенов, что почти в четыре раза выше показателя 2023 г. [6; 7]. Для США данный опыт важен прежде всего с точки зрения раннего предупреждения, токсикологического учета и публичного информирования, поскольку новые синтетические опиоиды могут появляться в составе веществ, которые потребители воспринимают как героин, поддельные лекарственные препараты или иные наркотики.

Великобритания является показательным примером европейской страны, где распространение нитазенов выявляет не только рост новой угрозы, но и ограничения статистического учета. По данным Управления национальной статистики, в 2024 г. в Англии и Уэльсе в 1192 случаях, или 21,4 % смертей от отравления наркотиками, конкретное вещество не было указано в свидетельстве коронера [7]. Следовательно, для оценки угрозы

синтетических опиоидов важны не только итоговые показатели смертности, но и качество токсикологической отчетности.

Сравнение североамериканского и европейского опыта позволяет выделить два типа угроз. В США и Канаде речь идет о масштабном кризисе, где фентанил и его аналоги глубоко встроены в нелегальный рынок. В Европе ситуация чаще проявляется через риск распространения новых высокопотентных опиоидов, прежде всего нитазенов, и через отдельные вспышки отравлений. Это различие показывает, что международный опыт не следует использовать для прямого сопоставления статистики смертности. Его значение состоит в выявлении управленческих механизмов, необходимых для реагирования на синтетические опиоиды: доступности экстренной помощи, развития лечения зависимости, снижения вреда, токсикологического мониторинга и раннего предупреждения.

Для оценки мер США принципиально важно учитывать не только перечень реализуемых инструментов, но и уровень их институционального закрепления. В условиях четвертой волны кризиса отдельные меры дают ограниченный эффект, если они применяются фрагментарно, различаются по доступности между штатами или не сопровождаются устойчивым обменом данными между медицинскими, социальными и правоохранительными структурами. Поэтому международный опыт позволяет поставить вопрос не только о наличии тех или иных мер, но и о качестве их координации.

ТАБЛИЦА 1. Международный опыт противодействия синтетическим опиоидам

| Страна / регион | Проявление угрозы | Практики реагирования | Критерий для США |
|---|---|---|---|
| США | В 2023 г. около 105 тыс. смертей от передозировок, почти 80 тыс. из них связаны с опиоидами | Налоксон, лечение зависимости, профилактика, правоохранительные меры | Баланс медицинских, социальных и силовых инструментов |
| Канада | 55 032 смерти от предполагаемой опиоидной токсичности с января 2016 г. по сентябрь 2025 г.; высокая роль фентанила и стимуляторов | Распространение налоксона, пункты контролируемого потребления, мониторинг токсичности | Комплексность мер и развитие снижения вреда |
| ЕС | С 2019 г. нитазены выявлены как минимум в 21 государстве ЕС | Система раннего предупреждения, лабораторный мониторинг, обмен информацией | Скорость выявления новых веществ |

| Страна / регион | Проявление угрозы | Практики реагирования | Критерий для США |
|---|---|---|---|
| Великобритания | Фиксация смертей, связанных с нитазенами; часть случаев требует уточнения из-за неполных токсикологических данных | Токсикологический учет, публичные предупреждения, профилактика передозировок | Учет меняющегося состава нелегального рынка |

Как показано в таблице 1, зарубежный опыт позволяет оценивать меры США по нескольким взаимосвязанным критериям: снижению смертности от передозировок, доступности лечения зависимости, развитию программ снижения вреда, качеству токсикологического мониторинга и скорости предупреждения о новых веществах. Такой подход не сводит эффективность политики только к правоохранительным показателям и позволяет учитывать медицинские и социальные последствия кризиса.

В итоге проведенное сопоставление показывает, что для США наиболее значимы три направления оценки. Во-первых, важно учитывать, насколько меры противодействия реально доступны группам риска в разных штатах. Во-вторых, необходимо оценивать, как медицинские, социальные и правоохранительные инструменты согласуются между собой. В-третьих, особое значение имеет способность системы быстро реагировать на появление новых синтетических веществ. Следовательно, международный опыт не заменяет анализ американской политики, но позволяет точнее определить ее сильные и слабые стороны в период четвертой волны опиоидного кризиса.

**Список используемых источников**

1. Centers for Disease Control and Prevention. Understanding the Opioid Overdose Epidemic. URL: https://www.cdc.gov/overdose-prevention/about/understanding-the-opioid-overdose-epidemic.html (дата обращения: 08.05.2026).

2. Ciccarone D. The Rise of Illicit Fentanyls, Stimulants and the Fourth Wave of the Opioid Overdose Crisis // Current Opinion in Psychiatry. 2021. Vol. 34, № 4. P. 344–350. DOI: 10.1097/YCO.0000000000000717.

3. The White House. National Drug Control Strategy. Washington, 2024. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-National-Drug-Control-Strategy.pdf (дата обращения: 08.05.2026).

4. Government of Canada. Opioid- and Stimulant-related Harms in Canada. URL: https://health-infobase.canada.ca/substance-related-harms/opioids-stimulants/ (дата обращения: 08.05.2026).

5. Health Canada. Supervised Consumption Explained: Types of Sites and Services. URL: https://www.canada.ca/en/health-canada/services/substance-use/supervised-consumption-sites/explained.html (дата обращения: 08.05.2026).

6. European Union Drugs Agency. European Drug Report 2025: Trends and Developments. URL: https://www.euda.europa.eu/publications/european-drug-report/2025_en (дата обращения: 08.05.2026).

7. Office for National Statistics. Deaths Related to Drug Poisoning in England and Wales: 2024 Registrations. URL: https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/deaths/bulletins/deathsrelatedtodrugpoisoningineng-landandwales/2024registrations (дата обращения: 08.05.2026).

*Статья представлена кандидатом исторических наук, заведующим кафедрой истории и регионоведения СПбГУТ, доцентом А. Б. Гехтом.*

## INTERNATIONAL EXPERIENCE IN COUNTERING SYNTHETIC OPIOIDS AS A TOOL FOR ASSESSING U.S. MEASURES DURING THE FOURTH WAVE OF THE OPIOID CRISIS

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

*This article examines the proliferation of synthetic opioids and the transformation of the opioid crisis in the United States. International approaches to overdose prevention, addiction treatment, harm reduction, and early warning are analyzed. International experience is used to compare with American measures and identify evaluation criteria.*

***Key words:*** *opioid crisis, synthetic opioids, fentanyl, nitazenes, drug policy, harm reduction, United States, international experience*

**УДК 338.242.2; 338.242.4**
**ГРНТИ 06.52.35**

# РАНГОВЫЙ МЕТОД ВЫБОРА НАИЛУЧШЕГО ИНВЕСТИЦИОННОГО ПРОЕКТА

**В. И. Котов**

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

*Описана методика многокритериального выбора наилучшего инвестиционного проекта по показателям эффективности, окупаемости и степени рискованности вложений. Предложена компьютерная модель, позволяющая решить поставленную задачу ранговым методом и сравнить с решениями аддитивным методом, методом близости к наилучшему и макси-максным методом. В модели предусмотрена возможность учета субъективных предпочтений инвесторов с помощью соответствующих весовых коэффициентов.*

***инвестиционный проект, эффективность, окупаемость, риск, многокритериальный выбор, ранжирование***

## Постановка задачи

Имеется некоторая совокупность инвестиционных проектов, для каждого из которых рассчитаны прогнозные показатели эффективности, окупаемости финансовых вложений и степени их рискованности. Такими показателями могут быть [2, 3]:

1. NPV (Net Present Value) – чистая текущая стоимость проекта на горизонте планирования (тыс. руб.).

2. PI (Profitability Index) – индекс прибыльности инвестиций в проект на горизонте планирования (б/р).

3. ITS (Index Total Sensitivity)– индекс полной чувствительности проекта в пределах всего горизонта планирования, (б/р).

4. PbP (Payback Period) – срок окупаемости инвестиций в проект с учетом дисконтирования (в периодах).

5. I (Investment) – объем инвестиций в проект (тыс. руб.).

По первым двум показателям можно утверждать, что чем больше каждый из них, тем лучше проект при прочих равных условиях. Для оставшихся трех показателей, чем меньше каждый из них, тем лучше проект при прочих равных условиях. Как показывает практика, среди множества проектов практически не бывает проекта, который бы доминировал над остальными по всем этим показателям. Таким образом приходится иметь дело с сово-

купностью противоречивых показателей как критериев оценки проектов. Например, чем больше требуется получить NPV тем, как правило, больше требуется объем инвестиций и при этом будет больше степень рискованности проекта.

Сравнивая проекты между собой, при выборе наилучшего среди них инвестору необходимо принять решение на основе компромисса между прибыльностью, объемом необходимых инвестиций, окупаемостью и рискованностью.

Кроме того, у инвестора могут быть свои субъективные предпочтения о степени значимости каждого из перечисленных критериев. При сравнении проектов между собой эти предпочтения можно учесть с помощью соответствующих весовых коэффициентов для каждого критерия. Таким образом, мы имеем дело с классической задачей многокритериального выбора (МКВ) [1, 4, 5]. Рассмотрим возможный алгоритм МКВ.

## Алгоритм многокритериального выбора

Составляем исходную матрицу вариантов проектов, каждый из которых характеризуется набором из 5-ти показателей, как видно на рисунке 1.

| № варианта ( *i* ) | В колонке *B* название проекта | Критерии *( j )* | *NPV* | *PI* | Индекс риска *(ITS)* | Срок окупаемости *(PbP)* | Объем инвестиций *I* | |
|---|---|---|---|---|---|---|---|---|
| | | Ед. измерения | тыс. руб. | б/р | б/р | период | тыс. руб. | |
| | | *j* = | *1* | *2* | *3* | *4* | *5* | |
| | В колонке "C" автор проекта | *Влияние критерия:* | *a=+1 если РОСТ значения критерия ведет к УВЕЛИЧЕНИЮ интегральной оценки варианта* | | | | | |
| | | | *a=-1 если РОСТ значения критерия ведет к СНИЖЕНИЮ интегральной оценки варианта* | | | | | |
| | | *α* = | *1* | *1* | *-1* | *-1* | *-1* | Сумма баллов |
| | | Значимость критерия по экспетным оценкам: | 5 | 3 | 4 | 1 | 2 | 15 |
| 1 | ИП 1 | | 7 000 | 2.0 | 1.000 | 4.0 | 5000 | |
| 2 | ИП 2 | | 8 800 | 3.0 | 3.000 | 8.0 | 2000 | |
| 3 | ИП 3 | | 8 000 | 4.0 | 5.000 | 6.0 | 3000 | |
| 4 | ИП 4 | | 12 000 | 3.1 | 2.000 | 9.0 | 8000 | |
| 5 | ИП 5 | | 10 000 | 5.0 | 6.000 | 10.0 | 4000 | |
| 6 | ИП 6 | | 7 200 | 3.5 | 3.500 | 9.5 | 7000 | |
| 7 | ИП 7 | | 14 000 | 2.5 | 2.300 | 6.5 | 6000 | |
| 8 | ИП 8 | | 9 000 | 3.2 | 3.700 | 7.0 | 4500 | |
| 9 | ИП 9 | | 10 500 | 3.3 | 3.800 | 11.0 | 8500 | |
| 10 | ИП 10 | | 11 000 | 3.4 | 5.100 | 13.0 | 6500 | |
| 11 | ИП 11 | | 5 000 | 2.8 | 1.500 | 5.0 | 4300 | |
| 12 | ИП 12 | | 9 500 | 3.6 | 3.700 | 7.2 | 2500 | |
| 13 | ИП 13 | | 8 100 | 4.5 | 4.500 | 6.1 | 3500 | |
| 14 | ИП 14 | | 10 000 | 3.9 | 1.600 | 10.3 | 7500 | |
| 15 | ИП 15 | | 11 400 | 6.0 | 5.200 | 9.2 | 4600 | |
| 16 | ИП 16 | | 7 500 | 3.7 | 4.000 | 8.0 | 7600 | |
| 17 | ИП 17 | | 15 000 | 2.7 | 2.500 | 7.3 | 5500 | |
| 18 | ИП 18 | | 9 800 | 3.7 | 3.100 | 6.2 | 5200 | |
| 19 | ИП 19 | | 12 300 | 3.8 | 3.700 | 10.5 | 8100 | |
| 20 | ИП 20 | | 11 500 | 4.2 | 4.900 | 13.1 | 6600 | |

Рис. 1. Матрица исходных данных (см. лист «Модель»)

Из этих 20-ти вариантов необходимо выбрать один наилучший проект. Каждый критерий по-разному влияет на интегральную оценку варианта, поэтому необходимо согласовать эти различия. Так для критериев $j$ = 1, 2 (*NPV, PI*), ***рост*** которых приводит к ***росту*** интегральной оценки варианта, вводим индекс влияния $a$ =+1, а для критериев $j$ = 3, 4, 5 (*ITS, PbP, I*), ***рост*** которых приводит к ***снижению*** интегральной оценки варианта, вводим индекс влияния $a$ = -1.

Поскольку субъективная значимость каждого критерия для инвестора может быть различной, рассчитаем на основе бальных оценок весовые коэффициенты $W_j$, которые учитывают степень важности критерия для данного инвестора. Оценки критериев выставляем по следующей шкале:

$w_{jB}$ = (1 – самый незначимый, … 5 – самый значимый),

причем оценки не должны повторяться. Далее по этим бальным оценкам с помощью (1) рассчитываем весовые коэффициенты так, чтобы сумма всех весов равнялась единице (или 100 %):

$$W_j = \frac{w_{jB}}{\sum_{j=1}^{n} w_{jB}} \le 1 \qquad (1)$$

Весовые коэффициенты могут быть рассчитаны методом парных сравнений каждого критерия с каждым как показано в [2, 3]. При числе одновременно оцениваемых критериев более 3-х для определения весовых коэффициентов лучше использовать метод парных сравнений, т.к. субъективные оценки инвестора в этом случае будут более адекватными, чем в случае прямых бальных оценок (1).

Для каждого метода определения весовых коэффициентов производим ранжирование по каждому критерию отдельно в соответствующих листах модели.

## Ранговый метод МКВ

– Ранжируем исходную таблицу (рис. 1) по ***убыванию*** данных поочередно для первых двух критериев: *NPV, PI.* Нумеруем проекты от 1-го (***наибольшее*** значение критерия) до 20-го (***наименьшее*** значение). Здесь чем больше окажется номер проекта (ранг), тем хуже вариант. Копируем полученные ранги в колонку «*C*» соответствующего листа модели.
– Ранжируем исходную таблицу (рис. 1) по ***возрастанию*** данных поочередно для каждого из оставшихся критериев: *ITS, PbP, I.* Нумеруем про-

екты от 1-го (***наименьшее*** значение критерия) до 20-го (***наибольшее*** значение). Здесь чем больше номер проекта (ранг), тем хуже вариант. Копируем полученные ранги в колонку «*C*» соответствующего листа модели.

– Находим сумму рангов по всем 5-ти критериям для каждого варианта проекта без учета весов критериев.
– Находим сумму рангов по всем 5-ти критериям для каждого варианта проекта с учетом весов критериев.
– Определяем победителя (ранговый выбор) по минимальной сумме взвешенных рангов по всем критериям.

Этот метод не требует нормирования исходных данных о проектах. На рисунке 2 показана итоговая таблица обработки результатов ранжирования по всем критериям.

| **Ранги по всем критериям** | | *Веса по экспертным оценкам* | *33.3%* | *20.0%* | *26.7%* | *6.7%* | *13.3%* | 100% | 0 | Экспертные оценки значимости критерия по 5-ти бальной шкале | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | *Веса на основе МПС* | *30.0%* | *20.0%* | *20.0%* | *10.0%* | *20.0%* | 100% | | | |
| | | | **Количество вариантов:** | | 20 | | | | | | |
| | *В колонке B название проекта* | *Критерии ( j )* | *NPV* | *PI* | *Индекс риска (ITS)* | *Срок окупаемости (PbP)* | *Объем инвестиций I* | | | | |
| | | **Ед. измерения** | тыс. руб. | б/р | б/р | период | тыс. руб. | | | | |
| | | *j =* | *1* | *2* | *3* | *4* | *5* | | | | |
| | | *Влияние критерия:* | *a=+1 если РОСТ значения критерия ведет к УВЕЛИЧЕНИЮ интегральной оценки варианта* | | | | | | | | |
| | | | *a=-1 если РОСТ значения критерия ведет к СНИЖЕНИЮ интегральной оценки варианта* | | | | | | | | |
| *№ варианта ( i )* | **В колонках от *D* до *H* ранги проектов БЕЗ весов** | *a =* | *1* | *1* | *-1* | *-1* | *-1* | | *Результаты обработки по всем критериям БЕЗ весов* | | *Результаты обработки по всем критериям С весами* |
| | | **Значимость критерия по экспетным оценкам:** | **5** | **3** | **4** | **1** | **2** | **Сумма рангов по всем критериям БЕЗ весов** | **Номер проекта-победителя БЕЗ весов** | **Взвешенная сумма рангов по всем критериям** | **Номер проекта-победителя С весами** |
| **1** | **ИП 1** | **Ранги** | 19 | 20 | 1 | 1 | 9 | 50 | | 11.867 | |
| **2** | **ИП 2** | **Ранги** | 14 | 16 | 7 | 10 | 1 | 48 | | 10.533 | |
| **3** | **ИП 3** | **Ранги** | 16 | 5 | 17 | 3 | 3 | 44 | | 11.467 | |
| **4** | **ИП 4** | **Ранги** | 4 | 15 | 4 | 12 | 18 | 53 | | 8.600 | |
| **5** | **ИП 5** | **Ранги** | 9 | 2 | 20 | 15 | 5 | 51 | | 10.400 | |
| **6** | **ИП 6** | **Ранги** | 18 | 11 | 9 | 14 | 15 | 67 | | 13.533 | |
| **7** | **ИП 7** | **Ранги** | 2 | 19 | 5 | 6 | 12 | 44 | | 7.800 | |
| **8** | **ИП 8** | **Ранги** | 13 | 14 | 10 | 7 | 7 | 51 | | 11.200 | |
| **9** | **ИП 9** | **Ранги** | 8 | 13 | 13 | 18 | 20 | 72 | | 12.600 | |
| **10** | **ИП 10** | **Ранги** | 7 | 12 | 18 | 19 | 13 | 69 | | 12.533 | |
| **11** | **ИП 11** | **Ранги** | 20 | 17 | 2 | 2 | 6 | 47 | | 11.533 | |
| **12** | **ИП 12** | **Ранги** | 12 | 10 | 11 | 8 | 2 | 43 | | 9.733 | |
| **13** | **ИП 13** | **Ранги** | 15 | 3 | 15 | 4 | 4 | 41 | **ИП 13** | 10.400 | |
| **14** | **ИП 14** | **Ранги** | 10 | 6 | 3 | 16 | 16 | 51 | | 8.533 | |
| **15** | **ИП 15** | **Ранги** | 6 | 1 | 19 | 13 | 8 | 47 | | 9.200 | |
| **16** | **ИП 16** | **Ранги** | 17 | 8 | 14 | 11 | 17 | 67 | | 14.000 | |
| **17** | **ИП 17** | **Ранги** | 1 | 18 | 6 | 9 | 11 | 45 | | 7.600 | **ИП 17** |
| **18** | **ИП 18** | **Ранги** | 11 | 9 | 8 | 5 | 10 | 43 | | 9.267 | |
| **19** | **ИП 19** | **Ранги** | 3 | 7 | 12 | 17 | 19 | 58 | | 9.267 | |
| **20** | **ИП 20** | **Ранги** | 5 | 4 | 16 | 20 | 14 | 59 | | 9.933 | |
| | | | | | | | | *Min:* | *41* | *Min:* | *7.600* |

Рис. 2. Результаты МКВ с помощью рангового метода (см. лист «Ранги по всем критериям)

Здесь приведены результаты МКВ без учета весовых коэффициентов и с учетом весовых коэффициентов на основе бальных оценок (экспертные оценки). Без учета весов наилучшим оказался проект ИП 13, а с учетом ве-

сов лучшим оказался проект ИП 17, причем при двух вариантах выбора весовых коэффициентов (бальные оценки и МПС).

**Заключение**

Для выбранного массива проектов с помощью рангового метода МКВ можно получить различные варианты наилучших проектов в зависимости от метода определения весовых коэффициентов. Окончательный выбор из наилучших вариантов можно сделать, привлекая дополнительную информацию об этих проектах с учетом предпочтений инвестора.

Для автоматизации расчетов была разработана компьютерная *EXCEL*-модель, которая позволяет анализировать и сравнивать между собой одновременно до 100 вариантов проектов. В нашей модели предусмотрена возможность расчета весовых коэффициентов значимости критериев как на основе непосредственного оценивания в баллах («0» в желтой клетке *D118* листа «*Model*»), так и с использованием метода парных сравнений («1» в желтой клетке *D118* листа «*Model*»). Описанная *EXCEL*-модель является универсальной так как в ней можно использовать любые известные критерии оценки проектов, включив их в модель. Кроме того, она позволяет проводить МКВ с помощью аддитивного метода, метода близости к наилучшему и максимаксного метода [2, 3]. Модель рассчитана на 100 вариантов проектов. С моделью можно ознакомиться по ссылке:

https://disk.yandex.ru/i/n4og11zDSOZWhg

Структура модели:

– Лист «Порядок работы с моделью» – инструкция.
– Лист «Теория». – описание методов МКВ и расчетные формулы.
– Лист «*Model*». – исходные данные о проектах и три метода МКВ.
– Лист «МПС». – матрица парных сравнений критериев.
– Лист «*NPV*» – ранжирование по критерию *NPV*.
– Лист «*PI*» – ранжирование по критерию *PI*.
– Лист «*ITS*» – ранжирование по критерию *ITS*.
– Лист «*PbP*» – ранжирование по критерию *PbP*.
– Лист «*I*» – ранжирование по критерию *I*.
– Лист «Ранги по всем критериям» – итоги МКВ по ранговому методу.
– Лист «Отчет».

На основе этой модели в СПбГУТ на кафедре Экономики данных ежегодно проводится конкурс студенческих курсовых бизнес-проектов. Исходные данные по критериям оценки проектов студенты получают из разрабо-

танных ими соответствующих бизнес-планов. Расчеты всех критериев оценки проектов проводятся на основе динамической модели Cash-Flow [2, 3].

**Список используемых источников**

1. Корнеенко В. П. Многокритериальное ранжирование и выбор в ранговых градациях объектов, измеренных в разнотипных шкалах / В. П. Корнеенко // Прикладная математика и вопросы управления. 2023 № 4 С. 55–69. DOI: 10.15593/2499-9873/2023.4.03.

2. Котов В. И., Калимуллина О. В., Егорова М. А. Динамическая модель денежных потоков – инструмент прогнозирования показателей эффективности, окупаемости и риска инвестиционных проектов. Журнал «Электросвязь», (9) 2025.

3. Котов В. И. Инвестиционные проекты. Риск-анализ и оценка эффективности. Учебное пособие для вузов / В. И. Котов. Санкт-Петербург: Лань, 2024. 180 с.

4. Микони С. В. Теория принятия управленческих решений / С. В. Микони. Санкт-Петербург: Лань, 2015, 448 с. Для бакалавров и магистров.

5. Пужаев А. В. Управленческие решения. СПб.: МБИ, 2004. 152 с.

## RANKING METHOD FOR SELECTING THE BEST INVESTMENT PROJECT

**Kotov V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*A methodology was proposed for multi-criteria selection of the best investment project in terms of efficiency, payback and degree of investment risk. A computer model is presented that allows you to solve the problem using the rank method and compare it with solutions using the additive method and the proximity to the best method.*

***Key words:*** *investment project, efficiency, payback, risk, multi-criteria choice*

**УДК 664:338.45**
**ГРНТИ 65.01.33**

# АНАЛИЗ ЭФФЕКТИВНОСТИ ПЕРЕХОДА НА ОТЕЧЕСТВЕННЫЕ ЦИФРОВЫЕ РЕШЕНИЯ В ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ

**В. В. Куликов, Р. А. Сметанин**

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

*В настоящей работе проанализированы результаты замены зарубежного программного обеспечения, используемого для управления производственными процессами и диспетчерского контроля и сбора данных, применяемых в пищевой промышленности (молочной и пивоваренной отрасли) и других отраслях перерабатывающей промышленности. Проведен анализ эффективности отечественных MES-платформ и SCADA-систем. Выявлены ключевые экономические и операционные эффекты, позволяющие снижать издержки простоя, сокращать потерь сырья, гарантировать качество продукции. Рассмотрены технические механизмы переходного периода, связанного с совместимостью протоколов, переносом архивов, обучением персонала. Детально проанализирован случай замещения на систему SYFORA и MEScase.*

***импортозамещение ПО, MES-системы, SCADA-системы, пищевая промышленность, управление производственными процессами***

Курс на импортозамещение в агропромышленном комплексе и перерабатывающей промышленности России активизировался после 2022 г. в связи с уходом западных вендоров программного обеспечения. В пищевой промышленности, особенно на высокоавтоматизированных пивоваренных и молочных заводах, критически важны системы управления производством (MES) и диспетчерского контроля (SCADA). Доступность и эффективность отечественных решений в этой сфере ранее оставались недостаточно изученными.

Таким образом, целью настоящего исследования является – оценка эффективности замещения зарубежных MES- и SCADA-систем на российские программные продукты (MEScase, SYFORA) в сегменте пивоваренных и молочных заводов, включая экономические и технические аспекты перехода.

*Объект исследования* – процессы импортозамещения промышленного программного обеспечения на высокоавтоматизированных предприятиях пищевой промышленности (на примере пивных и молочных заводов).

*Предмет исследования* – количественные и качественные показатели эффективности внедрения отечественных MES (MEScase) и SCADA (SYFORA) взамен зарубежных аналогов (WinCC, ProLeiT/Plant iT/brewmaxx, Siemens SIMATIC IT, Rockwell FactoryTalk. Aveva WW), включая сроки замещения, экономию от предотвращения простоев, масштаб внедрения и технические инструменты переноса данных.

Для достижения поставленных целей были решены следующие задачи:

1. Выявить данные о проектах замещения SCADA отечественного производства в секторе FMCG (с фокусом на пивные и молочные производства).

2. Проанализировать экономическую эффективность замены цифрового продукта через оценку издержек простоев промышленных предприятий.

3. Изучить эффективность внедрения MES-системы SYFORA на молочном комбинате (инвестиции, этапы, ожидаемые эффекты).

4. Проанализировать эффективность перехода на отечественное ПО и определить риски при переходе для пищевых заводов.

5. Сформулировать практические рекомендации для предприятий, планирующих импортозамещение MES и SCADA.

Уход зарубежных вендоров создал для предприятий пищевой промышленности критические риски: невозможность upgrade систем и продления лицензий, отсутствие технической поддержки, ограничения на масштабирование систем. В этих условиях переход на отечественные решения становится не только стратегической, но и экономической необходимостью.

## Анализ эффективности: SCADA-решения (SYFORA)

### Масштабный проект импортозамещения на заводах FMCG (включая пивные и молочные)

На встрече ведущих специалистов, занимающихся импортозамещением ПО, в апреле 2026 года, были представлены результаты перехода промышленных предприятий FMCG-сектора (товары повседневного спроса, куда входят пиво и молочная продукция) на отечественные SCADA-решения [1]. Ключевым стал проект замещения на семи производственных площадках. Масштаб внедрения:

– более 1 000 000 технологических тегов;
– около 1 000 промышленных контроллеров;
– свыше 2 600 операторских экранов;

– модернизировано 122 производственных участка.

Срок реализации проекта составил порядка 1,5 года. Ключевым техническим требованием было обеспечение **непрерывности производства** в процессе перехода. Переход выполнялся в параллельном режиме: старая и новая SCADA работали одновременно, а операторы в течение месяца использовали обе системы до полного отключения устаревшего решения. В рамках проекта была проведена оптимизация драйвера Ethernet/IP, позволившая достичь передачи порядка **40 000 тегов за 2 секунды** [1].

### Экономическое обоснование замещения SCADA

На том же встрече были приведены оценки экономических последствий простоев на промышленных предприятиях [1]:

– на небольших и средних предприятиях простой составляет почти 1 млн рублей в час;
– за сутки потери могут достигать до 17 млн рублей;
– на крупных производствах простой может составлять до 43 млн рублей в сутки.

Как отмечают специалисты, даже масштабные проекты перехода на SCADA отечественного производства оказываются экономически оправданными на фоне альтернативных издержек простоя производства в случае отказа зарубежных систем. Средний срок внедрения SCADA-системы, по оценкам спикеров, составляет около 3 месяцев для средних проектов и до 1 года для крупных внедрений [1].

Таким образом, для пивных и молочных заводов, где непрерывность технологических циклов критична, переход на отечественные SCADA(SYFORA) позволяет не только устранить санкционные риски, но и обеспечить положительный экономический эффект за счет предотвращения потенциальных простоев.

### Анализ эффективности: MES-решения (MEScase)

### Казанский молочный комбинат

ООО «Казанский молочный комбинат» (входит в ГК «Комос Групп») реализует масштабный проект по цифровой трансформации производства с внедрением «Создание цифровой экосистемы управления современным молочным производством» в т.ч. на базе российских платформ MEScase, SYFORA (разработчик – ГК «Солисофт») [2, 3].

*Инвестиции и государственная поддержка.* На реализацию проекта предприятие получило грант Российского фонда развития информационных технологий (РФРИТ) в размере **108,8** млн рублей [2]. Общий объем инвестиций в цифровизацию предприятия превышает 226,3 млн рублей [2]. Проект по внедрению «Создание цифровой экосистемы управления современным молочным производством» включен в реестр особо значимых решений в рамках нацпроекта «Экономика данных и цифровая трансформация государства» [3].

*Ожидаемые эффекты.* Интеграция SYFORA [4] (управление всеми технологическими процессами) и MEScase (обработка производственных данных, анализ, отчетность, контроль качества) обеспечит автоматический контроль процессов, сбор и анализ производственных данных в реальном времени, а также оперативное реагирование на отклонения. Заявленные цели:

– повышение прозрачности и управляемости всех этапов технологического цикла – от приемки сырья до отгрузки готовой продукции;
– сокращение производственных потерь;
– снижение ошибок планирования;

увеличение прозрачности текущих процессов для оперативного влияния на них.

*Статус реализации.* По состоянию на январь 2026 года Казанский молочный комбинат завершил второй этап проекта («Написание функциональных требований») [2]. Подготовлены детальные бизнес-требования к SYFORA и функциональные требования к MEScase. Параллельно подрядная организация приступила к третьему этапу – «Разработка частного технического задания», который рассчитан на период с января по сентябрь 2026 года [2]. Разработанные подходы и инструменты планируется в дальнейшем растиражировать на другие предприятия молочного субхолдинга [2].

## Технические инструменты замещения с ProLeiT (Plant iT / brewmaxx) на SYFORA

После ухода компании Schneider Electric (владельца ProLeiT) и прекращения технической поддержки предприятия, использующие Plant iT и отраслевой пакет brewmaxx, оказались перед необходимостью поиска альтернативных решений для управления производством.

Российская группа компаний «SOLISOFT» предлагает, как альтернативу российский продукт SYFORA. В версии SYFORA 2.2, анонсированной

в 2025 году, разработчики предусмотрели инструменты для перехода с минимальным временем простоя [5]:

– ядро системы, совместимое с Plant iT – алгоритмы работы технологического оборудования не меняются и функционируют как в Plant iT/brewmaxx [5];
– импорт/экспорт через Microsoft Excel – наборы параметров, рецепты, шаговые последовательности мигрируют по принципу «1 к 1» для версий Plant iT 7 и выше [5];
– расширенная библиотека классов – добавлены классы, идентичные по функционалу классам Plant iT/brewmaxx, что позволяет технологам работать с привычным функционалом системы [5].

Данные технические возможности обеспечивают минимизацию ручного перепрограммирования и снижают риски сбоев, связанных с миграцией, что особенно важно для пивоваренных и молочных заводов с длительными рецептурными циклами.

## Ключевые факторы успеха и зоны риска (аналитическое обобщение)

### Факторы, обеспечивающие эффективность перехода

1. Государственная поддержка. Наличие грантов (в рассмотренном случае – 108,8 млн рублей от РФРИТ) позволяет предприятиям существенно снизить финансовую нагрузку первого этапа цифровой трансформации [2].

2. Специализированные инструменты замены ПО. Проведен сравнительный анализ отечественных и зарубежных систем, который показал эффективность данной замены, в виде сокращения трудозатрат на перепрограммирование и снижение риска остановки производства [5].

3. Параллельный режим перехода. Возможность одновременной работы старой и новой SCADA, позволяет сохранить непрерывность производства [1].

4. Жесткий контроль экономики простоев. Понимание фактических издержек (до 43 млн руб./сутки на крупных производствах) делает замену экономически оправданной [1].

### Зоны риска и ограничения

1. Перенос архивов. Полный перенос многолетних исторических данных занимает значительное время.

2. Необходимость доработок под нестандартное оборудование. Несмотря на поддержку основных протоколов (ModbusTCP, OPC, Ethernet/IP), отдельные виды оборудования могут требовать индивидуальной настройки.

## Заключение

Таким образом, полученные предварительные результаты по импортозамещению на отечественное ПО показали экономическую эффективность и минимизируют риски остановки производства:

1. SCADA-решения показали измеримую экономическую эффективность. Проект перехода на 7 заводах FMCG (более 1 млн тегов, 1000 контроллеров, 2600 экранов), среди которых есть пивные и молочные предприятия, продемонстрировал технологическую возможность масштабного перехода с сохранением непрерывности производства. Оценки издержек простоя (до 43 млн руб./сутки на крупных производствах) позволяют количественно обосновать целесообразность замены зарубежных систем [1].

2. MES-решения на базе MEScase находятся в стадии активного внедрения с государственной поддержкой. Проект Казанского молочного комбината (грант 108,8 млн рублей, включение в реестр особо значимых проектов) демонстрирует высокий приоритет и ресурсное обеспечение цифровой трансформации молочной отрасли [2, 3].

3. Технический переход с зарубежных систем реализуема. Наличие плагина совместимости SYFORA 2.2 с Plant iT/brewmaxx, импорта через Excel и расширенной библиотеки классов позволяет предприятиям, использующим ProLeiT, осуществлять переход без изменения алгоритмов работы оборудования [5].

4. Экономическая эффективность перехода подтверждается не только прямыми эффектами, но и предотвращением потерь. С учетом рисков невозможности продления лицензий и отсутствия техподдержки зарубежных вендоров, даже значительные инвестиции в отечественные MES и SCADA обеспечивают более высокую предсказуемость и управляемость производственных процессов на пивных и молочных заводах.

**Список использованных источников**

1. В России обсудили переходы предприятий на российские SCADA-системы // РБК Компании. 2026. URL: https://companies.rbc.ru/news/TsjeLnJ6PU/v-rossii-obsudili-perehod-predpriyatij-fmcg-na-rossijskie-scada-sistemyi/ (дата обращения: 27.04.2026)

2. «Казанский молочный комбинат» завершил второй этап проекта по цифровой трансформации производства // Комос Групп. 2026. URL: https://komos.ru/press-center/news/33155/#up (дата обращения: 27.04.2026).

3. Компания «Солисофт групп» является участником программы по созданию цифровой экосистемы управления современным молочным производством в АО «Милком» // MilkLife. 2025. URL: https://milklife.ru/company_news/14020.html (дата обращения: 27.04.2026).

4. Softysol. Syfora: программная платформа нового поколения для разработки и внедрения АСУ ТП. URL: https://www.softysol.com/ru/syfora (дата обращения: 27.04.2026).

5. SYFORA 2.2: новое решение для импортозамещения АСУ ТП на пищевых предприятиях // Sfera.fm. 2025. URL: https://sfera.fm/articles/mzhi/syfora-22-novoe-resheniedlya-importozameshcheniya-asutp-na-pishchevykh-predpriyatiyakh (дата обращения: 27.04.2026).

## ANALYSIS OF THE EFFECTIVENESS OF SWITCHING TO DOMESTIC DIGITAL SOLUTIONS IN THE FOOD INDUSTRY

**Kulikov V., Smetanin R.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper analyzes the results of the replacement of foreign software used for production process control and dispatching control and data collection used in the food industry (dairy and brewing industries) and other processing industries. The effectiveness of domestic MES platforms and SCADA systems has been analyzed. The key economic and operational effects have been identified, allowing to reduce downtime costs, reduce losses of raw materials, and guarantee product quality. The technical mechanisms of the transition period related to protocol compatibility, archive transfer, and staff training are considered. The case of substitution for the SYFORA and MEScas systems is analyzed in detail.*

***Key words:*** *software import substitution, MES systems, SCADA systems, food industry, production process management*

**УДК 55**
**ГРНТИ 87.01**

# АНАЛИЗ БИОЛОГИЧЕСКОГО РАЗНООБРАЗИЯ В УСЛОВИЯХ РАЗВИВАЮЩЕЙСЯ ГОРОДСКОЙ ЗАСТРОЙКИ СЫКТЫВКАРА С ПРИМЕНЕНИЕМ ГИС

**А. Н. Логиновская, В. А. Ожегов**

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

*В работе представлены результаты исследования биологического разнообразия в условиях развития территорий, занимаемых застройкой в Сыктывкаре с применением геоинформационных систем. Было выявлено снижение разнообразия растений на местах недавнего проведения застройки. Сбор материалов космической съемки осуществлялся в разные временные периоды с учетом возможностей спутников Landsat-5, Landsat-7, Landsat-8. Анализ выявил уменьшение площадей зеленых территории города, что является следствием увеличения городской застройки и приводит к потере качества биологического разнообразия.*

***г. Сыктывкар, ГИС, застройка, зеленые территории, космическая съемка***

Активный рост городов воздействует на биоразнообразие и природу. Современная городская застройки не всегда учитывает сохранение зеленых пространств. Биоразнообразие – важнейший показатель качества окружающей природной среды, который указывает на экологическую целостность и функциональность экосистемы. Данный показатель необходимо учитывать при плановой застройке города, именно биоразнообразие указывает на экологическое качество территории [1, 2].

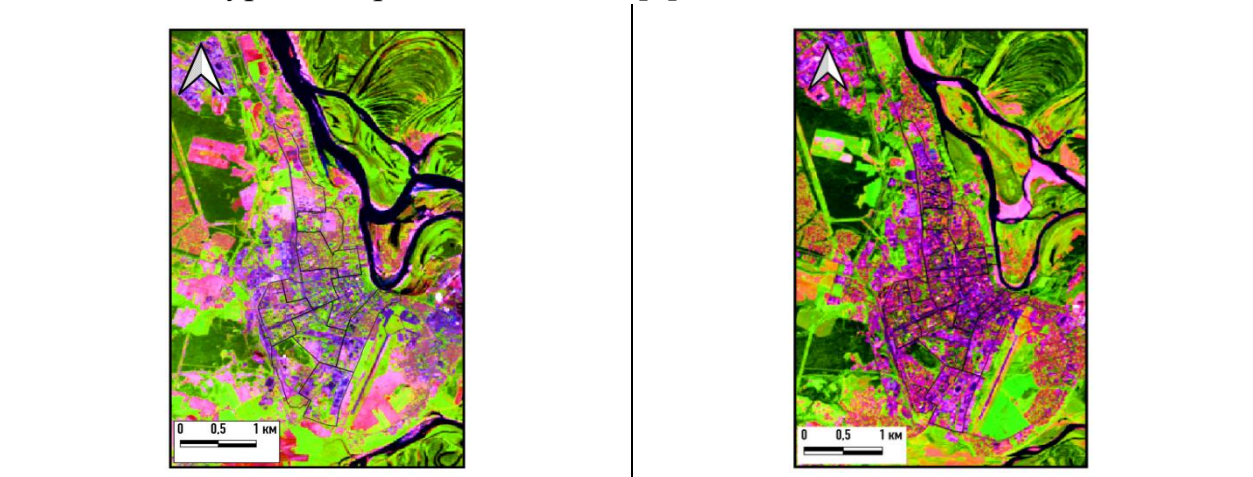
Исследование динамики городской застройки эффективно осуществляется посредством анализа многолетних космических снимков, интегрированных в регулярную пространственную сетку. Данный подход обеспечивает простоту анализа и визуализации полученных данных [2, 3]. Для исследования биологического разнообразия в условиях развития территорий были собраны данные о застройке города Сыктывкара за 39 лет (1986 – 2025 г.). Анализ космических снимков проводился с шагом в 4 года.

При заполнении регулярной сетки исследуемую территорию поделили на застройку и зеленые участки. Зеленые участки определяются как естественные, не сильно нарушенные или полностью искусственно созданные ландшафты. При этом, прибрежные территории, парковые зоны, насаждения вдоль дорог не считаются естественными. Естественные экосистемы в пределах парковых зон, где преобладают местные виды, включаются

в анализ. Сингапурский индекс на практике так же учитывает «восстановленные экосистемы» и «озелененные территории» [3]. Основой регулярной сетки послужила территория г. Сыктывкара, которая включает в себя 10 жилых кварталов.

Для изучения изменений в городской застройке были задействованы спутниковые снимки с аппаратов Landsat-5, Landsat-7 и Landsat-8. Эти данные, обладающие пространственным разрешением 30х30 м/пиксель и включающие мультиспектральные каналы [4], послужили основой для определения размера ячейки регулярной сетки, также составляющей 30х30 метров.

Для получения подробных результатов были выбраны каналы: 3 канал (Green), 4 канал (Red) и 5 канал (Near Infrared). Каналы 3 и 4 охватывают видимый спектр, а канал 5, измеряющий ближний инфракрасный диапазон, особенно ценен для экологических исследований благодаря сильному отражению от листвы растений. Анализ проводился с использованием стандартной комбинации 5-4-3, известной как "искусственные цвета". На карте (Рис. 1) растительность отображается зеленым, городские районы – фиолетовым, а почва – от темно- до светло-коричневого. Хвойные леса выглядят темнее, чем лиственные. Эта популярная комбинация каналов широко применяется для оценки состояния растительности и, в последнее время, для изучения изменений в урбанизированных зонах [4].



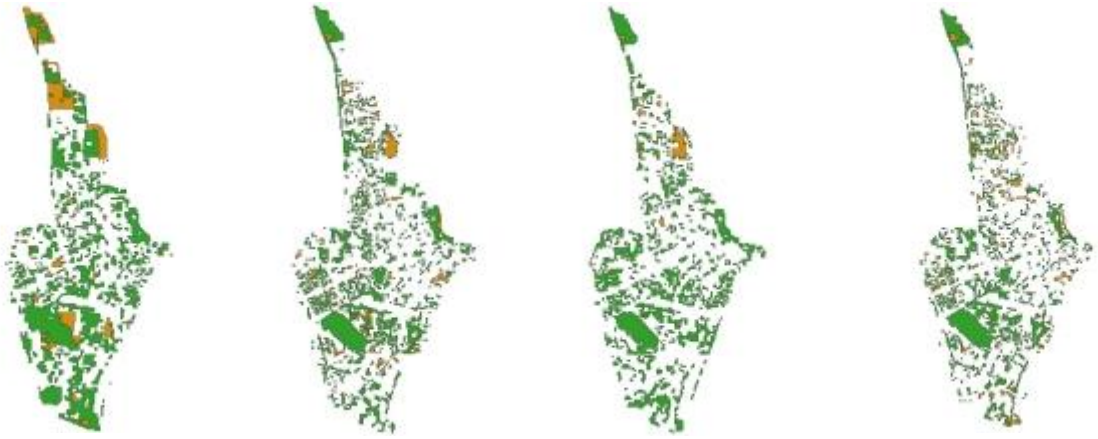

*а* *б*

Рис. 1. Беличий парк и Центральное городское кладбище г. Сыктывкар:
*а* – снимок спутника Landsat-5 (комбинация каналов 5-4-3) (1986 год);
*б* – снимок спутника Landsat-9 (комбинация каналов 6-5-4) (2025 год)

Анализ космических снимков и последующее построение регулярной сетки позволили провести количественную оценку площадей, занятых застройкой и зелеными территориями. При заполнении ячеек сетки применялся принцип однозначности: учитывались только те участки, где домини-

ровал один тип покрытия (застройка или растительность). Территории с минимальным или отсутствующим растительным покровом, ввиду сложности их разделения, были интегрированы в категорию зеленых зон города.

Анализ данных за рассмотренный период выявил устойчивую тенденцию к уменьшению площади озелененных территорий, что коррелирует с непрерывным процессом урбанизации и расширением застройки. Наиболее значительные трансформации земельного покрова зафиксированы в интервале 1986-1990 гг., когда прирост застроенной территории составил 97,9 га. Аналогичные, хотя и менее выраженные, изменения наблюдались в периоды 2006-2010 гг. (+23,1 га) и 2018-2025 гг. (+36,9 га). Визуализация полученных результатов представлена в виде отдельного слоя сетки на карте (рис. 2), где зеленый цвет маркирует участки с растительным покровом, а светло-коричневый – прилегающие к ним почвенные участки.



а б в г

Рис. 2.Результат заполнения регулярной сетки: *а* – 1986 год; *б* – 1998 год; в – 2010 год; *г* – 2026 год.

Урбанизация Сыктывкара сопровождается сокращением площади растительного покрова и озелененных пространств. Тем не менее, в отдельных зонах города, преимущественно в районах застройки 1960-1980 годов, зафиксировано увеличение доли озелененных территорий. Данное явление обусловлено естественным ростом древесных насаждений, высаженных в период после завершения строительства. Необходимо отметить, что скорость трансформации Сыктывкара создает риски для природного разнообразия, требующие особого контроля и использования инструментов городского планирования.

Одной из первых и самых главных задач исследования было определить участки разного возраста застройки для проведения видового описания (Рис. 3). За фоновый участок взят сквер по улице Димитрова (ныне Беличий парк) – единственное место в городе, где сохранился нетронутый лесной участок. Район железнодорожного вокзала г. Сыктывкар вместе с домами по улице Коммунистической были застроены чуть более 50 лет назад, взятый на описание участок расположен в одном из дворов по ул. Коммунистическая, 80, стоит отметить, что на данном участке летом не производятся работы по благоустройству, не косят траву и не спиливают сухие ветки деревьев. Следующий участок проведения ботанического описания расположен на улице Давпонская, 110, начало застройки которого производилось около 35 лет назад, на данной территории на момент проведения описания еще не проводились работы управляющей компании по покосу травы. Участок, расположенный в районе Орбита по улице Малышева, 25, был застроен около 15 лет назад, на момент проведения описания его также удалось застать нетронутым. Последние участки, взятые на описание, расположены в районе ЖК Атлантида, первый участок находится по адресу проспект Октябрьский, 208, застройка завершилась в 2020 году, второй участок расположен по адресу проспект Октябрьский, 218, застройка завершилась в 2022 году, оба участка находятся под постоянным присмотром управляющей компании.

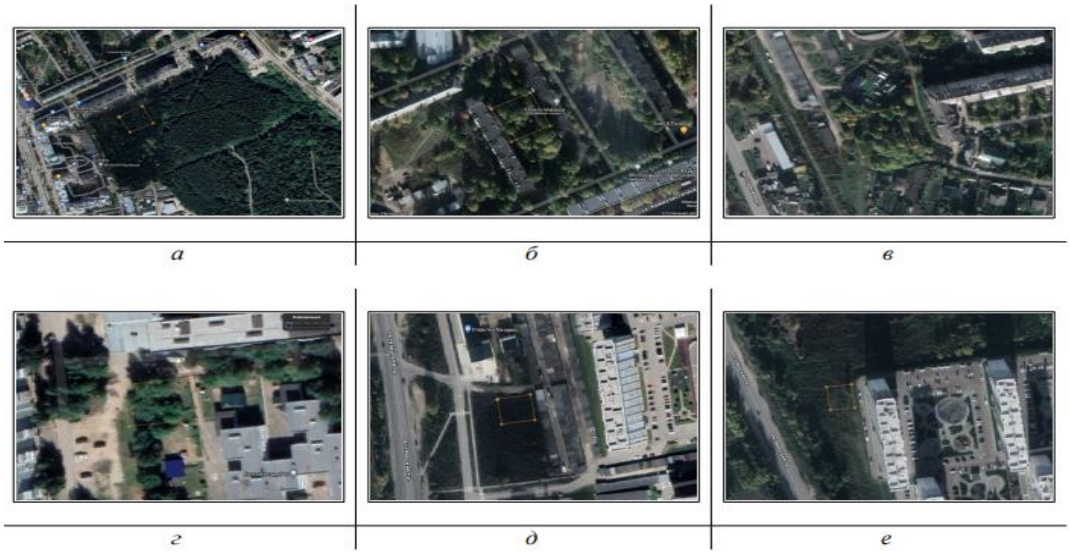



Рис. 3. Участки проведения ботанического описания (снимки Google Satellite Hybryd):

*а* – Беличий парк по ул. Димитрова (фоновый участок); *б* – участок описания на ул.Коммунистическая, 80; в – участок описания на ул. Давпонская, 110; *г* – участок описания на ул.Малышева, 18; *д* – участок описания на ул. проспект Октябрьский, 208; *е* – участок описания на ул.проспект Октябрьский, 218

Исследование биоразнообразия с использованием математических методов включает в себя анализ видового состава сообществ с помощью статистических индексов, рассчитанных на основе данных о количестве видов (S) и их обилии (N). В среде R были посчитаны индексы альфа-разнообразия: индексы Шеннона (характеризует разнообразие и выравненность сообщества) и Пиелу (мера выравненности индекса Шеннона, показывает насколько сообщество выравнено вдоль рассматриваемого градиента среды), оценка достоверности различий между значениями индекса Шеннона для двух сообществ вычислялась с помощью критерия Стьюдента [5]. Индексы бета-разнообразия: индексы Жаккара (показатель сходства между двумя площадками, сходство видов будем считать абсолютным при индексе, равном 1, сильным, если значение принимает вид от 0.75 до 1, средним – от 0.5 до 0.75, слабым – от 0.25 до 0.5, отсутствующим, если индекс был меньше 0.25, при нулевом значении площадки считаем абсолютно различными) и Коха (общая степень сходства некоторого числа видовых списков).

Далее, по полученным данным распределения растений, в среде R был посчитан индекс Шеннона и мера его выравненности (Индекс Пиелу). Выбор этой пары индексов связан как с тем, что они достаточно известны отечественным ботаникам, так и с тем, что здесь возможна оценка степени достоверности проводимых сравнений (достоверность различий была проверена через критерий Стьюдента).

Полученные значения по индексу Шеннона отражают обеднение разнообразия раннее определенных экологических групп растений в сторону недавнего проведения застройки. Индекс Пиелу отражает плохо выравненные сообщества на участке описания по улице проспект Октябрьский, 208 и на участке по ул. проспект Октябрьский, 218. Схожим значением индекса Шеннона и его меры выравненности обладают фоновый участок по ул. Димитрова и участок описания по ул. Коммунистическая, 80, при сравнении достоверности различия участков критерий Стьюдента не переходит пороговое значение. Можно предположить, что участок, застроенный более 50 лет назад, приблизился к исходному состоянию видового разнообразия. Также в рамках исследования была проведена ординация методом главных компонент в полях двух признаков – на основе значений индекса Шеннона (таблица 1) и меры его выравненности.

ТАБЛИЦА 1 Индекс Шеннона (I_Sh) и мера его выравненности (E_Sh)

| | а | б | в | г | д | е |
|---|---|---|---|---|---|---|
| I_Sh | 2,27 | 2,22 | 1,98 | 1,86 | 1,38 | 1,03 |
| E_Sh | 0,88 | 0,86 | 0,89 | 0,87 | 0,57 | 0,66 |
| var_I | 0,0015 | 0,0013 | 0,0011 | 0,0012 | 0,0013 | 0,0013 |
| m_I | 0,0001 | 0,0001 | 0,0001 | 0,0001 | 0,0001 | 0,0001 |

где: *а* – Беличий парк по ул. Димитрова (фоновый участок); *б* – участок описания на ул. Коммунистическая, 80; в – участок описания на ул. Давпонская, 110; *г* – участок описания на ул. Малышева, 18; *д* – участок описания на ул. проспект Октябрьский, 208; *е* – участок описания на ул. проспект Октябрьский, 218.

Дифференцирующее разнообразие было рассчитано для взятых на описание площадок через индекс Коха. Для попарных сравнений взяты индексы Жаккара (таблица 2). Сходство видов будем считать абсолютным при индексе, равном 1, сильным, если значение принимает вид от 0.75 до 1, средним – от 0.5 до 0.75, слабым – от 0.25 до 0.5, отсутствующим, если индекс был меньше 0.25, при нулевом значении площадки считаем абсолютно различными [5]. Обобщенным индексом для сравнения нескольких площадок является индекс биотической дисперсии Коха, который в стандартной форме используется как индекс сходства. В данном случае индекс принимает крайне низкое значение 0.07, что означает высокое видовое разнообразие территории.

ТАБЛИЦА 2 Индекс Жаккара (I_J)

| V_I_J | *а* | *б* | *в* | *г* | *д* | *е* |
|---|---|---|---|---|---|---|
| *а* | 1.00 | 0.60 | 0.39 | 0.34 | 0.24 | 0.21 |
| *б* | 0.60 | 1.00 | 0.43 | 0.42 | 0.38 | 0.12 |
| *в* | 0.39 | 0.43 | 1.00 | 0.48 | 0.47 | 0.12 |
| *г* | 0.34 | 0.42 | 0.48 | 1.00 | 0.54 | 0.17 |
| *д* | 0.24 | 0.38 | 0.47 | 0.54 | 1.00 | 0.15 |
| *е* | 0.21 | 0.12 | 0.12 | 0.17 | 0.15 | 1.00 |

где: *а* – Беличий парк по ул. Димитрова (фоновый участок); *б* – участок описания на ул. Коммунистическая, 80; в – участок описания на ул. Давпонская, 110; *г* – участок описания на ул. Малышева, 18; *д* – участок описания на ул. проспект Октябрьский, 208; *е* – участок описания на ул. проспект Октябрьский, 218.

Варьирование попарных отличий здесь происходит в широком диапазоне от 0.12, что означает отсутствующее сходство (сравнивались участок описания по ул. Коммунистическая, 80 и участок описания по ул. проспект Октябрьский, 218) до 0.60, число которое означает среднее сходство (срав-

нивались участок описания по ул. Димитрова и участок описания по ул. Коммунистическая, 80), такое сходство может быть вызвано непосредственной близостью участков описания.

Исследование биологического разнообразия при помощи важнейших индексов альфа- и бета-разнообразия показало снижение разнообразия растений на местах недавнего проведения застройки. Такие значения рассматриваемых индексов могут быть связаны с выявленными раннее необратимыми изменениям, которым подвергаются участки в процессе застройки. Напротив, стоит отметить, что участок старой застройки по своим показателям важнейших индексов приближен к показателям фонового участка, на котором не происходила застройка.

**Список используемых источников**

1. Барталев С. А., Егоров В. А., Жарко В. О., Лулян Е. А., Плотников Д. Е., Хвостиков С. А., Шабанов Н. В. Спутниковое картографирование растительного покрова России. М.: ИКИ РАН, 2016. 208 с.

2. Подольская Е. С. , Ершов Д. В., Ковганко К. А. Метод определения размера ячейки регулярной сети для инфраструктурного зонирования территории с целью охраны лесов от пожаров. М.: Центр по проблемам экологии и продуктивности лесов РАН, 2023. № Т. 6. № 2.. С.149-162.

3. Chan, L., O. Hillel, T. Elmqvist, P. Werner, N. Holman, A. Mader, E. Calaterra. User's Manual on the Singapore Index on Cities' Biodiversity (also known as the City Biodiversity Index). Singapore, 2014. URL: https://www.cbd.int/authorities/doc/Singapore-Index-User-Manual-20140730-en.pdf (дата обращения: 21.10.2025).

4. Keeler, B. L., P. Hamel, T. McPhearson, M. H. Hamann, M. L. Donahue, K. A. Meza Prado, K. K. Arkema, et al. "Social-Ecological and Technological Factors Moderate the Value of Urban Nature". 2019. Nature Sustainability 2 (1): 29–38. https://DOI.org/10.1038/s41893-018-0202-1 (дата обращения: 21.10.2025).

5. Мэгарран Э. Экологическое разнообразие и его измерение. М.: Мир, 1992. 181 с.

## ANALYSIS OF BIODIVERSITY IN THE CONTEXT OF DEVELOPING URBAN AREAS IN SYKTYVKAR USING GIS

**Loginovskaya A., Ozhegov V.**
The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

*This paper presents the results of a study of biodiversity in Syktyvkar's newly developed areas using geographic information systems. A decrease in plant diversity was identified in areas of recent development. Satellite imagery was collected over various time periods, taking into account the capabilities of the Landsat-5, Landsat-7, and Landsat-8 satellites. The analysis revealed a decrease in the city's green space, a consequence of increased urban development and a loss of biodiversity.*

***Key words:*** *Syktyvkar, GIS, development, green spaces, satellite imagery*

**УДК 338.1**
**ГРНТИ 06.54.51**

# МЕТОДИЧЕСКИЕ ОСНОВЫ МУЛЬТИФАКТОРНОГО АНАЛИЗА ПРИВЛЕКАТЕЛЬНОСТИ ВЕРТИКАЛЕЙ ЦИФРОВЫХ ЭКОСИСТЕМ

**В. В. Макаров, А. С. Михайлова, А. С. Шишкова**

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

*Для обеспечения конкурентоспособности цифровых экосистем необходимо использовать экономически обоснованный подход к выбору вертикалей их присутствия и развития в зависимости от потенциальной прибыльности, перспектив роста и сопутствующих рисков. Комплексный всесторонний анализ различных аспектов деятельности цифровых экосистем позволяет сформировать основания для принятия стратегических решений о целесообразных направлениях развития компании в среднесрочной и долгосрочной перспективе. В статье представлено авторское определение цифровой экосистемы, вертикали цифровой экосистемы, этапы мультифакторного анализа привлекательности вертикалей цифровых экосистем и их содержание.*

***цифровая платформа, цифровая экосистема, вертикаль цифровой экосистемы, Gap Analysis, стратегия фокусирования, стратегия диверсификации***

В условиях современной экономики экосистемный бизнес-подход приобретает все большее распространение, становясь драйвером роста компаний и расширения сфер их деятельности. Возможность комплексного удовлетворения потребностей клиента в едином бесшовном процессе на основе применения цифровых технологий дает огромные преимущества, связанные как со снижением издержек, а значит повышением рентабельности деятельности, так и с повышением лояльности потребителей, а значит перспективами дополнительного дохода. Рынок цифровых экосистем характеризуется высокой степенью конкуренции, особый характер которой предопределен лежащими в их основе цифровыми платформами, представляющими собой по своей сути многосторонние рынки. Повышение конкурентоспособности цифровых экосистем в высоко конкурентной и динамично изменяющейся среде может быть обеспечено за счет использования экономически обоснованного подхода к выбору вертикалей присутствия на основе комплексного анализа факторов, определяющих потенциала роста доходности цифровых

экосистем с учетом сопутствующих рисков. Этим определяется актуальность темы исследования.

Под цифровой платформой в рамках проводимого исследования понимается реализованный с помощью информационных технологий сервис взаимовыгодного взаимодействия экономических агентов нескольких типов, в процессе которого происходит обмен информацией (цифровыми сервисами), продуктами, услугами.

Цифровая система в этом контексте представляет собой интегрированную структуру различных цифровых участников, цепочек создания стоимости и деловых отношений, построенную на базе цифровой платформы, связанной с другими цифровыми платформами и /или цифровыми сервисами одной компании или группы компаний-партнеров, осуществляющую свою деятельность на нескольких отраслевых рынках путем предоставления совокупности сервисов [1].

Причиной существенного роста экосистемных компаний по сравнению с традиционными структурами лежит их способность быстро реагировать на рыночные, технологические, политические изменения, то есть эффективно адаптироваться к происходящим во внешней среде изменениям, сохраняя необходимую гибкость в принятии внутренних управленческих решений, но при этом оставаясь верными миссии компании, ее целям и задачам [2].

Российский рынок цифровых экосистем стремительно развивается на протяжении последних пяти лет [3], эта тенденция сохраняется и количество экосистемных компаний постоянно растет. На сегодняшний день на различных отраслевых рынках, таких как e-commerce, рынок доставки, развлекательные сервисы, финтех, рынок AI, путешествия, такси и др. присутствует более десяти конкурирующих между собой российских цифровых экосистем. Ключевыми участниками рынка цифровых экосистем в России являются Сбер, VK, Яндекс, Т-Банк, МТС, Wildberries, Ozon, ВТБ, Мегафон и др.

Изначально развитие экосистемных компаний происходило в основных для них отраслях, однако на определенном этапе развития формируется готовность к выходу за пределы привычных отраслевых сегментов и развитию в новых для себя отраслях, иначе называемых вертикалями цифровых экосистем. Вертикали экосистемы – это отдельные отраслевые направления, вокруг которых строится развитие экосистемы. Каждая вертикаль сфокусирована на определенном «основном» виде деятельности и кроме того, вклю-

чает специализированные сервисы его дополняющие. Связь между элементами цифровых платформ и экосистем внутри вертикали и между вертикалями обеспечивается за счет единого ID, сервисов подписок, программ лояльности, цифровых ассистентов. Динамика развития крупнейших российских цифровых экосистем отражена на рис. 1.

Очевидно, что крупнейшие российские цифровые экосистемы ведут свою деятельность практически во всех ключевых вертикалях, концентрируясь на основной вертикали и постепенно расширяя присутствие в новых для себя вертикалях.

| | Развлечения | Финансовые сервисы | Образование | Покупки и доставка | Путешествия | Информация | Коммуникации | Гаджеты | Здоровье | Дети |
|---|---|---|---|---|---|---|---|---|---|---|
| Яндекс | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ✓ | ↑ | ↓ | ✓ |
| Сбер | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ✓ | ↑ | ✓ | ✓ |
| МТС | ↑ | ↑ | ✓ | ✓ | ✓ | ↑ | ↑ | ✓ | ↑ | ✓ |
| Т-Банк | ✓ | ↑ | ✓ | ✓ | ✓ | ✓ | ↑ | --- | ✓ | ✓ |
| VK | ↑ | ✓ | ↑ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

↑ Усиление вертикали
↓ Ослабление вертикали
✓ Присутствие в вертикали без динамики

Рис. 1. Развитие российских цифровых экосистем в ключевых вертикалях в 2025 г

Для успешной реализации плана внедрения и развития необходимо обеспечить динамичный мультифакторный анализ экономической привлекательности вертикалей с целью определения потенциала реализации разных направлений деятельности в рамках единой платформы в зависимости от целей и задач деятельности организации. Цель анализа состоит в том, чтобы определить, в каких вертикалях экосистема может максимально эффективно развиваться с учетом имеющихся ресурсов, конкурентной среды и потребностей пользователей. Методика анализа привлекательности вертикалей для цифровых экосистем строится на использовании количественных и качественных методов оценки бизнес-показателей, отраслевых трендов и пользовательского восприятия. Ключевые этапы анализа привлекательности вертикалей цифровых экосистем отражены на рис. 2.

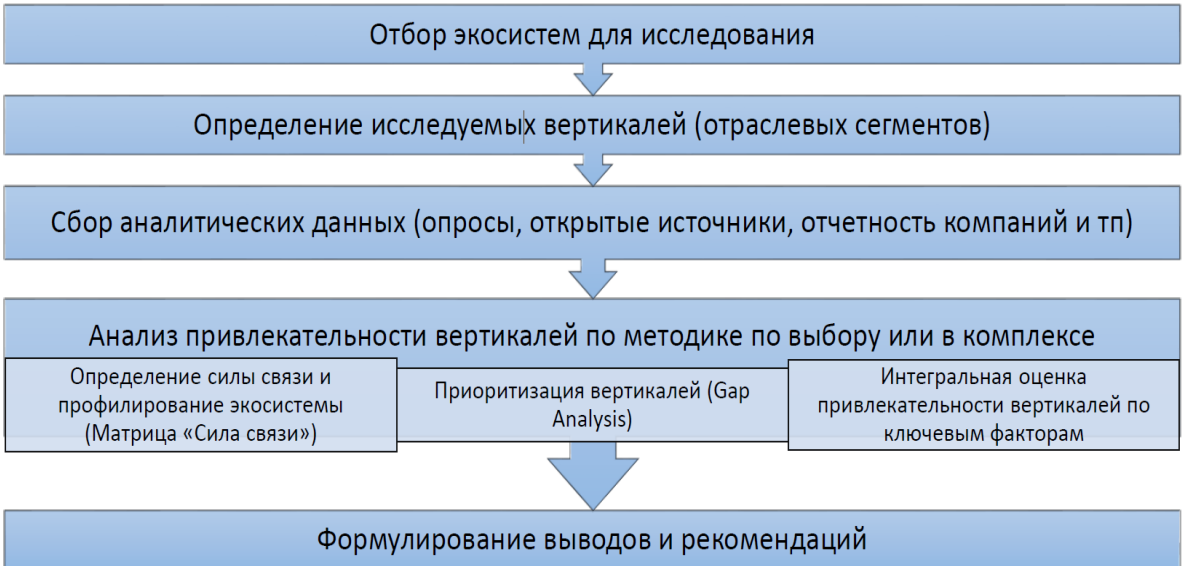



Рис. 2. Ключевые этапы анализа привлекательности вертикалей

Для анализа привлекательности вертикалей оцениваемые **факторы влияния** могут быть объединены в четыре основные группы: рыночные факторы, экосистемные факторы, финансовые факторы, технологические регуляторные факторы. Анализируемые в рамках каждой группы факторы и их содержание отражены в таблице 1.

ТАБЛИЦА 1. Структура факторов для анализа привлекательности вертикалей цифровых экосистем

| Группа | Факторы | Содержание анализа |
|---|---|---|
| Рыночные факторы | Объем и динамика рынка | Определение фактического или потенциального спроса на товары/услуги в динамике |
| | Конкурентная среда | Анализ уровня монополизации и угрозы появления новых игроков. Оценка присутствия конкурентов в вертикали, их стратегий, сильных и слабых сторон |
| | Уровень проникновения | Оценка степени охвата аудитории цифровыми услугами в выбранной вертикали |
| | Востребованность у пользователей | Выявление потенциала для роста пользовательской аудитории в рамках выбранной вертикали на основе оценки удовлетворенности |
| Экосистемные факторы | Перекрестные продажи | Оценка возможности конвертации базы из одной вертикали в клиенты другой вертикали |
| | Эффект данных | Оценка возможности использования полученной информации (данных) о поведении пользователей в одной вертикали (в одном |

| Группа | Факторы | Содержание анализа |
|---|---|---|
| | | сегменте рынка) для персонализации предложений в другой |
| | Снижение транзакционных издержек | Оценка размера возможной экономии за счет единой инфраструктуры |
| Финансовые факторы | Маржинальность вертикали | Ключевой показатель оценки финансовой эффективности бизнеса |
| | Прогнозируемая пожизненная ценность клиента | Оценка совокупной прибыли или дохода, который может быть получить от одного клиента за все время взаимодействия с ним |
| | Капиталоемкость входа в новый сегмент | Анализ объема требуемых инвестиций на инфраструктуру для развития в новой вертикали по отношению к ожидаемому приросту дохода |
| | Затраты на цифровую трансформацию | Оценка интенсивности затрат на внедрение и обслуживание техники, программных продуктов и подготовку кадров, связанных с цифровыми технологиями [4] |
| Технологические и регуляторные факторы | Уровень цифровизации | Влияние возможности применения искусственного интеллекта для оптимизации процессов, наличие возможностей для обеспечения бесшовной передачи данных между сервисами |
| | Регуляторные риски | Перспективы антимонопольных ограничений и ужесточения законодательно установленных требований к капиталу экосистем [5] |

Использование интегральных показателей позволяет получить комплексную оценку эффективности экосистемы. При этом весовой коэффициент значимости каждого фактора определяется исходя из целей и задач конкретной экосистемы в краткосрочной и долгосрочной перспективе. Для оценки следует использовать шкалу, построенную с учетом уникальности каждой экосистемы [6].

Глубокий мультифакторный анализ позволяет сформулировать выводы о перспективности исследуемых вертикалей для развития цифровой экосистемы, предложить рекомендации по выбору стратегии присутствия, масштабированию или оптимизации и разработать план их внедрения.

Важно учитывать, что рынок и тренды постоянно меняются, поэтому методика анализа должна быть гибкой и адаптируемой к новым условиям за счет динамичности анализа, планирования и контроля. Решения по реализу-

емой стратегии должны приниматься, исходя из среднесрочных и долгосрочных целей деятельности фирмы, и подвергаться своевременной корректировке.

**Список используемых источников**

1. Шишкова А. С., Макаров В. В. Российские цифровые экосистемы в сегменте b2c: текущее состояние и перспективы развития // Вестник СПбГУТ. 2025. Т. 3. № 3. EDN: LFRGFM.

2. Макаров В. В., Шишкова А. С. Современные экосистемы как результат эволюции концепции экосистем и цифровой трансформации экономики // Экономика и качество систем связи. 2025. № 4(38). С. 4-17. EDN: LEDRCU/.

3. Гузь А. Р. Стефанова Н.А. Модель цифровой экосистемы: лидеры российского b2c-рынка и их адаптация к современным вызовам // Журнал монетарной экономики и менеджмента. 2025. № 1. С. 84-94. DOI: 10.26118/2782-4586.2025.79.65.012. EDN: BBRGQA. (дата обращения: 01.04.2026).

4. Коровин Г. Б. Интегральная оценка уровня развития цифровых экосистем в субъектах РФ // Экономика региона. 2026. № 22(1). С. 16–28. URL: https://DOI.org/10.17059/ekon.reg.2026-1-2 (дата обращения: 30.04.2026).

5. Головко С. М. Цифровые экосистемы как новая модель ведения бизнеса в условиях турбулентности в экономике / С. М. Головко // Вестник евразийской науки. 2023. Т. 15. № s2. URL: https://esj.today/PDF/17FAVN223.pdf (дата обращения: 25.04.2026).

6. Каленов О. Е. Оценка эффективности деятельности бизнес-экосистем в цифровой экономике / О. Е. Каленов // Вестник Российского экономического университета имени Г. В. Плеханова. 2023. Т. 20. № 1(127). С. 162-174. DOI: 10.21686/2413-2829-2023-1-162-174. EDN: VJXTRC (дата обращения: 15.04.2026).

## METHODOLOGICAL FOUNDATIONS OF MULTIFACTOR ANALYSIS OF THE ATTRACTIVENESS OF DIGITAL ECOSYSTEM VERTICALS

**Makarov V., Mikhailova A., Shishkova A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*An economically valid approach is needed to ensure the competitiveness of digital ecosystems and to choose the verticals of presence of digital ecosystems, depending on their profitability, growth potential and associated risks. A comprehensive analysis of the economic, technological, social and regulatory aspects of the functioning of digital ecosystems forms the basis for making strategic decisions regarding determining the company's development directions in the medium and long term. The article presents the author's definition of a digital ecosystem, the vertical of a digital ecosystem, and a methodological framework for multifactorial analysis of the attractiveness of digital ecosystem verticals.*

***Keywords:*** *digital platform, digital ecosystem, digital ecosystem vertical, Gap Analysis, focus strategy, diversification strategy*

**УДК 338.46:004.9**
**ГРНТИ 06.81.85**

# ТРАНСФОРМАЦИЯ КРИТЕРИЕВ КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЙ УСЛУГ ПОД ВОЗДЕЙСТВИЕМ ПРОЦЕССОВ ЦИФРОВИЗАЦИИ

**В. В. Макаров[1], Н. Д. Петровский[2]**

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

*В статье рассматриваются изменения критериев конкурентоспособности предприятий сферы услуг, вызванные цифровой трансформацией экономики. На основе анализа классических работ М. Портера и К. Шваба, а также современных исследований цифровых платформ выделены традиционные и новые цифровые критерии. Показано, что в условиях цифровизации возрастает значение таких факторов, как качество цифрового взаимодействия с клиентом, уровень автоматизации процессов и способность работать в экосистемах. Предложена авторская классификация критериев конкурентоспособности для сервисных предприятий в цифровой среде.*

***конкурентоспособность предприятия, сфера услуг, цифровизация, критерии конкурентоспособности, цифровая трансформация, сервисная экономика, цифровые платформы***

Традиционные подходы к оценке конкурентоспособности предприятий сферы услуг, обобщенные в работах М. Портера, основывались на таких критериях, как цена, качество обслуживания, дифференциация и издержки [1, с. 112].

Однако массовое внедрение цифровых технологий, которое К. Шваб определяет как четвертую промышленную революцию, привело к тому, что классические критерии перестали быть достаточными для удержания рыночных позиций [2, с. 45]. В экономике данных на первый план выходят новые факторы, связанные с эффективностью использования информации, автоматизацией взаимодействия с потребителем и гибкостью бизнес-моделей.

Цель исследования – выявить и систематизировать изменения в системе критериев конкурентоспособности предприятий сферы услуг под влиянием цифровизации. В качестве методов использованы анализ научной литературы, сравнительный и структурно-логический методы.

Традиционно конкурентоспособность предприятия услуг оценивали через три группы критериев: ценовые (уровень тарифов, скидки), качествен-

ные (скорость оказания услуги, дружелюбность персонала, гарантии) и репутационные (отзывы, известность бренда). Данные критерии были сформулированы в доцифровую эпоху, когда главным каналом взаимодействия оставался личный контакт.

Сегодня, как отмечают В. А. Казаков и Ю. Ф. Тельнов, цифровые платформы индустрии четвертого поколения коренным образом изменяют структуру транзакционных издержек и информационную асимметрию [3, с. 38].

В результате анализа публикаций последних лет автором выделены четыре группы новых критериев конкурентоспособности, актуальных для цифровой экономики.

Первая группа – цифровая доступность и удобство. Она включает наличие у предприятия собственного мобильного приложения, качество работы сайта, возможность онлайн-записи и оплаты, скорость ответа в мессенджерах. Исследования показывают, что для потребителей услуг (образование, медицина, транспорт, телекоммуникации) удобство цифровых каналов стало важнее, чем цена в ряде сегментов.

Вторая группа – способность к персонализации на основе данных. Цифровизация позволяет накапливать информацию о поведении потребителей. Предприятия, которые используют технологии для предложения индивидуальных условий (целевые скидки, рекомендации, напоминания), получают устойчивое конкурентное преимущество. Таким образом, критерий «глубина аналитики клиентских данных» становится значимым [4].

Третья группа – автоматизация и скорость реакции. В условиях высокой динамики спроса важна способность предприятия в реальном времени изменять параметры услуги (например, ценообразование, маршруты, расписание). Это требует внедрения цифровых систем управления (CRM, ERP, BI). Следовательно, уровень цифровой зрелости процессов выступает самостоятельным критерием конкурентоспособности.

Четвертая группа – кибербезопасность и доверие. Переход услуг в цифровую среду сопровождается рисками утечки персональных данных. Для потребителя становится критичным, насколько надежно предприятие защищает его информацию. Поэтому критерий «безопасность цифрового взаимодействия» следует включать в оценку конкурентоспособности наравне с качеством самой услуги [5].

На рисунке 1 представлена трансформация весовых коэффициентов критериев конкурентоспособности для типичного предприятия бытовых

услуг (например, клининг или ремонт) в период 2010-2025 годов. Видно, что доля традиционных ценовых и репутационных критериев снижается, а значимость цифровой доступности и автоматизации растет.

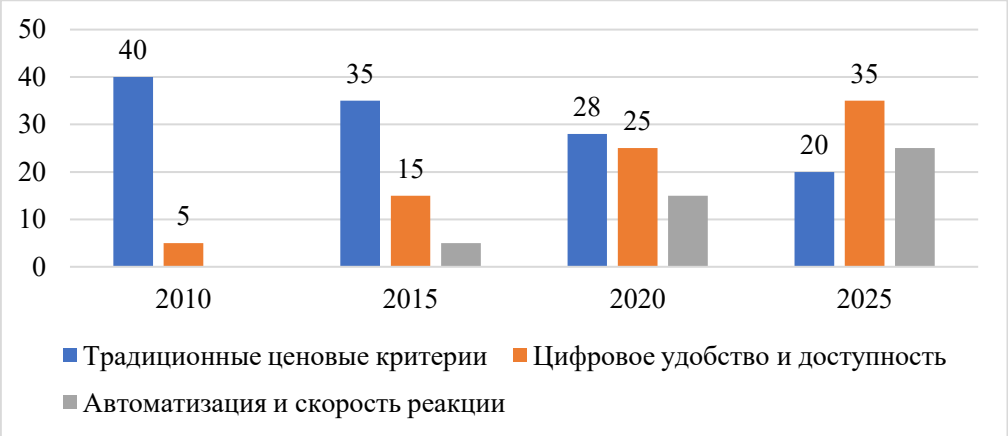



Рис. 1. Изменение весов критериев конкурентоспособности предприятия услуг в процессе цифровизации

Как показано на рисунке 1, к 2025 году цифровые критерии суммарно превышают традиционные по значимости для потребителя. Кроме того, важно учитывать, что трансформация критериев происходит не единовременно, а в зависимости от степени цифровизации конкретной отрасли.

В таблице 1 приведено сопоставление классических и новых критериев для трех типов услуг (телекоммуникационных, образовательных, бытовых).

ТАБЛИЦА 1. Сравнение традиционных и цифровых критериев конкурентоспособности по видам услуг

| Вид услуг | Традиционные критерии | Цифровые критерии |
|---|---|---|
| Телекоммуникационные | Зона покрытия, цена | Качество мобильного приложения, скорость поддержки в чате |
| Образовательные | Квалификация преподавателей, место расположения | Доступность онлайн-курсов, персонализация траектории обучения |
| Бытовые (клининг, ремонт) | Цена, опыт работы | Онлайн-запись, рейтинг на цифровых платформах, трекинг исполнителя |

Согласно данным таблицы 1, в телекоммуникациях цифровые критерии уже доминируют, тогда как в бытовых услугах они дополняют традиционные. Это подтверждает гипотезу о неравномерной трансформации.

В заключительной части статьи отметим, что для практического использования предложенного подхода предприятиям сферы услуг необходимо пересмотреть внутренние системы оценки эффективности. Рекомендуется ввести регулярный мониторинг цифровых индикаторов: доля онлайн-заказов, время ответа в цифровых каналах, индекс цифровой лояльности клиентов.

Дальнейшие исследования могут быть направлены на разработку интегрального показателя конкурентоспособности, учитывающего как классические, так и новые цифровые критерии.

**Список используемых источников**

1. Портер М. Конкурентное преимущество: Как достичь высокого результата и обеспечить его устойчивость: практическое руководство. 4-е изд. Москва: Альпина Паблишер, 2026. 16 с. ISBN 978-5-9614-5727-8.

2. Шваб К. Четвертая промышленная революция. Москва: Эксмо, 2016. (Top Business Awards). ISBN 978-5-699-90556-0.

3. Казаков В. А., Тельнов Ю. Ф. Многоагентная система сетевого предприятия на основе цифровой платформы индустрии четвертого поколения // Открытое образование. 2025. Т. 29, № 2. С. 34-45. DOI: 10.21686/1818-4243-2025-2-34-45.

4. Михайлова А. С., Макаров В. В. Влияние цифровой экономики на развитие государства и общества // Вестник СПбГУТ. 2025. Т. 3. № 4. С. 2. EDN: TNGIHZ.

5. Макаров В. В., Слуцкий М. Г., Устриков Н. К. Проблемы и задачи цифровой трансформации экономики России // Международный журнал гуманитарных и естественных наук. 2020. № 4–1 (43). С. 174–177. DOI: 10.24411/ 2500-1000-2020-10329. EDN: MOMOLZ

## CHANGES IN COMPETITIVENESS CRITERIA OF SERVICE ENTERPRISES CAUSED BY DIGITAL TRANSFORMATION

**Makarov V.[1], Petrovsky N.[2]**
[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications
[2]Gatchina State University

*The article examines changes in the competitiveness criteria of service enterprises caused by the digital transformation of the economy. Based on an analysis of classical works by M. Porter and K. Schwab, as well as modern research on digital platforms, traditional and new digital criteria are identified. It is shown that in the context of digitalization, the importance of factors such as the quality of digital customer interaction, the level of process automation, and the ability to operate in ecosystems increases. The authors propose an original classification of competitiveness criteria for service enterprises in the digital environment.*

***Key words:*** *enterprise competitiveness, service sector, digitalization, competitiveness criteria, digital transformation, service economy, digital platforms*

**УДК 330.34**
**ГРНТИ 06.03**

# БОЛЬШИЕ ДАННЫЕ КАК УНИКАЛЬНЫЙ РЕСУРС ЦИФРОВОЙ ЭКОНОМИКИ

**А. В. Мешков, А. А. Симонина**

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

*Большие данные являются ключевым ресурсом цифровой экономики. Но этот ресурс трудно описать в рамках традиционной экономической теории. Большие данные одновременно обладают свойствами свободного и экономического блага, частного и общественного, предельная полезность их воспроизводства стремится к нулю и в отношении них не действует закон убывающей отдачи. Эти и другие уникальные особенности данных и исследуются в данной статье.*

***большие данные, цифровая экономика, экономика данных, экономическая ценность***

Большие данные (*Big Data*) обычно описывают пятью характеристиками, часто называемыми в литературе 5*V* по первой букве соответствующих английских слов. Объем (*Volume*). Суточные массивы данных превышают 150 Гб (стандартный объем оперативной памяти компьютера 8 Гб). Такие объемы данных невозможно эффективно обрабатывать и анализировать традиционными методами. Скорость (*Velocity*). Данные поступают непрерывно и требуют анализа в режиме реального времени. Разнообразие (*Variety*). Данные различаются по формату и разнообразию источников. Это могут быть социальные сети, интернет-платформы, мобильные приложения, трансакционные системы торговых сетей и т.д. Ценность (*Value*). На основе больших данных принимаются более обоснованные стратегические решения для развития бизнеса, научных исследований, государственного управления и в других сферах. Достоверность (*Veracity*). Большие массивы данных могут содержать ошибки, дубликаты, поврежденные файлы. Поэтому необходимо их очищать и проверять перед использованием в анализе.

Здесь хотелось бы особо обратить внимание на то, что Большие данные имеют высокую ценность и именно это делает их экономическим ресурсом. Но ценность имеют не любые данные, а только достоверные. Поэтому для экономического анализа 4 и 5*V* имеет особое значение.

Итак, Большие данные – ценный экономический ресурс. С легкой руки математика и предпринимателя К. Хамби широко распространилась по миру фраза: «Данные – это новая нефть». Но, если легко согласиться с утверждением, что данные столь же ценный экономический ресурс для цифровой экономики, как нефть для экономики индустриальной, то при более внимательном анализе становится очевидным, что данные ни с нефтью, ни с любым другим ресурсом традиционной экономики (труд, земля, капитал) имеют очень мало общего.

Известно, что все экономические ресурсы, согласно неоклассической экономической теории, должны обязательно обладать двумя характеристиками. Во-первых, они ограничены по сравнению с потребностью в них. Во-вторых, они, как правило, обладают свойством исключительности в потреблении. Это означает, что потребление этих благ одним экономическим субъектом делает невозможным их потребление другим субъектом.

Именно эти характеристики и придают экономическим благам ценность в обмене (стоимость) т.е. способность благ обмениваться на другие блага в определенной пропорции. Экономическая ценность является основой рыночной цены. Блага, не обладающие этими характеристиками, именуются свободными. Они не ограниченные по сравнению с потребностью в них и поэтому экономической ценности не имеют. Спрос на них удовлетворяется полностью по нулевой цене. Неоклассическая экономическая теория относит к свободным благам только природные ресурсы, доступные каждому без ограничений (атмосферный воздух, солнечный свет, вода из природного источника).

Однако, данные исходя из такого понимания, в гораздо большей степени можно определить как свободное благо, а не экономическое. Рассмотрим соотношение производства и потребления Больших данных.

В 2015 г. объем сгенерированных в мире данных составил 15,5 зетабайт (1ЗБ = 1 млрд терабайт). В 2020 г. он достиг 64,2 ЗБ, в 2025 г. составил уже 181 ЗБ [1]. Таким образом, происходит экспоненциальный рост объема Больших данных, что связано с развитием информационных технологий, повышением уровня цифровизации и распространением интернета.

В то же время, потребность в Больших данных пока очень скромна. Только 3 % данных правильно собираются и хранятся и лишь эти идеальные данные можно проанализировать [2].

Таким образом, можно сделать вывод, что Большие данные – это неограниченный ресурс по сравнению с современной потребностью в них.

Следовательно, исходя из постулатов неоклассической экономической теории, это свободное благо и более уместно сравнивать данные с солнечным светом, чем с, не только ограниченным, но и невоспроизводимым ресурсом – нефтью. Тем не менее, как было сказано выше, одной из важнейших характеристик Больших данных является их высокая ценность. Значит данные являются одновременно и свободным и экономическим благом.

Отсюда можно сделать вывод, что некоторые постулаты традиционной экономической теории, которые описывают экономику с ограниченными ресурсами, не работают для анализа цифровой экономики.

Но что же придает данным ценность? Для ответа на этот вопрос, по мнению авторов, надо опираться не столько на неоклассическую теорию, сколько на теорию одного из отцов-основателей маржинализма Карла Менгера. Согласно его теории, вменением собственной ценностью обладают только потребительские блага. Они наделяют ценностью производственные ресурсы, участвующие в их изготовлении. Ценность вменяется производственным благам в силу их нужности для существования потребительских благ [3]. Опираясь на теорию вменения можно утверждать, что сами по себе Большие данные никакой экономической ценности не имеют. Ценность им придают блага, созданные на основе их анализа. Собственно, именно об этом говорил Дж. Кеннеди, который еще в 2014 г. дал следующее определение экономике данных: «Экономика данных-область, в которой большое количество экономической ценности создается за счет эффективного использования данных» [4].

Неприменимость ряда постулатов неоклассики проявляется и при анализе вопроса о том, что определяет рыночную цену данных. Согласно традиционной экономической теории, равновесная рыночная цена – это цена, при которой объем спроса равен объему предложения, или это цена, при которой предельная полезность блага равна предельным издержкам.

Затраты на сбор, очистку и структурирование данных могут быть достаточно велики. Но стоимость их копирования и передачи посредствам цифровых технологий крайне незначительна. Таким образом, предельные издержки на воспроизводство данных сводятся к нулю. Один из фундаментальных законов индустриальной экономики – закон убывающей предельной производительности не действует относительно важнейшего ресурса цифровой экономики. При околонулевых предельных издержках ценность данных, а, следовательно, рыночная цена определяется только спросом, в основе которого лежит предельная полезность. Но предельная полезность

данных весьма различна для разных пользователей. Для одних она очень высока, а для других те же базы данных не представляют особой ценности. В этом случае, по мнению авторов, ценовая дискриминация на рынке данных не только допустима, но и желательна. Ценовая дискриминация означает продажу одного и того же блага разным потребителям по разным ценам и трактуется неоклассической экономической теорией как злоупотребление монопольной властью. В экономике данных с нулевыми предельными издержками воспроизводства даже совершенная ценовая дискриминация, при которой каждый пользователь приобретает ресурс по своей цене спроса вполне имеет право на существование.

Далее, если данные являются экономическим благом, хотя и весьма специфическим, то следует ли их рассматривать как частное или как общественное благо? С точки зрения авторов, они обладают всеми признаками блага общественного и, в то же время, чистым общественным благом не являются. Как любое общественное благо данные обладают, во-первых, свойством неконкурентности в потреблении. Потребление данных одними пользователями не уменьшает их доступность для других. Во-вторых, все общественные блага, неисключаемые в потреблении. Высокие трансакционные издержки защиты и спецификации прав собственности не позволяют исключить кого-либо из процесса потребления данных (за исключением тех данных, которые являются государственной тайной). Главная проблема в производстве общественных благ-проблема безбилетника. Ведь, если все могут пользоваться такими благами без ограничений, то всегда находятся люди, которые отказываются их оплачивать. Отсюда, в соответствии с еще одним постулатом неоклассики, производство общественных благ не приносит прибыли и потому их может производить только государственный сектор.

Что касается данных, то действительно, в их воспроизводстве большую роль играет государство. Достаточно упомянуть принятый в 2025 г. в России национальный проект «Экономика данных и цифровая трансформация государства». Вместе с тем, следует отметить, что эта программа частно-государственного партнерства, в которой бизнес должен принять самое деятельное участие. На 2025-2030 гг. затраты федерального бюджета на эту программу оцениваются в 1 трлн рублей, а внебюджетные инвестиции в 1,3 трлн рублей [5]. Данные, обладая свойствами общественного блага могут являться и рыночным активом. Объем российского рынка Больших данных

и искусственного интеллекта достиг 520 млрд рублей в 2025 г. и имеет среднегодовой темп роста около 20 % [5].

Но ценность больших данных для бизнеса не может быть оценена только в денежном выражении. Проблема «безбилетника» в пользовании Большими данными преодолевается тем, что многие цифровые блага предоставляются пользователям не совсем бесплатно, а в обмен на их данные. Данные становятся платежным средством цифровой экономики.

В заключении хотелось бы отметить, что Большие данные – это уникальный экономический ресурс новой, постиндустриальной экономики. Хотя и предпринимаются попытки свести этот ресурс к одной из форм капитала («информационный капитал», «цифровой капитал») с точки зрения авторов подобный подход не продуктивен. Данные не являются особым видом капитала поскольку способны изменять природу всех факторов производства, в том числе и физического капитала. Труд все больше осуществляется с использованием данных, например, платформенная занятость [6]. Физический капитал (станки, автомобили, здания) становятся «умными» за счет встроенных датчиков и постоянному потоку данных [7].

**Список используемых источников**

1. Дмитриев А. П., Лейба С. Ш. Стремительный рост цифровых данных: анализ мировых трендов и прогноз развития в России // Журнал Региональная и отраслевая экономика 2024. № 1. С.141-152. URL: https://roecon.ru/archive?page=4 (дата обращения 20.05.2026).

2. Жуков В. «Только 3 % данных правильно собираются и хранятся»: вот как работать с ними лучше // Электронный журнал Russian Business 2023. URL: https://rb.ru/columns/about-data-quality/ (дата обращения 20.05.2026).

3. Менгер К. Основание политической экономики //Территория будущего, 2005, 496с, ISBN 978-5-7333-0175-9.

4. Лапидус Л. В. Онтогенез цифровой экономики и экономики данных: концепция «интеллектуальная гиперсвязанность в Индустрии Х.0» // Российский журнал менеджмента 2024. Т. 22. № 3. URL: https://rjm.spbu.ru/article/view/20411 (дата обращения 20.05.2026)ю

5. Кузьмина В. Большие данные пошли в рост. Как бизнес и государство строят экономику данных // Коммерсант 2026. URL: https://www.kommersant.ru/doc/8335113 (дата обращения 20.05.2026).

6. Мешков А. В., Симонина А. А. Трансформация рынка труда в цифровой экономике: платформенная занятость // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025): сб. науч. ст. в 3-х т. СПб.: СПбГУТ, 2025. Т. 3. С. 195-200.

7. Абрамов В.И., Гордеев В.В., Столяров А.Д. Экономика данных как новая парадигма экономического развития: концептуальный анализ // Научный журнал Фундаментальные исследования 2026. № 3. С 69-76. URL: https://fundamental-research.ru/ru/article/view?id=43994 (дата обращения 20.05.2026).

## BIG DATA AS A UNIQUE RESOURCE FOR THE DIGITAL ECONOMY

**Meshkov V., Simonina A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Big data is a key resource of the digital economy. However, this resource is difficult to describe within the framework of traditional economic theory. Big data simultaneously possesses the properties of a free and economic good, a private and public good, and its marginal utility of reproduction tends to zero, and the law of diminishing returns does not apply to it. These and other unique features of data are explored in this article.*

***Key words:*** *Big data, digital economy, data economy, economic value*

**УДК 398.3**
**ГРНТИ 13.91.**

# К ВОПРОСУ ОБ АКТУАЛЬНОСТИ «КАЛЕВАЛЫ»: ДАННЫЕ СОЦИОЛОГИЧЕСКОГО ОПРОСА

**В. С. Михайлюк, Т. В. Молчанова**

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

*В начале 1840-х годов набирает силу национальное движение в Финляндии. Воодушевленная европейским романтизмом университетская молодежь принялась изучать народную культуру и собирать устно-поэтические произведения. Среди этих энтузиастов был в томи числе Элиас Леннрот, который взял на себя задачу собрать фольклор Финляндии. Его труд стал известен в 1835 г. как «Калевала», национальный эпос страны. В статье представлены данные социологического опроса, посвященного изучению значимости «Калевалы» для современных жителей Финляндии.*

***Калевала, социологическое исследование, финский эпос, Элиас Леннрот, культура Финляндии***

Многовековое нахождение Финляндии в составе Шведского королевства обусловило прочные узы, сохранявшиеся между этими странами [1]. Интерес финнов к устно-поэтическим произведениям старинной, «калевальской», метрики можно проследить со времен начала финского книгопечатания, возникновение которого связано с Реформацией в Швеции и Финляндии (первая половина XVI в.).

Уже в начале 1840-х годов, когда национальное движение в Финляндии набирало силу [2], воодушевленная новыми идеями европейского романтизма, университетская молодежь Финляндии принялась изучать народную культуру и собирать устно-поэтические произведения. Среди этих энтузиастов был и финский лингвист и фольклорист Элиас Леннрот. Следуя традициям романтизма, Леннрот взял на себя задачу собрать фольклор Финляндии, и его труд стал известен в 1835 г. как «Калевала», национальный эпос страны [2].

Несмотря на существенную значимость «Калевалы» как литературно-исторического памятника Финляндии, в настоящее время можно наблюдать утрату интереса финской молодежи к своему наследию. Авторы данной ра-

боты решили провести небольшое социологическое исследование по данному вопросу.

Была сформулирована следующая гипотеза: жители современной Финляндии мало информированы о сущности «Калевалы» и не проявляют интересу к ней.

Формализованная часть опроса.

Цель исследования: определить степень информирования финнов о «Калевале» и ее социокультурном значении для жителей Финляндии.

Социальная сеть: «Reddit», сообщество «r/Finland».

Респонденты: финны и лица, имеющие гражданство Финляндии.

Количество человек: 97.

Выборка: Опрос был опубликован в сообществе «r/Finland», где пользователи узнали об опросе через ленту новостей.

Время прохождения: ноябрь 2025 – февраль 2026.

Вопросы, предложенные участникам исследования:

1. «Do you know about Kalevala?» («Знаете ли вы о Калевале?»)

2. «Did you read Kalevala?» («Читали ли вы Калевалу?»)

3. «Do you know how was Kalevala written?» («Вы знаете как Калевалу написали/Вы знаете историю написания Калевалы?»)

4. «Do you know who wrote Kalevala?» («Вы знаете кто написал Калевалу?»)

5. «Do you celebrate Kalevala day? (28th February, also Finnish culture day/Finnish flag day)» («Вы отмечаете День Калевалы? (28 февраля, так же известный как День финской культуры/День финского флага)»)

6. «Does Kalevala in some way influence your life?» («Влияет ли как-либо Калевала на вашу жизнь?»)

7. Дополнительный вопрос (38 ответов): «If yes, then how?» («Если да, то как?»)

8. Дополнительный вопрос (25 ответов): «If no, then why?» («Если нет, то почему?»)

Далее проанализируем полученные в ходе анкетирования данные.

Первый вопрос был о знании «Калевалы»: знают ли финны о ее существовании. Каждый респондент ответил положительно (рис. 1).

Второй вопрос был про то, читали ли респонденты «Калевалу». Здесь заметна разница ответов, однако большинство читали «Калевалу» (рис. 1).

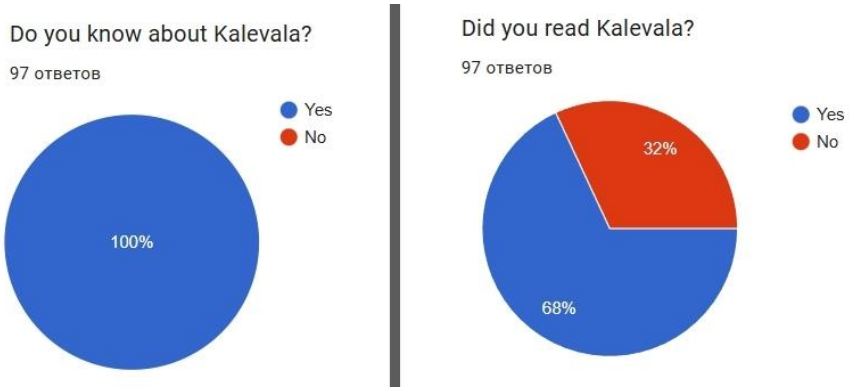



Рис. 1. Первый вопрос: «Знаете ли вы о Калевале?»; второй вопрос: «Читали ли вы Калевалу?»

Третий вопрос был про знание истории написания «Калевалы», о том, как Элиас Леннрот собирал руны и писал эпос. Отрицательно ответили 2,1 % респондентов. То есть большинство в курсе создания данного литературного памятника (рис. 2).

Четвертый вопрос был про знание автора «Калевалы». Как и в прошлом вопросе – преобладающее большинство (96,9 %) имеют представления о личности Элиаса Леннрота (рис. 2).

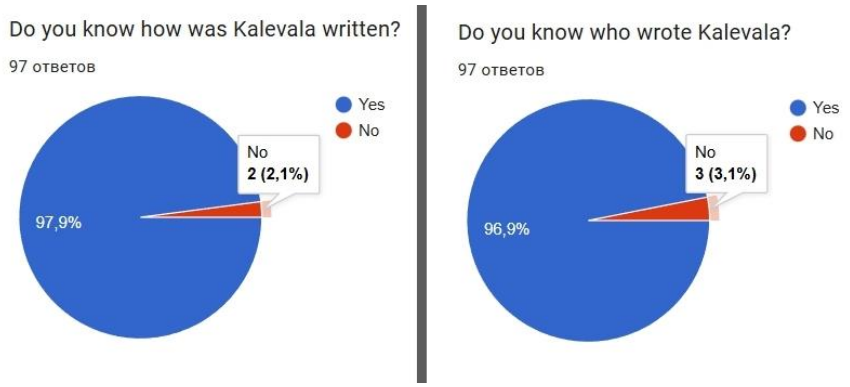



Рис. 2. Третий вопрос: «Вы знаете историю написания Калевалы?»; четвертый вопрос: «Вы знаете кто написал Калевалу?»

Пятый вопрос был про одну из важнейших культурных дат Финляндии.

Данные опроса показывают, что лишь 10,3 % отмечают празднование Калевалы. Некоторые респонденты отметили, что школах могут рассказывать о «Калевале», показывать программы по телевизору, но многие даже не знают о существовании этого праздника [3]. Скорее всего, это связано с тем, что для обывателей 28 февраля ассоциируется исключительно с Днем финского флага, который никто не отмечает. Несмотря на это, бывают некоторые инициативы со стороны частных лиц в организации мероприятий и фестивалей, хоть и не ежегодных [4, 5] (рис. 3).

Шестой вопрос был про влияние «Калевалы» на жизнь респондентов. В этом конкретном вопросе можно заметить почти равное количество голосов. Но только некоторые обосновали свои ответы. Из этого можно сделать вывод, что «Калевала» имеет место в культурном поле финнов, она проявляется в повседневной жизни: в творчестве, в произведениях (Рис. 3).

52,6 % респондентов указывают на то, что «Калевала» повлияла на их интерес к культуре и фольклору, привила интерес к музыке, писательству и искусству. Многие также упоминают детскую книгу «Собачья Калевала: Маури Куннас»: они читают ее своим детям, либо же сами ознакомляются с «Калевалой» таким способом, так как самые первые издания «Калевалы» использовали достаточно сложную и устаревшую версию финского языка (ранний новофинский).

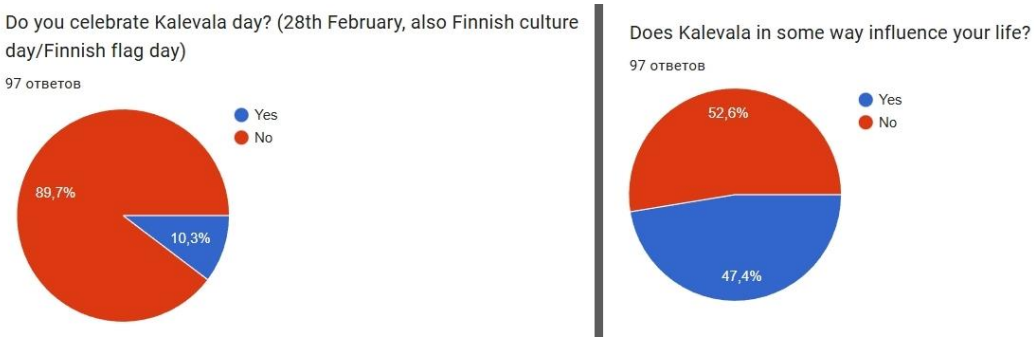



Рис. 3. Пятый вопрос: «Вы отмечаете День Калевалы?»;
шестой вопрос: «Влияет ли как-либо Калевала на вашу жизнь?»

В подтверждении этого, стоит процитировать некоторые показательные ответы респондентов.

«I think it influences part of Finnish culture in an understated way. I think many values that Finnish people and Finnish culture regard highly (for example sisu, loyalty, honesty) are visible in Kalevala. Kalevala maybe also represents something of our own and not something Nordic, and I think many Finnish legends and myths are forgotten, so it's important that we still have Kalevala» (пер. «Я думаю, что ее влияние на финскую культуру недооценено. Я думаю, что многие ценности, которые финский народ и финская культура высоко ценят (например, «сису», верность, честность), можно увидеть в «Калевале». Калевала, возможно, тоже представляет собой что-то наше, а не что-то скандинавское, и я думаю, что многие финские легенды и мифы забыты, поэтому важно, чтобы у нас все еще была Калевала.»;

«The language is awesome and I believe it should be living tradition like it was back in the day when it was transmitted orally. Of course, it has influenced Finnish culture in many ways that are not immediately obvious in day-to-day life»

(пер. «Язык (стиль написания) потрясающий, и я считаю, что должна быть традиция, которая была в те времена, когда «Калевала» передавалась/пелась устно. Конечно, она оказала влияние на финскую культуру многими способами, которые не сразу заметны в повседневной жизни»).

«I'm a follower of Väenusko. Kalevala is obviously not a religious text in and of itself, it's just a fictional story that is based on the mythos of my religion. However, it's what originally brought me to Väenusko» (пер. «Я последователь “Väenusko” (религия, основанная на духовных традициях коренных народов Финляндии). Очевидно, что «Калевала» сама по себе не является религиозным текстом, это всего лишь вымышленная история, основанная на мифах моей религии. Однако именно она изначально привела меня к “Väenusko”»).

«I cite the Kalevala in my speech sometimes; I sing choir arrangements that use some of the text from the Kalevala (and the Kanteletar) and I sometimes write poems in the Kalevala meter (trochaic tetrameter) for fun. It’s also often referenced by Finnish artists» (пер. «Иногда я цитирую «Калевалу» в своих выступлениях, пою хоровыми аранжировками, в которых используются некоторые тексты из «Калевалы» (и «Кантелетар»), и иногда я пишу стихи в стиле «Калевалы» (хореическим тетраметром) для развлечения. На нее также часто ссылаются финские художники»).

Восьмой вопрос («Если нет, то почему?») имеет, в основном, однотипные и достаточно негативные ответы: «она никак не влияет» и «почему она должна влиять?». Из 25 ответов есть и развернутые комментарии: «It has very little effect or presence in Finnish culture these days. Kalevala could be seen as an instrument of the creation of a "nation myth", which was especially important in the early 20th century, but its influence has since diminished» (пер. «В наши дни она практически не имеет влияния на финскую культуру. «Калевалу» можно рассматривать как инструмент создания «национального мифа», который был особенно важен в начале 20-го века, но с тех пор ее влияние уменьшилось».

«Although I roughly know the story of Kalevala and have read a children's adaptation of it, and I like Finnish folklore, Kalevala itself doesn't really act part of it. I think our culture and mythology is more than Kalevala, Kalevala only representing a slither of it collated into a narrative form» (пер. «Хоть я примерно и знаю историю «Калевалы» и читал ее детскую экранизацию, и мне нравится финский фольклор, сама «Калевала» на самом деле не является ее частью. Я думаю, что наша культура и мифология – это нечто большее, чем

«Калевала», и она представляет собой лишь ее фрагмент, облеченный в повествовательную форму»).

В заключении стоит сказать, что опрос частично показывает актуальность «Калевалы» в современном мире, но она недостаточна. Из 97 ответов, развернутых отрицательных было 25 – но при этом, 38 развернутых ответов говорили о влиянии «Калевалы» на их жизнь. Из диаграммы (рис. 3) можно сделать вывод о том, что большинство людей (52, 6 %) не считает, что данный эпос как-либо влияет на их жизнь. В финской социокультурной действительности не хватает вовлечения жителей страны по отношению к своей культуре и популяризации наследия «Калевалы» среди населения, в частности – среди молодежи, что следует из диаграммы про празднование Дня «Калевалы» (рис. 3), где 89, 7 % респондентов ответили, что не отмечают данный праздник.

**Список используемых источников**

1. Гехт А. Б. Шведский добровольческий корпус в советско-финляндской войне 1939-1940 гг. // Проблемы истории, филологии, культуры. 2014. № 4. С. 183-194.

2. Песонен П., Риихинен О. Динамичная Финляндия: пер. с англ. А. Рупасова: Европейский Дом, 2014. 388 с.

3. How Kalevala day is celebrated? // reddit.com. URL: https://www.reddit.com/r/ Finland/comments/1ossnom/how_kalevala_day_is_celebrated/ (дата обращения 03.02.2026).

4. Experience the Kalevala Like Never Before: A Special 190th Anniversary Celebration in Kainuu // interreg-npa.eu. URL: https://www.interreg-npa.eu/projects/n-lite/home/news-events/experience-the-kalevala-like-never-before-a-special-190th-anniversary-celebration-in-kainuu/ (дата обращения 03.02.2026).

5. The Kalevala Week // juminkeko.fi. URL: https://www.juminkeko.fi/en/ tapahtuma/kalevala-viikko/ (дата обращения 03.02.2026).

## ON THE RELEVANCE OF THE “KALEVALA”: SOCIOLOGICAL SURVEY DATA

**Molchanova T., Mikhailyuk V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In the early 1840s, the national movement in Finland gained momentum. Inspired by European romanticism, university youth began to study folk culture and collect oral poetry. Among these enthusiasts was Elias Lönnrot, who took on the task of collecting Finnish folklore. His work became known in 1835 as «Kalevala», the national epic of the country. The article presents the data of a sociological survey devoted to the study of the importance of «Kalevala» for modern residents of Finland.*

***Key words:*** *Kalevala, sociological research, Finnish epic, Elias Lönnrot, culture of Finland.*

**УДК 004**
**ГРНТИ 06.54.51**

# ПРОБЛЕМЫ И ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ПЛАТФОРМЫ НАЦИОНАЛЬНОЙ СИСТЕМЫ ПЛАТЕЖНЫХ КАРТ

**Р. О. Мустафин, В. И. Шилков**

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина

*В статье обсуждаются вопросы развития национальной системы платежных карт, созданной с целью обеспечения процессов безопасного хранения и передачи данных при проведении расчетов, взаимозачетов и платежей с помощью отечественных информационных технологий и платежных инструментов. Названы основные организационно-технологические, информационные, психологические и правовые проблемы. Обозначены основные направления развития компонентов информационно-экономической безопасности национальной системы платежных карт.*

***информационные технологии, платежные карты, безналичный расчет, информационная безопасность***

Неотъемлемой частью мировой экономики стали банковские карты, позволяющие осуществлять платежные операции путем безналичных расчетов. Несмотря на то, что в мире существует большое количество различных платежных систем, предназначенных для оплаты товаров, услуг и переводов денежных средств, наиболее широкое распространение получили зарубежные платежные системы «Visa» и «MasterCard». Однако для снижения зависимости российской экономики от воздействия неблагоприятных факторов, обусловленных нестабильностью мировой политической и экономической обстановки, в Российской Федерации были приняты решения по созданию и развитию национальной системы платежных карт «Мир», которая к настоящему времени стала одним из важнейших инструментов системы безналичных расчетов.

В работе [1] отмечено, что карта «Мир» демонстрирует стабильный количественный и оборотный рост, заняв к началу 2020-х существенную долю национального рынка. Объем проводимых операций и общая сумма транзакций показывают устойчивую положительную динамику, свидетельствуя о постепенном замещении иностранных аналогов и укреплении позиций отечественного продукта. В соответствии со сведениями, приведенными

в [2], по уровню охвата населения карта «Мир» уже опередила международные аналоги карт, используемые в России. Подавляющее большинство респондентов выбирают данный инструмент в качестве основного для повседневных расчетов. Технологический функционал полностью соответствует современным стандартам, обеспечивая полный спектр банковских операций, включая торговый эквайринг, переводы и наличные операции.

Актуальность и необходимость исследования вопросов и международного и отечественного опыта функционирования систем платежных карт, обусловлена необходимостью решения ряда организационно-технологических проблем, препятствующих реализации стратегии развития национальной системы платежных карт «Мир». Анализ показывает, что несмотря на положительное восприятие пользователями платежных карт «Мир» существует ряд проблем, нуждающихся к скорейшему решению.

Так, например, по мнению авторов работы [3] психологические препятствия для развития системы платежных карт «Мир» и формирования позитивного рыночного восприятия продукта в ряде случаев возникают из-за административно-директивных методов массового распространения платежных инструментов. Процедура обязательной выдачи карт в рамках зарплатных проектов воспринимается потребителями как избыточная бюрократическая нагрузка и снижает лояльность не только физических лиц, но и представителей корпоративного сектора. В работе [4] отмечено, что держатели пластиковых карт к основным недостаткам карт относят: отсутствие возможностей бесконтактной оплаты; медленную обработку транзакций и большую стоимость обслуживания, по сравнению с картами ряда других платежных систем.

К проблемам, сдерживающим цифровизацию финансово-экономической сферы в Российской Федерации и, в частности, развитие национальной системы платежных карт, автор работы [5] относит: отсутствие необходимых финансовых навыков; наличие различных рисков, сопутствующих финансовым инновациям и психологические особенности экономического менталитета граждан. Низкий уровень лояльности к цифровым платежным средствам также могут проявлять граждане, предпочитающие сохранять анонимность платежных операций, что может быть связано с их участием в деятельности теневого сектора экономики. Однако, в большинстве случаев, низкий уровень доверия граждан, объясняется: привычкой населения использовать наличные средства; отсутствием необходимых знаний по кибербезопасности обращения с цифровыми платежными средствами; ожида-

ниями возможных финансовых потерь цифровых активов в случае экономической нестабильности; финансовыми потерями, связанными с многочисленными мошенничествами в сфере использования безналичных платежных средств.

Авторы работы [6] обращают внимание на необходимость проведения инфраструктурной трансформации банковского оборудования, так как на значительном количестве устройств самообслуживания пока еще отсутствуют встроенные модули для считывания QR-маркеров. Аппаратная модернизация и оснащение каждого устройства считывателем требует значительных капиталовложений. Для масштабной реконструкции парка терминалов, насчитывающего миллионы единиц, требуются инвестиции на уровне десятков миллиардов рублей, что создает серьезное финансовое напряжение для участников рынка. Несмотря на то, что для банков-участников тарифы на обслуживание карты существенно ниже, чем тарифы обслуживание международных платежных систем, авторы работы [7] указывают на существенную величину эксплуатационных издержек по обслуживанию карт для конечных пользователей, для которых, тарифы за годовое обслуживание могут варьироваться в диапазоне, например, от двухсот до одной тысячи рублей. Возможность онлайн-оплаты реализована исключительно на ограниченном числе маркетплейсов, тогда как значительная часть крупных интернет-ресурсов остается вне зоны покрытия, а функционал дистанционных расчетов демонстрирует выраженные ограничения в части интеграции с цифровыми торговыми площадками.

Авторы работы [8] отмечают, что инициативы по расширению международного присутствия сталкиваются с институциональными барьерами, так как с 2022 года инициированы рестриктивные меры в отношении зарубежных кредитных организаций, взаимодействующих с отечественным процессинговым оператором. Санкции спровоцировали массовый выход иностранных финансовых институтов из партнерских программ, консервируя систему преимущественно во внутреннем контуре.

Несмотря на то, что в работе [9] сообщается о планах организации функционировании карты «Мир» в Иране, Таиланде, Индии, в настоящее время, относительно уверенное присутствие национальной платежной системы «Мир» на зарубежных рынках ограничивается достаточно малым количеством зарубежных стран, к которым относятся, Беларусь, Вьетнам, Абхазия, Южная Осетия, Армения, Казахстан, Таджикистан. К причинам, сдерживающим присутствие национальной платежной системы на зарубеж-

ных рынках, следует отнести ограниченное количество стран, обеспечивающих технологический прием карт, что обусловлено отсутствием технической совместимости с ведущими мобильными экосистемами и международными и локальными системами электронных расчетов, что существенно сужает возможности бесконтактных расчетов и спектр доступных пользовательских сценариев, а внедрение инфраструктуры, например, в торговом секторе требует от ритейлеров проведения масштабной и дорогостоящей модернизации необходимого оборудования.

Вместе с тем несмотря на то, что платежная система «Мир» сформирована на основе современных информационно-технологических решений, важным направлением развития системы платежных карт «Мир» является развитие организационно-технологической платформы и повышение уровня информационной безопасности, что обусловлено как агрессивными современными технологиями, применяемыми злоумышленниками, так и необходимостью расширения перечня функций, выполняемых платежной системой. Расширение продуктовой линейки системы платежных карт сопровождается активным внедрением бесконтактных технологий и программ клиентской лояльности. Регулятор установил четкие сроки для обязательной поддержки банками расчетов посредством динамических QR-кодов, генерируемых мобильными устройствами. Данная инициатива направлена на модернизацию платежной инфраструктуры, снижение зависимости от физических носителей и повышение доступности цифровых финансовых сервисов.

Дальнейшее развитие платформы предполагает: разработку, направленных на преодоление географических барьеров, механизмов интеграции с зарубежными электронными торговыми площадками; повышение универсальности платежного инструмента в цифровой среде; расширение функциональных возможностей и разработку моделей совместимости мобильных платежных сервисов с устройствами ведущих технологических корпораций, которые позволят нивелировать текущие аппаратные ограничения.

Архитектура взаимодействия международных платежных шлюзов выступает критически важным компонентом системы обеспечения национальной безопасности. На территории страны они функционируют как технологические операторы и ключевые расчетные и клиринговые функции делегированы национальному центру. Подобная модель гарантирует бесперебойное обслуживание существующего портфеля карт независимо от внешнеполитических ограничений или санкций со стороны зарубежных

эмитентов. Устойчивое развитие национальной системы платежных карт должно быть неразрывно связано с системными инвестициями в контур информационной защиты. Ключевыми направлениями выступают регулярные обновления программных сред, внедрение передовых протоколов шифрования и строгое соблюдение международных стандартов хранения платежных данных, что формирует надежный фундамент для долгосрочного функционирования платформы в условиях цифровых угроз. Одним из направлений повышения уровня информационной безопасности национальной системы платежных карт «Мир» может стать, например, внедрение способов многофакторной аутентификации.

Контуры информационной безопасности должны базироваться на применении верификационного протокола, адаптированного на основе международных стандартов трехэтапной защиты. Параллельно с развитием карточных продуктов должна развиваться программная среда для осуществления бесконтактных расчетов посредством мобильных устройств, что значительно расширяет пользовательские сценарии и повышает удобство проведения повседневных финансовых операций

Автор работы [10] отмечает, что в будущем торговые и сервисные предприятия страны смогут размещать свои предложения на общенациональной платформе, созданной для обслуживания всех держателей карт «Мир». По мнению автора работы [11], для повышения востребованности и привлекательности карты «Мир» необходимо: адаптировать и развивать с учетом текущих условий функциональные возможности приложения системы «Мир», обеспечивающего доступ к получению коммерческих, муниципальных и государственных услуг; развивать программы лояльности в сферах туризма, гостиничного сервиса, бронирования авиа и железнодорожных билетов; расширять при безналичном способе оплаты применение инновационных технологий блокчейна и биометрии.

Одним из перспективных направлений развития национальной платежной системы «Мир», по мнению авторов работы [12], может стать внедрение нефинансовых сервисов, в которых могут быть заинтересованы не только пользователи платежных инструментов, но, например, и территориальные органы исполнительной власти. Внедрение нефинансовых сервисов, реализуемое в рамках концепции цифрового агрегирования, сможет способствовать: росту популярности и востребованности пластиковых карт; снижению относительной стоимости производства платежного средства и издержек информационного обмена ; увеличению скорости и объема данных

мобильного обмена; сокращению наличных платежей в экономике; значительному расширению возможностей использования цифрового платежного инструмента; повышению качества и количества услуг, предоставляемых пользователям; прозрачности экономики и решению ряда важнейших государственных задач. Техническая реализация такого платежного средства возможна с помощью различных способов, к которым можно отнести, например: запись дополнительной информации на чип карты обеспечивающей высокую степень защиты; размещение на карте платежного и неплатежного чипов; использование технологии Hash-PAN, облегчающей взаимодействие с мобильными технологиями.

По результатам проведенного исследования можно сделать вывод, что несмотря на то, что платежная карта «Мир» стала важным и необходимым элементом системы безналичных расчетов, существует достаточно большое количество проблем, нуждающихся в решении. Внедрение платежной карты «Мир» сопровождается рядом системных организационных, информационно-технологических, психологических и экономических рисков. Основные направления развития платежной системы «Мир» связаны с применением инновационных технологий; повышением уровня информационно-экономической безопасности; расширением перечня функций; повышением комфортности обслуживания и выходом на зарубежные финансовые рынки.

**Список используемых источников**

1. Грушко А. Н., Грушко Е. С. Проблемы развития финансовых и информационных технологий в экономике в условиях санкций // В сборнике: Факторы развития экономики России. Сборник трудов Международной научно-практической конференции. Тверь, 2022. С. 56-63.

2. Митчина Т. Е., Вандышева И. С. Платежные системы пластиковых карт // Финансовый вестник. 2022. № 3(58). С. 70-76.

3. Устенко Ю. К. Тенденции развития национальной системы платежных карт «МИР» в современных условиях // Вестник науки. № 3 (48). 2022. С. 119-126.

4. Кислицкая Н. А. Формирование системы национальных платежных карт, как фактор укрепления финансовой безопасности страны // В сборнике: Развитие и реализация программы повышения финансовой грамотности взрослого населения в Ростовской области. Материалы межрегиональной научно-практической конференции (в рамках Проекта Минфина России «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации»). 2018. С. 105-108.

5. Смирнова Н. А. Тенденции цифровизации монетарной сферы Российской экономики // Вестник Волгоградского государственного университета. Экономика. 2022. Т. 24. № 4. С. 28-42.

6. Филиппова А. А., Либина М. А. Инновации в системе платежных карт "МИР" // Проблемы развития предприятий: теория и практика. 2023. № 1-2. С. 101-104.

7. Васильева Е. Г., Темзоков А. Р. Правовые аспекты развития национальной платежной системы «МИР» // Право. 2020. С. 193-199.

8. Лалабекова В. Р., Хагагортян И. А. Анализ и перспективы развития национальных платежных систем на примере «АРКА» И «МИР» // Вестник Российско-Армянского (Славянского) университета: гуманитарные и общественные науки. 2025. № 4 (55). С. 50-73.

9. Бельмач И. В., Пынько Л. Е. Современные информационные технологии экономики и управление социально-экономическими процессами в контексте развития цифровой экономики // Общество и цивилизация. 2022. Т. 4. № 4. С. 53-56.

10. Голубева А. А. Сотворение "МИРа": создание Российской национальной системы платежных карт // Российский журнал менеджмента. 2021. С. 592-613.

11. Онопюк Е. Ю. Направления развития и перспективы платежных карт "МИР". Национальная Ассоциация Ученых. 2021. № 69-2. С. 62-65.

12. Жуков Я. В., Лысенко Р. Ю., Протас Н. Г., Тарасова Г. М. Расширение функций и возможностей банковских карт // Бизнес. Образование. Право. 2021. № 2 (55). С. 60-64.

## PROBLEMS AND PROMISING DIRECTIONS OF DEVELOPMENT OF THE INFORMATION TECHNOLOGY PLATFORM OF THE NATIONAL PAYMENT CARD SYSTEM

**Mustafin R., Shilkov V.**
Ural Federal University named after the first President of Russia B. N. Yeltsin

*The article discusses the development of a national payment card system created to ensure the safe storage and transmission of data during settlements, offsets and payments using domestic information technologies and payment instruments. The main organizational, technological, informational, psychological and legal problems are mentioned. The main directions of development of information and economic security components of the national payment card system are outlined.*

***Key words:*** *Information technology, payment cards, cashless payment, information security*

**УДК 378.147**
**ГРНТИ 14.35.09**

# АНАЛИЗ ПОДХОДОВ К ФОРМИРОВАНИЮ БАЗОВЫХ ЦИФРОВЫХ КОМПЕТЕНЦИЙ ГОРНЫХ ИНЖЕНЕРОВ

**К. Н. Никитин, Л. С. Оруджова, Ю. В. Перязева**

Санкт-Петербургский горный университет императрицы Екатерины II

*Исследование анализирует подходы к формированию базовых цифровых компетенций в образовательных программах по специальности 21.05.04 «Горное дело». Показано, что элементы цифровой грамотности системно охватываются на 1–2 курсах, тогда как компетенции в области алгоритмического мышления, программирования, анализа данных, искусственного интеллекта и ответственного использования ИИ-ассистентов вводятся на более поздних этапах, остаются в вариативной части или вовсе не представлены.*

***цифровые компетенции, цифровая грамотность, учебные планы, образовательные программы***

Массовое внедрение информационных технологий (ИТ) трансформирует экономику и социальную сферу [1]. Решающую роль в конкурентоспособности бизнеса и государства играют цифровизация и внедрение технологий искусственного интеллекта (ИИ), машинного обучения (ML), анализа данных и моделирования. Эта тенденция заметна и в добывающих отраслях: применение цифровых решений в нефтегазовой и горнодобывающей промышленности стало системным и целенаправленным, устойчиво расширяя масштабы и эффект их использования [2]. В России реализуется национальный проект «Экономика данных и цифровая трансформация государства», нацеленный на цифровую трансформацию государственного и муниципального управления, экономики и социальной сферы за счет развития кибербезопасности, доступной связи, кадровых программ для ИТ, цифрового государственного управления, отечественных платформ и программного обеспечения (ПО), перспективных разработок и ИИ [3].

Требования к компетенциям инженеров меняются: критически важно владение современными цифровыми инструментами. Спрос смещается от модели «ИТ-специалист в связке с отраслевым экспертом» к модели «цифровых инженеров» – специалистов с развитыми цифровыми навыками, спо-

собными самостоятельно решать задачи цифровой трансформации. Для формирования таких продвинутых цифровых компетенций на старших курсах необходимо обеспечить освоение базовых цифровых компетенций на 1–2 курсах.

Цифровые компетенции (ЦК) – совокупность умений, знаний и навыков для работы в цифровой среде и с цифровыми продуктами, охватывающая создание и сбор данных, их обработку и анализ, а также автоматизацию процессов с использованием компьютерных технологий [4].

Существуют различные модели ЦК: международные European/International Computer Driving Licence (ECDL/ICDL), рамки компетенций ЮНЕСКО по использованию ИКТ в образовании (UNESCO ICT Competency Frameworks), европейские DigComp (для преподавателей и граждан) и другие, а также модели вузов. Цифровым компетенциям посвящено множество исследований: например, в обзоре [5] систематизированы цифровые компетенции студентов на основе зарубежных публикаций. Краткое и структурированное описание ЦК представлено в Концепции развития цифровых компетенций студентов НИУ ВШЭ [4], разработанной на основе различных международных моделей, модель состоит из трех частей: цифровая грамотность; алгоритмическое мышление и программирование; анализ данных, искусственный интеллект и генеративные модели и в ней выделены следующие компетенции:

1) навыки поиска, отбора, структурирования и использования данных и цифровых ресурсов;

2) осознанное и ответственное поведение в цифровой среде с соблюдением этических норм, авторского права и правовых требований;

3) умения защиты устройств и персональных данных и настройки безопасности;

4) понимание возможностей современных цифровых устройств и сетевых сервисов и умение самостоятельно осваивать и внедрять их в работу;

5) умение эффективно пользоваться ИИ-ассистентами: формулировать точные запросы, проверять и критически оценивать ответы;

6) владение офисным ПО: обработка текстов и таблиц, работа с данными, подготовка презентаций, совместная работа и базовая автоматизация;

7) навыки программирования, решения ресурсоемких задач, умение формализовать задачу в алгоритм;

8) применение математических методов и методов искусственного интеллекта для построения моделей на больших данных, решения профессиональных задач.

Пункты 1–5 относятся к цифровой грамотности, которая должна быть сформирована у всех студентов на 1–2 курсах; для пунктов 7–8 предусматриваются уровни освоения, и на 1–2 курсах они должны быть сформированы на начальном и базовом уровнях.

Современные стандарты образования предъявляют требования к результатам освоения образовательных программ в виде набора компетенций [6]. Индикаторы достижения компетенций (ИДК) – это характеристики, уточняющие формулировку компетенции в виде результатов обучения и конкретных действий обучающегося; они должны быть измеримы средствами образовательного процесса. Для измерения ИДК применяются дескрипторы – качественные критерии оценивания, описывающие уровень проявления ИДК и позволяющие определить степень их сформированности. Модель компетенций образовательной программы представляет собой композицию ИДК; дескрипторы используются для их оценивания. Компетентностные модели образовательных программ должны содержать цифровые компетенции.

Цель работы – оценить, в какой мере образовательные программы по специальности 21.05.04 «Горное дело» в российских вузах интегрируют базовые ЦК и насколько эти модели согласованы с международными и российскими моделями цифровых компетенций.

Гипотеза: доля программ, включающих компоненты цифровой грамотности на первом и втором курсах, статистически выше доли программ, включающих компоненты алгоритмического мышления, программирования, анализа данных и искусственного интеллекта; соответствующие дисциплины либо отсутствуют, либо перенесены на старшие курсы и/или вынесены в вариативную часть, несмотря на актуальность искусственного интеллекта и экономики данных.

Проведен сравнительный анализ частей компетентностных моделей образовательных программ по специальности 21.05.04 «Горное дело», направленных на формирование ЦК, с существующими моделями цифровых навыков. Исследование основано на сборе данных с сайтов вузов, анализе текстов основных профессиональных образовательных программ (ОПОП), учебных планов и рабочих программ дисциплин (РПД). Выделялись ЦК, ИДК и дисциплины, формирующие ЦК; из РПД извлекались соот-

ветствующие дескрипторы (знания, умения, навыки). Выявлено 46 вузов, реализующих специальность 21.05.04 «Горное дело», из них 11 – филиалы; в анализ включены 35 вузов.

Анализ образовательных программ показал, что для формирования начальных и базовых цифровых компетенций из федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по специальности 21.05.04 «Горное дело» выбирают следующие компетенции: УК-1 «Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий»; УК-4 «Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия»; УК-6 «Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни»; ОПК-8 «Способен работать с программным обеспечением общего и специального назначения и пакетами моделирования горных и геологических объектов»; ОПК-21 «Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности».

На формирование базовых цифровых компетенций, помимо традиционных дисциплин – таких как «Информатика», «Информационные технологии», «Начертательная геометрия и инженерная графика», «Компьютерная графика», – ориентированы также дисциплины: «Основы цифровой грамотности», «Интеллектуальное ПО», «Цифровое моделирование», «Интеллектуальные средства автоматизации», «Основы работы в программном обеспечении общего назначения», «Цифровые технологии в профессиональной деятельности», «Введение в сквозные цифровые технологии», «Цифровизация инженерной деятельности», «Вычислительные методы и прикладные программы», «Информационная среда и защита данных» и ряд других.

Для составления профиля покрытия по восьми выбранным компетенциям для каждого университета сформирована бинарно-дробная матрица: восемь компетенций – по столбцам, вектор значений – по строке для вуза. Присутствие оценивалось по ИДК, дескрипторам и содержанию из РПД с помощью генеративных моделей (GPT-5, OpenAI, 2025, версия от 7 августа 2025, DeepSeek V3.1) для генерации и анализа текста. Шкала: 1 – компетенция явно и полно присутствует в образовательной программе; 0,5 – ча-

стичное покрытие; 0 – отсутствует в явном виде или упоминания неконкретны. Результаты по среднему покрытию компетенций (Таблица 1).

ТАБЛИЦА 1. Среднее покрытие компетенций

| № | Краткое описание | Среднее покрытие |
|---|---|---|
| 1 | Навыки работы с информацией. | 1.0 |
| 2 | Стратегии поведения в цифровой среде. | 0,3 |
| 3 | Основы ИБ (пользователь). | 0,7 |
| 4 | Понимание технических возможностей устройств/интернета. | 1,0 |
| 5 | Навыки работы с ИИ-помощниками. | 0,1 |
| 6 | Офисные приложения. | 1,0 |
| 7 | Программирование для автоматизации/данных. | 0,6 |
| 8 | Методы ИИ/ML/математические модели. | 0,4 |

Компетенции 1, 4 и 6 закрыты полностью; наименее закрыта компетенция по работе с ИИ-ассистентами. Компетенции 7 и 8 покрыты умеренно, при этом пункт 8 – преимущественно за счет математического моделирования.

Дополнительные показатели. Средняя зачетная единица трудоемкости (ЗЕТ) на вуз для дисциплин, формирующих базовые ЦК, составила 10,2 ЗЕТ (максимум – 21 ЗЕТ, минимум – 4 ЗЕТ; 1 ЗЕТ = 36 академических часов). Средняя «жесткость контроля» – 3,3 на 10 ЗЕТ; число экзаменов – 1,4 на 10 ЗЕТ; среднее число семестров включения – 2,3. Это указывает, что контроль в блоке базовых ЦК умеренный и может ограничивать достижение качественных образовательных результатов.

Полученные результаты показывают почти полное закрытие компонентов цифровой грамотности (навыки работы с информацией, офисные приложения, понимание возможностей устройств/сервисов), что согласуется с ядром DigComp и базовыми модулями ECDL/ICDL. Вместе с тем плохо представлены компетенции, связанные с взаимодействием с ИИ-ассистентами, алгоритмическим мышлением, программированием, анализом данных и ИИ/ML. Это расходится с актуализированными рамками UNESCO ICT-CF и современной потребностью в навыках работы с данными, автоматизации и критической оценке ответов ИИ.

Причины перекоса. Смещение акцента в сторону «офисной» и прикладной ИКТ-подготовки объяснимо историей стандартизации учебных планов и преобладанием дисциплин «Информатика/ИКТ» и «Инженерная и компьютерная графика» на ранних курсах. Курсы по программированию, анализу данных и ИИ чаще переносятся на старшие курсы, делают вариативными или привязывают к профильным модулям. В горном деле высокая доля «моделирования» обеспечивает умеренное покрытие компетенции 8, но в основном за счет математического моделирования и инженерных пакетов, а не методов ИИ/ML и обработки данных. Это создает разрыв между отраслевой практикой (рост спроса на AI/ML, цифровые двойники, предиктивную аналитику) и ранней подготовкой студентов.

Выбор компетенций УК-1, УК-4, УК-6, ОПК-8 и ОПК-21 для формирования базовых ЦК представляется корректным, однако внутри ОПК-21 целесообразно выделить ИДК, связанные с обработкой данных, автоматизацией и ИИ, чтобы избежать растворения цифровых целей в общей формулировке «использовать ИТ».

Ограничения исследования. Неполнота РПД, формальные формулировки и различия терминологии; использование генеративной модели для извлечения ИДК и дескрипторов ускорило анализ, но добавило риски (неоднозначность терминов, чувствительность к формулировкам, различия структур документов). Несмотря на ручную проверку на подвыборке, возможны неточности. Бинарно-дробная шкала проста и интерпретируема, но груба.

Выводы. В образовательных программах по специальности 21.05.04 «Горное дело» базовые элементы цифровой грамотности в целом сформированы и системно представлены на 1–2 курсах. Недостаточно рано покрываются компетенции, связанные с алгоритмическим мышлением, программированием, анализом данных, ИИ/ML и ответственным использованием ИИ-ассистентов. Полученные результаты подтверждают гипотезу: доля программ, включающих компоненты цифровой грамотности на 1–2 курсах, статистически выше доли программ, включающих компоненты программирования/данных/ИИ; соответствующие дисциплины часто переносятся на старшие курсы или в вариативную часть.

Перспективы дальнейшей работы: расширение выборки (включая филиалы), переход к многоуровневой шкале оценивания и оценка динамики изменений в учебных планах.

**Список использованных источников**

1. Litvinenko V. S. Digital economy as a factor in the technological development of the mineral sector //Natural Resources Research. 2020. Т. 29. № 3. С. 1521–1541. DOI: 10.1007/s11053-019-09568-4. EDN: WGABFS.

2. Samylovskaya, E.; Makhovikov, A.; Lutonin, A.; Medvedev, D.; Kudryavtseva, R.-E. Digital Technologies in Arctic Oil and Gas Resources Extraction: Global Trends and Russian Experience. Resources 2022, 11, 29. DOI: 10.3390/resources11030029.

3. Национальный проект «Экономика данных и цифровая трансформация государства». URL: http://government.ru/rugovclassifier/923/about/ (дата обращения 26.04.2026).

4. Концепция развития цифровых компетенций студентов НИУ ВШЭ. URL: https://www.hse.ru/mirror/pubs/share/969166457.pdf (дата обращения 26.04.2026).

5. Tzafilkou K., Perifanou M, Economides A.A. Development and validation of students' digital competence scale // International Journal of Education Technology in Higher Education. 2022. Article number 30. DOI: 10.1186/s41239-022-00330-0.

6. Полетайкин А. Н., Кунц Е. Ю., Кулешова Н. В. Оптимизационная модель построения индикаторов достижения компетенций // Информатизация образования и науки. 2020. № 1. С. 64–81. EDN: PKBRBZ.

## AN ANALYSIS OF APPROACHES TO THE FORMATION OF CORE DIGITAL COMPETENCIES FOR MINING ENGINEERS

**Nikitin K., Orudzhova L., Peryazeva J.**
Empress Catherine II Saint Petersburg Mining University

*The study examines approaches to developing core digital competencies in educational programs for specialty 21.05.04 «Mining Engineering». It shows that elements of digital literacy are systematically covered in the 1st–2nd years, whereas competencies in algorithmic thinking, programming, data analysis, AI/ML, and the responsible use of AI assistants are introduced at later stages, remain in the elective track, or are not included at all.*

***Key words:*** *digital competencies; digital literacy; curricula; educational programs*

**УДК 336.71**
**ГРНТИ 06.73.55**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ESG-ПРАКТИК РОССИЙСКИХ БАНКОВ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

**О. А. Посохова**

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

*Актуальность исследования обусловлена возрастающей ролью принципов устойчивого развития, биоэкономики и необходимостью их интеграции в бизнес-модели кредитных организаций на фоне активного внедрения и использования цифровых технологий. Целью работы является анализ подходов российских банков к реализации ESG-повестки. Методологическую основу составляют анализ открытых источников, сравнительный подход и обобщение современных тенденций развития банковского сектора. Полученные результаты могут быть использованы для дальнейших исследований и практического совершенствования стратегий устойчивого развития в банковской сфере.*

***ESG, устойчивое развитие, банковский сектор, коммерческие банки, цифровая трансформация, ESG-практики, корпоративное управление***

Согласно общепризнанной терминологии, ESG-факторы включают экологические (Environmental), социальные (Social) и управленческие (Governance) аспекты деятельности организаций [1]. ESG-факторы определяют ключевые направления устойчивого развития, а ESG-практики являются практическими способами их реализации. В текущих реалиях ESG – практики требуют особого внимания в связи с повышенной актуальностью данной тематики. Отдельно стоит выделить поручение Президента РФ об утверждении Стратегии долгосрочного развития биоэкономики в России на период до 2036 года [2]. Концепция биоэкономики достаточно тесно связана с ESG-подходом, поскольку ориентирована на устойчивое использование биологических ресурсов, экологическую безопасность, развитие человеческого капитала и долгосрочную устойчивость экономики. В российской стратегической повестке данное направление должно получить институциональное закрепление через формирование Стратегии долгосрочного развития биоэкономики Российской Федерации до 2036 года.

Кроме того, актуальность исследования обусловлена возрастающей ролью принципов устойчивого развития и необходимостью их интеграции

в бизнес-модели кредитных организаций на фоне активного внедрения и использования цифровых технологий [3]. В текущих экономических реалиях в совокупности с цифровой трансформацией с одной стороны усиливается не только технологическая, но и психоэмоциональная нагрузка на сотрудников банковского сектора, что в конечном итоге несет определенные риски для устойчивости компаний с другой позволяет использовать инструменты для мониторинга предотвращения критических ситуаций. В современной практике ESG – подходы рассматриваются уже не столько, как элементы экологической и социальной ответственности, но уже скорее как инструменты повышения инвестиционной привлекательности, долгосрочной устойчивости и даже конкурентоспособности компании в целом.

Банковский сектор в целом характеризуется высокой интенсивностью труда, а также регулярной значимой технологической и психоэмоциональной нагрузкой на сотрудников. В концепции ESG-подхода вопросы сохранения человеческого капитала, благополучия сотрудников и предотвращения профессионального выгорания становятся значимым направлением устойчивого развития организаций.

Специфика деятельности банковских учреждений заключается в сочетании высокой степени цифровизации и регламентированности бизнес-процессов с необходимостью сохранения эффективного межличностного взаимодействия. Несмотря на активное внедрение цифровых технологий, автоматизацию значительно части операций и стандартизацию большинства процедур, значительная часть банковской деятельности, особенно в сегменте работы с юридическими лицами, по-прежнему строится на доверии, качестве коммуникации и устойчивых социальных взаимодействиях между людьми. В этой связи возрастает значение человеческого капитала, вовлеченности персонала и нематериальных механизмов мотивации сотрудников.

Кроме того, именно в банковской отрасли общее негативное состояние сотрудников может считываться, как угроза безопасности денежных средств и компании в целом. Что в итоге может создавать репутационные риски, так как значительная часть ключевых клиентов, таким или иным образом находится в тесном контакте с определенными банковскими сотрудниками. В связи с этим возрастает необходимость формализованной оценки, которая на практике часто реализуется через системы рейтинговых показателей. Рейтинги ESG используются для оценки и прогнозирования рисков в экологической, социальной сферах, а также в части оценки эффективности управления организацией. По итогам отчетности за 2024 год

можно отметить, что число банков, публикующих нефинансовые данные в том или ином виде, увеличилось на 42,9 %, и достигло 20 организаций [4] RAEX. Вопросы методологии ESG-оценки и формирования ESG-рейтингов подробно рассматриваются в модельной методологии Банка России, включающей подходы к оценке экологических, социальных и управленческих факторов [5].

Банк России отмечает проблему недостаточной сопоставимости ESG-рейтингов из-за различий в методологиях, критериях оценки и используемых источниках данных. В целях повышения прозрачности и сопоставимости ESG-оценок Банком России разработана модельная методология ESG-рейтинга, содержащая рекомендации по оценке экологических, социальных и управленческих факторов.

В текущих реалиях одной из ключевых проблем ESG-анализа остается отсутствие полной унификации подходов к ESG-рейтингам. Разнообразие методических подходов, используемых рейтинговыми агентствами, снижает сопоставимость получаемых оценок.

Следует отметить, что в современных исследованиях социальный компонент ESG все чаще рассматривается не столько через формальные показатели социальной ответственности, но и через обеспечение устойчивости человеческого капитала, развитие корпоративной культуры, поддержание благополучия сотрудников и создание условий для долгосрочной профессиональной эффективности персонала.

При этом цифровая трансформация не только изменяет условия труда в рамках профессиональной нагрузки, но и создает дополнительные возможности для более своевременного выявления признаков эмоционального истощения, снижения вовлеченности персонала и прочих факторов, способных оказывать влияние на эффективность работы сотрудников и качество взаимодействия как внутри организации, так и с клиентами.

Далее рассмотрим особенности реализации ESG-практик на примере пяти банков, репрезентирующих неоднородность российского банковского сектора по масштабу и уровню ESG-интеграции.

ПАО «Сбербанк» относится к числу крупнейших российских банков, системно раскрывающих ESG-информацию в составе интегрированной годовой отчетности [6]. В отчете за 2024 год банк выделяет большой отдельный ESG блок. Отчет обеспечивает довольно высоких охват ESG-тематики, в рамках стандартной отчетности и внешней рейтинговой верификации. Также следует отметить, что Национальное рейтинговое агентство также

фиксирует высокий уровень интеграции ESG-компонентов, по сводной оценке, на уровне AAA.esg. Подтверждение данного уровня рейтинга обусловлено продолжающейся реализацией ESG-стратегии Банка.

Следует отметить, что так же, как и ПАО «Сбербанк» – ПАО Банк ВТБ продолжает регулярное развитие ESG-практик. Наблюдательным советом Банка ВТБ в 2021 году была утверждена Стратегия Банка ВТБ (ПАО) в области устойчивого развития (ESG) на 2022–2025 годы и компания продолжает следовать установленному курсу. ESG-раскрытие осуществляется в структуре отчета об устойчивом развитии и охватывает основные компоненты ESG-повестки банка. В части управления ESG-рисками отмечается их интеграция в действующую систему риск-менеджмента банка. Следует отметить, что в рамках стратегии управления рисками и капиталом был установлен качественный риск-аппетит, который содержит в себе ограничения на финансирование тех проектов и контрагентов, которые не соответствующих целям устойчивого развития.

ПАО «Промсвязьбанк» опубликовал первый публичный отчет за 2024 год об устойчивом развитии, в котором раскрываются экологические, социальные и управленческие аспекты деятельности банка [7]. Документ подготовлен с ориентацией на международные подходы к раскрытию нефинансовой информации. В экологическом блоке отражены проекты, связанные с энергосбережением, развитием экономики замкнутого цикла и внедрением «зеленых» практик в операционной деятельности. Социальный блок включает инициативы в сфере софинансирования пенсионных накоплений, финансовой грамотности, образовательных программ, волонтерства и развития спортивной инфраструктуры. В части корпоративного управления раскрываются подходы к соблюдению стандартов управления, и интеграции принципов устойчивого развития в корпоративные практики. Также следует отметить цифровизацию обслуживания клиентов МСП. Банк ПСБ на базе отечественного ПО разработал и запустил цифровую платформу онлайн-кредитования «Лимит открыт».

Банк Уралсиб имеет исторический опыт публикации нефинансовой и отчетности в области устойчивого развития, однако при этом современные ESG-практики банка раскрываются весьма ограниченно.

Экологические инициативы Банка «Синара» в значительной степени связаны с цифровизацией документооборота и развитием безбумажных технологий [8].

ТАБЛИЦА 1. ESG-практики российских банков (по публичным материалам)

| Критерий/Банк | Сбер | ВТБ | ПСБ | Синара | Уралсиб |
|---|---|---|---|---|---|
| ESG в корпоративных материалах | Системно представлено | Системно представлено | Представлено | Представлено фрагментарно | Представлено частично |
| Экологические инициативы | Да | Да | Да | Преимущественно через цифровизацию | Отдельные инициативы |
| Социальные инициативы | Да | Да | Да | Цифровая доступность сервисов | социальные и благотворительные инициативы |
| Элементы ESG в корпоративном управлении и стратегии | Да | Да | Да | Ограниченно представлены | Частично |

Проведенный в табл. 1 анализ показывает, что уровень интеграции ESG-практик значительно различается в зависимости от масштаба банка и степени цифровой трансформации. Если крупнейшие банки, как правило, рассматривают ESG как часть стратегического управления и цифровой экосистемы, то банки среднего масштаба чаще ограничиваются раскрытием отдельных социальных и экологических инициатив без формирования комплексной ESG-модели. Это свидетельствует о сохраняющейся неоднородности ESG-зрелости российского банковского сектора.

Таким образом, цифровая трансформация банковского сектора не снижает значимость человеческого фактора, а, напротив, усиливает его стратегическую значимость. По мере автоматизации процессов критически возрастает значимость качественного клиентского взаимодействия, доверия и устойчивости человеческого капитала. В этих условиях вопросы вовлеченности персонала, профилактики профессионального выгорания и формирования благоприятной корпоративной среды становятся значимым направлением ESG-повестки и фактором долгосрочной устойчивости банковских организаций.

**Список используемых источников**

1. Официальный сайт Банка России. Глоссарий терминов в области финансирования устойчивого развития и климатического регулирования: электронный ресурс. URL: https://www.cbr.ru/develop/ur/faq/ (дата обращения: 07.05.2026).

2. Официальный сайт Интерфакс. Путин поручил утвердить Стратегию долгосрочного развития биоэкономики. электронный ресурс. URL:https://www.interfax-russia.ru/moscow/news/putin-poruchil-utverdit-strategiyu-dolgosrochnogo-razvitiya-bioekonomiki (дата обращения: 06.05.2026).

3. Егорова М. А., Калимуллина О. В. Ключевые тенденции цифровой трансформации в сфере финансовых услуг // Информационные процессы: концептуальный базис цифровой трансформации экономики: сб. науч.-теорет. статей посвященный 30-летию факультета Цифровой экономики, управления и бизнес-информатики (ЦЭУБИ). СПб.: СПбГУТ им. проф. М. А. Бонч-Бруевича, 2024. С. 98–110.

4. ESG в финансовом секторе России – 2025: аналитическое исследование: электронный ресурс. URL: https://raexpert.ru/researches/sus_dev/esg_fin_rus_2025/#part1 (дата обращения: 08.05.2026).

5. Модельная методология ESG-рейтингов / Центральный банк Российской Федерации, [Департамент корпоративных отношений]. Москва: Банк России, 2023. 44 с.: табл. (Доклад для общественных консультаций). URL: https://library.cbr.ru/catalog/lib/books/989537/ дата обращения: 07.05.2026).

6. Официальный сайт Сбербанка. Годовой отчет за 2024 г. URL: https://www.sberbank.com/ru/investor-relations/groupresults/annual (дата обращения: 22.05.2026).

7. Официальный сайт банка ПСБ. Отчет об устойчивом развитии за 2024 год. URL: https://www.psbank.ru/bank/investors/esg (дата обращения: 22.05.2026).

8. Банк Синара. Банк Синара значительно сократил потребление бумаги благодаря цифровым технологиям // Банк Синара: официальный сайт. 2023. URL: https://sinara.ru/press-centr/news/2023/bank-sinara-znachitelno-sokratil-potreblenie-bumagi-blagodarya-tsifrovym-tekhnologiyam (дата обращения: 22.05.2026).

*Статья представлена кандидатом экономических наук, и.о. заведующего кафедрой ЭД СПбГУТ, доцентом О. В. Калимуллиной.*

## COMPARATIVE ANALYSIS OF ESG PRACTICES OF RUSSIAN BANKS IN THE CONTEXT OF DIGITAL TRANSFORMATION

***Posokhova O.***
*The Bonch-Bruevich Saint Petersburg State University of Telecommunications*

*The relevance of this study stems from the growing role of sustainable development principles, the bioeconomy, and the need to integrate them into the business models of credit institutions amid the active adoption and use of digital technologies. The aim of this study is to analyze Russian banks' approaches to implementing the ESG agenda. The methodological basis is based on an analysis of open sources, a comparative approach, and a summary of current trends in the banking sector. The results obtained can be used for further research and the practical improvement of sustainable development strategies in the banking sector.*

***Key words:*** *ESG, sustainable development, banking sector, commercial banks, digital transformation, ESG practices, corporate governance*

**УДК 334.021**
**ГРНТИ 06.81.12**

# ЦИФРОВЫЕ ТЕХНОЛОГИИ КАК ОСНОВА РАЗВИТИЯ СОВРЕМЕННОГО БИЗНЕСА

**М. А. Сафиуллин, И. Б. Щербаков**

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

*В статье рассматривается роль цифровых технологий как основы развития современного бизнеса. Анализируются сущность и особенности цифровых технологий, их основные направления применения, а также влияние на эффективность деятельности предприятий. Особое внимание уделяется процессу цифровой трансформации, который затрагивает бизнес-процессы, организационную структуру и стратегию развития компаний. Рассматриваются ключевые преимущества цифровизации, включая повышение операционной и маркетинговой эффективности, а также снижение издержек и улучшение качества управленческих решений. Наряду с этим выделяются основные риски и ограничения внедрения цифровых технологий, такие как финансовые затраты, кадровые проблемы и угрозы информационной безопасности. В заключение определяются перспективы дальнейшего развития цифровых технологий в условиях цифровой экономики, включая расширение применения искусственного интеллекта, Big Data и облачных решений.*

***цифровые технологии, цифровизация, цифровая трансформация, бизнес, предприятие, эффективность, искусственный интеллект, Big Data, автоматизация, облачные технологии, интернет вещей, маркетинг, управление***

В условиях стремительного развития цифровой экономики цифровые технологии становятся одним из ключевых факторов, определяющих направления и темпы развития современного бизнеса. Их внедрение приводит к глубоким структурным изменениям в деятельности предприятий, трансформации традиционных бизнес-моделей, перестройке внутренних процессов и изменению способов взаимодействия с потребителями и партнерами. В современных условиях цифровизация уже не рассматривается как вспомогательный инструмент или набор отдельных решений, а выступает как стратегическое направление развития организаций, обеспечивающее их устойчивость, адаптивность и конкурентоспособность в долгосрочной перспективе [1]. Актуальность данной темы объясняется тем, что цифровые технологии оказывают системное воздействие на все уровни функциониро-

вания предприятия – от операционного управления и логистики до маркетинга, аналитики и стратегического планирования.

Под цифровыми технологиями в бизнесе понимается комплекс методов, инструментов и программных решений, обеспечивающих сбор, обработку, хранение и передачу информации в цифровой форме с целью повышения эффективности деятельности предприятия. К таким технологиям относятся системы анализа больших данных, облачные вычисления, искусственный интеллект, интернет вещей, цифровые платформы, а также различные автоматизированные системы управления бизнес-процессами. Их основное значение заключается в том, что данные становятся центральным ресурсом управления, а способность быстро и точно их анализировать формирует основу принятия управленческих решений. В отличие от традиционных методов управления, цифровые технологии позволяют работать с большими массивами информации в режиме реального времени, что существенно повышает точность прогнозов, снижает неопределенность и позволяет компаниям быстрее реагировать на изменения внешней среды [2].

Современные цифровые технологии можно рассматривать как совокупность взаимосвязанных направлений. Одним из наиболее значимых является анализ больших данных (Big Data), который позволяет выявлять скрытые закономерности, прогнозировать поведение потребителей и оценивать рыночные тенденции. Существенную роль играют технологии автоматизации бизнес-процессов, такие как ERP- и CRM-системы, которые обеспечивают интеграцию различных подразделений предприятия, оптимизацию ресурсов и повышение производительности труда. Облачные технологии предоставляют компаниям доступ к вычислительным ресурсам и программному обеспечению без необходимости создания дорогостоящей инфраструктуры, а применение искусственного интеллекта и машинного обучения позволяют при этом автоматизировать довольно сложные аналитические и управленческие задачи, такие как прогнозировать спрос, оптимизировать логистическую инфраструктуру и осуществить персонализацию маркетинговых предложений. Кроме того, технологии интернета вещей, обеспечивают сбор данных с физических объектов в режиме реального времени, а это повышает уровень контроля над производственными и логистическими процессами и позволяет более эффективно управлять ресурсами.

Применение цифровых технологий оказывает существенное влияние на эффективность деятельности предприятий [3], так как значительно повы-

шается эффективность за счет автоматизации рутинных процессов, происходит сокращение времени выполнения операций и осуществляется снижение издержек. При этом применение автоматизации минимизирует влияние человеческого фактора, уменьшает количество ошибок и повышает стабильность работы всех бизнес-процессов. Кроме того, цифровые системы управления делают более прозрачной всю структуру бизнес-процессов и тем самым дают возможность руководству получать актуальную информацию о состоянии всех подразделений в режиме реального времени. Все это способствует повышению качества и обоснованности при принятии управленческих решений, а также дает возможность оперативно реагировать на изменения, происходящие во внешней среде [4].

Нельзя забывать и о том, что цифровизация влияет и на маркетинговую деятельность предприятий, ведь современные цифровые инструменты могут более точно сегментировать рынок и анализировать поведение потребителей, а использование цифровых каналов коммуникации, таких как социальные сети, мобильные приложения и онлайн-платформы, обеспечивает целевое взаимодействие с клиентами и расширяет охват аудитории. Персонализация предложений становится важным конкурентным преимуществом, поскольку позволяет повышать уровень удовлетворенности клиентов и формировать долгосрочную лояльность.

В современных условиях внедрение отдельных цифровых технологий уже недостаточно для обеспечения устойчивого конкурентного преимущества, поэтому предприятия переходят к цифровой трансформации. Цифровая трансформация представляет собой комплексный процесс интеграции цифровых технологий во все сферы деятельности организации, сопровождающийся изменением бизнес-модели, организационной структуры и стратегии развития. В отличие от простой автоматизации, она затрагивает не отдельные процессы, а всю систему функционирования предприятия. Цифровая трансформация может осуществляться поэтапно, когда технологии внедряются постепенно, либо радикально, предполагая полное переосмысление бизнес-модели компании. Важную роль играет клиентоориентированный подход, при котором основное внимание уделяется улучшению взаимодействия с потребителями, повышению качества сервиса и формированию индивидуального клиентского опыта. В рамках цифровой трансформации выделяются ключевые направления изменений, включающие трансформацию клиентского опыта, операционных процессов и биз-

нес-модели, что позволяет комплексно оценить влияние цифровизации на деятельность предприятия [5].

Несмотря на имеющиеся преимущества, цифровизация сопровождается рисками и ограничениями, которые необходимо учитывать при внедрении цифровых технологий. Основным фактором являются высокие финансовые затраты, связанные с приобретением программного обеспечения, оборудования, обучением персонала и модернизацией имеющейся инфраструктуры. Существенным ограничением также является низкий уровень имеющихся цифровых компетенций у сотрудников, что может снизить эффективность использования новых цифровых технологий и вызвать существенное сопротивление происходящим изменениям. Организационные изменения могут сопровождаться внутренним сопротивлением персонала, особенно если отсутствует четкая стратегия управления осуществляемыми изменениями. Существенную угрозу представляет и информационная безопасность, поскольку увеличение передачи объемов цифровых данных повышает риск кибератак и утечек информации. Кроме того, существуют технологические и правовые риски, связанные с выбором альтернативных решений, их возможной совместимостью и необходимостью соблюдения существующих нормативных требований в области обработки данных.

Развитие цифровых технологий связаны с дальнейшим расширением применения искусственного интеллекта, технологий Big Data, облачных решений и интернета вещей. Искусственный интеллект будет все больше и активнее использоваться для создания аналитических отчетов и управления бизнес-процессами в принятии управленческих решений. Развитие технологий анализа данных даст возможность предприятиям точнее осуществлять прогноз поведения потребителей и адаптировать существующие стратегии дальнейшего развития. Облачные технологии позволят снизить затраты и ускорят внедрение инноваций. Цифровые платформы помогут сформировать новые экосистемы и объединить участников рынка. Одновременно должна возрасти роль и кибербезопасности для защиты данных, что станет важным условием устойчивого развития всей цифровой системы предприятия.

Цифровые технологии в настоящее время являются фундаментом для развития современных предприятий, так как они осуществляют автоматизацию бизнес-процессов, повышают эффективность управления и формируют новые бизнес-модели взаимодействия. Использование современных цифровых технологий позволит предприятиям не только повысить текущую эф-

фективность, но и создаст возможность адаптироваться к условиям быстро меняющейся цифровой среды, создавая устойчивые конкурентные преимущества.

**Список используемых источников**

1. Влияние глобальных тенденций цифровизации на трансформацию бизнес-моделей промышленных компаний / И. Н. Краковская [и др.] // Регионология. 2022. Т. 30. № 4. С. 823–850.

2. Цифровая экономика и сквозные технологии: теория и практика / под ред. д-ра экон. наук, проф. А. В. Бабкина. СПб.: ПОЛИТЕХ-ПРЕСС, 2019. 623 с.

3. Хусаинова Е. А. Влияние информационных технологий на развитие бизнеса / Е. А. Хусаинова, Н. А. Серкина // Международный научно-исследовательский журнал. – 2024. № 4 (142). URL: https://research-journal.org/archive/4-142-2024-april/10.23670/IRJ.2024.142.110 (дата обращения: 27.05.2026).

4. Цифровые технологии как фактор устойчивого развития малого бизнеса / К. А. Мызрова, Н. Ж. Мявлина, Ю. Н. Захарова, А. С. Заводцков // Креативная экономика. 2024. Т. 18. № 9. С. 2193-2210.

5. Миролюбова Т. В., Радионова М. В. Оценка влияния факторов цифровой трансформации на региональный экономический рост // Регионология. 2021. Т. 29. № 3 (116). С. 486–510.

## DIGITAL TECHNOLOGIES AS THE BASIS FOR THE DEVELOPMENT OF MODERN BUSINESS

**Safiullin M, Shcherbakov I.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article examines the role of digital technologies as the basis for the development of modern business. The essence and features of digital technologies, their main applications, as well as their impact on the efficiency of enterprises are analyzed. Special attention is paid to the process of digital transformation, which affects business processes, organizational structure and development strategy of companies. The key advantages of digitalization are considered, including increasing operational and marketing efficiency, as well as reducing costs and improving the quality of management decisions. Along with this, the main risks and limitations of the introduction of digital technologies are highlighted, such as financial costs, personnel problems and threats to information security. In conclusion, the prospects for further development of digital technologies in the digital economy are determined, including the expansion of the use of artificial intelligence, Big Data and cloud solutions.*

***Key words:*** *digital technologies, digitalization, digital transformation, business, enterprise, efficiency, artificial intelligence, Big Data, automation, cloud technologies, Internet of things, marketing, management*

**УДК 378.02:372.850.4**
**ГРНТИ 14.35.00**

# ПРОБЛЕМЫ ЭКОЛОГИЧЕСКОГО ОБРАЗОВАНИЯ В РОССИИ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ

**В. И. Стурман**

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

*Представлены содержание и результаты обсуждения хода и перспектив реформирования высшего экологического образования в России на состоявшемся пленуме Учебно-методического объединения университетов по наукам о Земле. Раскрыты проблемы и противоречия, выявившиеся в ходе реформирования высшего образования, изложены сформулированы преподавательским сообществом предложения.*

***экологическое образование, учебно-методическое объединение, науки о Земле***

Вопросы реформирования высшей школы России обсуждаются уже 4-й год [1]. Однако обсуждение, состоявшееся (с участием автора) на пленуме 23-24 апреля на базе РГПУ им. А.И. Герцена Учебно-методического объединения университетов по наукам о Земле, выявило, увы, невысокую степень готовности конструктивных решений и соответствующих документов. Проблемы начинаются с того, что не решены вопросы целеполагания намечаемого реформирования. Выход из Болонского процесса едва ли может рассматриваться как самоцель, а призыв к формированию национальной системы образования, в которой будет представлено все лучшее… неконкретен. При этом никаких официальных проектов участникам пленума представлено не было, и излагаемые ниже предложения вносились от имени общественных организаций (Ассоциация классических университетов России и др.), рабочих групп и вузов, участвующих в «пилотных проектах».

Министерство недвусмысленно выразило намерение сократить число укрупненных групп специальностей и направлений подготовки (УГСН) и самих направлений (специальностей). Мотивируется это якобы избыточностью их числа при существующем положении, хотя более правдоподобной может быть версия об элементарном стремлении органа управления к облегчению своих управленческих функций.

Направление подготовки (специальность) «Экология и природопользование», согласно представленных разработок, входит в УГСН 3 «Науки о Земле», наряду с географией и картографией, геологией, гидрометеорологией. Объединение географии с картографией и геоинформатикой, предлагаемое в качестве компромисса, встретило критику заинтересованных ведомств, таких как Роскартография, Роскадастр. И в самом деле, много ли общего в профессиях учителя географии и кадастрового инженера? Вопрос риторический.

Основное содержание представленных нововведений выглядит следующим образом. Федеральные государственные образовательные стандарты (ФГОСы) будут создаваться не для отдельных направлений (специальностей), а для целых УГСН. Срок базового высшего образования по наукам о Земле составит 5 лет. Из них первые 2 года будет занимать освоение «фундаментального ядра», единого для всей УГСН. «Ядро» включает: социально-гуманитарные дисциплины (30 з.е.), дисциплины математики и информатики (15 з.е.), науки о Земле (география, геология, учения об атмосфере, гидросфере, биосфере) – 30 з.е., из которых 6 з.е. отводится на «обязательные элективы», призванные все же отличить геолога от эколога и т.п., учебные практики (15 з.е.). Итого набирается 90 з.е., что несколько меньше стандартных для 2 лет обучения 120 з.е. Однако если учесть, что из приведенного перечня как-то выпали естественные науки (физика, химия, биология…), то недостающие 30 з.е. как раз этому примерно и соответствуют. Непонятно только, где здесь место для такой важнейшей науки о Земле (и в то же время биологической), как почвоведение. Не потерять бы. Далее, на последующих 3 курсах следует часть учебного плана, формируемая участниками образовательных отношений (174 з.е.) и государственная итоговая аттестация (6 з.е., в формах выпускной квалификационной работы, госэкзамена, или стартапа). Итого набирается 300 з.е. Предусматривается не менее 2 профильных практик, в т.ч. не менее 1 на рабочем месте.

Данная структура подверглась резкой критике со стороны участников пленума по следующим мотивам. УГСН «Науки о Земле», хотя и немногочисленна и, казалось бы, однородна, в реальности содержит направления подготовки и сферы профессиональной деятельности, весьма далекие по своему содержанию и требованиям к содержанию обучения. Так, для метеоролога математика – важнейший рабочий инструмент, и физико-математическая подготовка для этой специальности традиционно велась на уровне

физических факультетов. В современных условиях всеобщего перехода к численным методам прогноза погоды эти особенности только усилились. Геологу математика, конечно же, тоже нужна, но… Автор этих строк первые 9 лет своей трудовой жизни работал в геолого-поисковой партии в системе Министерства геологии РСФСР, в должности геолога. И на основании данного опыта могу констатировать: математика геологу-производственнику требовалась только для составления ежемесячных «ведомостей по категориям» для буровых бригад, для чего вполне хватало изученных в начальной школе 4 арифметических действий. И как программу по математике сформировать так, чтобы и метеорологу хватило, и геолога лишним не перегрузить? То же в отношении физики, химии, учебных полевых практик. Они, конечно, жизненно необходимы во всех науках о Земле. Но разные. Метеорологу геологический молоток нужен не более, чем геологу метеорологические приборы. И как совместить интересы тех и других? На старших курсах поздно, там на производственную практику надо отправляться, и отправляться подготовленным, с некоторыми уже полученными профессиональными навыками.

В качестве мотивировки идеи «фундаментального ядра» министерство указывает на возможность беспрепятственного перехода студентов в рамках УГСН с одного направления (специальности) на другое. Но много ли таких студентов в реальности, и лучшие ли это студенты? Особенно с учетом ограниченности числа бюджетных мест в вузах. Поэтому в резолюцию пленума была включена формулировка о недопустимости ухудшения условий и качества подготовки всех ради удобства крайне немногочисленных любителей переходов. Странный приоритет.

Большой интерес вызвало выступление представителя Тюменского государственного университета, где общее для всех «ядро» было введено уже в 2017 г. Результатом стали весьма своеобразные переходы, с биологии на экономику, с физики на экологию и т.п. Решили все же сделать 2 ядра: hard и soft. Общие результаты – снижение доли профильных дисциплин, сокращение практик, депрофессионализация.

Также министерство продвигает возможность получения по ходу обучения рабочих профессий и соответствующих квалификаций. Неясно только, когда это делать, если первые 2 года полностью занимает «фундаментальное ядро», и места для чего-либо еще там не остается. Неясно также, что такое рабочая профессия применительно к сфере экологии и природопользования.

Важное место во многих выступлениях заняли вопросы трудоустройства выпускников и взаимодействия с работодателями. И здесь также проявились большие различия между направлениями (специальностями). Если у метеорологов и картографов есть «якорные» работодатели, то к экологам это не относится ни в малейшей степени. Экологи трудоустраиваются только поодиночке, и в каждом регионе – своя специфика рынка труда для экологов [2].

Состоялся разговор и о судьбе магистратуры в условиях перехода к 5-летнему сроку базового образования. Отказываться от нее не предлагал никто, но общим стал вывод о целесообразности ее сохранения в качестве подготовительного уровня образования перед аспирантурой, и для выпускников бакалавриата из зарубежных стран.

В целом, состоявшееся обсуждение показало невысокий уровень продуманности намечаемой реформы высшего образования.

**Список используемых источников**

1. Указ Президента РФ от 12.05.2023 N 343 «О некоторых вопросах совершенствования системы высшего образования». URL https://www.consultant.ru/law/hotdocs/80246.html (дата обращения 03.02.2026).

2. Стурман В. И., Малькова И. Л., Захарова С. А. Анализ рынка труда экологов как необходимое условие формирования образовательных программ направления подготовки «Экология и природопользование» // Вестник Удмуртского университета. Серия: биология, науки о Земле. № 4. 2013. С. 179-183.

## PROBLEMS OF ENVIRONMENTAL EDUCATION IN RUSSIA AT THE PRESENT STAGE OF DEVELOPMENT

**Sturman V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article presents the content and results of the discussion on the progress and prospects of reforming higher environmental education in Russia at the plenary session of the Educational and Methodological Association of Universities in Earth Sciences. The problems and contradictions that emerged during the reform of higher education are identified, and proposals formulated by the teaching community are presented.*

***Key words:*** *environmental education, educational and methodological association, Earth Sciences*

**УДК 303.687**
**ГРНТИ 15.81.25**

# УЧЕБНАЯ МОТИВАЦИЯ И УЧЕБНАЯ АКТИВНОСТЬ СТУДЕНТОВ: ЗОНА УПРАВЛЕНИЯ

**С. И. Хитрин, И. Ю. Хитрина**

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

*Учебная мотивация студентов представляет собой сложное, многокомпонентное образование. Она испытывает влияние множества факторов – от личностных особенностей студентов до организационных условий и стиля педагогического общения. Опыт внедрения в учебный процесс балльно-рейтинговой системы с элементами геймификации показывает, что она является эффективным инструментов управления учебной мотивацией и учебной активностью студентов.*

***учебная мотивация, учебная активность, коммуникативные барьеры, балльно-рейтинговая система, геймификация***

В психолого-педагогической науке под мотивацией понимают совокупность внутренних и внешних побудительных сил, которые направляют поведение человека, придают ему смысл и определяют его активность [1]. Применительно к учебной деятельности мотивация – это система побуждений, заставляющих студента осваивать знания, развивать умения и навыки, стремиться к достижению образовательных результатов. Мотивация учебной деятельности включает три компонента.

1. Потребностно-смысловой компонент отражает, какие личностные потребности удовлетворяет учеба: это может быть стремление к новым знаниям, желание занять достойное место в группе или потребность в достижениях.

2. Ценностный компонент связан с тем, какое значение студент придает образованию в целом и изучению конкретных дисциплин. Стремится ли студент преуспеть в профессии или учится формально, ради получения диплома.

3. Эмоционально-волевой компонент проявляется в том, насколько устойчив интерес студента к учебе, способен ли он преодолевать трудности, как относится к своим успехам и неудачам [2].

В зависимости от того, откуда исходит побуждение, различают внешнюю и внутреннюю мотивацию.

Внешняя мотивация связана с факторами, лежащими за пределами самой учебы. Это может быть стремление получить высокую оценку, избежать наказания, заслужить одобрение родителей или преподавателей. Человек, движимый внешними побуждениями, учится потому, что «так надо», а не потому, что ему интересно.

Внутренняя мотивация, напротив, обусловлена интересом к самому процессу познания. Студент получает удовольствие от того, что разбирается в сложных вопросах, осваивает новый материал, понимает, как полученные знания могут пригодиться в жизни.

Педагогический опыт показывает, что наиболее устойчивой и продуктивной является именно внутренняя учебная мотивация. Студент, который учится потому, что ему это интересно, проявляет большую настойчивость при встрече с трудностями, глубже осваивает учебный материал, испытывает меньшее эмоциональное напряжение [3].

По содержательной направленности различают познавательные и социальные мотивы. Познавательные связаны с интересом к содержанию учебного материала, стремлением разобраться в сложных вопросах, удовлетворить любознательность. Социальные отражают стремление студента занять определенное положение в группе, получить признание, подготовиться к будущей профессиональной деятельности [2].

Мотивационная сфера студента формируется под влиянием множества факторов, которые можно разделить на несколько групп.

Личностные факторы связаны с индивидуальными особенностями самого студента. Сюда относят его познавательную активность, уровень притязаний, самооценку, тревожность, волевые качества [1].

Социальные факторы связаны с окружением студента, его взаимодействием с другими участниками образовательного процесса. Не маловажную роль играет учебная группа [4].

Организационные факторы охватывают условия, в которых протекает учебная деятельность. Сюда входят качество преподавания, доступность учебных материалов, техническое оснащение учебного процесса, расписание занятий, организация самостоятельной работы.

Среди всех факторов, влияющих на учебную мотивацию, особого внимания заслуживает ясность требований и объективность оценки знаний. Практика показывает, что именно неясность критериев и субъективность преподавателя выступают наиболее частыми причинами снижения интереса к учебе и возникновения конфликтов [5].

Отношения в диаде «преподаватель-студент» занимают особое место среди факторов, влияющих на учебную мотивацию. Преподаватель выступает для студента не только как источник знаний, но и как значимый взрослый. Его отношение, оценка, поддержка или критика оказывают мощное воздействие на учебную активность и самооценку студента.

Учебная мотивация студентов, будучи сложной системой мотивов, испытывает влияние множества факторов, как внутренних, идущих от личности студента, так и внешних, связанных с образовательной средой и особенностями стиля педагогического воздействия. Понимание этих факторов создает основу для поиска способов оптимизации взаимодействия между преподавателями и студентами, направленных на повышение учебной мотивации и учебной активности студентов и снижение конфликтогенности образовательной среды.

Эффективность взаимодействия в диаде «преподаватель-студент» во многом определяется тем, насколько успешно участники образовательного процесса обмениваются информацией, понимают друг друга, согласовывают свои ожидания и действия. Однако на пути этого взаимодействия нередко возникают препятствия, которые затрудняют или искажают коммуникацию, приводят к недопониманию, а в конечном итоге – к конфликтным ситуациям и снижению учебной мотивации. В теории коммуникации такие препятствия получили название коммуникативных барьеров. Под коммуникативными барьерами понимаются факторы, которые препятствуют эффективному общению, затрудняют передачу и восприятие информации, создают искажения в понимании смысла сообщений.

В образовательной среде коммуникативные барьеры могут возникать как по объективным причинам (недостаточная техническая оснащенность, высокая учебная нагрузка), так и по субъективным (личностные особенности участников, различия в ценностных ориентациях, несовпадение коммуникативных стилей).

Особенность коммуникативных барьеров в педагогическом взаимодействии заключается в том, что они не только затрудняют передачу учебной информации, но и влияют на эмоциональный фон общения, формирование доверия, готовность сторон к открытому диалогу. Преодоление этих барьеров требует от участников осознанного отношения к процессу коммуникации, развития соответствующих навыков и использования доступных инструментов [6].

В научной литературе выделяются различные основания для классификации барьеров общения. Наиболее распространенным является деление на психологические, социальные и организационные барьеры, каждый из которых имеет свою специфику проявления в образовательной среде.

Психологические барьеры связаны с индивидуальными особенностями участников взаимодействия. К их числу относятся:

– барьеры восприятия, возникающие, когда один участник общения неадекватно воспринимает другого на основе сложившихся стереотипов или установок [1];
– барьеры установки, проявляющиеся в готовности участника коммуникации оценивать информацию определенным образом без ее фактического осмысления.

Эмоциональные барьеры возникают на фоне сильных переживаний – тревоги, обиды, гнева, разочарования. В состоянии эмоционального возбуждения участник общения неспособен адекватно воспринимать информацию [1].

Барьеры невербальной коммуникации проявляются в несоответствии между вербальными и невербальными сигналами (мимика, жесты, интонация, поза).

Социальные барьеры обусловлены различиями в социальном положении, статусе, принадлежности к определенным группам. В образовательной среде наиболее значимыми социальными барьерами являются:

– статусно-ролевые барьеры, связанные с асимметрией власти в диаде «преподаватель-студент» [7];
– генерационные барьеры, которые связаны с различиями в ценностных ориентациях, жизненном опыте, способах коммуникации между поколениями. Несовпадение коммуникативных стилей может порождать взаимное непонимание и раздражение [8].

Ценностные барьеры возникают, когда у участников общения существует различное понимание целей образования, критериев успешности, допустимых норм поведения. Для преподавателя важнейшей ценностью может быть глубокое освоение предмета, для студента – получение высокого балла с минимальными усилиями. Такое расхождение ценностных установок создает почву для постоянных противоречий и конфликтов [9].

Внедрение цифровых технологий в образовательный процесс внесло существенные изменения в коммуникацию между преподавателями и студентами, породив новые типы барьеров: асинхронность коммуникации, сни-

жение невербальной составляющей, размывание границ (ожидание доступности преподавателя 24/7), технические барьеры.

Наличие устойчивых коммуникативных барьеров оказывает негативное влияние на все аспекты образовательного процесса. Снижается качество передачи учебной информации, студенты хуже понимают требования преподавателя, преподаватели не получают адекватной обратной связи о том, насколько успешно усвоен материал. Ухудшается эмоциональный фон общения, нарастает взаимное раздражение, формируются устойчивые негативные установки по отношению друг к другу. Наиболее серьезным последствием становится повышение конфликтогенности образовательной среды. Барьеры, которые не были своевременно замечены и устранены, создают почву для возникновения конфликтных ситуаций. При этом сам конфликт часто разворачивается не вокруг содержательных вопросов (качество знаний, корректность оценки), а вокруг тех самых барьеров, которые исказили восприятие и взаимопонимание сторон.

Таким образом, выявление и преодоление коммуникативных барьеров представляет собой важнейшую задачу управления взаимодействием в диаде «преподаватель-студент». Понимание природы этих барьеров, их разновидностей и специфики проявления в условиях цифровизации создает основу для поиска эффективных способов их минимизации, в том числе с использованием современных цифровых инструментов (в частности, в сфере оценочных решений).

Разработанная на кафедре экономики данных СПбГУТ доцентом И. Ю. Хитриной и старшим преподавателем С. И. Хитриным балльно-рейтинговая система (БРС) с элементами геймификации направлена на решение вышеуказанных проблем. БРС находится на стадии экспериментального тестирования в пяти группах второго курса по дисциплинам «Менеджмент» и «Управление конфликтами и деловые переговоры». На данный момент система реализована в офлайн-формате в виде документов, правил, критериев и их применения в оценке учебной активности студентов. Сведения о заработанных баллах и рейтинге студентов в учебной группе периодически доводятся до студентов в виде Excel-таблиц через сообщения в личном кабинете. Полноценная цифровая реализация БРС дорабатывается. Особенностью экспериментальной БРС является не просто зарабатывание студентами баллов за выполнение учебных заданий и определение рейтинга достижений по сравнению с другими членами группы, а включение в учебный процесс соревнования, командной работы, творческих дополнительных

заданий. Помимо индивидуального вознаграждения за учебную активность, система включает командное вознаграждение и вознаграждение за помощь другим членам группы, удовлетворяющие потребности в компетентности, отношениях с другими людьми и автономии.

На основании полученного опыта использования геймифицированной БРС можно констатировать усиление учебной мотивации и активности студентов на лекциях и практических занятиях, в выполнении творческих и дополнительных заданий. Анализ итогов первого этапа эксперимента предполагает не только его продолжение, но и распространение на другие учебные дисциплины и использование автоматизированной версии.

**Список используемых источников**

1. Хьелл Л., Зиглер Д. Теории личности. Санкт-Петербург: Питер. 2022. 608 с.
2. Зборовский Г. Е. Социология образования. М.: Гардарики. 2018. 304 с.
3. Анцупов А. Я., Шипилов А. И. Конфликтология: учебник для вузов. М.: ЮНИТИ-ДАНА. 2020. 591 с.
4. Вайндорф-Сысоева М. Е., Панькина Е. В. Управление педагогическими конфликтами в цифровой образовательной среде // Профессиональное образование в России и за рубежом. 2021. № 3 (43). URL: https://cyberleninka.ru/article/n/upravlenie-pedagogicheskimi-konfliktami-v-tsifrovoy-obrazovatelnoy-srede (дата обращения: 31.05.2026).
5. Орлова Е. С. Вертикальные конфликты в образовательной среде // Форум молодежной науки. 2021. № 1. URL: https://cyberleninka.ru/article/n/vertikalnye-konflikty-v-obrazovatelnoy-srede (дата обращения: 30.05.2026).
6. Кибанов А. Я. Конфликтология. М.: ИНФРА-М. 2023. 302 с.
7. Куприянов, Р. В. Межличностные конфликты в диаде преподаватель – студент: [монография] / Р. В. Куприянов. Казань: КГТУ. 2011. 194 с. 193 с. ISBN 978-5-7882-1185-5. URL: https://rucont.ru/efd/229640 (дата обращения: 30.05.2026).
8. Гришина Н. В. Психология конфликта. Санкт-Петербург: Питер, 2022. 576 с.
9. Дмитриев А. В. Конфликтология. Москва: Гардарики. 2009. 320 с.

## STUDENTS' LEARNING MOTIVATION AND LEARNING ACTIVITY: MANAGEMENT AREA

**Khitrin S., Khitrina I.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Students' learning motivation is a complex, multicomponent education. She is influenced by many factors, from the personal characteristics of students to the organizational conditions and style of pedagogical communication. The experience of introducing a point-rating system with gamification elements into the educational process shows that it is an effective tool for managing students' learning motivation and learning activity.*

***Key words:*** *educational motivation, learning activity, communication barriers, point rating system, gamification*

**УДК 94(489)**
**ГРНТИ 03.09.55**

# ОБЩЕСТВЕННОЕ ДВИЖЕНИЕ ПРОТИВ АТОМНОГО ОРУЖИЯ В ШВЕЦИИ ВО ВТОРОЙ ПОЛОВИНЕ XX В. (НА ПРИМЕРЕ AMSA)

**И. А. Цверианашвили**

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

*Статья посвящена основанию и деятельности «Инициативной группы против атомной бомбы» – общественного объединения шведских граждан, преимущественно из числа творческой интеллигенции, зародившегося в конце 1950-х гг., и декларировавшего неприятие ядерного (атомного) вооружения в стране. За относительно небольшой срок AMSA смогло добиться перемен в общественных настроениях в стране и повлиять на правящую социал-демократическую партию в вопросе финансирования ядерных разработок. Несмотря на скорый роспуск, группа смогла стать ярким явлением в шведской общественной жизни и повлиять на идею развития «мирного атома» в стране.*

***Швеция, общественное движение, атомная энергия, атомная бомба, экологический активизм***

Опыт коллективной травмы, полученной человечеством в результате сброса атомных бомб летом 1945 г. даже спустя многие десятилетия остается предметом дискуссий. В разное время, в государствах мира появлялись общественные движения и инициативные группы граждан, выступавшие, как против атомного вооружения, так и против развития атомной энергетики в целом. Не стала исключением и Швеция, где общественная борьба с атомным вооружением была, возможно, наиболее активной в Скандинавии, и достигшей определенных успехов. Эти успехи, не в последнюю очередь, были связаны с деятельностью AMSA (швед. Aktionsgruppen mot svensk atombomb), основу которой составила творческая интеллигенция страны.

В конце августа 1945 г. в Швеции начались собственные разработки атомного вооружения, а к концу 1948 г. стало ясно, что страна способна создать собственное атомное вооружение в течение ближайших 10 лет, а с иностранной помощью, предположительно, американской, еще быстрее. В начале 1950-х гг. идея развития атомного вооружения была поддержана ча-

стью социал-демократических сил, и лично – премьер-министром и главой Социал-демократической партии Швеции Таге Эрландером (1901 – 1985) [1]. Военное ведомство страны, во главе с Торстеном Нильссоном (1905 – 1997) также активно поддерживало проект. При этом, даже по самым оптимистичным расчетам, программа по созданию данного типа вооружений обходилась бы в половину военного бюджета страны.

Параллельно с этим, преимущественно в Стокгольме, формируется группа активных граждан, на кого события 1945 г. произвели неизгладимый эффект, и кто не мог оставаться в стороне от вопроса появления ядерных мощностей в стране. В их числе были: художницы Молли Фаустман (1883 – 1966) и Анна Щедаль (1934 – 2001), политики Брор Эдберг (1899 – 1987) и Эльса Седергрен (1893 – 1996), геолог Гуннар Бесков (1901 – 1991), архиепископ Уппсалы Ингве Брилиот (1891 – 1959), литературный критик Стиг Карлсон (1920 – 1971) и целый ряд литераторов: Карл-Эмиль Энглунд (1903 – 1964), Гуннар Вальстрем (1903 – 1983), Барбру Альвинг (1909 – 1987), Астрид Петтерссон (1909 – 1998), Карл Отто Саморе (1904 – 1988). Негласными лидерами объединения являлись писатели Сара Лидман (1923 – 2004) и Пер Андерс Фогельстрем (1917 – 1998). Многие участники движения также придерживались пацифистских взглядов, состояли в феминистском движении. Наконец, в 1958 г. этот коллектив оформляется в «Инициативную группы против атомной бомбы» [2], ставшую объектом изучения не только для истории общественных движения страны, но и для истории национальной науки и техники.

AMSA сразу же высказалась принципиально против появления атомного вооружения в стране, по их мнению, оно было «бесполезно с военной точки зрения, политически ошибочным и морально предосудительным» [3]. Члены AMSA писали, что «враги страны» (не уточняя, имеется ли ввиду СССР или другое недружественное государство), уже в данный момент располагают арсеналом из тысяч боезарядов и на этом фоне обладание Швецией собственным ядерным запасом становится бессмысленным – у других стран подобного оружия будет всегда больше. Кроме того, обладание собственным ядерным арсеналом не только не уберегло бы Швецию от будущих конфликтов, но и было бы негативно воспринято потенциальным противником.

Особенности географического положения и социально-экономического развития страны в конце 1950-х гг. свидетельствовали и о том, что потенциальному противнику было бы достаточно всего пяти бомб для уничто-

жения пяти крупнейших городов (Стокгольма, Мальме, Гетеборга, Уппсалы и Вестероса) и почти миллиона жителей. Даже такое число сброшенных бомб означало бы полную катастрофу и немедленную капитуляцию. В связи с этим, сама концепция национальной обороны страны ставилась под большое сомнение [3]. Более того, присоединение Швеции к ядерной гонке усиливало бы и без того стремительно нараставшее ощущение глобального страха и нестабильности.

На страницах своих листовок AMSA пытались рассуждать и лицемерии международных отношений, отразив тот факт, что в двусторонних и многосторонних переговорах не учитываются нормы морали, человечности, гуманизма. Использование атомного оружия глубоко противоречит человеческой природе и морали, затрагивает не только живущее, но и будущие поколения [4]. Таким образом, для использования атомного оружия не может быть морального оправдания, а ценность человеческой жизни и свободы утрачиваются [5]. В этих рассуждениях AMSA предвосхитили идеи и принципы устойчивого развития, которые станут актуальными спустя четверть века.

Дальнейшие рассуждения участников AMSA естественным образом продолжали упомянутые тезисы: можно ли внести вклад в мирное развитие человечества путем создания атомных бомб? Члены группы предлагали уделить больше внимания борьбе с голодом, эпидемиями и нищетой и тратить ресурсы на гуманитарные нужды, а не военные, предвосхитив статус Швеции как ведущей гуманитарной державы конца 1990-х – начала 2000-х гг. Для конца 1950-х гг. данная общественная риторика была еще не столь привычной.

Еще в 1957 г. Пер Андерс Фогельстрем частично выразил идеи будущей AMSA на страницах газеты «Folket i Bild», принадлежавшей социал-демократам, где был опубликован ряд его статей. Эти публикации, а также петиция писательницы Ингегерд Гранлунд (1903 – 1978) против ядерного оружия, позволили заинтересовать антиядерными идеями десятки тысяч человек, даже несмотря на их радикальность по тем временам. Необычным было участие в движении и епископа Брилиота, ведь церковь страны крайне редко высказывалось по конкретным поводам, а само участие высокопоставленного священника было неслыханным. При этом, как отмечает Торд Бьерк, в группу запрещено было принимать коммунистов, чтобы избежать критики СССР [6].

К 1961 г. AMSA фактически перестает существовать, выполнив, однако, две цели – широко заразив антиядерными идеями население страны, и, внеся раскол в правящую социал-демократическую партию. Появляется новая общественная организация – КМА (швед. Kampanjen mot atomvapen), возглавляемая журналистом Бертилем Сванстремом (1907 – 1972), открытая для молодежи и левых. В конце 1960-х гг., американский «ядерный зонт» достиг Швеции, и острая необходимость в собственных разработках начала отпадать. Летом 1968 г. страна подписала Договор о нераспространении ядерного оружия, ратифицировав его спустя полтора года [7]. Несмотря на то, что в стокгольмских лабораториях эксперименты с оружейным плутонием велись до 1972 г., ядерных амбиций Швеция более не испытывала. На примере AMSA можно судить о силе общественного североевропейского движения, неравнодушии собственных граждан к будущему страны и истории и о том, что даже относительно небольшая группа людей способна влиять на национальную внутреннюю и внешнюю политику.

**Список используемых источников**

1. Корунова Е. В. От ядерных амбиций к добровольному отказу: шведская ядерная программа в условиях холодной войны (1945-1970) // Клио. 2025. № 9 (225). С. 52-57.

2. Agrell W. Övrig illegal verksamhet: övervakningen av de svenska kärnvapenmotståndarna 1958-1968. Stockholm: Wahlström & Widstrand, 1999. 217 s.

3.. Aktionsgruppen mot svensk atombomb (AMSA). Programkommentar. URL: https://sklivedata.blob.core.windows.net/content-files/SSA/1280_AMSA/SE_SSA_1280_program.pdf (дата обращения: 07.05.2026).

4. Skall Sverige ha atombomb?: åtta anföranden om ÖB och atomkapprustningen. Stockholm, Sigtuna: Civiltr., 1958. 69 s.

5. Mot svensk atombomb: meddelanden från AMSA (Aktionsgruppen mot svensk atombomb). Stockholm: Embe boktr., 1958. 1 s.

6. Björk T. Nordisk folkrörelsehistoria. 7. Det utopiska ambulansförsvaret. URL: https://web.archive.org/web/20070808201526/http://www.folkrorelser.nu/alternativnorden/alternativnorden7.html (дата обращения: 07.05.2026).

7. Jonter T. Sweden and the bomb. The Swedish plans to acquire nuclear weapons, 1945-1972. 88 pp. URL: https://inis.iaea.org/records/ef28x-8zt39 (дата обращения: 07.05.2026).

*Статья представлена кандидатом исторических наук, доцентом кафедры истории и регионоведения СПбГУТ О. А. Яковлевым*

# THE PUBLIC MOVEMENT AGAINST NUCLEAR WEAPONS IN SWEDEN IN THE SECOND HALF OF THE XXTH CENTURY (ON THE EXAMPLE OF AMSA)

**Tsverianashvili I.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article explores the founding and activities of the «Action Group Against the Atomic Bomb», a public association of Swedish citizens, primarily from the creative intelligentsia, formed in the late 1950s and declaring its opposition to nuclear weapons in the country. In a relatively short period of time, AMSA succeeded in changing public sentiment and influencing the ruling Social Democratic Party on the issue of funding nuclear research. Despite its rapid dissolution, the group became a prominent figure in Swedish public life and influenced the development of «peaceful atoms» in the country.*

***Key words:*** *Sweden, social movement, atomic energy, atomic bomb, environmental activism*

**УДК 654.078**
**ГРНТИ 06.71.11**

# ОСОБЕННОСТИ ВЛИЯНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА РАБОТУ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПАНИИ

**И. Б. Щербаков, М. А. Янковский**

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

*В современном мире телекоммуникационные компании активно внедряют технологии искусственного интеллекта, что существенно трансформирует характер труда персонала и подходы к управлению человеческими ресурсами. В условиях высокой конкуренции и цифровизации экономики использование искусственного интеллекта становится важнейшим инструментом повышения эффективности бизнеса, оптимизации процессов и улучшения качества обслуживания клиентов. В работе рассмотрены особенности влияния искусственного интеллекта на деятельность персонала в телекоммуникационной компании, выделены ключевые направления трансформации трудовых функций, проанализированы преимущества и риски внедрения искусственного интеллекта, а также обозначены перспективы дальнейшего развития взаимодействия человека и интеллектуальных систем.*

***искусственный интеллект, телекоммуникации, персонал, автоматизация, цифровизация***

Современные телекоммуникационные компании используют искусственный интеллект (ИИ) для решения широкого спектра задач. Интеллектуальные алгоритмы применяются при обработке обращений клиентов, анализе больших объемов информации, управлении сетевой инфраструктурой и прогнозировании нагрузки на телекоммуникационное оборудование. Благодаря этому предприятия могут повысить скорость выполнения операций и сократить издержки [1].

Особенностью внедрения искусственного интеллекта является изменение характера труда сотрудников. Однотипные и повторяющиеся операции автоматизируются, а их выполнение передается интеллектуальным системам, что позволяет снизить нагрузку на персонал и уделять внимания задачам принятия. Так, например, виртуальные помощники и чат-боты способны самостоятельно обрабатывать типовые запросы абонентов, и обеспечивать быстрое получение необходимой информации, сокращая время ожидания ответа.

Алгоритмы искусственного интеллекта позволяют формировать цифровой профиль каждого абонента на основе анализа потребления оказанных услуг и истории обращений в службу поддержки клиентов, что помогает решать проблемы у абонентов еще до их обращения в компанию.

Внедрение интеллектуальных диалоговых систем обеспечивает круглосуточную поддержку абонентов, мгновенно обрабатывая типовые запросы, и корректно переводят решения сложных ситуаций на специалистов-операторов. Такой подход повышает лояльность и удовлетворенность у существующих абонентов и способствует увеличению дохода на одного пользователя за счет эффективных продаж необходимых абоненту телекоммуникационных услуг.

Развитие технологий искусственного интеллекта меняет требования к квалификации работников, так как на рынке труда есть потребность в специалистах, обладающих навыками программирования и навыками в обеспечении информационной безопасности. Сотрудникам телекоммуникационных компаний необходимо совершенствовать профессиональные компетенции и осваивать новые цифровые сервисы, так как операторы связи планируют активно применять искусственный интеллект для автоматизации управления и повышения качества клиентского сервиса. Все это позволит существенно увеличить производительность труда, снизить операционные расходы и повысить устойчивость телекоммуникационных систем.

Но, несмотря на очевидные преимущества, внедрение искусственного интеллекта оказывает неоднозначное влияние на персонал компаний. Автоматизация может привести к сокращению рабочих мест, связанных с выполнением стандартных операций, но при этом развитие искусственного интеллекта связано с появлением новых профессий и направлений деятельности, требующих высокой квалификации и глубоких технических знаний.

Одной из наиболее значимых особенностей влияния искусственного интеллекта на работу телекоммуникационной компании является переход от традиционных методов эксплуатации сетей к концепции автономного управления. В рамках данного подхода алгоритмы машинного обучения осуществляют непрерывный анализ телеметрических данных, поступающих с сетевых элементов базовых станций, маршрутизаторов, оптических узлов в режиме реального времени. Системы на базе искусственного интеллекта способны с высокой точностью прогнозировать пиковые нагрузки и аномальные состояния, заблаговременно инициируя перераспределение ресурсов (например, балансировку нагрузки между сотами) и предотвращая тем самым изменения показателей качества обслуживания.

Кроме того, применение искусственного интеллекта для динамической оптимизации маршрутизации трафика, учитывающей не только статическую топологию сети, но и прогнозируемое поведение пользователей, позволяет существенно повысить общую пропускную способность сети при одновременном снижении операционных издержек. Автоматизация управления полным жизненным циклом сетевых элементов минимизирует влияние человеческого фактора, сокращает время вывода на рынок новых сервисов и повышает общую отказоустойчивость телекоммуникационной инфраструктуры.

Дополнительные изменения происходят и в организационной структуре компаний, так как цифровые интеллектуальные технологии развивают дистанционный формат работы и участвуют при взаимодействии сотрудников, повышая значение командной деятельности при управлении персоналом [2].

Можно выделить основные преимущества применения искусственного интеллекта в деятельности телекоммуникационной компании: рост производительности труда, уменьшение количества совершаемых ошибок при выполнении операций, ускорение обработки и анализа информации для принятия оптимального управленческого решения, повышение качества обслуживания различных групп абонентов, оптимизация существующих бизнес-процессов компании.

Однако, нельзя забывать о том, что существуют определенные сложности, связанные с внедрением искусственного интеллекта, а именно: существенный риск сокращения персонала, необходимость дополнительных затрат на обучение и повышения квалификации работников, увеличение зависимости от цифровых технологий, вероятность возникновения киберугроз и утечки данных компании, а также психологическое сопротивление осуществляемым изменениям со стороны сотрудников.

В телекоммуникационной отрасли искусственный интеллект применяется для мониторинга состояния сетей, обнаружения неисправностей и предотвращения технических сбоев.

Системы искусственного интеллекта способны выявить заранее возможные проблемы и спрогнозировать перегрузки оборудования, а это повысит надежность предоставляемых услуг и снизит вероятность возникновения аварийных ситуаций [3].

Интеллектуальные технологии используются и для изучения поведения клиентов. Анализ пользовательских данных позволяет компаниям создавать индивидуальные тарифные планы и учитывать потребности абонен-

тов, которые положительно влияют на уровень клиентской лояльности и финансовые показатели организации.

Влияние искусственного интеллекта на деятельность телекоммуникационных компаний будет усиливаться, так как происходит дальнейшая интеграция интеллектуальных систем в существующие бизнес-процессы оператора связи. А наиболее эффективной моделью станет сотрудничество человека и ИИ, при котором цифровые технологии будут дополнять профессиональные возможности сотрудников, а не заменять их.

Для успешной адаптации телекоммуникационных компаний к новым условиям необходим комплексный подход, включающий развитие человеческого капитала, модернизацию существующих бизнес-процессов и формирование современной корпоративной культуры с учетом ИИ.

**Список используемых источников**

1. Искусственный интеллект в сетях связи пятого и последующих поколений / Бородин А. С., Волков А. Н., Мутханна А. С., Кучерявый А. Е. // Электросвязь. 2021. С. 17-22.

2. Макарова О. Н., Мартыненко О. В., Полещук С. М., Шалыгина Е. В. Использование технологий искусственного интеллекта в управлении организации // Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». 2025. № 3. С. 66-75.

3. Савчук Д. О., Фокин А. Б., Лазарев М. М. Искусственный интеллект в телекоммуникациях // Актуальные исследования. 2025. № 28 (263). Ч. I. С. 24-28.

## FEATURES OF THE INFLUENCE OF ARTIFICIAL INTELLIGENCE ON THE WORK OF A TELECOMMUNICATIONS COMPANY

**Shcherbakov I, Yankovsky M.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In the modern world, telecommunications companies are actively implementing artificial intelligence technologies, which significantly transforms the nature of staff work and approaches to human resource management. In conditions of high competition and digitalization of the economy, the use of artificial intelligence is becoming an essential tool for increasing business efficiency, optimizing processes and improving the quality of customer service. The paper considers the features of the influence of artificial intelligence on the activities of personnel in a telecommunications company, highlights the key areas of transformation of labor functions, analyzes the advantages and risks of introducing artificial intelligence, and outlines the prospects for further development of human interaction and intelligent systems.*

***Key words:*** *artificial intelligence, telecommunications, personnel, automation, digitalization.*

**УДК 339.9**
**ГРНТИ 06.51.02**

# КОНЦЕПТУАЛЬНЫЕ ХАРАКТЕРИСТИКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ КИТАЯ

**Т. И. Юкина**

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

*Исследование цифровой трансформации обрабатывающей промышленности Китая проведено с позиции концептуальных характеристик данной предметной области. С этой целью рассматривается соответствующий опыт применения цифровых технологий и сервисов в таких отраслевых направлениях, как: машиностроение, потребительские товары и сырье. Практико-ориентированным кейсом решения конкретных промышленных задач выступают примеры китайских предприятий, формирующих фактор глобальной конкурентоспособности страны.*

***цифровая экономика, цифровая трансформация, 15-й пятилетний план развития Китая, обрабатывающая промышленность, совокупная факторная производительность***

Цифровая трансформация обрабатывающей промышленности Китая вступила в стадию масштабной популяризации – доля крупных предприятий в обозначенном процессе достигла 89,6 %, а уровень внедрения цифрового оборудования в основные звенья производственного процесса превысил 50 % [1, с. 10, 23]. Достижение технологического суверенитета и импортозамещения с соответствующими траекториями роста формируется за счет проактивного развития «новых качественных производительных сил».

В соответствии с 15-м пятилетним планом национального экономического и социального развития на 2026-2030 гг. поставлены задачи содействия цифровой трансформации промышленности и развития интеллектуального, экологически чистого и сервисно-ориентированного производства для ускорения модернизации отраслевых моделей и организационных форм предприятий [2]. Основополагающие направления обозначенного процесса: государственно-центричная модель с опорой на стратегическое планирование и долгосрочные программы, создание инфраструктуры на основе экосистемного подхода, платформенная экономика с акцентом на межотраслевое взаимодействие, циркулярная экономика, углеродная нейтральность, доми-

нирование вертикальной интеграции, смещение акцентов с крупнейших предприятий на малые и средние (поддержка «малых гигантов»), гибкость и кастомизация – обеспечение выпуска мелких парий товаров с эффективностью массового производства.

Цифровая трансформация промышленности с точки зрения иерархического распределения и системы оценочных показателей подразделяется на пять основных уровней: начальный, базовый, интеграционный, зрелый и продвинутый. На начальном этапе достигается стандартизация управления производством и автоматизация ключевых процессов. Базовый уровень обеспечивает сбор и использование данных в ключевых бизнес-процессах, поддерживая внедрение сервисов визуализации и транспарентного управления. Для обеспечения интеграции данных, совместимости и сетевого управления цифровыми системами осуществляется объединение участников соответствующих каналов связи. На зрелом этапе комплексная оптимизация всего бизнес-процесса с сетевым взаимодействием достигается интеллектуальной аналитикой решений на основе данных, что способствует определенным инновациям в коммерческих моделях. Для перехода к продвинутому уровню необходимо выполнить всестороннюю взаимосвязь всех ключевых элементов в целях интеллектуального самоанализа и принятия решений.

Большинство промышленных предприятий Китая находится на начальном и базовом этапах цифровой трансформации (10,4 % и 48,4 %), в основном достигнув стандартизации управления производством и операциями, автоматизации ключевых процессов, а также сбора и применения данных в рамках ключевых бизнес-звеньев. Почти 30 % предприятий (29,1 %) достигли этапа межотраслевой интеграции, а около 11 % вступили в этап комплексной оптимизации. Небольшое число ведущих предприятий (1,0 %) постепенно внедряют высокоуровневые интеллектуальные приложения [1, с. 11], достигая глубокой интеграции цифровых технологий в различные сферы бизнеса, исследуя инновации и обеспечивая модернизацию коммерческих моделей.

Всесторонняя трансформация традиционных отраслей промышленности способна обеспечить повышение совокупной факторной производительности (СФП) и мультипликативный эффект внедрения цифровых технологий и сервисов. С позиции стабилизации роста СФП, вызванная влиянием цифровой экономики, является ключевым фактором смягчения краткосрочных колебаний в экономике.

Вклад темпов роста совокупной факторной производительности цифровой экономики в экономический рост Китая, представленный на рис. 1, продолжает увеличиваться, достигнув около 23,75 % в 2024 году, что выше показателя предыдущего года (22,07 %) и значительно выше, чем вклад других технологических и институциональных дивидендов за тот же период (19,73 %).

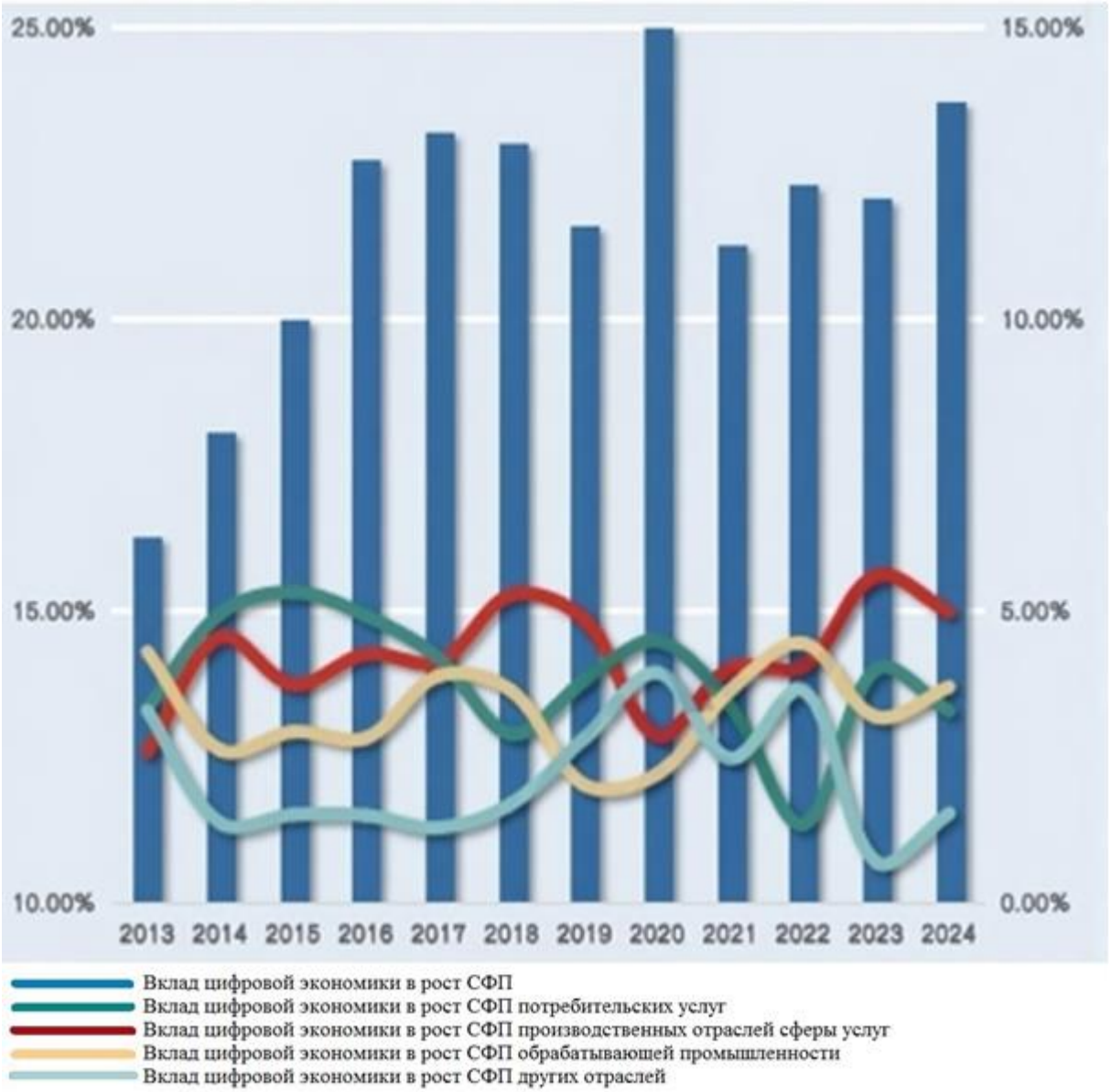



Рис. 1. Вклад цифровой экономики в рост совокупной факторной производительности по отраслям, 2013-2024 гг. [3, с. 30]

В долгосрочной перспективе – с 2013 по 2024 гг. вклад цифровой экономики в темпы роста совокупной факторной производительности увеличился с 16,30 % до 23,75 %. При этом столбчатая диаграмма (рис. 1.) демонстрирует достаточно неустойчивую тенденцию за счет периода 2018-2024

гг. с нестабильным ростом – замедлением процесса цифровизации. Период 2013-2017 гг. характеризуется быстрым ростом, а улучшение совокупной факторной производительности цифровой экономики в основном обусловлено сектором потребительских услуг – его средний вклад составил 4,54 %, что выше, чем у сектора производственных услуг. Широкое применение цифровых технологий и сервисов позволило сектору услуг преодолеть ограничения «затраты – выпуск» и достаточно быстро повысить эффективность за счет включения новых бизнес-форматов и моделей.

Совокупная факторная производительность является концентрированным отражением издержек и выгод цифровой экономики на макроуровне, а ее динамика напрямую влияет на темпы экономического роста страны. Глубинная трансформация производственной модели обеспечивает снижение трансакционных издержек с возможностью ускорения экономического роста [4]. Эффект снижения затрат и повышения эффективности, достигаемый благодаря цифровой экономике, на данный момент в Китае подавляется множеством факторов, что ослабляет ее поддерживающую роль в экономическом росте. Однако внедрение цифровых технологий во всю производственную цепочку значительно уменьшило информационную асимметрию, снизив предельные и трансакционные издержки и смягчив проблему эффекта Баумоля.

Рассмотрим в табл. 1 концептуальное содержание цифровой трансформации Китая на примере отраслей обрабатывающей промышленности с учетом структурных различий.

ТАБЛИЦА 1. Содержание цифровой трансформации Китая на примере отраслей обрабатывающей промышленности

| Отрасль промышленности | Специфика цифровой трансформации отрасли и примеры предприятий |
|---|---|
| Машиностроение | Автомобильная промышленность:<br>гибкое производство на основе «островной сборки»; виртуальная отладка с использованием цифровых двойников; цифровая система планирования для управления автоматизированными транспортными средствами; интегрированная архитектура «облако – канал – терминал»; облачная платформа больших данных; гибкий замкнутый цикл продуктов, определяемых данными<br>Примеры: компания Seres Automotive, заводы Audi FAW New Energy Vehicle Co., Ltd. и Brilliance BMW Shenyang Lydia |
| | Судостроительная промышленность:<br>«безчертежное» строительство на основе единого источника данных; полноэлементная трехмерная цифровая модель; система управ- |

| Отрасль промышленности | Специфика цифровой трансформации отрасли и примеры предприятий |
|---|---|
| | ления логистикой промежуточных продуктов с помощью технологии промышленного интернета; интеллектуальная платформа поддержки эксплуатации судов<br><br>Примеры: завод Jiangnan, компании Nantong COSCO KHI Ship Engineering Co., Ltd. (NACKS) и China Merchants Energy Shipping Co., Ltd. |
| Потребительские товары | Текстильная и швейная промышленность:<br><br>основанная на данных гибкая система цепочки поставок с быстрым реагированием; автоматическая генерация микрозаказов и распределение их по фабрикам с соответствующими мощностями; облачное сотрудничество с использованием данных электронной коммерции (прогнозирование самых продаваемых товаров); фрагментированное планирование производства и реагирование на массовые нестандартные заказы; точное управление запасами в многоканальной торговле; технология IoT для соединения всей цепочки – интеллектуальное распределение от складирования и хранения до продаж<br><br>Примеры: компания Shenzhen Xiyin E-commerce Co., Ltd., интеллектуальный склад Hailan Home |
| | Фармацевтическая промышленность:<br><br>цифровые модели для достижения стандартизированного массового промышленного производства; технология анализа процессов и распределенная система управления; контроль качества на основе цифрового соответствия; система отслеживания сырья, производства и оборота на основе технологии блокчейн; ИИ-модели виртуального скрининга и прогнозирования свойств большого количества соединений<br><br>Примеры: фармацевтическая группа Yangtze River Pharmaceutical Group (YRPG), компании China Resources Sanjiu Medical & Pharmaceutical Co., Ltd. и Jiangsu Hengrui Medicine Co., Ltd. |
| Сырьевая промышленность | Нефтехимическая промышленность:<br><br>система автоматического управления и оптимизации в режиме реального времени на основе механического моделирования и технологии больших данных; цифровое управление и контроль охраны труда, техники безопасности и окружающей среды с помощью промышленного интернета; прогнозируемое техническое обслуживание на протяжении всего жизненного цикла оборудования<br><br>Примеры: компании Wanhua Chemical Group Co., Ltd и PetroChina Dushanzi Petrochemical Company |
| | Цветная металлургия:<br><br>интеллектуальное взаимодействие и замкнутый контур управления всем процессом плавки; управление углеродными активами и оптимизированное планирование энергопотребления; платформа отслеживания углеродного следа продукции<br><br>Пример: компания Yunnan Aluminium Co., Ltd. |

Технологические изменения в сочетании с профильной реструктуризацией свидетельствуют о том, что цифровая трансформация Китая прошла процесс от экспериментальной стадии к практическому применению и используется как ключевой драйвер развития обрабатывающей промышленности. Полученные результаты исследования могут быть идентифицированы в качестве предпосылок формирования инициативы «Цифровой Шелковый путь».

**Список используемых источников**

1. 制造业数字化转型发展报告（2025年）(Отчет о развитии цифровой трансформации производства (2025)). 北京： 中国信息通信研究院 (Пекин: Китайская академия информационных и коммуникационных технологий, 2026年2月. 66页.

2. 中华人民共和国国民经济和社会发展第十五个五年规划纲要 / Основные положения 15-го пятилетнего плана национального экономического и социального развития Китайской Народной Республики // Официальный сайт Центрального народного правительства КНР. URL: https://www.gov.cn/yaowen/liebiao/202603/content_7062633.htm (дата обращения: 01.05.2026).

3. 中国数字经济发展研究报告（2025年）(Отчет об исследовании развития цифровой экономики Китая (2025)). 北京： 中国信息通信研究院 (Пекин: Китайская академия информационных и коммуникационных технологий, 2026年3月. 51页.

4. Мешков А. В., Симонина А. А. Цифровая экономика и проблемы ускорения экономического роста // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. С. В. Бачевского; сост. А. Г. Владыко, Е. А. Аникевич. СПб.: СПбГУТ, 2018. Т. 3. С. 515-520.

## CONCEPTUAL CHARACTERISTICS OF CHINA'S DIGITAL TRANSFORMATION OF MANUFACTURING INDUSTRY

**Iuiukina T.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The research of China's digital transformation of manufacturing industry is conducted from conceptual characteristics' position of this subject domain. For this purpose, the relevant experience of introduction digital technologies and services in such industry areas as mechanical engineering, consumer goods and raw materials is being considered. A practice-oriented case for definite industrial problems solution is provided by examples of Chinese enterprises that form country's global competitiveness factor.*

***Key words:*** *digital economy, digital transformation, China’s 15th five-year development plan, manufacturing industry, total factor productivity*

# СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**УДК 355.233.23**
**ГРНТИ 78.15.00**

## ПОДГОТОВКА СПЕЦИАЛИСТОВ СПЕЦИАЛЬНОЙ СВЯЗИ К РАБОТЕ НА ТЕЛЕКОММУНИКАЦИОННОМ ОБОРУДОВАНИИ В УСЛОВИЯХ ПРОВЕДЕНИЯ СВО

**А. В. Брыдченко, В. А. Гриднев, Д. А. Груздев**

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

*В статье рассматривается способ подготовки специалистов специальной связи в военном учебном центре (ВУЦ) с помощью применения учебно-тренировочной карты (УТК) для совершенствования навыков работы на первичном мультиплексоре (МП). Так же с УТК МП применяется способ изучения карты по определенной методике. Применения способа обучения с использованием УТК помогает совершенствовать навыки работы на первичном мультиплексоре, обеспечивает формирование точных двигательных и мыслительных реакций, что положительно влияет на надежность эксплуатации и качество установления связи* в *ходе проведения специальной военной операции (СВО), повышает уровень профессиональных компетенций.*

***способ совершенствования подготовки специалистов в области телекоммуникационных технологий в условиях проведения специальной военной операции с помощью методики обучения по учебно-тренировочной карте***

В условиях проведения специальной военной операции (СВО) актуальной остается проблема быстрой и качественной подготовки квалифицированных специалистов специальной связи для войск связи.

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].

Подготовленные специалисты по связи в войсках быстрее осваивают должность, штатную технику и средства связи, а также успешно эксплуатируют новые образцы отечественного и иностранного производства.

В ходе вооруженного противостояния происходит быстрая смена способов вооруженной борьбы и соответственно используемых вооружений. В войсках связи быстрая смена средств связи, вызывает необходимость такой же быстрой подготовки специалистов связи способных обеспечивать связь в интересах управления командованием частей и соединений огнем и оружием в сложных условиях.

Для решения указанной проблемы необходимым условием является поиск и внедрение в учебный процесс ВУЦ новых способов и методик направленных на подготовку специалистов специальной связи с учетом опыта специальной военной операции (СВО), а также сокращение сроков обучения специалистов специальной связи и повышение качества их подготовки по широкому спектру средств связи. Опыт подготовки специалистов по связи в ходе СВО подтверждает необходимость качественной профессиональной подготовки связистов. Причем, не просто только практической, но и теоретической, чтобы управление оборудованием осуществлялось осознанной с учетом технических возможностей средства связи.

В данной статье в качестве примера рассмотрим подготовку студентов только по небольшой части широкого спектра средств связи, которая имеется в ВУЦ. Наиболее емким направлением подготовки является область телекоммуникационного оборудования различных аппаратных и узлов связи. В частности, рассмотрим направление подготовки студентов по первичным мультиплексорам (МП), используемым на кафедре телекоммуникаций в ВУЦ с применением УТК.

Для совершенствования учебного материала по первичному мультиплексору в УТК МП был добавлен метод для формирования умственных и профессиональных навыков, который теперь можно использовать при подготовке специалистов специальной связи в ВУЦ.

Первый этап – мотивирование на изучение МП. Устойчивая мотивация возможна только после правильной формулировки цели занятия. Целью занятия должно являться не просто получение высокой оценки за настройку и эксплуатацию МП, но и возможность получения твердых навыков в работе и формирование профессиональных компетенций. Также можно повысить накал в учебной борьбе между студентами путем организации сорев-

нования на самого лучшего специалиста, фото которого будет размещено на информационной доске ВУЦ для общего обозрения всеми студентами.

Второй этап – изучение УТК МП с применением приемов и способов запоминания пошаговых действий при настройке и эксплуатации телекоммуникационного оборудования. Каждый шаг определяет последовательность действий по настройке, а затем и по работе на МП. Всю последовательность действий обучаемые закрепляют, используя приемы запоминания (либо по количеству шагов, либо используя метод крючков, применяемый в психологии). Такие приемы запоминания обеспечивают качество запоминания необходимых действий, их последовательность и последующее воспроизведение изученного материала.

Закрепив эти шаги, студент может переходить к следующему этапу. Разрешение на переход к следующему этапу он получает от руководителя занятия после получения оценки и комментариев о качестве освоения этого материала.

Третий этап – доклад действий по настройке и эксплуатации МП непосредственно перед началом работы. На этом этапе руководитель должен проверить правильность изложенных действий по УТК и технологию выполнения действий.

Перед началом настройки и эксплуатационного обслуживания МП студенты должны устно доложить порядок всех действий по настройке и переходу к работе. Данный метод позволяет сформировать у студентов правильную структуру действий при настройке МП и закреплять необходимые для этого знания, и навыки. Такая процедура, в свою очередь, потом обеспечивает точность действий при настройке МП, что снижает количество ошибок и защищает оборудование от неправильной эксплуатации. По правилам ведения обмена, информация является переданной после подтверждения корреспондентом сведений о ее полном приеме, которые он отправляет после сверки контрольных сумм принятой информации.

Указанные выше шаги положительно влияют на продолжительность бесперебойной работы МП, а также сокращают время обучения. В результате оборудование МП находится больше времени в правильной эксплуатации, и студенты получают возможность больше его эксплуатировать, что способствует повышению уровня их практических навыков и компетенций. В результате такого подхода повышается общий уровень компетенции учебной группы, снижается время, затрачиваемое на обучение, и сохраняется учебно-материальная база ВУЦ.

Предлагаемая методика подготовки студентов по эксплуатационному обслуживанию телекоммуникационного оборудования была опробована в ходе практических занятий на МП. Полученные результаты подтвердили правильность идеи обучения студентов по УТК с применением метода формирования умственных действий и практических навыков у студентов, который осуществляется в 3 этапа. Полученный опыт с учетом доработок предлагается внедрить в процесс подготовки специалистов специальной связи в ВУЦ и можно еще добавить метод соревнования между студентами с целью усиления мотивационной составляющей в процессе обучения.

Применение вышеуказанной методики в ходе подготовки специалистов по специальной связи позволяет формировать у студентов быстрое принятие решений за счет обучения всем необходимым приемам на практических занятиях. Задача программы обучения в ВУЦ заключается в том, чтобы подготовить классных специалистов по специальной связи, которые были бы способны выполнять все квалификационные требования, определенные заказчиком. Поэтому необходимость закрепить знания на практике и довести их до четкого, и правильного выполнения возможны только на практических занятиях. И только на практических занятиях и всевозможных тренажах возможно проверить уровень практической подготовленности студента путем сдачи нормативов и учебных задач.

Таким образом, проблему подготовки квалифицированных специалистов в области телекоммуникаций на кафедре ПЭС и ФПС ВУЦ решают путем унификации и доработки уже имеющихся методик и УТК. При подготовке учебного материала учитывается опыт подготовки специалистов по связи в условиях СВО. Комплексный подход и новые предложения реализуются в новых методиках по подготовке специалистов. Это позволяет повысить уровень подготовки и компетенций выпускников ВУЦ в сфере телекоммуникационного оборудования.

По отзывам из войск и в ходе встреч с выпускниками прошлых лет подтверждается гипотеза постоянного поиска и совершенствования методик подготовки. За счет поддержания постоянных контактов преподавателей кафедры и выпускников разных выпусков сформировалась группа в социальных сетях, которая делится своим опытом и обращается за помощью в случае необходимости к преподавателям ВУЦ.

**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

## TRAINING OF SPECIAL COMMUNICATIONS SPECIALISTS USING A TRAINING CARD TO IMPROVE THE SKILLS OF WORKING ON TELECOMMUNICATIONS EQUIPMENT IN THE CONDITIONS OF ITS

**Brydchenko A., Gridnev V., Gruzdev D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article discusses a method for training special communications specialists at a military training center (VUC) using a training card (UTK) to improve the skills of working on a primary multiplexer (MP). Also, with UTK MP, a method of studying the map is used according to a certain methodology. The use of the UTK training method helps to improve the skills of working on the primary multiplexer, ensures the formation of accurate motor and mental reactions, which positively affects the reliability of operation and the quality of communication during a special military operation, and increases the level of professional competencies.*

***Key words:*** *a way to improve the training of specialists in the field of telecommunications technologies in the context of a special military operation using a training card training methodology*

**УДК 623.626**
**ГРНТИ 78.25.41**

# ТЕХНОЛОГИЧЕСКИЕ УСЛОВИЯ, ОПРЕДЕЛЯЮЩИЕ ТАКТИКУ ПРИМЕНЕНИЯ МУЛЬТИСЕРВИСНЫХ ИНФОТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

**Д. Н. Васильев, А. К. Сагдеев, Д. С. Самаркин**

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

*Совершенствование форм специальных операций против систем управления основано на тщательном изучении принципов построения, технической оснащенности, планов и программ развития систем управления и их элементов с целью определения уязвимых мест, выход из строя которых сорвет управление. Составление моделей систем управления осуществляет техническая разведка, реализуя тем самым разведывательное обеспечение информационной войны. При решении задач по управлению в конкретных условиях обстановки появляются доминирующие требования к связи и сети связи. Динамика изменения состояний сети связи в общем случае выше динамики остальных элементов системы управления, так как изменение обстановки по связи может инициироваться органом управления, условиями функционирования сети связи, действиями должностных лиц при управлении связью.*

***система управления, техническая разведка, мультисервисные инфотелекоммуникационные сети***

Совершенствование форм специальных операций против систем управления основано на тщательном изучении принципов построения, технической оснащенности, планов и программ развития систем управления и их элементов с целью определения уязвимых мест, выход из строя которых сорвет управление [1]. Составление моделей систем управления (их элементов) осуществляет ТР, реализуя тем самым разведывательное обеспечение информационной войны [2].

При решении задач по управлению в конкретных условиях обстановки появляются доминирующие требования к связи и сети связи. Динамика изменения состояний сети связи в общем случае выше динамики остальных элементов системы управления, так как изменение обстановки по связи может инициироваться органом управления, условиями функционирования сети связи, действиями должностных лиц при управлении связью. В связи с этим уровень неопределенности обстановки по связи выше уровня неопределенности условий функционирования. Поэтому возможны два пути обес-

печения требований к сети связи: синтез инвариантной структуры сети к состояниям ее элементов и внешним воздействиям; синтез структуры под определенные условия функционирования. На практике в рациональном сочетании используются оба подхода [3]. Первый подход позволяет определить стратегическую цель (план связи), а второй является основой ситуационного управления структурой сети (тактика управления). Размерность множества вариантов структур зависит от принятых принципов классификации состояний по условиям функционирования [4]. Состояние системы – положение системы в заданный момент, отвечающее определенному условию. Число возможных состояний системы с учетом их вероятностей используется как исходные данные для текущего контроля состояния системы [5].

Такой подход позволяет представить сеть связи динамической, управляемой системой. Операторная структура системы управления такой сети представлена на рисунке 1.

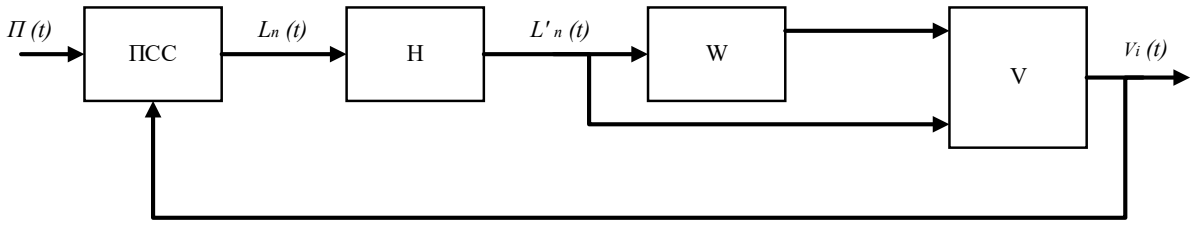



Рис. 1. Операторная структура системы управления сети

Состояние сети связи зависит от обстановки по связи, поэтому можно задать вектор $\vec{L}(t) = L_1(t), \dots, L_n(t)$, элементы которого отражают структуру сети и протекающие в ней процессы. Внешнее воздействие зададим вектором $\vec{\Pi}(t)$. Система управления контролирует состояние сети с некоторой точностью и формирует вектор наблюдения $\vec{X}(t)$. По результатам наблюдения формируется вектор оценки состояний $\overrightarrow{L_n^*}(t)$. Каждому значению вектора $\overrightarrow{L_n^*}(t)$ ставится в соответствие управляющее воздействие $Y_i(t)$. Решается эта задача оператором управления *W*, который включает подоператор планирования *(V)* и оперативного управления *(U)*. Оператор *V* каждому значению вектора $\overrightarrow{L_n^*}(t)$ ставит в соответствие значение $\overrightarrow{L_n}(t)$., отражающее планируемое состояние (структуру сети). Оператор *U* сравнивает планируемое состояние $\overrightarrow{L_n}(t)$ с текущим $\overrightarrow{L_n^*}(t)$ и вырабатывает управляющее воздействие

$$Y_j = U\{\overrightarrow{L_n}(t) - \overrightarrow{L_n^*}(t)\}.$$

В общем случае функциональный оператор $W$ осуществляет управление маршрутами, распределение и управление потоками сообщений и резервами, причем $W_i = V_i \cdot U_i$. Двухэтапная процедура управления сетью позволяет свести многокритериальную задачу синтеза к последовательному решению оптимизационных задач: синтез структуры сети для заданных условий функционирования (синтез вариантов защиты, состояний); синтез структуры оперативного управления сетью (управление состояниями и параметрами структуры). Для синтеза структуры сети связи необходимо уточнить существующую систему показателей качества функционирования, для чего необходимо уяснить физические процессы, протекающие в структуре при технологическом управлении.

**Список используемых источников**

1. Груздев Д. А., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Инфотелекоммуникационная система специального назначения и система радиоподавления как объект конфликта // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 696-699.

2. Глушко А. В., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Методы повышения достоверности распознавания объектов при ведении технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 684-687.

3. Аникеев А. И., Васильев Д. Н., Григорчук А. Н., Сагдеев А. К., Семин А. В. Обобщенная структура физической топологии защищенной мультисервисной сети передачи данных, функционирующей в интересах инфотелекоммуникационной сети специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 643-645.

4. Аникеев А. И., Григорчук А. Н., Дробяскин А. Н., Сагдеев А. К., Семин А. В. Общая характеристика защищенной мультисервисной сети передачи данных, функционирующей в интересах инфотелекоммуникационной сети специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 658-661.

5. Куранда А. И., Малинин О. Д., Сагдеев А. К., Самаркин Д. С. Модель информационно-телекоммуникационной сети военного назначения, интегрированной с ССОП ЕСЭ РФ, как объекта контроля защищенности от технической компьютерной разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). XII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2023. С. 810-814.

# TECHNOLOGICAL CONDITIONS DETERMINING THE TACTICS OF USING MULTISERVICE INFOTELEC COMMUNICATION NETWORKS

**Vasiliev D., Sagdeev A., Samarkin D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Improving the forms of special operations against control systems is based on a thorough study of the principles of construction, technical equipment, plans and programs for the development of control systems and their elements in order to identify vulnerabilities, the failure of which will disrupt management. The creation of control system models is carried out by technical intelligence, thereby providing intelligence support for information warfare. When solving management tasks in specific environmental conditions, dominant requirements for communication and the communication network appear. The dynamics of changes in the states of the communication network is generally higher than the dynamics of other elements of the control system, since a change in the communication situation can be initiated by the management body, the operating conditions of the communication network, and the actions of officials in managing communications.*

***Key words:*** *management system, technical intelligence, multiservice infotelecommunication networks*

**УДК 355.233.23**
**ГРНТИ 78.15.00**

# ВАРИАНТ ПРИМЕНЕНИЯ «ДВОЙНОГО ТУННЕЛИРОВАНИЯ» В СЕТЯХ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**А. В. Глушко, А. Н. Григорчук, В. А. Гриднев, Р. С. Знобищев**

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

*В статье рассматривается ряд факторов, непосредственно влияющих на эффективность применения глобальной информационной сети «Интернет» (ГИС), как элемента транспортной сети связи (ТСС) всех звеньев управления. И ряд шагов, направленных на повышения эффективности применения транспортной сети связи, включающей ресурсы ГИС «Интернет». А также проводится анализ существующих VPN-протоколов (Virtual Private Network), на предмет выбора наиболее подходящего по заданным критериям. Исходя из вышеизложенного анализа, проводится попытка выработки стратегии, позволяющей совместно использовать сильные стороны одних и других VPN-протоколов, дополняя друг друга и не снижая при этом показатели всей СССН.*

***сети связи специального назначения, применение «двойного туннелирования с целью поддержания и наращивания инфраструктуры транспортной сети связи для обеспечения надежного доступа к ресурсам ГИС «Интернет».***

В современных зарубежных вооруженных конфликтах особое значение при организации сети связи специального назначения (СССН) имеет применение ГИС, как элемента ТСС всех звеньев управления, которая зачастую остается единственным средством привязки подразделений к узлам связи пунктов управления.

Вместе с тем, имеет место ряд факторов, непосредственно влияющих на эффективность применения такого элемента и повышение эффективности транспортной сети связи в целом, а именно: – зависимость доступа к ГИС от глубины ведения боевых действий и необходимость поддержания и наращивания инфраструктуры ТСС для обеспечения надежного доступа к ресурсам ГИС; – воздействие блокировок провайдеров, а также иностранных спецслужб на доступ к ресурсам ГИС, требующее обеспечения устойчивости СССН и защиты от несанкционированного (НСД) ее ресурсов; – необходимость передачи большого информационного трафика (видеопотоков от беспилотного летательного аппарата (БЛА) и др.), требующая обеспечения высокой пропускной способности СССН.

**Таким образом, для повышения эффективности применения ТСС, включающей ресурсы ГИС «Интернет», целесообразно:**

1. Развернуть инфраструктуру ТСС, обеспечивающую надежный доступ подразделений связи к ресурсам ГИС, включающую:
– средства беспроводной широкополосной передачи данных (БШПД), работающие вне диапазона существующих средств РЭБ (50-80 ГГц);
– воздушные линии связи на оптическом волокне (прокладываемые БЛА);
– мобильные терминалы спутниковой связи;
– собственную частную сеть LTE (Long-Term Evolution, Private).

2. Развернуть резервную, децентрализованную сеть связи, основанную на принципе зашифрованной Mesh-сети (Ячеистая топология сети) и принципиально новых протоколах типа RNS (Reticulum Network Stack), объединяющих различные физические среды для передачи данных на большие расстояния и способных работать без ГИС (либо поверх ГИС).

3. Создать динамическую, глобально рассредоточенную сеть арендованных VPS (virtual private server) (отечественных и зарубежных).

4. Внедрить на серверах, узлах доступа и в подразделениях современные, максимально эффективные VPN-протоколы, обеспечивающие надежную аутентификацию, шифрование трафика, высокую пропускную способность сети, а также ее защиту от блокировок провайдеров.

**Анализ существующих VPN-протоколов**

В целях принятия решения о выборе VPN-протоколов для СССН рассмотрим характеристики и особенности наиболее эффективных из них, исходя из вышеизложенных ключевых критериев:
– надежность алгоритмов аутентификации и шифрования;
– защита от блокировок провайдеров (в том числе обход глубокой проверки пакетов (DPI));
– высокая пропускная способность.

**SSTP** (Secure Socket Tunneling Protocol) – обеспечивает безопасную передачу данных через SSL/TLS (обычно порт TCP(Transmission Control Protocol)/443), эффективно обходит брандмауэры и NAT (Network Address Translation), маскируя трафик под HTTPS (Hyper Text Transfer Protocol Secure). Работает через порт 443, аналогично HTTPS-трафику, что делает его трудноблокируемым, но не для DPI (Deep Packet Inspection). Использует SSL/TLS для шифрования и аутентификации, обеспечивая высокую степень защиты данных.

Недостатки: Производительность. Подвержен «TCP meltdown» (снижение скорости из-за двух уровней TCP), требует больше ресурсов, чем UDP-

протоколы (User Datagram Protocol). Ограниченность. Изначально разработан для Windows, хотя поддерживает и другие [1].

В настоящее время SSTP заметен для DPI и блокируется провайдерами.

**L2TP/IPsec.** L2TP/IPsec – безопасный VPN-протокол, объединяющий туннелирование L2TP (без шифрования) с безопасностью IPsec (Internet Protocol Security) (шифрование AES-256). Он обеспечивает целостность данных, аутентификацию и конфиденциальность. Работает через UDP-порты 500 и 4500, широко поддерживается ОС, но из-за двойной инкапсуляции (L2TP внутри IPsec) работает медленнее современных аналогов типа WireGuard

Недостатки: Снижение скорости из-за двойной инкапсуляции данных (L2TP, затем IPsec), что увеличивает нагрузку на процессор. Менее эффективен, чем OpenVPN или WireGuard. Может блокироваться брандмауэрами, которые фильтруют UDP [1].

**IKEv2/IPSec.** IKEv2 – протокол обмена ключами, входящий в набор протоколов IPSec. Обеспечивает высокую безопасность данных, скорость и стабильность работы. Использует технологию MOBIKE, позволяющую переключаться между Wi-Fi и мобильной сетью без разрыва VPN-соединения.

Поддерживает AES-256 и ChaCha20, использует Diffie-Hellman для обмена ключами с Perfect Forward Secrecy (при компрометации ключа прошлые сессии остаются защищенными). Работает только через UDP, который блокируется некоторыми корпоративными файрволами. В условиях агрессивного DPI также легко обнаруживается [2].

**OpenVPN**– протокол с открытым исходным кодом, гибкими настройками, поддержкой основных алгоритмов шифрования через библиотеку OpenSSL. Работает через UDP (быстрее) и TCP (надежнее). Может использовать порт 443, маскируясь под обычный HTTPS-трафик. Поддерживает AES-256-GCM, который до сих пор считается стандартом безопасности. С 2025 года DPI-системы научились распознавать OpenVPN по характерным паттернам трафика. В ряде стран OpenVPN без дополнительной обфускации блокируется практически мгновенно [2].

**WireGuard** – современный, быстрый и безопасный протокол VPN с открытым исходным кодом (4000 строк в сравнении с 100 000 строк кода OpenVPN), работающий на уровне ядра операционной системы (ОС), обеспечивая высокую производительность и минимальное потребление ресурсов, по сравнению с OpenVPN или IPSec. Скорость. В тестах 2025 года WireGuard показывает пропускную способность до 1011 Мбит/с на гигабит-

ном канале. OpenVPN на том же канале выдает 258 Мбит/с. Разница почти в четыре раза. Пинг у WireGuard – 0,4 мс против 1,5 мс у OpenVPN.

Шифрование. ChaCha20 для шифрования данных, Poly1305 для аутентификации, Curve25519 для обмена ключами. Это современная криптография, которая работает быстрее AES на устройствах без аппаратного ускорения – то есть на большинстве смартфонов.

Недостатки. WireGuard использует статические IP-адреса и требует хранения пользовательских IP-адресов на сервере. Для приватности это минус. Поэтому NordVPN создал NordLynx – обертку над WireGuard с двойным NAT, которая решает эту проблему [2].

**VLESS Reality.** VLESS – прокси-протокол из проекта Xray, в сочетании с технологией Reality до недавнего времени успешно обходил DPI. VLESS Reality требует базовых навыков работы с командной строкой. Готовые клиенты (v2rayN для Windows, Nekoray для Linux, Shadowrocket для iOS) упрощают процесс, но порог входа выше, чем у коммерческих VPN [2].

**Amnezia VPN** – сервис с открытым исходным кодом, позволяющий создать личный VPN на сервере пользователя. В решении используются протоколы OpenVPN, WireGuard, Shadowsocks, IKEv2, VLESS и Cloak, позволяющий маскировать VPN-трафик. Amnezia WG – это модифицированная, высокоустойчивая к блокировкам версия популярного VPN-протокола WireGuard, разработанная для обхода систем DPI. Он маскирует VPN-трафик под обычные сетевые запросы, предотвращая обнаружение и блокировку, сохраняя при этом высокую скорость и безопасность оригинала. Ключевые особенности и преимущества:

Маскировка трафика (обфускация). AmneziaWG изменяет заголовки пакетов и случайным образом меняет параметры, из-за чего системы DPI не могут распознать его как VPN. Основан на WireGuard. Использует надежное шифрование WireGuard, обеспечивая высокую производительность и низкое энергопотребление. Устойчивость. Отлично подходит для работы в сетях с жесткими ограничениями, где блокируются стандартные VPN-протоколы.

Развитие. Новые версии имитируют популярные протоколы, такие как QUIC (Quick UDP Internet Connections) или DNS (Domain Name System), делая трафик невидимым для систем DPI.

Собственный сервер (Self-hosted). Работает в составе приложения AmneziaVPN, позволяя пользователю настроить свой личный сервер, не требуя технических знаний [3].

Проведенный анализ показывает, что ряд основных современных VPN-протоколов в каких-то характеристиках превосходят остальные, а в каких-

то уступают, в связи с чем назвать лучших по всем параметрам не представляется возможным.

**Вместе с тем, следует отметить протоколы, имеющие высокие показатели по обозначенным ранее критериям:**

– AmneziaVPN – гибкий сервис, использующий ряд эффективных протоколов, благодаря чему имеющий механизмы защиты от DPI и высокие показатели пропускной способности;
– WireGuard – безопасный и быстрый протокол, имеющий надежное шифрование (не требующее аппаратного ускорения) и высокую пропускную способность (из-за сравнительно малой длинны кода).

**Применение «двойного туннелирования»**

Исходя из вышеизложенного анализа, целесообразно выработать такую стратегию, которая позволила бы совместно использовать сильные стороны одних и других VPN-протоколов, дополняя друг друга и не снижая при этом показатели всей СССН.

Такой стратегией организации защищенных сетей с надежными алгоритмами аутентификации и шифрования, защитой от блокировок и высокой пропускной способностью, представляется целесообразным выбрать «двойное туннелирование» на разных VPN-протоколах, используя их сильные стороны, при этом:

– протокол 1-го туннеля (транспортного) должен быть «клиент-серверным», между арендованным VPN-сервером и клиентами в первую очередь должна обеспечиваться защита от блокировок и высокая пропускная способность;
– 2-й туннель (информационный) должен строиться на базе адресов транспортного туннеля исключительно между клиентами, не обращаясь к серверу 1-го туннеля напрямую и используя его как транспортный хаб. При этом протокол 2-го туннеля в первую очередь должен обеспечивать надежность аутентификации и шифрования данных, а также высокую пропускную способность.

Для принятия решения о выборе протоколов на роль 1 и 2 туннеля рассмотрим ряд комбинаций вышеуказанных протоколов для установления наиболее эффективной пары. При этом, для анализа будем ориентироваться на протоколы, поддерживаемые ОС RouterOS (на ПАК с надежными характеристиками), наиболее распространенной и применимой для вышеуказанных целей в СССН.

Сравним по основным критериям (эффективности обхода DPI, пропускной способности, а также нагрузке на CPU и сложности настройки) 3 варианта комбинаций протоколов (поддерживаемых RouterOS), имеющих достаточно высокие показатели аутентификации и шифрования:

Вариант 1: SSTP + WireGuard

Вариант 2: L2TP/IPsec + WireGuard

Вариант 3: AmneziaWG + WireGuard

**Обход блокировок (DPI)**

SSTP + WireGuard: высокий (маскировка под HTTPS).

L2TP/IPsec + WireGuard: низкий (легко идентифицируется по UDP-портам 500/4500 или служебным пакетам).

AmneziaWG + WireGuard: очень высокий (специально создан для обхода DPI: "шум", искажение сигнатур пакетов).

**Скорость (на примере RB4011)**

SSTP + WireGuard: низкая (< 100-150 Мбит/с). Из-за TCP-over-TCP и отсутствия аппаратного ускорения.

L2TP/IPsec + WireGuard: средняя (300-500 Мбит/с). Из-за двойной инкапсуляции и оверхеда L2TP.

AmneziaWG + WireGuard: высокая (~250+ Мбит/с на базе Arm64). Работает через нативный WireGuard, а «шум» добавляется отдельно.

**Нагрузка на CPU**

SSTP + WireGuard: высокая (однопоточный SSL).

L2TP/IPsec + WireGuard: средняя (IPsec аппаратно, L2TP софтварно).

AmneziaWG + WireGuard: низкая (использует быстрый WireGuard-код).

**Выводы**

**SSTP + WireGuard:** SSTP хорошо маскируется, но очень медленный, работает поверх TCP, а при работе внутри него еще одного туннеля (WireGuard) TCP-over-TCP приведет к огромным задержкам и падению скорости до нуля при малейшей потере пакетов.

**L2TP/IPsec + WireGuard:** L2TP/IPsec имеет высокую пропускную способность, но легко обнаруживается системами DPI по характерным портам (UDP 500/4500) и служебным пакетам обмена ключами. Для обхода блокировок он бесполезен, а накручивание поверх него WireGuard только добавит оверхеда без пользы для маскировки.

**AmneziaVPN + WireGuard:** AmneziaVPN имеет высокую эффективность для обхода DPI (может использовать протоколы WireGuard, VLESS Reality и др.), а WireGuard в роли 2-ого туннеля имеет высокую пропускную

способность и низкую нагрузку на CPU из-за использования быстрого WireGuard-кода, что делает эту комбинацию наиболее оптимальной и эффективной для реализации «двойного туннелирования» в СССН.

Таким образом, применение в сетях связи специального назначения принципа «двойного туннелирования» с использованием защищенных, устойчивых и высокоскоростных протоколов/сервисов, обладающих надежными алгоритмами аутентификации и шифрования, механизмами обхода DPI и высокой пропускной способностью информационного трафика, позволит эффективно использовать ГИС «Интернет», как элемент ТСС, обеспечив при этом безопасность, достоверность и своевременность связи во всех звеньях управления войсками и оружием.

**Список используемых источников**

1. Салита А. Что такое VPN-протоколы и какие они бывают // Академия Selectel. URL: https://selectel.ru/blog/vpn-protocols (дата обращения 10.05.2026).

2. Digital Report. Лучшие VPN-протоколы 2025–2026: сравнение скорости и безопасности. URL: https://digirpt.com/2025/12/07/luchshie-vpn-protokoly-2025-2026-sravnenie-skorosti-i-bezopasnosti/ (дата обращения 10.05.2026).

3. Википедия. Официальный сайт. URL: https://ru.wikipedia.org/wiki/VPN (дата обращения 10.05.2026).

*Статья представлена кандидатом технических наук, доцентом кафедры электропроводной и фельдъегерско-почтовой связи ВУЦ СПбГУТ подполковником А. В. Брыдченко.*

## A VARIANT OF THE "DOUBLE TUNNELING" APPLICATION IN SPECIAL-PURPOSE COMMUNICATION NETWORKS

**Glushko A., Grigorchuk A., Gridnev V., Znobischev R.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article considers a number of factors that directly affect the effectiveness of the global information network "Internet" (GIS) as an element of the transport communication network (TCC) at all levels of management. And a number of steps aimed at improving the efficiency of the transport communication network, which includes GIS "Internet" resources. An analysis of existing VPN protocols (Virtual Private Network) is also being conducted to select the most appropriate one according to the specified criteria. Based on the above analysis, an attempt is being made to develop a strategy that allows you to share the strengths of one and other VPN protocols, complementing each other without reducing the performance of the entire VPN.*

*special-purpose communication networks, the use of "dual tunneling in order to maintain and build up the infrastructure of the transport communication network to ensure reliable access to GIS "Internet" resources*

**УДК 623.626**
**ГРНТИ 78.25.41**

# МЕТОДЫ ПЕРЕНАЦЕЛИВАНИЯ СРЕДСТВ ТЕХНИЧЕСКОЙ РАЗВЕДКИ ПРИ ВОЗДЕЙСТВИИ НА МУЛЬТИСЕРВИСНУЮ ИНФОТЕЛЕКОММУНИКАЦИОННУЮ СЕТЬ

**Р. В. Гордийчук, С. Л. Добровольский, А. К. Сагдеев, Д. С. Самаркин**

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

*Предлагаемые тезисы аргументируют, что результаты синтеза стратегии и программы технической разведки в значительной степени зависят от топологической и потоковой связности элементов мультисервисной инфотелекоммуникационной сети, от их веса в топологии и функциональной взаимосвязи. Программа технической разведки зависит от веса носителей. Это подтверждает предположение о том, что существующая структура технической разведки, используя современную теорию распределения ресурса, способна «самоорганизоваться» для вскрытия существующих и перспективных мультисервисных инфотелекоммуникационных систем, в том числе и систем с распределенными структурами.*

***мультисервисная инфотелекоммуникационная сеть, техническая разведка, технические средства разведки***

## Физическая постановка задачи

Решение вышеприведенной задачи позволяет определить оптимальную стратегию технической разведки сети связи (синтезировать оптимальный вариант использования группировки ТСР). Значение $P_{\text{вкр}(S)}$ или $S$ характеризует потенциальные возможности группировки ТСР. Однако эти ТСР комплексируются по носителям, динамические характеристики которых существенно влияют на реализуемость потенциальных возможностей группировки ТСР. Поэтому необходимо так «организовать» работу ТСР, чтобы реализовать оптимальную стратегию ТР, т.е. необходима программа использования подсистем и ТСР [1]. В этом случае факт вскрытия элемента сети зависит от включения его в программу ТР. Это случайное событие и будем его оценивать вероятностью $P_k$, характеризующей попадание элемента сети в поле зрения ТР при учете динамических характеристик носителей. Назовем ее вероятностью контакта ТСР с объектом разведки. Обычно ее значение принимают равное 1, что приводит к переоценке возможностей группи-

ровки ТСР. Это объясняется тем, что условие $P_k = 1$ равносильно допущению о неограниченной пропускной способности системы воздействия. Сложность определения значения вероятности $P_k$ состоит в том, что «за противника» тяжело определить общее планируемое число объектов разведки на время ($t_p$). Поэтому значение вероятности $P_k$ определим по результатам гарантированных статистических оценок числа контактов, полученных при реализации оптимальных процедур распределения ресурса разведки по множеству объектов с учетом ограничений на функционирование ТСР [2]. Тогда физическую постановку задачи можно сформулировать так.

Имеется *N* носителей ($k = \overline{1,N}$) средств воздействия. Каждый тип носителя характеризуется «весом», определяемым его вкладом в добывание разведывательных данных. С учетом этого примем, что задан вектор «весов» носителей $\vec{B} = \{B_k\}\, k = \overline{1,N}$. Каждый носитель обладает ограниченным за время разведки количеством сеансов разведки (полетов, рабочих витков, просмотров диапазонов разведуемых частот). При заданном времени разведки (*t*), известных динамических характеристиках носителей, количество сеансов можно определить, поэтому примем, что вектор $\vec{J} = \{J_k\}\, k = \overline{1,N}$ задан. На каждом носителе, в общем случае, могут быть установлены любые ТСР. Примем, что на каждом носителе размещены ТСР, т.е. задан вектор $\vec{Y} = \{Y_k\}\, k = \overline{1,N}$. Необходимо составить такую программу функционирования ТСР (программу включений и перенацеливаний), которая обеспечит в условиях старения разведданных максимальное число контактов средств разведки с элементами сети (с учетом их важности). Количество элементов сети задано вектором $\vec{S} = \{S_j\}, j = \overline{1,N}$. Для решения этой задачи воспользуемся результатами ряда работ, обобщив их на все типы носителей и с учетом приведенной выше постановки задачи [3].

**Содержательная постановка задачи**

Необходимо определить матрицу назначений $X^0 = \left\|X_{vi}^0\right\|_{ST}$, обеспечивающую максимум целевой функции

$$F(X^0) = max \sum_{k=1}^{N} B_k \sum_{i=1}^{J} \sum_{y=1}^{Y_k} \sum_{j=1}^{N_{kiy}^{(s)}} F_j^{(kiy)} \cdot A_j(\tau)$$

при условии

$$X_j = F_j^{(kiy)} = \begin{cases} 1, \text{если } 0{,}5\, d_{kiy} \geq r_{p\,ky}; \\ R_{ck}^{(y)} \leq R_{ck\,tp}; \\ t_k \leq t_p^{(l)}; \\ \beta_{1,2,3}(j-1)\beta_{1,2,3}(\gamma, \gamma+1) \leq \beta_{1,2,3}\, max; \\ \gamma_p \leq \gamma_T; \\ \gamma_p(\theta^0) \leq \gamma(\theta^0)_T; \\ 0, \text{в остальных случаях} \end{cases}$$

и ограничениях $N_{kiy} \leq {}^{t_p}/_{t_k}$; $t_{p(kiy)} \leq t_{p(kiy)\,\text{доп}}^{(l)}$;

$$\sum_{i=1}^{J} N_{kiy} \leq max\, N_{ky}^{(tp)};\ 0 \leq B_k \leq 1;\ \sum_{i=1}^{J} t_{p\,(kiy)}^{(l)} \leq t_{p\,(kiy)}^{(tp)}.$$

где $N_{kiy}$ – количество контактов с элементом *j*-того типа по программе разведки *k*-го носителя за время разведки $(t_p), j \neq S$;

$k = \overline{1, N}$ – количество носителей ТСР;

$B_k$ – вклад *k*-го носителя в получение разведывательной информации;

*J* – число каналов разведки (рабочих витков для ИСЗ, самолето-вылетов для ЛПС, просмотров разведуемого диапазона частот) за время разведки;

*Y* – количество ТСР на борту носителя;

$A_j(\tau)$ – динамический коэффициент важности *j*-го элемента сети;

$\tau = t_p^j(i) - t_p^j(i-1)$ – интервал времени между планируемым *i*-м и предыдущим $i-1$ моментами наблюдения *j*-го элемента сети;

$d_{kiy}$ – ширина полосы обзора аппаратуры *y*-го типа на *i*-м витке и *k*-м носителе. Для наземной радио- и радиотехнической разведки $d_{kiy} = r_{p\,ky}$;

$N_{kiy(s)}$ – количество элементов сети, попадающих в полосу обзора у -го ТСР, *k* -го носителя на *i* -м сеансе разведки (количество обнаруженных радиоизлучений сети связи);

$r_{ky}$ – дальность разведки *y* -го ТСР на *k* -м носителе;

$R_{ck}^{(y)}$ – разрешающая способность *y* -го ТСР на *k* -м носителе;

$R_{ck\,tp}$ – требуемая разрешающая способность определения местоположения элементов сети;

$t_k$ – время, необходимое для фотографирования (съемки) или выделения первичных разведывательных признаков;

$t_p^{(l)}$ – допустимое время работы ТСР за один сеанс разведки;

$\beta_1, \beta_2, \beta_3$ – значения углов крена, вращения и тангажа соответственно, на которые должна повернуться линия визирования при переключении ТСР с $j$ -го на $(j+1)$ элемент. Для наземной разведки ограничение снимается;

$\gamma_{p(T)}$ – реальная (техническая) скорость сканирования линии визирования (скорость частотного поиска);

$\gamma_{p(T)}(\theta^0)$ – реальная (техническая) скорость сканирования линии визирования. Для наземной разведки ограничение снимается;

$N_{kiy}, N_{ky\,tp}$ – количество включений аппаратуры $y$ -го типа, на $i$ -м витке и $k$ -м носителе за один сеанс разведки за время разведки ($t_p$);

$t_{p(kiy)}$ – время непрерывного функционирования ТСР за один сеанс разведки;

$t_{p\,(kiy)}^{tp}$ – допустимое время функционирования ТСР за время разведки.

Значение динамического коэффициента важности $j$ -го элемента сети определяется его весом и потребностью в периодическом обосновании информации из-за ее старения при доставке или периодическом наблюдении [4]. С учетом этого можно записать $A_j(\tau) = A_j e^{-\tau/t_0}$, где $t_0$ – периодичность обновления информации.

Для оценки вероятности включения $j$ -го элемента сети в программу технической разведки необходимо определить общее количество контактов системы технической разведки с элементами сети за время разведки

$$N = \sum_{j=1}^{S} N_{kj},$$

тогда $P_k = N_{kj} \,/\, N_{sum}$

Включение объектов в программу разведки является необходимым условием их вскрытия. Ее значение позволяет оценить реализуемость потенциальных возможностей. С учетом этого в дальнейшем будем использовать следующую зависимость

$$P_{\text{вскр}} = P_k \cdot P_{\text{разв}}.$$

Физическая трактовка задачи формирования программы ТР может быть расширена [5]. В частности, если ввести понятие важности для определения участка поверхности, попадающего в полосу обзора ТР, то представляется возможным оценить эффективность программы обзорной и детальной ТР.

**Список используемых источников**

1. Груздев Д. А., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Инфотелекоммуникационная система специального назначения и система радиоподавления как объект конфликта // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 696-699.

2. Алехин И. Н., Новиков Н. С., Сагдеев А. К., Самаркин Д. С. Методика оценки комплекса радиоэлектронного подавления по возможности ведения радиоразведки // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025); сб. науч. ст.: в 3 т. / Под. ред. А. В. Рабина; сост. И. М. Татарникова: СПб.: СПбГУТ, 2025. Т. 2. 636 с. С. 603-608.

3. Алехин И. Н., Новиков Н. С., Сагдеев А. К., Самаркин Д. С. Методика оценки возможностей комплекса РЭП по радиоподавлению // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025); сб. науч. ст.: в 3 т. / Под. ред. А. В. Рабина; сост. И. М. Татарникова: СПб.: СПбГУТ, 2025. Т. 2. 636 с. С. 609-614.

4. Глушко А. В., Поляков А. А., Сагдеев А. К., Самаркин Д. С., Скрыков И. А. Методы повышения достоверности распознавания объектов при ведении технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 684-687.

5. Поляков А. А., Сагдеев А. К., Самаркин Д. С., Сидоренко Е. Н., Скрыков И. А. Входные данные для алгоритмической модели системы технической разведки // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). XIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2024. С. 754-757.

## METHODS OF RETARGETING TECHNICAL INTELLIGENCE TOOLS WHEN EXPOSED TO A MULTISERVICE INFOTELEC NETWORK

**Gordiychuk R., Dobrovolsky S., Sagdeev A., Samarkin D.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The proposed theses argue that the results of the synthesis of a strategy and a technical intelligence program largely depend on the topological and streaming connectivity of the elements of a multiservice infotelec network, on their weight in topology and functional interconnection. The technical intelligence program depends on the weight of the media. This confirms the assumption that the existing technical intelligence structure, using modern resource allocation theory, is capable of "self-organizing" to uncover existing and promising multiservice infotelec communication systems, including systems with distributed structures.*

***Key words:*** *multiservice infotelecommunication network, technical intelligence, technical intelligence tools*

**УДК 378.1**
**ГРНТИ 14.35.07**

# ФОРМИРОВАНИЕ ГРАЖДАНСКОЙ ИДЕНТИЧНОСТИ ОБУЧАЮЩИХСЯ ВОЕННЫХ УЧЕБНЫХ ЦЕНТРОВ: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВАНИЯ И КОНЦЕПТУАЛЬНАЯ ПЕДАГОГИЧЕСКАЯ МОДЕЛЬ

**А. Н. Дробяскин, А. И. Куранда, А. Н. Музыкантов**

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

*В статье предлагается решение проблемы формирования гражданской идентичности обучающихся военных учебных центров при высших учебных заведениях. Гибридная образовательная среда военных учебных центров создает объективные условия для интеграции гражданского и военно-профессионального воспитания. Однако на практике педагогические подходы сохраняют фрагментарный характер и не учитывают в полной мере закономерности двойной социализации.*

*В работе предлагается концептуальная педагогическая модель поэтапного формирования гражданской идентичности, охватывающая адаптационный, рефлексивный и интегративный этапы.*

***гражданская идентичность, военный учебный центр, патриотическое воспитание, педагогическая модель, цифровая диагностика ценностных ориентаций, когнитивный иммунитет, студент, воинский долг, гибридная образовательная среда***

## Введение

Геополитическая конфигурация, обострение информационного противоборства и трансформация ценностных матриц молодого поколения выводят проблему формирования гражданской идентичности в степень стратегических задач образовательной и оборонной политики. Традиционные институты социализации – семья, школа, общественные объединения – все заметнее уступают цифровой среде в формировании ценностных ориентаций молодежи. В этих обстоятельствах высшая школа вновь обращается к проблеме собственных воспитательных функций, долгое время остававшихся в тени профессиональной подготовки. Сложилось очевидное противоречие: вузы последовательно расширяют номенклатуру формируемых компетенций, тогда как гражданско-патриотическое воспитание фактически перемещено на периферию учебных планов и осуществляется фрагментарно. Военные учебные центры (ВУЦ), функционирующие при граждан-

ских вузах, в этой ситуации выступают одной из немногих организационных форм, в которых профессиональная и воспитательная составляющие сопряжены содержательно и процессуально. Здесь пересекаются две образовательные траектории: гражданская (профессиональная) и военная (специальная), что создает синергетические возможности для формирования у обучающихся целостного мировоззренческого стержня.

Указы Президента РФ от 09.11.2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» и от 07.05.2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до2036 года» [1, 2] закрепляют приоритет воспитания личности, осознающий принадлежность к исторической общности и готовой брать на себя ответственность за будущее страны. Однако нормативные рамки не снимают педагогических противоречий: сохраняется разрыв между запросом на специалистов с устойчивой гражданской позицией и фрагментарностью воспитательных программ; необходимость формировать идентичность в условиях информационного давления сталкивается с отсутствием научно обоснованных механизмов диагностики; высокий потенциал ВУЦ не реализуется в полной мере из-за неразработанности методик, учитывающих специфику двойной социализации. Необходимо теоретически обосновать структуру гражданской идентичности студентов ВУЦ и разработать рабочую педагогическую модель, обеспечивающей ее поэтапное формирование.

## Основная часть

Мы рассматриваем гражданскую идентичность не как статичную характеристику личности, а как динамичное многоуровневое образование, формирующееся в процессе социализации. В отечественной традиции ее изучение опирается на культурно-историческую теорию развития личности, деятельный подход и концепцию человека как субъекта исторического процесса. Методологическую основу исследования составляет системный, аксиологический, этнопедагогический, личностно-деятельный и средовой подходы. Объединение этих подходов дает возможность устранить упрощенность, характерную для ранних моделей патриотического воспитания, сводившихся к трансляции знаний или эмоциональному воздействию. Современная педагогика требует перехода от императивных форм к диалоги-

ческим, от монологической передачи смыслов к совместному конструированию ценностей в условиях гибридной реальности.

Авторами гражданская идентичность определяется как личностный многоуровневый динамичный и при этом целостный конструкт, характеризующийся внутренней потребностью личности в принятии позитивного образа страны, ее истории, культуры, норм, ценностей и традиций, проявляющейся в готовности и способности к осознанному выбору способов служения государству и обществу [3]. Формирование идентичности студента ВУЦ осуществляется в процессе двойной социализации и проявляющееся в устойчивой системе ценностно-смысловых ориентаций, определяющих отношение к Отечеству, его истории, культурному наследию и готовность к практическому участию в жизни общества, включая выполнение конституционного долга. Структурный анализ выделяет четыре взаимосвязанных компонента – мотивационный компонент, когнитивный компонент, поведенческий и эмоционально-оценочный. Эти компоненты находятся в динамическом взаимодействии и дефицит одного ведет к деформации идентичности. Задача модели заключается в обеспечении их синхронизации на каждом этапе обучения.

Современный образовательный процесс невозможно рассматривать в отрыве от цифровой среды, превратившейся в самостоятельное пространство социализации и ценностного выбора. Студенты ВУЦ живут в условиях перманентного информационного потока, где традиционные медиа; социальные сети и образовательные платформы формируют альтернативные системы смыслов. Цифровое пространство амбивалентно: расширяет доступ к знаниям и обеспечивает персонализацию воспитания, но создает риски фрагментации сознания и подверженности манипулятивным технологиям. Формирование идентичности требует учета цифровой среды как фактора, способного усиливать или ослаблять воспитательный эффект. При этом важным аспектом выступает развитие «когнитивного иммунитета личности». Под развитием когнитивного иммунитета личности понимается целенаправленно организуемый процесс формирования у обучающихся устойчивости к манипуляциям, дезинформации и алгоритмическому влиянию, обеспечивающий способность критически оценивать информацию, сохранять смысловую автономию и принимать ответственные решения в условиях цифровой среды [4]. Иными словами, способности критически оценивать информационные потоки, распознавать манипулятивные техники и сохранять ценностную устойчивость в условиях гибридного воздействия.

Этот навык формируется через практику анализа источников, сравнения нарративов, деконструкции идеологических конструктов и участия в медиаграмотных проектах. В контексте ВУЦ развитие когнитивного иммунитета приобретает особую значимость, поскольку будущие специалисты должны сохранять ясность мышления в условиях информационного противоборства. Информационное поле ВУЦ требует осознанного проектирования, основанного на принципах прозрачности, диалогичности и ценностной согласованности.

Учитывая выше сказанное, наша модель представляет собой управляемый процесс, структурированный по трем этапам, соотносящимся с годами обучения и соответствующим психолого-педагогическим закономерностям развития личности в юности. Адаптационный этап характеризуется высокой степенью неопределенности и поиском смыслов. Задача педагогического сопровождения на этом этапе обеспечить первичную диагностику, коррекцию ценностных ориентаций и формирование эмоциональной привязанности к среде ВУЦ. Диагностика выполняет функцию самопознания: студенты знакомятся с историей ВУЦ, традициями вуза, биографиями и достижениями выпускников. Формами работы выступают экскурсии, встречи с выпускниками ВУЦ, ветеранами, участие в памятных мероприятиях. Приоритет отдается не прямому транслированию готовых формулировок, а созданию эмоционально значимых ситуаций. Содержательно этап включает модули по истории, основам государственного устройства, этике служения и медиаграмотности. В результате у студентов происходит изменение отношения от индифферентного к принятию среды как личностно значимой. На рефлексивном этапе акцент смещается на внутреннюю работу со смыслами. Студент осознает двойственность своего статуса, обращается к вопросам личного выбора и месту человека в историческом процессе. Педагогическая задача заключается не в передаче содержания, а в его присвоении обучающимся. Содержание строится вокруг дискуссий, кейс-анализа, деловых игр, моделирования ситуаций морального выбора. Существенное значение приобретают проекты, требующие самостоятельной исследовательской работы: подготовка материалов к памятным датам, сохранение мемориалов, анализ региональных аспектов исторической памяти. Диагностика приобретает циклический характер, что позволяет отслеживать динамику структуры идентичности. В итоге происходит переход от внешнего принятия ценностей к их внутреннему согласованию, развитие эмпатии и готовности к самостоятельным действиям. На интегративном этапе происходит соединение

гражданской и военной идентичностей. Студент готовится к выпуску, военной службе или гражданской карьере. Задача состоит в закреплении ценностей через практику, наставничество и сетевое взаимодействие. Студенты постепенно становятся субъектами воспитательного процесса, передавая опыт младшим курсам. В основе модели лежат три принципа. Преемственность означает, что гражданское и военное воспитание не противопоставляются, а взаимодополняют друг друга. Ценностное единство предполагает согласование личных устремлений с интересами общества. Деятельностный подход исходит из того, что идентичность формируется в ситуациях реального выбора, когда человек принимает решение и несет ответственность за него. Содержательно модель реализуется через программу «Служить России», включающую нравственно-патриотическое, поисковое, спортивно-патриотическое, волонтерское и культурно-эстетическое направления. Данные практики рассматриваются как перспективный организационный каркас, теоретическая обоснованность которого опирается на анализ методических материалов. Эмпирическая верификация требует отдельного исследования.

**Заключение**

Предложенная педагогическая модель формирования гражданской идентичности студентов ВУЦ представляет собой научно обоснованный инструмент, адаптированный к специфике двойной социализации в гражданском вузе. Она преодолевает фрагментарность традиционных подходов, интегрируя аксиологический, средовой и деятельностный компоненты в единую траекторию, развернутую во времени. Теоретическое обоснование многокомпонентной структуры позволяет перейти от упрощенного понимания патриотизма к работе с глубинными мотивами, знаниями, поведенческими паттернами и эмоциональными установками. Реализация модели позволяет перевести обучающегося от диффузного состояния к устойчивому просоциальному уровню, что напрямую коррелирует с формированием осознанной готовности к выполнению конституционного долга. Модель не претендует на универсальность, но предлагает рабочий каркас, адаптируемый под ресурсное обеспечение и профиль конкретных высших учебных заведений. Системная, научно обоснованная работа способна обеспечить формирование поколения, готового не только профессионально реализовываться, но и осознанно нести ответственность за будущее страны.

Настоящая работа носит концептуально-проектный характер. Представленная педагогическая модель является теоретическим конструктом, разработанным на основе системного анализа нормативных требований, педагогических подходов и обобщения лучших практик воспитательной работы в ВУЦ. Статья не содержит эмпирических данных апробации, поскольку целью данного этапа является обоснование структурно-содержательного каркаса модели и проектирование механизмов ее реализации.

**Список использованных источников**

1. Указ Президента РФ от 09.11.2022 № 809 (ред. от 04.03.2026) «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». Доступ из справ.-правовой системы «КонсультантПлюс».

2. Указ Президента РФ от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года». Доступ из справ.-правовой системы «Гарант».

3. Музыкантов А. Н. Гражданская идентичность студентов военного учебного центра: опыт эмпирического исследования // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2024. Т. 29. № 1. С. 7-18.

4. Смирнов Д. А., Сахарова Н. А. Когнитивный иммунитет личности и общества в эпоху искусственного интеллекта // Интеллигенция и мир. 2026. № 1. С. 38–52.

## ORMATION OF CIVIL IDENTITY OF STUDENTS AT MILITARY EDUCATIONAL CENTERS: THEORETICAL AND METHODOLOGICAL FOUNDATIONS AND CONCEPTUAL MODEL

**Drobyaskin A., Kuranda A., Muzykantov A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article substantiates the solution to the problem of forming the civic identity of students of military training centers at higher educational institutions. The hybrid educational environment of military training centers creates objective conditions for the integration of civic and military-professional education. However, in practice, pedagogical approaches remain fragmented and do not fully take into account the patterns of dual socialization. The paper proposes a conceptual pedagogical model of the gradual formation of identity, which includes the adaptation, reflexive, and integrative stages.*

***Key words****: civic identity, military training center, patriotic education, pedagogical model, digital diagnostics of value orientations, cognitive immunity, student, military duty, hybrid educational environment*

**УДК 355/359.07**
**ГРИТИ 49.47.31**

# РАЗРАБОТКА АЛГОРИТМА УСКОРЕННОЙ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ФЕЛЬДЪЕГЕРСКОЙ СВЯЗИ

**В. В. Загорельский, А. А. Марченков**

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

*Фельдъегерь – профессия, связанная с сохранностью государственных и военных секретов, и требует от специалиста фельдъегерско-почтовой связи высоких профессиональных знаний, внимательности, аккуратности в оформлении сопровождающих документов, личного мужества и дисциплинированности. Отбор и подготовку таких специалистов из солдат срочной службы приходится делать в очень короткие сроки с высокой интенсивностью обучения. В докладе предложен алгоритм ускоренной подготовки специалистов фельдъегерской связи, существенно облегчающая работу должностных лиц узлов и станций фельдъегерско-почтовой связи.*

***фельдъегерско-почтовая связь, активные методы обучения, военно-специальная подготовка***

Об интерактивных методах в обучении и необходимости широко использовать их при подготовке специалистов фельдъегерско-почтовой связи (ФПС) мы говорили ранее. Использование данных методов позволяет направлять и координировать работу обучаемого, для достижения целей учебного процесса в максимально короткие сроки [1].

В повседневной деятельности специалистам ФПС приходится обрабатывать большой объем входящей и исходящей воинской корреспонденции, заполняя при этом много учетных регистрационных форм документов. Поэтому будущие фельдъегери и экспедиторы фельдъегерских отделений должны знать, как это делается и уметь собственноручно их заполнять.

Организация ФПС в условиях локального вооруженного конфликта, специальной военной операции показывает существенное увеличение нагрузки на ФПС, что потребовало применять новые подходы для подготовки специалистов в данной области. Развертывание дополнительных узлов (станций) ФПС вынуждают комплектовать эти подразделения мобилизационным ресурсом. Подготовка данных специалистов ложится на командный состав, и данная методика позволит в течение короткого времени подготовить военнослужащего, способного не только проверить правиль-

ность оформления документов ограниченного доступа, но и научить представителей приписанных к узлу (станции) ФПС воинских частей правильно оформлять, адресовать корреспонденцию и вносить исходящие данные в документы учета.

В данной статье рассматривается вопрос ускоренной подготовки фельдъегеря и экспедитора отделения фельдъегерской связи, когда взамен изучения «объемной» инструкции по работе с документами ограниченного доступа, предлагается алгоритм последовательных действий, предусматривающий все возможные нарушения и ошибки при обработке регистрируемых почтовых отправлений.

Разработанный алгоритм апробирован на студентах военного учебного центра, обучающихся по военно-учетной специальности «Организация фельдъегерско-почтовой связи» на групповых занятиях по военно-специальной подготовке. Используя Алгоритм, время на выполнения практических действий по приему, обработке, учету регистрируемых почтовых отправлений ограниченного доступа существенно сокращается по сравнению с аналогичными занятиями без применения Алгоритма, а студенты делают значительно меньше ошибок при составлении форм документов. По их мнению, Алгоритм интуитивно понятный и «комфортный» для руководства к действиям.

Ускоренная подготовка специалиста фельдъегерской связи направлена на быстрое освоение должностных обязанностей, необходимых для выполнения служебных задач в сфере доставки документов ограниченного доступа. Это дает возможность сократить количество часов теории, запланированных в расписании занятий по боевой подготовке.

Вашему вниманию предлагается отрывок Алгоритма ускоренной подготовки специалистов фельдъегерской связи – Прием документов ограниченного доступа в экспедиции отдела фельдъегерской связи узла ФПС (рис. 1).

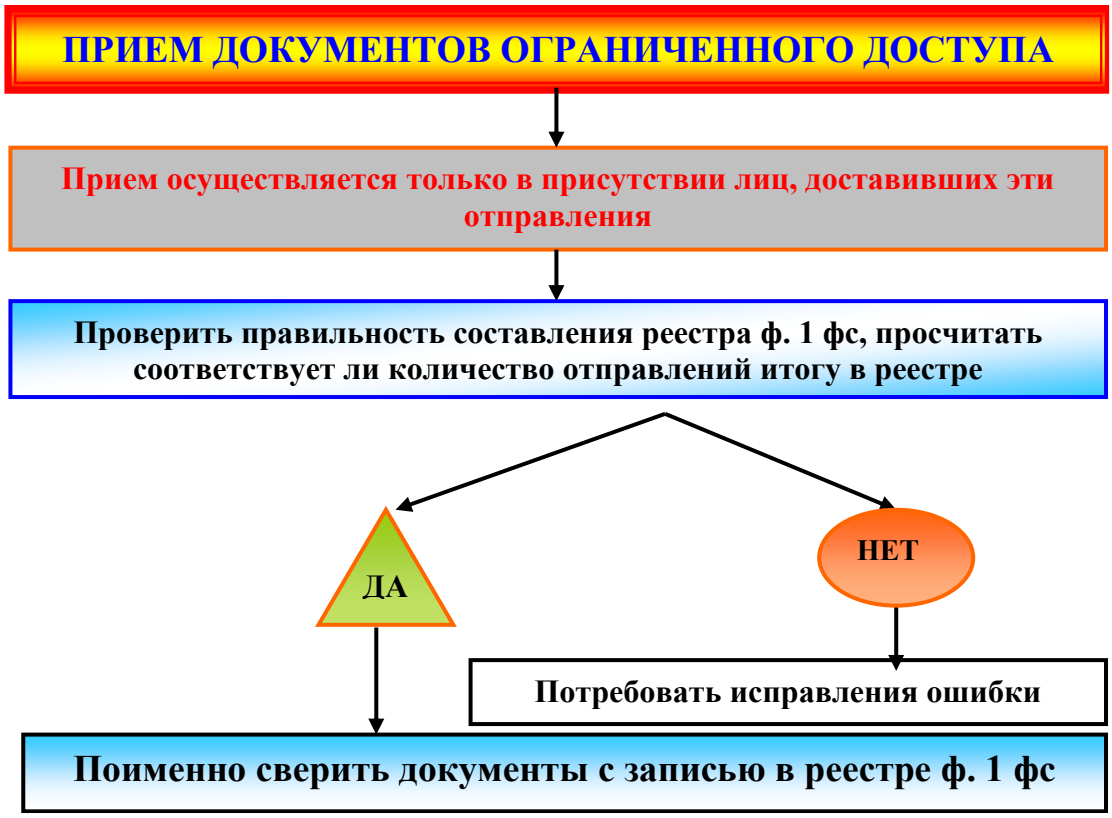



Рис. 1. Прием документов ограниченного доступа в экспедиции отдела фельдъегерской связи узла ФПС

## Вывод

Таким образом, предлагаемый Алгоритм ускоренной подготовки специалистов фельдъегерской связи позволит существенно сократить время на подготовку военнослужащих срочной (контрактной) службы для выполнения задач по предназначению.

### Список используемых источников

1. Загорельский В. В., Марченков А. А. Повышение эффективности обучения специалистов фельдъегерско-почтовой связи с использованием БКУТС. Актуальные проблемы инфотелекоммуникаций в науке и образовании. XIII Международная научно-техническая и научно-методическая конференция; сб. науч. ст. в 4 т. / Под. ред. Р. В. Кириченка; сост. А. А. Нестеров. СПб.: СПбГУТ, 2024. Т. 3. 846 с.

*Статья представлена научным руководителем, доцентом кафедры проводной электросвязи и фельдъегерско-почтовой связи, кандидатом технических наук, подполковником А. В. Брыдченко.*

# DEVELOPMENT OF AN ALGORITHM FOR ACCELERATED TRAINING OF COURIER COMMUNICATION SPECIALISTS

**Zagorelskiy V., Marchenkov A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*A courier is a profession related to the preservation of state and military secrets, and requires high professional knowledge, care, accuracy in processing accompanying documents, personal courage and discipline from a courier and postal specialist. The selection and training of such specialists from conscripts have to be done in a very short time with a high intensity of training. The report proposes an algorithm for accelerated training of courier communication specialists, which significantly facilitates the work of officials of courier communication hubs and stations.*

***Key words:*** *courier and postal communication, active training methods, military special training*

**УДК 004.89**
**ГРНТИ 28.23**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТРАДИЦИОННЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМ И АЛГОРИТМОВ ШИФРОВАНИЯ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

**А. И. Куранда[1], Е. И. Мерзликин[2], М. Н. Михайлов[2], О. Н. Стеценко[2]**

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[2] Белгородский государственный технологический университет им. В. Г. Шухова

*В работе выполнен сравнительный анализ традиционных алгоритмов шифрования и алгоритмов на основе нейронных сетей. Обоснована перспективность нейросетевых криптосистем на фоне растущих требований информационной безопасности и экспоненциального роста вычислительных мощностей. Исследованы принципы функционирования нейросетевых алгоритмов шифрования и проведено их сопоставление с традиционными блочными шифрами AES и шифрами семейства ГОСТ. Проведён анализ преимуществ, уязвимостей и криптостойкости использования нейронных сетей в криптографических протоколах с учётом экспериментального статуса и отсутствия формальных доказательств безопасности.*

***нейрокриптография, симметричное шифрование, древовидные машины четности, блочные шифры, криптостойкость, нейронные сети, алгоритм AES, ГОСТ Р 34.12-2015, постквантовая криптография.***

Современная криптография опирается на строгие математические модели, обеспечивающие вычислительную сложность, а также на механизмы, выполняющие псевдохаотичные преобразования данных. Однако развитие квантовых вычислительных технологий ставит под угрозу устойчивость традиционных криптосистем. В этих условиях возрастает интерес к альтернативным парадигмам защиты информации, среди которых теоретическую перспективность демонстрирует направление нейрокриптографии, которое объединяет методы искусственного интеллекта и криптографические модели.

Целью настоящей работы является проведение сравнительного анализа традиционных криптографических систем и алгоритмов шифрования на основе нейронных сетей. В рамках исследования формулируются архитектурные принципы нейросетевых криптосистем, оценивается их криптостойкость к известным векторам атак, анализируются практические ограничения

и перспективы внедрения с учетом требований безопасности и стандартизации.

Для начала рассмотрим архитектурные и математические основы нейросетевых криптосистем. Общие принципы использования нейросетевых алгоритмов шифрования базируются на способности взаимодействующих нейронных сетей формировать согласованные внутренние состояния в процессе взаимного обучения по открытому каналу связи. Основу данного направления заложили I. Kanter и W. Kinzel, предложившие протокол согласования криптографических ключей на основе древовидных машин четности Tree Parity Machine (TPM) [1]. Архитектура TPM представляет собой двухуровневую сеть прямого распространения без обратных связей, состоящую из $K$ скрытых нейронов, каждый из которых принимает $N$ входных сигналов. Векторы весовых коэффициентов $w_{ij}$ принимают целочисленные значения из диапазона *[-L, L]*, где параметр $L$ определяет синоптическую глубину и напрямую влияет на криптографическую стойкость шифросистемы [1, 2].

Синхронизация двух легитимных сетей (A и B) осуществляется путём стохастического взаимного обучения. На каждом шаге генерируется публичный входной вектор $X \in \{-1,1\}^{KN}$, далее вычисляются выходные сигналы $\tau_A$ и $\tau_B$. При условии $\tau_A = \tau_B$ векторы весов модифицируются согласно выбранному правилу обучения (Хебба, анти-Хебба или случайного блуждания). Процесс завершается при стабильном совпадении выходных сигналов, после чего согласованные векторы весов интерпретируются как совместный симметричный ключ [1, 2]. Время синхронизации легитимных узлов $t_{synch}$ увеличивается полиномиально с увеличением $L$, тогда как время синхронизации пассивного интруза $E(t_{learn})$ увеличивается в экспоненциальной зависимости, что формализуется неравенством $t_{learn} \gg t_{synch}$ при $L \geq 8$ [2]. Данная асимметрия временных характеристик обеспечивает теоретическую основу безопасности протокола, не опирающуюся на сложность задач теории чисел.

В работе [3] был предложен принципиально иной подход, в рамках которого предлагалось использовать комитетов нейронных сетей для построения шифра пропорциональной многоалфавитной замены. В этом случае предварительно создается обучающее множество с учётом частотности символов исходного алфавита. Это создает условия для равномерного распределение шифрограмм в пространстве кластеров. В ходе шифровании каждого последующего символа, происходит выбор соответствующей сети из

комитета. За счет этого обеспечивается многоалфавитное шифрование, что, в свою очередь значительным образом усложняет задачу статистического криптоанализа.

С учетом вышесказанного выполним сравнительный анализ нейросетевых и с традиционных блочных шифров (на примере AES и ГОСТ ГОСТ Р 34.12-2015). Сравнение выполним на основе наиболее критичных параметров шифров, а именно: математических базисов, механизмов формирования ключей, вычислительной производительности и статусу стандартизации.

Так, создание ключей в рамках традиционных симметричных криптосистем выполняется централизованно. При этом, для передачи ключа дополнительно требуется либо защищенный канал передачи, либо применение асимметричной криптосистемы. В то же время нейросетевые методы используют явление стохастической синхронизации, тем самым решая проблему согласования ключей через открытый канал. Отметим, что на данный момент TPM рассматривается лишь как исследовательский инструмент. Для целевого использования как TPM, так и прочие нейросетевые алгоритмы шифрования на сегодня ни ФСБ России, ни иными профильными структурами (включая NIST или ISO/IEC) не рекомендованы [4, 5].

Основу алгоритма AES составляет подстановочно-перестановочная сеть (SPN), а также операции в поле Галуа $GF(2^8)$. В отличие от AES, шифросистема ГОСТ Р 34.12-2015 базируется на сети Фейстеля, либо SPN, с нелинейными *S*-блоками. Оба алгоритма работают по детерминированным сценариям и обладают доказанной устойчивостью к раскрытию. В свою очередь, нейросетевые шифросистемы используют нелинейные функции активации, вероятностные схемы обучения сети с динамической корректировкой весов и векторные пространства высокой размерности. Криптографическая стойкость таких шифросистем носит эмпирический характер, не обосновываясь, при этом формальными условиями стойкости, в частности - теоремой Шеннона об абсолютной стойкости или редукционным доказательствам.

Традиционные шифры оптимизированы на аппаратном уровне, обеспечивая высокую пропускную способность при минимальных задержках. Нейросетевое шифрование требует же значительных вычислительных ресурсов для фазы синхронизации, а процесс непосредственного преобразования данных не обеспечивает постоянной длительности криптографического преобразования. Измерения показывают, что время синхронизации возрас-

тает пропорционально $L^2$, что при $L > 10$ приводит к задержкам, несопоставимым с требованиями телекоммуникационных протоколов реального времени [6]. В отличие от классических схем, нейронные протоколы не поддерживают аппаратную акселерацию в существующих криптографических сопроцессорах.

Что касается стандартизации шифров, то для предупреждения угроз квантовых вычислений Национальный институт стандартов и технологий США (NIST) представил документ IR 8105, в котором определён путь миграции на криптографию, устойчивую к квантовым атакам. Результатом этой работы стало принятие стандарта NIST FIPS 203 (CRYSTALS-Kyber) для инкапсуляции ключей, который прошёл многолетнюю открытую криптоаналитическую проверку и готов к промышленной интеграции [7]. Следует отметить, что нейросетевые протоколы не прошли аналогичного цикла верификации и отсутствуют в дорожных картах стандартизации ведущих криптографических агентств.

С позиции криптостойкости, надежность традиционных шифров оценивается через доказанную устойчивость к известным методам криптоанализа. Показатели же стойкости нейросетевых шифросистем имеют вероятностный характер, практически полностью определяемый параметрами топологии $K, N, L$. Так, сегодня наиболее продуктивными атаками на протокол TPM считаются геометрическая, мажоритарная и генетическая атака. При этом, вероятность эффективного исхода таких атак обратно пропорциональна значению величины $L$. В частности, рост $L$ ведет к сокращению вероятности $P$ успеха геометрической или генетической атаки. Такая взаимосвязь иллюстрируется выражением $P \approx \exp(-\alpha(L-\beta))$, где α и β – коэффициенты, определяемые топологии и правилами обучения нейросетевого шифра. В то же время рост параметра $K$ (его нечетных значений), начиная с $K > 3$, дополнительно снижает вероятность совпадения отталкивающих шагов у атакующей сети. Одновременно с этим, статистика реализованных атак указывает на ограничения заявленной зависимости. Например, при $L < 8$, TPM становится не стойким к геометрическим, мажоритарным и генетическим атакам. В ходе них злоумышленник может восстановить весовые векторы за время, сопоставимое с $t_{synch}$ Для этого используются оптимизированные генетические алгоритмы и мажоритарное голосование ансамбля сетей. Это доказывает тезис о критической зависимости стойкости TPM от выбранных параметров. Однако, когда величина $L \geq 10$, вычислительная сложность атаки увеличивается значений, ставящих под сомнение

ее целесообразность. С другой стороны, при этом возрастает и $t_{synch}$, тем самым сокращая эффективность TPM в системах с ограничениями по задержкам.

Вместе с тем, наиболее существенные угрозы для алгоритмов симметричного шифрования на основе нейросетей – это – кластерный анализ пространства шифрообозначений, а также обратный инжиниринг весовых матриц. В работе [3] утверждается, что криптографическая стойкость нейросетевого шифра пропорциональна размерности входного пространства значений и количеству кластеров, характеризующих символы. В этом случае задачу кластеризации можно сделать вычислительно неразрешимой за счет применения многоалфавитной замены через комитет сетей, поскольку это ведет к наложению областей шифрообозначений. С другой стороны, отсутствие формальных редукций к известным сложным задачам, ставит под сомнение возможность долгосрочной стойкости нейросетевых шифров. Утверждения же о потенциальной стойкости к квантовым атакам не подтверждены математически, либо анализом устойчивости к алгоритму Гровера.

С точки зрения практической реализуемости и перспектив развития, внедрение нейросетевых шифров в широко применяемые криптографические системы сталкивается с рядом технологических и нормативных ограничений. Таковыми являются отсутствие жесткой стандартизации, высокие требования к вычислительным ресурсам на этапе синхронизации, а также сложность верификации и сертификации стохастических алгоритмов. На сегодня также не существует сертифицированных гибридных схем, сочетающих TPM с ГОСТ или AES [8]. Нейросетевые протоколы остаются областью академических исследований и лабораторных экспериментов.

Выполненный сравнительный анализ шифросистем показывает, что нейросетевые алгоритмы шифрования сегодня являются хотя и экспериментальным, но теоретически перспективным направлением криптографии. Традиционные алгоритмы основаны на детерминированных математических преобразованиях. В отличие от них, нейросетевые алгоритмы обеспечивают потенциальную стойкость к классическим методам криптоанализа за счет применения стохастической синхронизации и нелинейной динамики сценариев. Однако сейчас такие алгоритмы не могут рассматриваться полноценной заменой традиционных шифросистем по причине отсутствия доказанной криптостойкости, критическая зависимость безопасности от основных параметров, а также вследствие высокой вычислительной сложности.

Сегодня TPM и сходные протоколы рассматриваются, в первую очередь, как исследовательские инструменты. Дальнейшее их развитие должно включать в себя обеспечение строгого математического доказательства безопасности, верификации устойчивости к различным типам атак, а также аппаратной оптимизации.

**Список используемых источников**

1. Kanter I., Kinzel W., Kanter E. Secure exchange of information by synchronization of neural networks // Europhysics Letters. 2002. Vol. 57. № 1. PP. 141–147.

2. Ruttor A. Neural synchronization and cryptography: Dissertation zur Erlangung des Doktorgrades. Würzburg: Julius-Maximilians-Universität, 2006. 121 p.

3. Солодовников В. И. Улучшение криптостойкости нейросетевого алгоритма симметричного шифрования за счет использования комитетов нейронных сетей // Новые информационные технологии в автоматизированных системах. 2017. № 20. С. 176–180.

4. NIST IR 8105. Post-Quantum Cryptography: Status Report // National Institute of Standards and Technology. Gaithersburg, 2016. 48 p.

5. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). Gaithersburg: National Institute of Standards and Technology, 2024. 34 p.

6. Урбанович П. П., Плонковски М. Д., Долецки М. Нейросетевые технологии в криптографических приложениях: монография. Минск: БГТУ, 2024. 221 с.

7. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М. Стандартинформ, 2015. 32 с.

8. NIST FIPS PUB 197. Advanced Encryption Standard (AES). Gaithersburg: National Institute of Standards and Technology. 20 p.

*Статья представлена научным руководителем, кандидатом технических наук, доцентом кафедры ПОВТАС БГТУ им. В. Г. Шухова А. М. Хлоповым.*

## COMPARATIVE ANALYSIS OF TRADITIONAL CRYPTOGRAPHIC SYSTEMS AND NEURAL NETWORK-BASED ENCRYPTION ALGORITHMS

**Kuranda A.[1], Merzlikin E.[2], Mikhailov M.[2], Stetsenko O.[2]**
[1]The Bonch-Bruevich Saint Petersburg State University of Telecommunications
[2]Belgorod Shukhov State Technological University

*The paper provides a comparative analysis of traditional encryption algorithms and algorithms based on neural networks. It substantiates the prospects of neural network cryptosystems in the context of growing information security requirements and exponential growth of computing power. The paper explores the principles of neural network encryption algorithms and compares them with traditional block ciphers such as AES and the GOST family. It also analyzes the advantages, vulnerabilities, and cryptographic strength of using neural networks in cryptographic protocols, taking into account their experimental status and lack of formal security proofs.*

***Key words:*** *neurocryptography, symmetric encryption, tree-based parity machines, block ciphers, cryptographic strength, neural networks, AES algorithm, GOST R 34.12-2015, and post-quantum cryptography*

## ИННОВАЦИИ ДЛЯ АРКТИКИ

**УДК 004.421**
**ГРНТИ 47.14.17**

# ВЫБОР ГРАФИЧЕСКОГО ПРОЦЕССОРА ДЛЯ РЕАЛИЗАЦИИ АЛГОРИТМОВ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ С ПРИМЕНЕНИЕМ ВЕЙВЛЕТОВ

**А. В. Запайщиков, А. В. Круглова**

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

*Данная работа посвящена обзору некоторых из графических процессоров для реализации алгоритмов цифровой обработки сигналов с применением технологии вейвлет-анализа. Приводятся различные типы вычислителей, которые возможно использовать под конкретную задачу, их технические характеристики, и делается выбор в пользу наиболее подходящего. Исходя из всего этого, оценивается реальная возможность применения того или иного устройства для решения поставленной задачи.*

***цифровая обработка сигналов, алгоритм вейвлет-анализа, вычислитель, графический процессор, центральный процессор, параллельные вычисления***

Целью данной работы является обзор вычислителей на графических процессорах, которые возможно использовать для цифровой обработки сигналов с применением технологии вейвлет-анализа.

На сегодняшний день цифровая обработка сигналов является очень актуальной, важной, необходимой, и, достаточно часто, весьма трудоемкой задачей с точки зрения вычислительных затрат.

Цифровой обработкой сигналов называется способ обработки сигналов, основанный на численных методах с применением цифровой вычислительной техники для получения конкретного результата: например, выделения информационной составляющей, содержащейся в сигнале [1, 2].

Все дело в том, что в современном мире все чаще и чаще требуются быстрые, качественные вычисления, с использованием компактных и относительно недорогих устройств-вычислителей.

Вейвлет-анализ (частотно-временной анализ) сигналов, является мощным математическим аппаратом, позволяющим анализировать различные виды сигналов как по времени, так и по частоте. В совокупности это позволяет получить больше информации об обрабатываемом сигнале [3].

Математическая формула для непрерывного интегрального вейвлет-преобразования сигнала $s(t)$ имеет следующий вид [3]:

$$W(a,b) = \frac{1}{\sqrt{a}} \int s(t) \cdot \psi\left(\frac{t-b}{a}\right) dt,$$

где $a -$ коэффициент масштаба; $b -$коэффициент сдвига; $s(t) -$ исходный сигнал; $\psi -$ материнский (базисный) вейвлет.

Задача состоит в том, чтобы подобрать такой вычислитель, который должен будет обеспечивать в реальном времени выполнение этой интегральной операции по нескольку раз и, более того, параллельно проводя аналогичные вычисления по другим группам сигналов $s_N(t)$, где $N -$ количество таких сигналов, находящихся в общем ансамбле реализаций.

В общем случае, существующие на текущий момент вычислители можно условно подразделить на использующие:
– центральный процессор: CPU;
– графический процессор: GPU.

Центральный процессор (CPU) обеспечивает хорошую и бесперебойную работу при выполнении последовательных задач. Но он не способен эффективно справляться с параллельными задачами.

Графический процессор (GPU) обеспечивает хорошую многозадачность и параллельность вычислений. Чаще всего, он предназначен именно для обработки графических данных и выполнения сложных вычислений.

Исходя из вышесказанного, для поставленной задачи было бы логичным выбрать именно графический процессор.

На рисунке 1 представлены основные виды графических процессоров.

Таким образом, к вычислителю на графическом процессоре можно выдвинуть следующие требования:
– высокая производительность;
– наличие сразу нескольких интерфейсов, позволяющих осуществлять ввод/вывод данных;
– наличие собственной операционной системы, позволяющей удобно и гибко реализовать на ней алгоритм обработки и вейвлет-анализа сигналов [1, 2];
– компактность;
– возможность подключения внешнего монитора через HDMI.

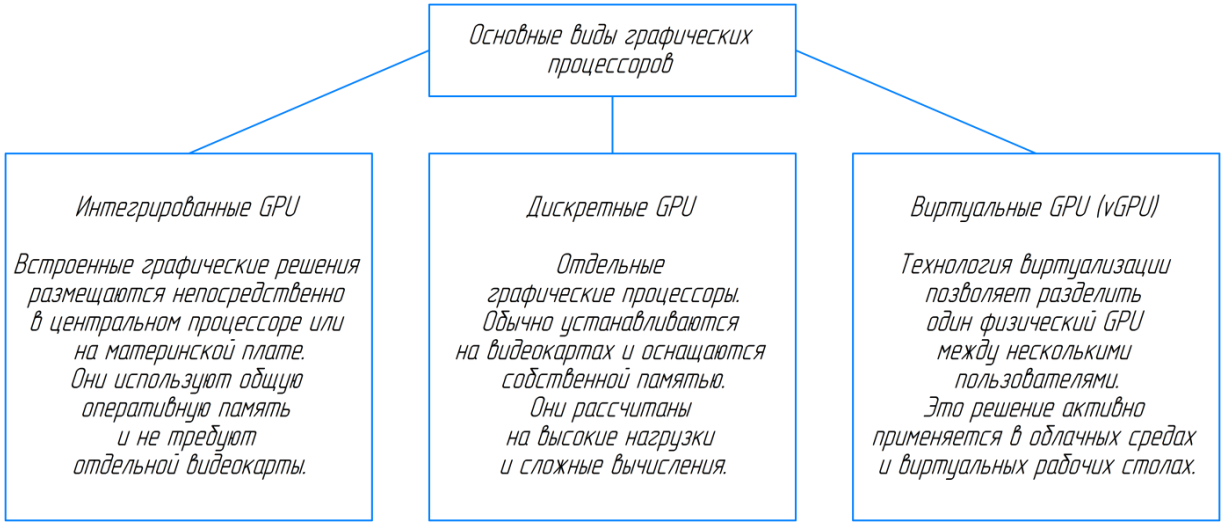



Рис. 1. Основные виды GPU

Исходя из вышеперечисленных требований, на рынке обратили на себя внимание следующие вычислители, а именно:

1. Raspberry Pi 4 Model B (рис. 2), обладающий следующими основными техническими характеристиками [4]:

– центральный процессор: 4-ядерный 64-битный CPU на ARM Cortex A72;
– графический процессор: VideoCore VI GPU с тактовой частотой 500 МГц;
– оперативная память: 4ГБ LPDDR4-2400 SDRAM;
– максимальное выходное разрешение: 4K (3840×2160, 60 Гц);
– поддержка различных операционных систем семейства Linux;
– порты периферии: 2× USB 2.0, 2× USB 3.0;
– порт для связи с сетью Интернет: Gigabit Ethernet RJ-45;
– порт для экрана: Display Serial Interface (MIPI DSI).



Рис. 2. Raspberry Pi 4 Model B

2. Orange Pi 5 (рис. 3), обладающий следующими основными техническими характеристиками:
– центральный процессор: 8-ядерный 64-битный CPU Rockchip RK3588S (4 × Cortex-A76 и 4 × Cortex-A55);
– графический процессор: Mali-G610;
– оперативная память: 4ГБ LPDDR4X или LPDDR5;
– максимальное выходное разрешение: 8K;
– сеть: Gigabit Ethernet;
– USB: USB 3.0 и USB 2.0;
– GPIO: 40-пиновый разъем.

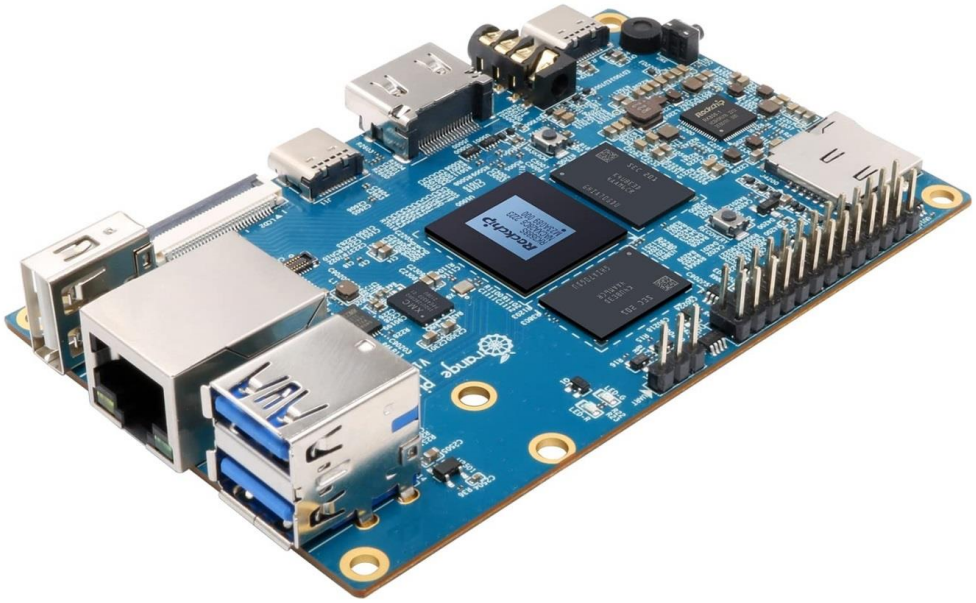


Рис. 3. Orange Pi 5

3. Banana Pi BPI-M5 (рис. 4), обладающий следующими основными техническими характеристиками:
– центральный процессор: 4-ядерный 64-битный CPU Amlogic S905X3;
– графический процессор: Mali-G31 MP2;
– оперативная память: 4ГБ LPDDR4;
– сеть: Gigabit Ethernet;
– HDMI
– USB: USB 3.0 и USB 2.0;
– GPIO: 40-пиновый разъем.

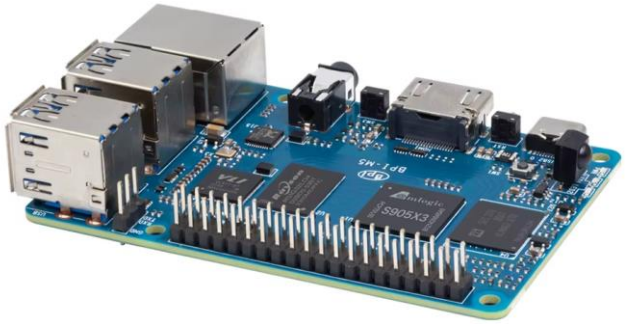


Рис. 4. Banana Pi BPI-M5

4. Nvidia Jetson Nano (рис. 5), обладающий следующими основными техническими характеристиками:

– центральный процессор: 4-ядерный 64-битный CPU на ARM Cortex A57 с тактовой частотой 1,43 ГГц;
– графический процессор: 128-ядерный GPU Maxwell, обладающий вычислительной мощностью в 0,5 терафлопс;
– оперативная память: 4 Гб 64-бит LPDDR4 25,6 ГБ/с;
– встроенное постоянное запоминающее устройство: 16 ГБ eMMC;
– максимальное выходное разрешение: 4K (3840×2160, H.264/H.265, 60 Гц);
– полноценная операционная система: Ubuntu 18.04 LTS;
– интерфейс камер: 12 линий MIPI CSI-2 DPHY 1.1 (1,5 Гб/с);
– порты подключения к внешнему дисплею: Display Port 1.4 и HDMI 2.0;
– порт для связи с Сетью: Gigabit Ethernet RJ-45;
– USB интерфейс: 4× USB 3.0, USB 2.0, micro USB Type B;
– другие интерфейсы: GPIO, I2C, I2S, SPI, UART.



Рис. 5. Nvidia Jetson Nano 4 ГБ

Каждый из представленных выше вычислителей по-своему хорош. Однако несомненным лидером данной выборки можно назвать Nvidia Jetson Nano 4 ГБ, обладающий самым производительным графическим процессором. Являясь одноплатным микрокомпьютером, он даже вместе с платой расширения, имеет достаточно скромные габариты по сравнению с обычным ПК. Все эти преимущества дают возможность использовать его в различных сферах, требующих многопоточной и параллельной цифровой обработки сигналов в реальном времени, а именно, для вейвлет-анализа и других аналогичных видов анализа сигналов [3, 5].

**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. Гарет Халфакри Raspberry Pi. Официальное руководство для начинающих / пер. с англ. С. В. Черникова. М.: ДМК Пресс, 2021. 262 с.

4. Ронкин М. А., Зенков Л. Р. Функциональная диагностика нервных болезней. Руководство для врачей. Изд. 5-е, Издательство МЕДпресс-информ, 2013, 488 с.

*Статья представлена научным руководителем: заместителем директора Института Магистратуры СПбГУТ по учебной работе, кандидатом технических наук, доцентом, доцентом кафедры Радиотехники А. Б. Степановым.*

## CHOOSING A GRAPHICS PROCESSOR FOR IMPLEMENTING DIGITAL SIGNAL PROCESSING ALGORITHMS USING WAVELETS

**Zapayshchikov A., Kruglova A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper is devoted to an overview of some of the graphics processors for implementing digital signal processing algorithms using wavelet analysis technology. Various types of computers that can be used for a specific task, their technical characteristics are given, and a choice is made in favor of the most suitable one. Based on all this, the real possibility of using a device to solve the task is being assessed.*

***Key words:*** *digital signal processing, wavelet analysis algorithm, computer, graphics processor, central processing unit, parallel computing*

**УДК 004.421**
**ГРНТИ 47.14.17**

# ОБЗОР МЕТОДОВ АНАЛИЗА БИОМЕДИЦИНСКИХ СИГНАЛОВ

**А. В. Запайщиков, А. В. Круглова**

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

*Данная работа посвящена обзору некоторых математических методов анализа биомедицинских сигналов. Приводится классификация возможных биомедицинских сигналов. Рассматриваются статистические, вариационные, спектральные, корреляционные методы, а также методы вейвлет-анализа. Частично затрагиваются методы нелинейной динамики. Приводятся и подробно расшифровываются основные математические формулы, описывающие каждый из конкретных методов. Оцениваются достоинства и недостатки некоторых из методов анализа.*

***биомедицинские сигналы, частотно-временной анализ, вейвлет-анализ, статистический метод, вариационный метод, спектральный метод***

Целью данной работы является обзор возможных математических методов анализа, применимых к биомедицинским сигналам.

На сегодняшний день разработка устройств персонализированной медицины, способных автоматически анализировать различные виды биомедицинских сигналов, является актуальной и очень важной задачей [1, 2].

Биомедицинскими сигналами называются такие сигналы, которые несут в себе информацию о физических проявлениях физиологических процессов живого организма, которая может быть измерена и представлена в виде, удобном для обработки с помощью вычислительной техники [3].

Важно понимать, что в целом, любые сигналы можно подразделить на детерминированные (заранее известные) и стохастические (случайные). Так вот, любой биомедицинский сигнал, содержащий в себе необходимую информацию, всегда будет случайным. И, если же он окажется детерминированным, то уже не будет представлять информационного интереса (будет пустым в информационном смысле), так как вся информация о нем будет уже заранее известна. Следовательно, нам будут требоваться математические методы для обработки именно случайных сигналов.

На рисунке 1 представлена схема, содержащая различные виды биомедицинских сигналов [4, 5, 6].

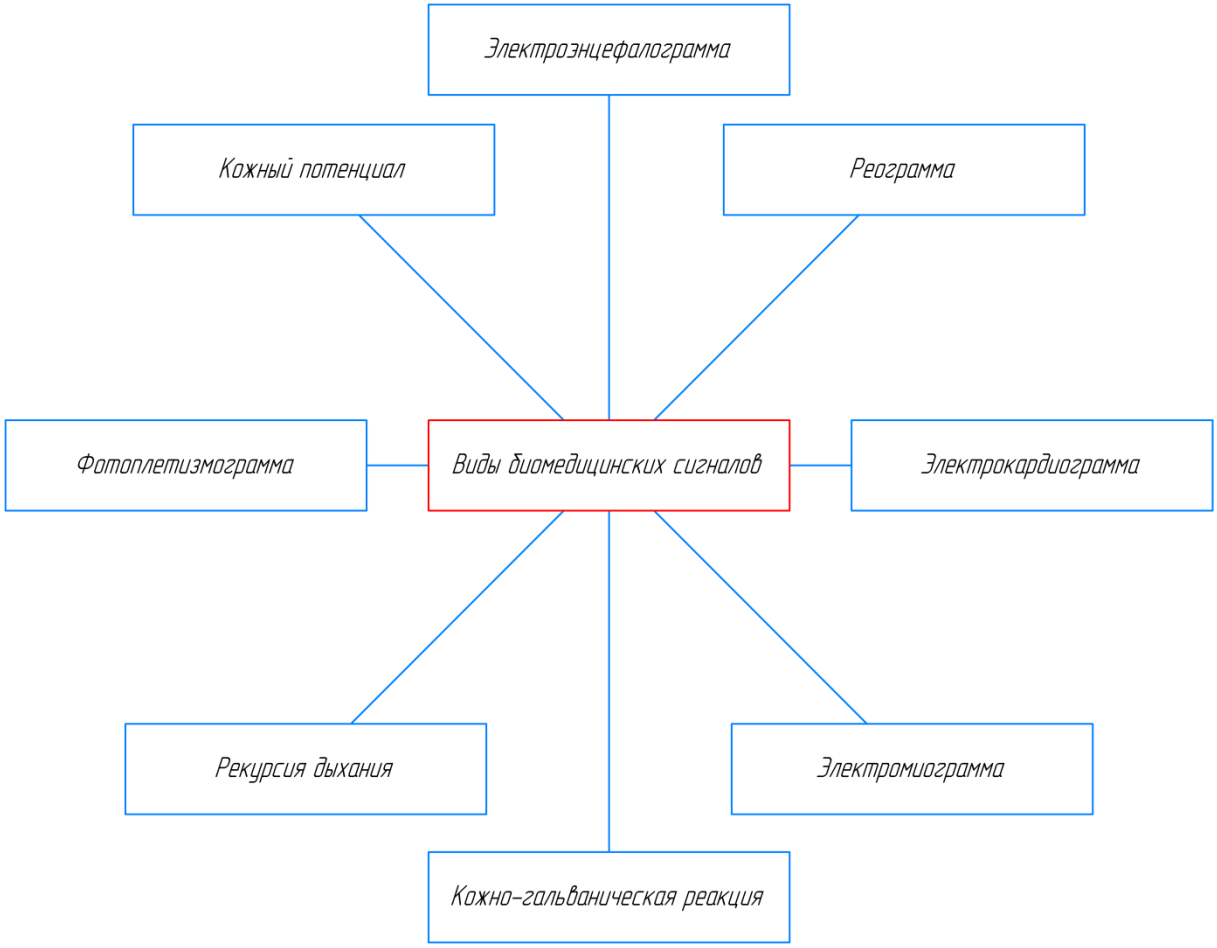



Рис. 1. Основные виды биомедицинских сигналов

Для каждого вида биомедицинских сигналов целесообразно использовать свой, наиболее подходящий для данной задачи метод математического анализа. Собственно базовые методы анализа биомедицинских сигналов можно подразделить на:

– статистические методы;
– вариационные методы;
– спектральные методы;
– корреляционные методы;
– методы вейвлет-анализа;
– методы нелинейной динамики.

Существующие статистические методы часто применяются для непосредственной прямой количественной оценки, например, временных рядов сигналов вариабельности сердечного ритма. Данные методы используют следующие показатели:

– среднее значение (математическое ожидание):

$$M = \frac{1}{N}\sum_{i=1}^{N} NN_i,$$

где $N -$ количество элементов временного ряда $NN; NN_i$ – отсчет этого ряда.

– среднеквадратическое отклонение на интервале наблюдения:

$$CKO = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(NN_i - M)^2},$$

где $N -$ количество элементов временного ряда $NN; NN_i$ – отсчет этого ряда; $M -$ математическое ожидание.

Коэффициент вариации – отношение $CKO$ к среднему значению. Выражается в процентах:

$$KB = \frac{CKO}{M} \cdot 100\ \%,$$

где $CKO -$ среднеквадратическое отклонение, $M -$ математическое ожидание.

Вариационные методы, в свою очередь, рассматривают биомедицинские сигналы с точки зрения случайных величин и изучают закон их распределения. Используют графики и гистограммы распределений. На рисунке 2 представлено изображение гистограммы нормального (Гауссового) распределения:

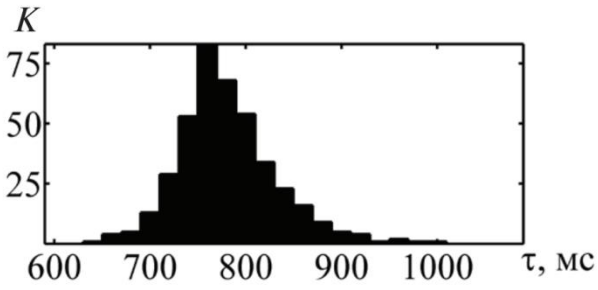



Рис. 2. Пример гистограммы нормального распределения

Спектральные методы применяются для точной количественной оценки периодических процессов в биомедицинском сигнале [7]. Спектральный анализ позволяет качественно и количественно оценить соотношения частотных компонент сигнала. Для непрерывных сигналов используется интегральное преобразование Фурье [7]:

$$S(f) = \int_{-\infty}^{+\infty} s(t)e^{-j2\pi ft}dt,$$

где $S(f)$ – результат отображения сигнала в частотной области; $s(t)$ – исходный сигнал; $j$ – мнимая единица.

На рисунке 3 представлено изображение, наглядно демонстрирующее отображение сигнала из временной области в частотную [8]:

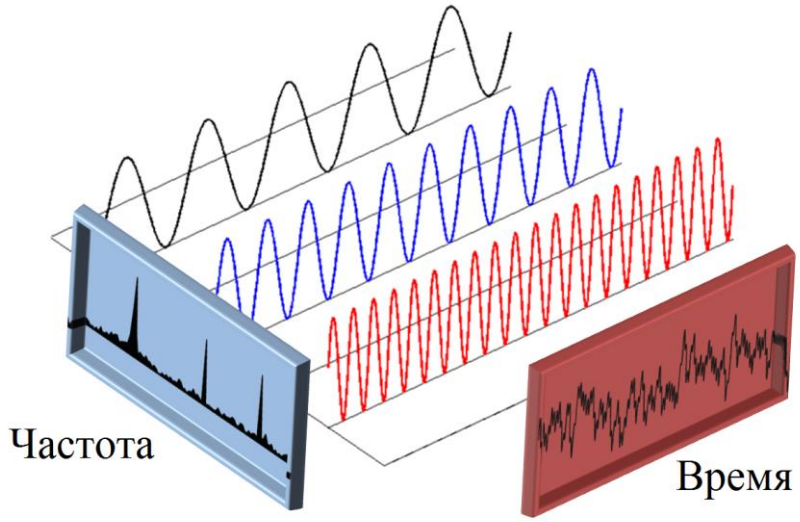



Рис. 3. Отображение сигнала из временной области в частотную

Корреляционные методы изучают внутреннюю структуру временных рядов путем последовательного анализа «схожести» пар сигналов. Основой данных методов является взаимная корреляционная функция:

$$R(\tau) = \int_{-\infty}^{+\infty} s_1(t)s_2(t-\tau)dt,$$

где $s_1(t)$ – эталонный сигнал (тот, который известен заранее и с которым будет производиться сравнение), $s_2(t)$ – исходный сигнал, который будет сравниваться с первым.

Общая энергия двух сигналов при этом будет иметь какое-то значение *N*. Но, том случае, когда сигнал $s_2(t)$ будет являться точной копией сигнала $s_1(t)$, взаимная корреляционная функция будет автокорреляционной. Общая энергия двух сигналов будет иметь максимально возможное значение, нежели в предыдущем случае. На основании этого и можно сделать вывод о том, что сигналы полностью одинаковые.

Методы вейвлет-анализа (частотно-временного анализа) сигналов, позволяют анализировать биомедицинские сигналы как по времени, так и по частоте, что дает возможность получения большей информации об обрабатываемом сигнале [9, 10, 11].

Уравнение для непрерывного интегрального вейвлет-преобразования анализируемого сигнала $s(t)$ имеет следующий вид [5, 9]:

$$W(a,b) = \frac{1}{\sqrt{a}} \int s(t) \cdot \psi\left(\frac{t-b}{a}\right) dt,$$

где $a$ – коэффициент масштаба; $b$ –коэффициент сдвига; $s(t)$ – исходный сигнал; $\psi$ – материнский (базисный) вейвлет.

На рисунке 4 представлен результат вейвлет-анализа биомедицинского сигнала, полученный с помощью MATLAB:

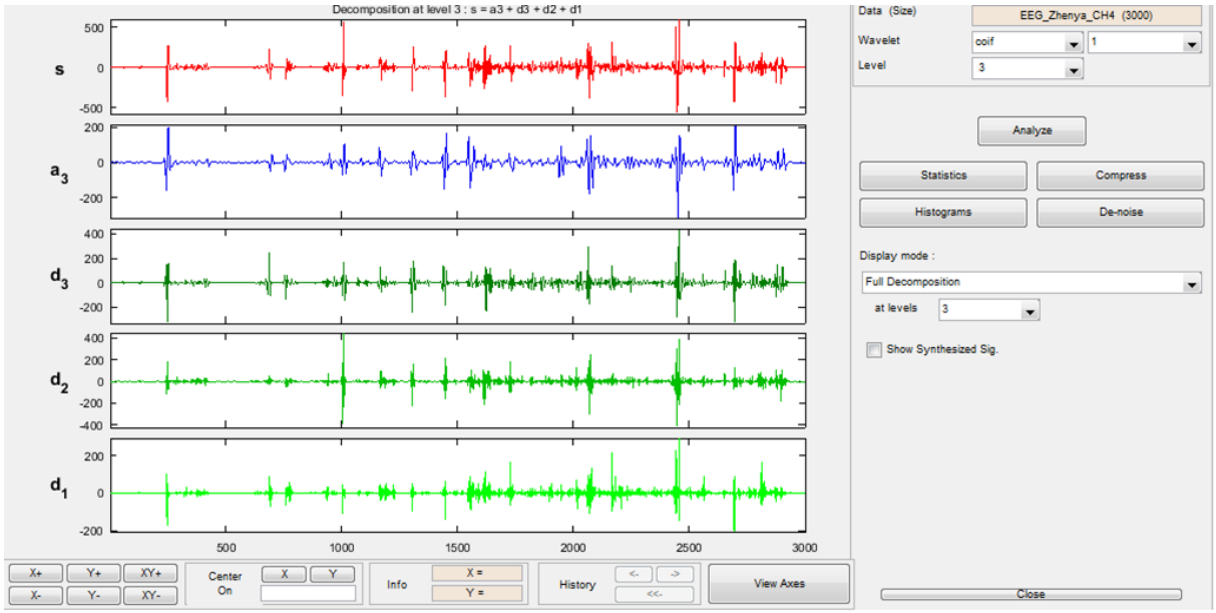



Рис. 4. Вейвлет-анализ биомедицинского сигнала

Методы нелинейной динамики были придуманы для получения количественных соотношений между частотными компонентами изучаемых биомедицинских сигналов, так как вышеизложенные методы не всегда и не во всех случаях позволяют качественно охарактеризовать динамику нелинейных процессов, которые формируются сложными системами. Из основных можно выделить следующие:

– энтропия Колмогорова;
– размерности Реньи;
– показатель Херста;
– показатели Ляпунова.

Проанализировав основные методы анализа биомедицинских сигналов, можно сделать вывод о том, что каждый из подвидов по-своему уникален для каждого конкретного типа сигнала. Однако к одним и тем же сигналам бывает возможно применить сразу несколько методов анализа. Тут уже все будет зависеть от конкретных задач: где-то лучше подойдут спектральные методы анализа, где-то методы нелинейной динамики. А где-то было бы целесообразно использовать методы вейвлет-анализа, являющиеся почти универсальными за счет уже существующих базисных вейвлетов, которые можно подобрать почти к любому биомедицинскому сигналу для получения качественного и требуемого результата его цифровой обработки.

**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. Поляков А. О. Введение в основы информационной медицины: учеб. пособие / А.О. Поляков. СПб.: Изд-во СПбГПУ, 2005. 150 с.

4. Арбузов С. М., Степанов А. Б. Применение методов вейвлет-анализа в электроэнцефалографии. СПб.: Линк, 2009. 104 с.

5. Кубланов В.С. Анализ биомедицинских сигналов в среде MATLAB: учебное пособие / В. С. Кубланов, В. И. Борисов, А. Ю. Долганов. Екатеринбург: Изд-во Урал. ун-та, 2016. 120 с.

6. Ронкин М. А., Зенков Л. Р. Функциональная диагностика нервных болезней. Руководство для врачей. Изд. 5-е, Издательство МЕДпресс-информ, 2013, 488 с.

7. Acharya, U. Rajendra; Vinitha Sree, S.; Swapna, G.; Martis, Roshan Joy; Suri, Jasjit S. (June 2013). "Automated EEG analysis of epilepsy: A review". Knowledge-Based Systems. 45: 147–165.

8. Ogilvie, Robert D.; Simons, Iain A.; Kuderian, Roxanne H.; MacDonald, Thomas; Rustenburg, John (January 1991). "Behavioral, Event-Related Potential, and EEG/FFT Changes at Sleep Onset". Psychophysiology. 28 (1): 54–64.

9. Козлов Д. В., Степанов А. Б. Алгоритм выполнения частотно-временного анализа сигналов с применением непрерывного вейвлет-преобразования и метода периодограмм и его реализация на графическом процессоре // Вестник Воронежского государственного технического университета. 2021. Т. 17. № 3. С. 85-93.

10. Stark H.-G. Wavelets and Signal Processing. Berlin: Springer, 2005. 158 p.

11. Витязев В. В. Вейвлет-анализ временных рядов. СПб.: Изд-во С.-Петерб. ун-та, 2001. 58 с.

*Статья представлена научным руководителем: заместителем директора Института Магистратуры СПбГУТ по учебной работе, кандидатом технических наук, доцентом, доцентом кафедры Радиотехники А. Б. Степановым.*

# OVERVIEW OF BIOMEDICAL SIGNAL ANALYSIS METHODS

**Zapayshchikov A., Kruglova A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper is devoted to a review of some mathematical methods for analyzing biomedical signals. A classification of possible biomedical signals is given. Statistical, variational, spectral, correlation methods, as well as methods of wavelet analysis are considered. The methods of nonlinear dynamics are partially affected. The basic mathematical formulas describing each of the specific methods are given and explained in detail. The advantages and disadvantages of some of the analysis methods are evaluated.*

***Key words:*** *biomedical signals, time-frequency analysis, wavelet analysis, statistical method, variational method, spectral method*

**УДК 677. 070**
**ГРНТИ 64.29.35**

# ПРОЕКТИРОВАНИЕ В СРЕДЕ MATLAB ПАКЕТА МАТЕРИАЛОВ, ПРИМЕНЯЕМЫХ ДЛЯ ПРОИЗВОДСТВА ИЗДЕЛИЙ, ЭКСПЛУАТИРУЕМЫХ В УСЛОВИЯХ АРКТИКИ

**Н. П. Лебедева[1], А. Б. Степанова[2]**

[1]Санкт-Петербургский государственный университет промышленных технологий и дизайна
[2]Санкт-Петербургский политехнический университет Петра Великого

*Комплексное развитие Арктики, расширение зоны социально-экономического воздействия и укрепление позиций в регионе приводит к открытию новых проектов. Особые климатические условия требуют правильно подобранного пакета материалов, предназначенного для данного региона. Среда MATLAB может помочь выполнить предварительный расчет с учетом температурных факторов и силы ветра.*

***пакет материалов, среда MATLAB, обработка данных***

Начиная с 2020 года, когда вышел Указ Президента о стратегическом развитии Арктической зоны, началось активное расширение экономических интересов, связанных с развитием Северного морского пути, строительством крупнотоннажных морских сооружений (в рамках проекта «Арктик СПГ 2»), модернизацией и строительством автомобильных и железных дорог, строительством морского терминала, расширением зоны добычи полезных ископаемых и т.п. Все это приводит к привлечению узкоспециализированных специалистов с разных регионов России.

Тяжелые погодные условия: суровые продолжительные зимы, когда температура воздуха может опускаться до -40°Си ниже, а экстремальные минимумы могут достигать -60°С, сильные ветра с метелью, снег и повышенная влажность еще больше ухудшают условия труда. Все эти факторы приводят к необходимости совершенствования комплектования материалов для изделий, необходимых для защиты человека от непростых погодных условий [1-3].

В связи с этим возникает острая необходимость проектирования наиболее оптимального пакета материалов, который будет отвечать погодным условиям.

Для достижения наиболее оптимального результата по защитным свойствам можно воспользоваться средой MATLAB для выполнения необходимых расчетов.

На рисунке 1 приведен пример расчета в среде MATLAB требуемой толщины пакета материалов для спецодежды, эксплуатируемой при экстремально

низких температурах с учетом теплозащитных и ветрозащитных свойств. В качестве переменных задавали изменяющуюся температуру: от – 40°С до – 60°С с шагом 5°С. Так же учитывали изменяющуюся скорость ветра: 10, 15 и 20 м/с.

Расчет выполняли на основании методики Кондратьева Г. М., предназначенной для определения теплоизоляционных свойств пакета материалов [4].

В качестве примера использовалась формула:

$$R = 0{,}175 \cdot I, \quad (1)$$

где $R$ – суммарное тепловое сопротивление одежды, $м^{2\cdot0}С/Вт$.

После этого $R$ переводят в толщину пакета. Для этого надо знать термическое сопротивление материалов и долю слоев (утеплитель и внешний слой материала). Скрипт, написанный на языке MATLAB, поможет на основании показателя R определить необходимую толщину пакета материала.

Индекс теплоизоляции $I$, определяющий, какая степень теплозащиты требуется в конкретных условиях, рассчитывается по формуле:

$$I = \frac{0{,}15 \cdot (33 - t_в)}{N} - \frac{5{,}7}{\alpha}, \quad (2)$$

где $N$ – показатель тепловой нагрузки;

$t_в$ – температура воздуха;

$\alpha$ – коэффициент теплоотдачи (зависит от ветра).

Индекс теплоизоляции зависит от разницы температур «тело-среда».

Показатель тепловой нагрузки определятся по формуле:

$$N = 0{,}78 \cdot \frac{M}{100}, \quad (3)$$

где $M$ – теплопродукция, Вт.

В расчете учитывают скорость ветра, т.к. она оказывает сильное влияние на коэффициент теплоотдачи $\alpha$.

В представленном скрипте сначала определили показатель тепловой нагрузки $N$. Затем показатель теплоизоляционной способности $I$.

Температура окружающего воздуха $t_в$ здесь отображена как *T_amb*.

Варианты скорости ветра отображаются в скрипте в виде *v_wind*.

Суммарное тепловое сопротивление пакета материалов *R_сум* показывает, насколько хорошо пакет материалов сопротивляется передаче тепла.

Толщину пакета материалов определяли по формуле:

$$\delta\_п = R\_сум \times \lambda\_э \quad (4)$$

где $\lambda\_э$ – эквивалентный коэффициент теплопроводности пакета целиком.

```
function arctic_kondratiev_wind_temp()
    % --- Исходные данные ---
    T_amb = [-40, -45, -50, -55, -60]; % температуры среды, °C
    v_wind = [10, 15, 20];             % скорости ветра, м/с
    M = 120;                            % теплопродукция (метаболизм), Вт

    % Характеристики материалов: термическое сопротивление на 1 мм (м^2·°C/Вт
    R_per_mm_insul = 0.038;             % Тинсулейт
    R_per_mm_shell = 0.015;            % Ветрозащитная мембрана

    % Доли слоёв в пакете: 80% утеплитель, 20% оболочка
    ratio_insul = 0.8;
    ratio_shell = 0.2;

    nT = length(T_amb);
    nv = length(v_wind);

    % Массивы для хранения результатов
    N_vals = zeros(nT, nv);
    I_vals = zeros(nT, nv);
    R_req = zeros(nT, nv);             % суммарное R по Кондратьеву
    t_total = zeros(nT, nv);           % итоговая толщина пакета, мм

    fprintf('Расчёт по методу Кондратьева (M = %.1f Вт)\n', M);
    fprintf('Сценарии: T = [%s] °C; v = [%s] м/с\n\n', ...
        strjoin(cellstr(num2str(T_amb')), ', '), ...
        strjoin(cellstr(num2str(v_wind')), ', '));

    % Двойной цикл: по температуре и по ветру
    for i = 1:nT
        t_v = T_amb(i); % температура воздуха t_в

        for j = 1:nv
            v = v_wind(j); % скорость ветра

            % Коэффициент теплоотдачи alpha (зависит от ветра)
            alpha = 10 + 7 * v^0.8; % Вт/м^2·°C

            % Формула 1: N = 0,78 * M / 100
            N_vals(i,j) = 0.78 * M / 100;

            % Формула 2: I = 0,15 * (33 - t_в) / N - 5,7 / alpha
            I_vals(i,j) = 0.15 * (33 - t_v) / N_vals(i,j) - 5.7 / alpha;

            % Формула 3: R = 0,175 * I
            R_req(i,j) = 0.175 * I_vals(i,j);

            % Пересчёт R в толщину пакета материалов
            R_insul_needed = ratio_insul * R_req(i,j);
            R_shell_needed = ratio_shell * R_req(i,j);

            t_insul = R_insul_needed / R_per_mm_insul;
            t_shell = R_shell_needed / R_per_mm_shell;
            t_total(i,j) = t_insul + t_shell;
        end
    end
```

Рис. 1. Пример расчета в среде MATLAB требуемой толщины пакета материалов

В предложенном скрипте данные распределены следующим образом между слоями. Далее, используя термическое сопротивление для каждого материала на миллиметр определили *R_per_mm_insul, R_per_mm_shell*.

Следует отметить, что методика Г. М. Кондратьева хоть и подходит для расчетов оценки теплозащитных свойств пакета материалов, но все-таки носит приближенный характер. Написание скрипта на языке MATLAB для выполнения вычисления, согласно методу Г. М. Кондратьева, позволяет быстро и качественно выполнить первичную оценку и исходные требования к пакету материалов.

**Список используемых источников**

1. Указ Президента Российской Федерации от 5 марта 2020 года № 164 «Об Основах государственной политики Российской Федерации в Арктике на период до 2035 года». URL: http://www.kremlin.ru/acts/bank/45255. Дата обращения: 25.05.2026.

2. Климат Арктики. Пастухова О. // Polar Travel Club. URL: https://polartravelclub.ru/info-for-travelers/articles/klimat-arktiki/. Дата обращения: 30.05.2026.

3. Исследование свойств параарамидных нитей под воздействием эксплуатационных факторов с использованием современного программного обеспечения. Лебедева Н. П., Степанова А. Б. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2025). Сборник научных статей XIV Международной научно-технической и научно-методической конференции. В 2-х томах. Санкт-Петербург, 2025. С. 705-709.

4. Учебно-методический комплекс дисциплины «Гигиена одежды» / Амурский государственный университет, кафедра конструирования и технологии одежды. Благовещенск: АмГУ, 2012. 66 с.

## MATLAB-BASED DESIGN OF MATERIALS PACKAGES USED IN THE PRODUCTION OF PRODUCTS OPERATING IN THE ARCTIC REGION

**Lebedeva N.[1], Stepanova A.[2]**
[1]Saint Petersburg State University of Industrial Technologies and Design
[2]Peter the Great Saint Petersburg Polytechnic University

*The comprehensive development of the Arctic, the expansion of the socio-economic impact zone, and the strengthening of positions in the region are leading to the opening of new projects. The specific climatic conditions require a properly selected package of materials tailored to the region. The MATLAB environment can help perform preliminary calculations based on temperature factors and wind strength.*

***Key words:*** *material package, MATLAB environment, data processing*

**УДК 621.3**
**ГРНТИ 47**

# ПРИМЕНЕНИЕ ОБОРУДОВАНИЯ ДЛЯ КОРОТКОВОЛНОВОЙ РАДИОСВЯЗИ В ГИБРИДНЫХ СЕТЯХ СВЯЗИ ЕДИНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ АРКТИЧЕСКОЙ ЗОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

**А. Б. Степанов**

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

*В работе рассматривается возможность применения оборудования для коротковолновой радиосвязи в гибридных сетях связи Единой информационной системы Арктической зоны Российской Федерации, предложенной автором. Приводится пример построения планируемой сети при проведении Арктической технологической экспедиции СПбГУТ в Республику Саха (Якутия) «На связи с будущим!». Описываются сложности организации коротковолновой радиосвязи в условиях Крайнего Севера, а также ограничения ее применения в составе гибридной сети связи.*

***единая информационная система Арктической зоны Российской Федерации, коротковолновая радиосвязь, гибридные сети связи, автоматический портативный электроэнцефалограф, передача данных***

Для Арктической зоны Российской Федерации (АЗРФ) характерна малая плотность населения, значительные расстояния между населенными пунктами, часто неразвитая инфраструктура и суровые климатические условия [1]. Среди основных задач, требующих решения в интересах развития арктических регионов, можно выделить следующие: ликвидация цифрового неравенства [2], развитие инфраструктуры и системы здравоохранения, внедрение передовых технологий и реализация экономического потенциала территорий.

Для достижения задач технологического лидерства нашей страны, обеспечения национальной безопасности и устойчивого развития арктических регионов автором данной работы ранее была предложена концепция Единой информационной системы Арктической зоны Российской Федерации (ЕИС АЗРФ) [3]. Ее реализация требует развертывание на всей территории АЗРФ гибридной сети связи нового поколения, обеспечивающей бесшовную передачу данных между ее элементами и системами, использующими при организации связи различные технологии. На рис. 1 представлен

пример такой сети. Кроме традиционных линий и средств связи, широко применяемых в других регионах, для АЗРФ особое значение имеют спутниковые, тропосферные и радиорелейные системы связи, а также коротковолновые (КВ) и ультракоротковолновые (УКВ) средства радиосвязи. Если УКВ радиосвязь широко применяется для организации связи на малых расстояниях, то КВ радиосвязь позволяет организовать передачу данных в широком диапазоне расстояний:

– на малые расстояния (в условиях прямой видимости);
– на расстояниях до нескольких сотен километров в зенитном режиме работы;
– на дальних и сверхдальних расстояниях (до нескольких тысяч километров) за счет эффекта отражения от ионосферы.

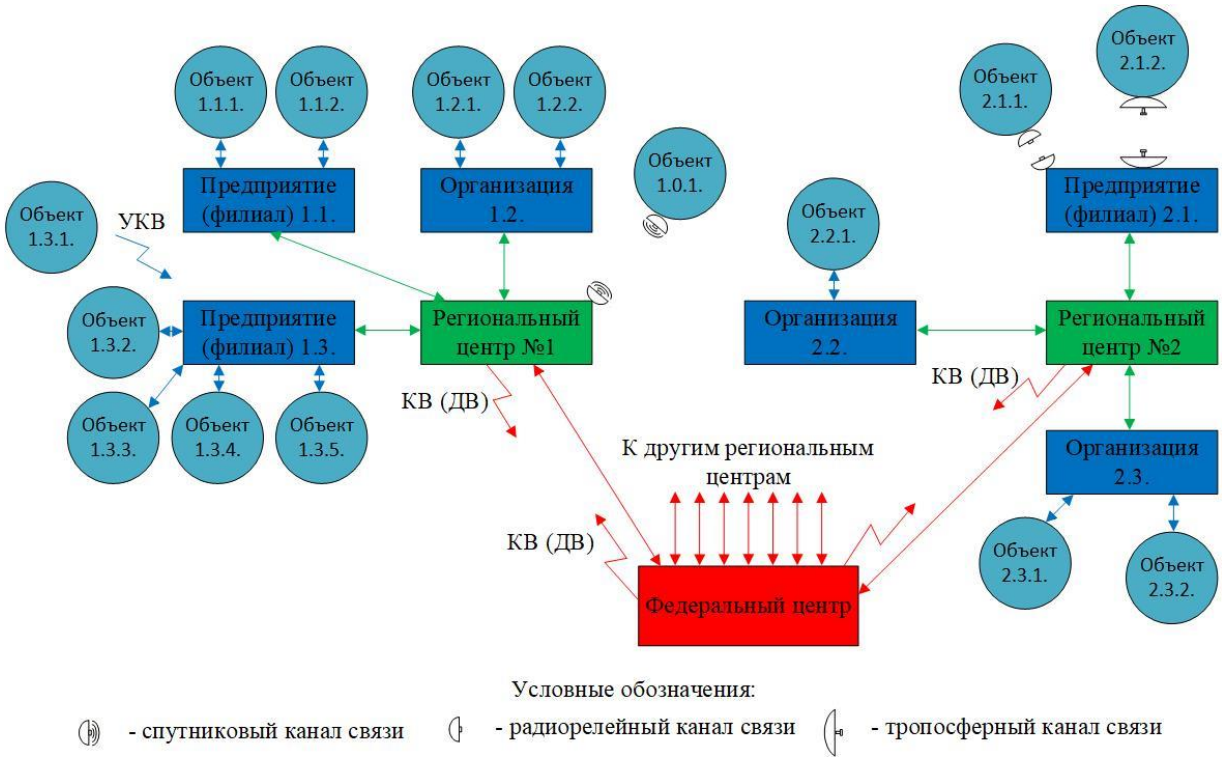



Рис. 1. Единая информационная система Арктической зоны Российской Федерации с использованием оборудования для спутниковой связи, КВ, СВ и ДВ радиосвязи в составе гибридной сети связи

Основным недостатком КВ радиосвязи для организации передачи данных на большие расстояния является громоздкость антенного оборудования и, как правило, достаточно высокая необходимая мощность. Кроме того, КВ радиосвязь подвержена влиянию различного рода помех, что затрудняет ее использование рядом с источниками электромагнитного излучения, напри-

мер, в зданиях. Для Крайнего Севера из-за магнитного излучения организация КВ радиосвязи может быть невозможна в течение нескольких дней [4]. Однако грамотный выбор частотного плана, использование эффективных антенн делает КВ радиосвязь основным резервным каналом связи в Арктике. Использование портативных антенн (в том числе, телескопических с катушками) и сверхлегких радиостанций малой мощности позволяет реализовывать носимые комплексы весом до 1 кг и использовать КВ радиосвязь на расстоянии до 150–200 км. Скорость передаваемых данных для КВ радиомодемов может отличаться. Уверенный прием может выполняться на скорости 2,4 Кбит/с. При оптимальных условиях скорость при использовании параллельного модема может составлять 9,6 Кбит/с. Этой скорости достаточно для передачи текстовых и голосовых сообщений, данных от различных датчиков и оборудования, также может передаваться фото и видео с прогрессивными алгоритмами сжатия. Для некоторых видов данных этой скорости недостаточно. Так, например, для передачи данных в реальном времени от восьмиканального автоматического портативного электроэнцефалографа «Катюша», разработанного под руководством автора данной статьи [5–8], при частоте дискретизации 250 Гц требуется скорость в 5 раз выше. Однако при использовании алгоритмов на основе математического аппарата вейвлетов, предложенных автором данной статьи ранее [9], позволяющих анализировать электроэнцефалограмму по ее сжатому представлению, объем передаваемой информации может быть уменьшен в 8 раз. В этом случае минимальная скорость передачи данных составляет 6 Кбит/с. Запас по скорости передачи данных позволяет нивелировать потенциальные кратковременные изменения в скорости передачи информации при воздействии внешних факторов.

Также оборудование на базе КВ радиосвязи может применяться для передачи данных от других медицинских устройств: электрокардиографов, устройств для регистрации и анализа электрогастрограммы, электромиограммы и пр. Интегрированное оборудование для КВ радиосвязи может применяться для передачи параметров технологических машин, в том числе при обнаружении дефектов в их конструкциях (например, с использованием алгоритмов на основе непрерывного вейвлет-преобразования [10]). Также КВ радиоканалы могут использоваться для передачи данных от тревожных кнопок, расположенных на различных объектах.

Таким образом, КВ радиоканал может рассматриваться как альтернативный канал связи и в случае, когда развертывание спутникового оборудования может считаться нецелесообразным.

Ультракоротковолновые приемопередатчики могут применяться при передаче данных различного вида на расстояния до нескольких десятков километров. Традиционные виды модуляции позволяют получить скорости до 50 Кбит/с. Под руководством автора данной статьи были разработаны энергоэффективные УКВ приемопередатчики семейства АЛИСА-С [11]. Их особенность заключается в энергоэффективности и дальности связи до 16 км. При минимальной мощности 0,1 Вт дальность составляет до 4 км. Применение ретрансляторов позволяет кратно увеличивать дальность связи. Данные приемопередатчики могут объединяться в mesh-сети.

Использование средневолновой (СВ) и длинноволновой (ДВ) радиосвязи в Арктической зоне Российской Федерации, как правило, связано с организацией специальных каналов связи и имеет свои ограничения, в том числе по скорости передачи данных.

На рис. 2 приведен фрагмент гибридной сети связи нового поколения, которую планируется развернуть в рамках Арктической технологической экспедиции СПбГУТ в Республику Саха (Якутия) в 2026 году. Она включает в себя следующее оборудование:

– коммутаторы, сервер и другое сетевое оборудование;
– телефонные аппараты;
– различные периферийные устройства, автоматический портативный электроэнцефалограф, датчики сейсмической активности, датчики технологических машин и другие датчики;
– спутниковое оборудование (носимая спутниковая станция СНАРК-100Р компании ООО «Рэйс-Коммуникейшн», абонентский терминал РС-30М компании АО «Информационные спутниковые системы имени академика М. Ф. Решетнева», терминал для низкоорбитальной группировки спутников, разработанный под руководством автора данной статьи, для спутников ГК «СПУТНИКС», приемник «Вьюнок» компании ГК «СПУТНИКС» и другое оборудование);
– оборудование для КВ радиосвязи;
– оборудование для УКВ радиосвязи (энергоэффективные приемопередатчики АЛИСА-С различных модификаций, в том числе, предназначенные для установки в зданиях, на мачтовом оборудовании с возможностью

электроснабжения от портативных ветренных генераторов, носимые или установленные на транспортных средствах);

– другое оборудование.

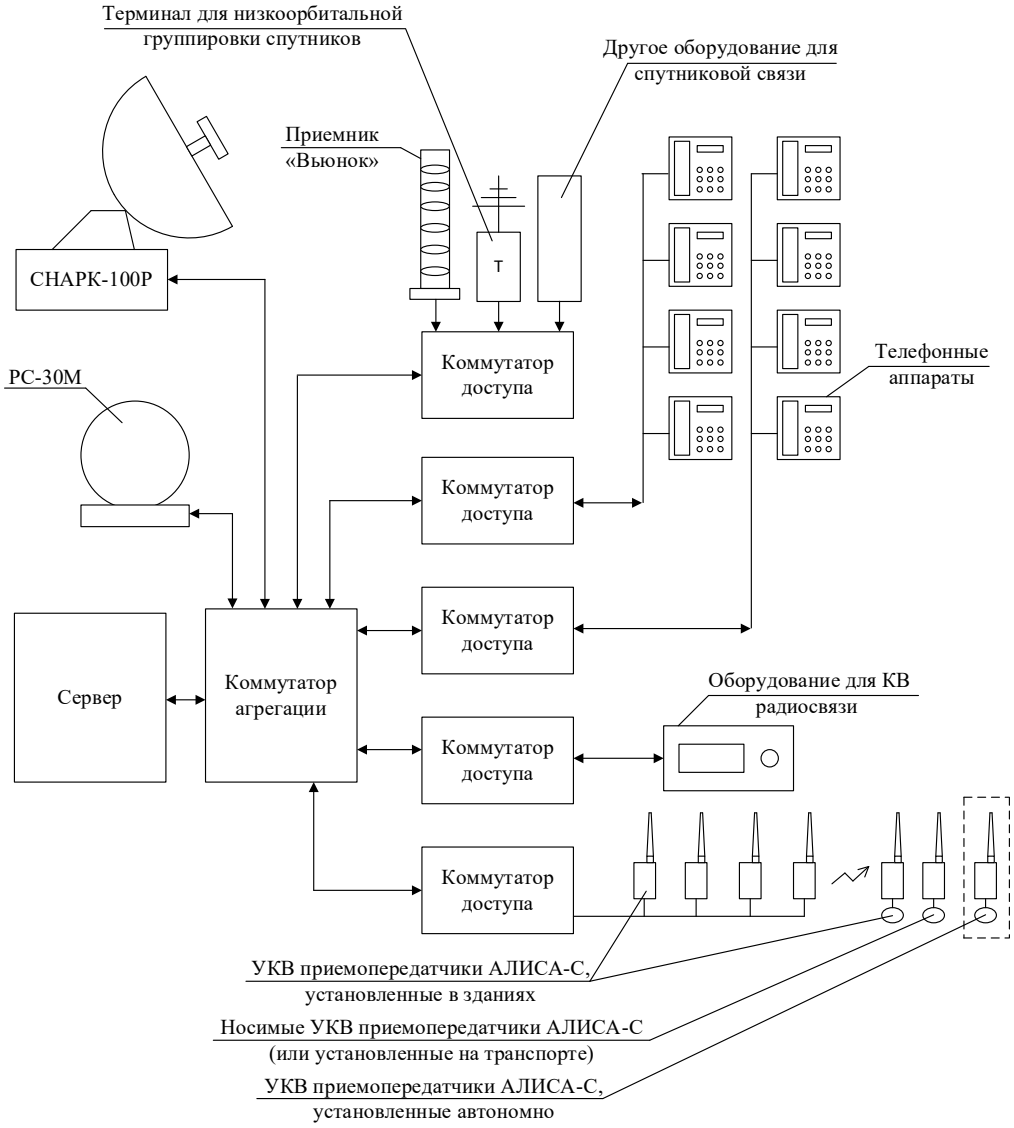



Рис. 2. Фрагмент гибридной сети связи, разворачиваемой в рамках Арктической технологической экспедиции СПбГУТ в Республику Саха (Якутия)

Работоспособность гибридной сети связи планируется протестировать при проведении видеоконференцсвязи с участием профильных министерств всех арктических регионов.

Экспедиция в Республику Саха (Якутия) «На связи с будущим!» реализуется СПбГУТ при поддержке конкурса «Открываем Россию заново» Высшей школы экономики и АНО «Россия – страна возможностей», Русского географического общества, Правительства Республики Саха (Якутия), Комитета по внешним связям Санкт-Петербурга, Постоянного представитель-

ства Республики Саха (Якутия) при Президенте Российской Федерации и др.

**Список используемых источников**

1. Указ Президента Российской Федерации от 26 октября 2020 г. № 645 «О Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года».

2. Распоряжение Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года.

3. Степанов А. Б. Разработка автоматического портативного электроэнцефалографа с возможностью интегрирования в Единую информационную систему Арктической зоны Российской Федерации / А. Б. Степанов // Электросвязь. 2024. № 12-2. С. 53-60. DOI: 10.34832/ELSV.2024.61.12.007. EDN: KPOWOQ.

4. Калинин А. И., Черенкова Е. Л. Распространение радиоволн и работа радиолиний, Издательство «Связь», М.: 1971, 440 с.

5. Степанов А. Б. Автоматический портативный электроэнцефалограф / А. Б. Степанов // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции, Санкт-Петербург, 30 ноября – 02 2021 года. Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2022. С. 150-153. EDN: AYANEX.

6. Свидетельство о государственной регистрации программы для ЭВМ № 2022667973 Российская Федерация. Программа, реализующая автоматический портативный электроэнцефалограф: № 2022667302: заявл. 21.09.2022: опубл. 29.09.2022 / А. Б. Степанов, Д. В. Козлов. EDN: LFCORV.

7. Патент № 2467384 C1 Российская Федерация, МПК G06F 17/14, A61B 5/0476. Способ анализа электроэнцефалограмм: № 2011127377/08: заявл. 28.06.2011: опубл. 20.11.2012 / А. Б. Степанов. EDN: PHYUJC.

8. Патент на полезную модель № 110632 U1 Российская Федерация, МПК A61B 5/0476, G06F 17/00. Автоматизированная система анализа электроэнцефалограмм: № 2011127360/14: заявл. 28.06.2011: опубл. 27.11.2011 / А. Б. Степанов. EDN: FLCTAN.

9. Stepanov A. B. Wavelet analysis of compressed biomedical signals / A. B. Stepanov // 20th Conference of Open Innovations Association FRUCT: Proceedings, Saint-Petersburg, 03–07 апреля 2017 года / LETI University, St.Petersburg, Russia; S. Balandin, A. Levina, T. Tyutina. St. Petersburg: FRUCT Oy, 2017. P. 434-440. DOI: 10.23919/FRUCT.2017.8071345. EDN: XOZYVF.

10. Stepanov A. Polynomial, neural network, and spline wavelet models for continuous wavelet transform of signals / A. Stepanov // Sensors. 2021. Vol. 21. N 19. P. 6416. DOI: 10.3390/s21196416. EDN: VCGNHB.

11. Степанов А. Б. Особенности построения сети передачи данных в деревне Летняя Золотица Архангельской области с применением УКВ приемопередатчиков АЛИСА-С / А. Б. Степанов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2025). XIV Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2025. Том 1. С. 710-714. EDN: XDXTPD.

# THE USE OF EQUIPMENT FOR SHORTWAVE RADIO COMMUNICATION IN HYBRID COMMUNICATION NETWORKS OF THE UNIFIED INFORMATION SYSTEM OF THE ARCTIC ZONE OF THE RUSSIAN FEDERATION

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

*The paper examines the possibility of using equipment for shortwave radio communication in hybrid communication networks of the Unified Information System of the Arctic Zone of the Russian Federation, proposed by the author. An example is provided of building the planned network during the Arctic Technological Expedition of St. Petersburg State University of Telecommunications to the Republic of Sakha (Yakutia) "In Touch with the Future!" The challenges of organizing shortwave radio communication in the conditions of the Far North are described, as well as the limitations of its use as part of a hybrid communication network.*

***Key words:*** *Unified Information System of the Arctic Zone of the Russian Federation, shortwave radio communication, hybrid communication networks, automatic portable electroencephalograph, data transmission*

**УДК 621.3**
**ГРНТИ 47**

# ТЕРМИНАЛ СВЯЗИ ДЛЯ НИЗКООРБИТАЛЬНОЙ ГРУППИРОВКИ СПУТНИКОВ С БЛОКОМ ЧАСТОТНО-ВРЕМЕННОГО АНАЛИЗА СИГНАЛОВ И С ФУНКЦИЕЙ ТРЕВОЖНОЙ КНОПКИ

**А. Б. Степанов**

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

*Статья посвящена описанию концепции, структуры и принципов работы терминала связи для низкоорбитальной группировки спутников с блоком частотно-временного анализа сигналов и с функцией тревожной кнопки, предложенной автором. Приводятся достоинства и недостатки математических моделей вейвлетов для непрерывного вейвлет-преобразования, которые могут быть использованы в алгоритме работы терминала. Описываются принципы формирования передаваемых сообщений с учетом применения терминала в условиях Крайнего Севера. Приводятся области применения терминала.*

***терминал спутниковой связи, низкоорбитальная группировка, вейвлет, синтезированные вейвлеты, непрерывное вейвлет-преобразование, тревожная кнопка***

Одной из ключевых задач на пути к устойчивому развитию Арктической зоны Российской Федерации (АЗРФ) остается организация бесперебойной связи для всех ее потребителей [1, 2]. Сдерживающими факторами в решении этой задачи остаются технологические сложности, связанные с суровым климатом Крайнего Севера, высокими широтами территории и особенностями распространения радиоволн, и экономическая нецелесообразность использования традиционных систем связи из-за малой плотности населения и значительных расстояний между соседними населенными пунктами. Использование спутникового оборудования, которое позволяет решить проблему цифрового неравенства в АЗРФ, часто ограничивается его значительной стоимостью и высокой абонентской платой за использование ресурса спутниковой группировки. При этом для многих задач на объектах АЗРФ не требуется организация высокоскоростного канала связи, достаточной является регулярная отправка коротких сообщений.

В работе предлагается терминал связи для низкоорбитальной группировки спутников, который обладает следующими особенностями:

1. Передача коротких сообщений (с полезной составляющей до 100 битов за сеанс).

2. Возможность выполнения предобработки сигналов от различного вида датчиков, устройств и систем за счет наличия блока частотно-временного анализа сигналов.

3. Возможность передачи сигнала тревожной кнопки с высокой вероятностью доставки сообщения.

4. Энергоэффективность.

5. Малый вес (1 кг).

6. Низкая стоимость оборудования (в 100 раз дешевле высокоскоростных спутниковых систем).

На рис. 1 показана концепция передачи сообщения от абонента (с использованием терминала) через спутник низкоорбитальной группировки в центр управления полетами (ЦУП), а далее по стандартным каналам связи потребителю. Такой подход позволяет значительно снизить требования к терминалу. Использование низкой орбиты спутника также позволяет уменьшить расстояние, преодолеваемое сигналов, а соответственно и требования к мощности излучения и используемой антенны. Совокупность этого позволяет применять на практике для передачи сообщений технологию LoRa.

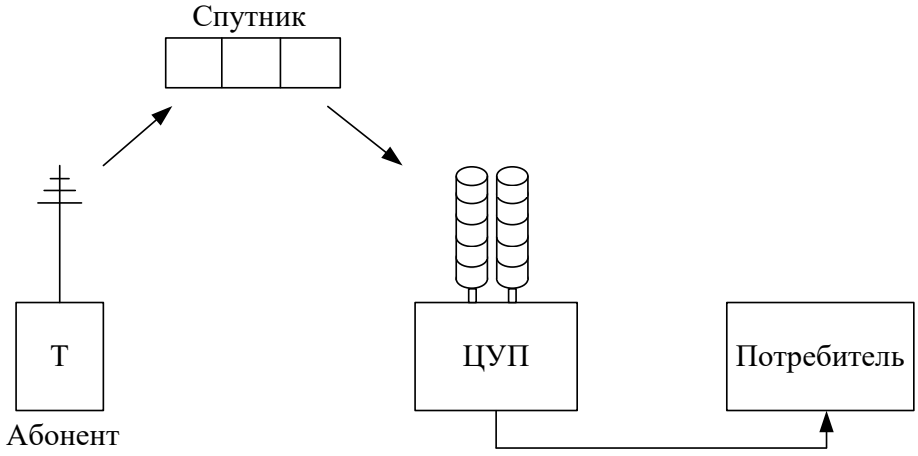



Рис. 1. Концепция взаимодействия оборудования сети

На рис. 2 представлена предлагаемая структура терминала. Она включает в себя:

– блок вычисления непрерывного вейвлет-преобразования сигналов (в том числе, многоканальных, с числом каналов $N_{кан.}$) с использованием синтезированных вейвлетов;

– блок обработки сигналов;
– блок формирования сообщений;
– блок передачи сообщений.

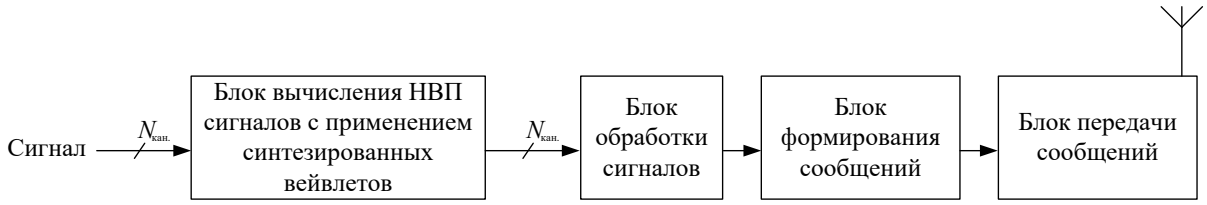



Рис. 2. Структура терминала связи для низкоорбитальной группировки спутников с блоком частотно-временного анализа сигналов и с функцией тревожной кнопки

Вейвлеты – это обобщенное название особых функций с нулевым интегральным значением, локализованные по оси времени, способные к сдвигу и масштабированию. Вейвлеты широко применяются для выполнения частотно-временного анализа сигналов. Непрерывное вейвлет-преобразование (НВП) сигнала или функции позволяет выявлять информационные признаки, а также локализовать их во времени. Применение при этом синтезированных вейвлетов позволяет значительно повысить точность анализа сигналов [3]. Автором данной работы были предложены три класса математических моделей вейвлетов [3]:

1. Модифицированная полиномиальная модель вейвлетов на основе алгебраического полинома. Достоинством данной модели является ее простота (малое число параметров). Требования к элементной базе при вычислении непрерывного вейвлет-преобразования с использованием вейвлетов на основе данной модели ниже, чем при использовании нейросетевых и сплайновых моделей.

2. Нейросетевые модели вейвлетов на основе многослойных персептронов и радиально-базисных функций. Достоинством данных моделей является высокая точность представления исходного образцового сигнала, что позволяет повысить локализацию информационного признака в сигнале. Данные модели являются более сложными по сравнению с модифицированной полиномиальной моделью, но менее сложные по сравнению со сплайновыми моделями.

3. Сплайновые модели вейвлетов. Данные модели позволяют получить гарантированную точность представления исходного образцового сигнала, однако имеют высокую сложность.

В зависимости от применяемой элементной базы может быть выбрана одна из перечисленных моделей. При реализации терминала спутниковой

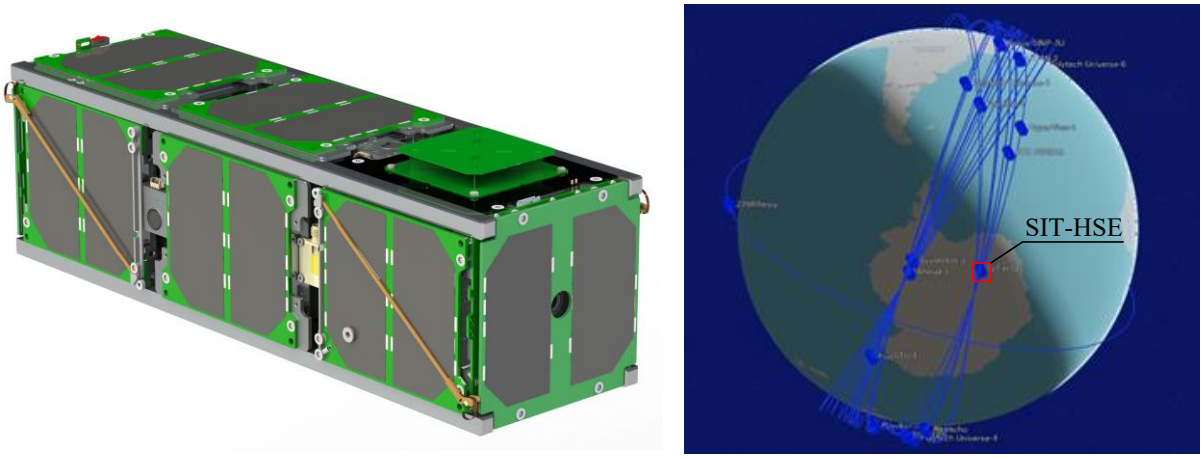
связи предлагается использовать одноплатные компьютеры Raspberry Pi или Nvidia Jetson (например, Nano). Графические процессоры Nvidia Jetson обладают высокой производительностью и позволяют выполнять обработку различных видов сигналов с использованием НВП.

Применение алгоритмов на основе НВП и синтезированных вейвлетов позволяет выполнять обработку сигналов различной природы [4–6]:

– биомедицинские (электроэнцефалограмма, электрокардиограмма, электрогастрограмма, электромиограмма и пр.);
– сейсмические сигналы (естественного или техногенного характера);
– сигналы от дефектоскопов (при контроле состояния целостности металлоконструкций технологических машин);
– сигналы от других датчиков и систем.

Использование предварительной обработки сигналов позволяет не передавать исходный сигнал по каналу связи, а передавать только результаты его анализа. Такой подход принципиально меняет модель взаимодействия с рядом удаленных систем АЗРФ и позволяет использовать низкоскоростные каналы связи.

На рис. 3 (*а*) представлена 3D модель спутника СПбГУТ (SIT-HSE) [7]. Этот спутник выполнен в форм-факторе 3U стандарта CubeSat, имеет позывной RC2336. Запуск спутника был произведен 05.11.2024 с космодрома «Восточный».




(*а*) (*б*)

Рис. 3. Спутник СПбГУТ (*а*) и его орбита (*б*) (SIT-HSE) [7]

На рис. 3 (*б*) показана орбита спутника СПбГУТ (SIT-HSE). Как показали исследования в рамках II Арктической технологической экспедиции СПбГУТ по побережью Белого моря в 2023 году, выполненные под научным руководством автора данной статьи, в деревне Летняя Золотица Архан-

гельской области время активного взаимодействия со спутником аналогичного типа в среднем составляет около 12 минут. По предварительным расчетам, за один сеанс связи может быть передано 5 пакетов данных, содержащих по 20 битов полезной информации в каждом (рис. 4).

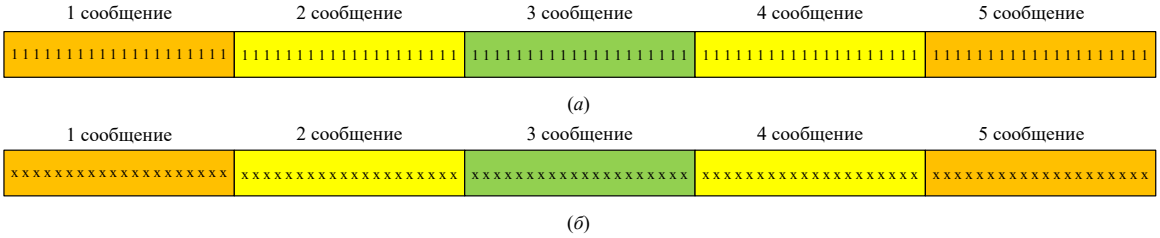



Рис. 4. Структуры информационной части сообщений: (*а*) сигнал тревоги, (*б*) другие виды сообщений

Как показали исследования, во время сеанса связи данные могут передаваться нестабильно. В начале сеанса связи пакеты могут повреждаться более серьезно. Поэтому наиболее важная информация должна предаваться в третьем пакете (зеленая зона), менее важная – во втором и четвертом (желтая зона), а также в первом и пятом (оранжевая зона). При возникновении внештатной ситуации на объекте во всех сообщениях в полезной части могут передаваться только «1» (рис. 4, *а*). Это обеспечивает наибольшую вероятность получения сигнала тревоги. При других видах сообщений полезная составляющая формируется в соответствии с настройками функционального интерфейса и указанными предложениями (рис. 4, *б*). При необходимости терминал может передавать оригинальные данные от датчиков и систем.

В заключение отметим, что предложенный терминал спутниковой связи может быть использован на следующих объектах АЗРФ:

– объекты добычи полезных ископаемых (оценка состояния технологических машин, в том числе повреждения их металлоконструкций и пр.);
– объекты медицинского профиля, логистические центры и прочие объекты, где проводится мониторинг состояния здоровья работников с использованием персональных мониторов (результаты с каждого монитора могут анализироваться блоком обработки терминала и передаваться в центр);
– объекты критической инфраструктуры;
– объекты контроля сейсмической, пожарной и лавинной обстановки;
– прочие объекты.

Планируется, что предложенный терминал спутниковой связи будет испытан в очередной Арктической технологической экспедиции СПбГУТ.

**Список используемых источников**

1. Указ Президента Российской Федерации от 26 октября 2020 г. № 645 «О Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года».

2. Распоряжение Правительства Российской Федерации от 24 ноября 2023 г. № 3339-р об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года.

3. Stepanov A. Polynomial, neural network, and spline wavelet models for continuous wavelet transform of signals / A. Stepanov // Sensors. 2021. Vol. 21. N 19. P. 6416. DOI: 10.3390/s21196416. EDN: VCGNHB.

4. Степанов А. Б. Разработка автоматического портативного электроэнцефалографа с возможностью интегрирования в Единую информационную систему Арктической зоны Российской Федерации / А. Б. Степанов // Электросвязь. 2024. № 12-2. С. 53-60. DOI: 10.34832/ELSV.2024.61.12.007. EDN: KPOWOQ.

5. Степанов А. Б. Автоматический портативный электроэнцефалограф / А. Б. Степанов // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2021): Всероссийская научно-методическая конференция магистрантов и их руководителей. Сборник лучших докладов конференции, Санкт-Петербург, 30 ноября – 02 2021 года. СПб.: СПбГУТ, 2022. С. 150-153. EDN: AYANEX.

6. Степанов А. Б. Устройство для анализа сейсмических сигналов / А. Б. Степанов, А. В. Запайщиков, Д. В. Козлов // Подготовка профессиональных кадров в магистратуре для цифровой экономики (ПКМ-2022): Сборник лучших докладов Всероссийской научно-технической и научно-методической конференции магистрантов и их руководителей, Санкт-Петербург, 06–08 декабря 2022 года / Сост. Н. Н. Иванов. СПб.: СПбГУТ, 2023. С. 163-167. EDN: EYJKTW.

7. Официальный сайт Космического проекта программы «Дежурный по планете» URL: https://spacepi.space (дата обращения 01.05.2026 г.).

## COMMUNICATION TERMINAL FOR A LOW-ORBIT SATELLITE GROUP WITH A FREQUENCY-TIME ANALYSIS BLOCK AND AN ALARM BUTTON FUNCTION

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

*The article is devoted to describing the concept, structure, and operating principles of a communication terminal for a low-orbit satellite constellation, featuring a signal frequency-time analysis unit and a panic button function proposed by the author. The advantages and disadvantages of mathematical models of wavelets for continuous wavelet transform, which can be used in the terminal's operating algorithm, are presented. The principles of generating transmitted messages are described, taking into account the use of the terminal in the Far North conditions. The areas of application of the terminal are presented.*

***Key words:*** *satellite communication terminal, low-orbit grouping, wavelet, synthesized wavelets, continuous wavelet transform, panic button*

**УДК 519.6, 677.070**
**ГРНТИ 64.01.77, 64.29.35**

# ПРОГРАММНЫЕ СРЕДСТВА ДЛЯ ИЗУЧЕНИЯ СВОЙСТВ МАТЕРИАЛОВ ТЕХНИЧЕСКИХ ИЗДЕЛИЙ, ЭКСПЛУАТИРУЕМЫХ В УСЛОВИЯХ АРКТИКИ

**А. Б. Степанова**

Санкт-Петербургский политехнический университет Петра Великого

*Начиная с 2020 года, интересы России направлены, в том числе, и на активное комплексное развитие Арктики, расширение зоны социально-экономического воздействия и на укрепление позиций в регионе. Особые климатические условия требуют и особых материалов для технических изделий, которые лучше всего подходят для данного региона. Среда MATLAB может помочь спроецировать и просчитать модель поведения технических материалов под воздействием различных факторов.*

***технический текстиль, среда MATLAB, обработка данных***

В начале 2020 г. вышел Указ Президента Российской Федерации № 164 (от 05.03.2020 г.) «Об Основах государственной политики Российской Федерации в Арктике на период до 2035 года», который послужил в дальнейшем концептуальной основой для дальнейших программ и законов по развитию Арктической зоны [1]. Мощный толчок наравне с безопасностью получили такие отрасли как транспорт и логистика (развитие Северного морского пути, железнодорожных магистралей, расширение сети аэропортов и возможности судоходства по рекам Арктической зоны), топливной промышленности и энергетики (разработка трудноизвлекаемых запасов углеродного сырья и т. п.), добыча и переработка природных ресурсов, развитие фундаментальных и прикладных наук, туризм, сохранение и развитие традиционных отраслей хозяйствования и пр.

Многие из перечисленных отраслей напрямую связаны с использованием различных технических изделий, изготовленных из материалов с особыми свойствами, которые способны выдерживать сложные климатические условия.

Остановимся более детально на экстремальных особенностях климата Арктики. Для данного региона характерны воздействия экстремально низких температур [2] (в некоторых регионах Арктики – до -60 $^0$C и ниже) в со-

четании с высокой влажностью, сильными ветрами, появлением обледенения, абразивного износа, воздействия УФ-излучений (ультрафиолетовых излучений), переменчивости погоды, воздействие морской среды, соленых брызг (на прибрежной территории) и т.п. Эти и другие факторы оказывают сильное влияние на механические и физические свойства материалов технических изделий и, как следствие, его функциональность и срок службы.

ГОСТ 15150-69 «Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды» устанавливает жесткие требования, предъявляемые к материалам и технике, эксплуатируемым в различных климатических зонах [3].

Ранее уже рассматривались применение параарамидных волокон и нитей в условиях пониженных температур [4-5].

Природные арктические условия накладывают свои отпечатки на материалы технических изделий, эксплуатируемые в данных условиях.

Рассмотрим некоторые из них.

Для тросов и строп исследуют:

– ползучесть под постоянной нагрузкой в условиях экстремально низких температур;
– истирание на месте прилегания к кромке льда и с дополнительным воздействием микрочастиц соли;
– конструкционную анизотропию, которая усиливается под влиянием температурных факторов;
– остаточные напряжения, которые возникают во время процесса «нагрева-охлаждения».

Для тентов, палаток и укрытий определяют:

– пиковые напряжения (суммарное воздействия рядов факторов, таких как сильный шквалистый вечер – импульсная нагрузка, обледенение приводит к увеличению массы снега, воздействующей на изделие, и дополнительно большая снеговая нагрузка – статическая нагрузка);
– устойчивость к УФ-излучениям (т. к. под воздействием сильного ультрафиолетового излучения в материалах происходит процесс фотоокисления, приводящий к разрыву макромолекулярных цепей и снижению молекулярной массы, это проявляется в падении разрывной нагрузки и росте хрупкости полотна;

– высокая уязвимость точек крепления, швов и мест проклейки (высокая концентрация напряжений в местах расположения люверсов, местах проколов). Кроме того, при использовании клеевых соединений, эти места могут стать хрупкими.

Проведение экспериментов в реальных условиях требует большого количества времени (на некоторые эксперименты могут уходить годы – с целью получить достоверную информацию с репрезентативной выборкой и достаточным количеством испытаний), кроме того, некоторые исследования следует проводить в реальных климатических условиях, что требует длительного пребывания в условиях низких температур. С помощью климатических камер можно смоделировать, воздействие низких температур, влажности, сымитировать перепады группы факторов (например, температуры и влажности, что соответствует перепаду температур в течение дня в реальных условиях), УФ-излучение, воздействие давления и т.п., но при этом полностью воспроизвести все природные воздействия намного сложнее. Так, в климатических камерах можно воспроизвести:

– замерзание влаги в порах и капиллярах, намокание материалов;
– устойчивость материалов технических изделий к экстремально низким температурам (после того, как образцы выдерживают заданный промежуток времени при определенной температуре, исследуют изменение его основных характеристик);
– термоциклирование – накопление усталостных характеристик, склонность к растрескиванию, появление хрупкости, изменение механических свойств в динамике и пр. характеристик при значительных перепадах температуры) – расчеты проводят в среде MATLAB;
– воздействие ультрафиолетового излучения и пр.

В быстро развивающихся условиях, когда необходимо оперативно получить определенные данные, спроектировать определенные условия и выполнить необходимые расчеты с применением различного программного обеспечения, можно выполнить определенные расчеты с помощью специальных программ, в частности:

1. Использование среды MATLAB для численного решения уравнений механики (например, при наличии зависимости модуля упругости от температуры, уравнение влагопереноса и т.п.).

2. Использование подсистемы блочного моделирования Simulink для расчета комплексного фактора воздействия на изделие технического назначения (например, можно собрать некоторую реальную систему воздействия

на то или иное изделие: воздействие нагрузки, затем процесс деформации, накопления повреждений и отказ системы (выход из строя) и при такой модели менять различные факторы воздействия – температуру, влажность, интенсивность ветра и т.п.

3. Использование программы ANSYS Fluent для моделирования тепловых и гидродинамических процессов.

4. Использование встроенного модуля MATLAB – Statistics and Machine Learning Toolbox – анализ данных испытаний.

5. Использование нескольких программ комплексно:

– MATLAB и ANSYS – подготовка параметрических расчетов, обработка результатов, построение метамодели;
– MATLAB и COMSOL Multiphysics (с помощью расширения LiveLink можно выполнить интеграцию между двумя программными средами); COMSOL используется для подготовки параметрических расчетов (создание модели для анализа факторов воздействия), а среда MATLAB для анализа результатов и расчета и пр.

Таким образом, применение специальных программ и методов исследования значительно упрощают задачу оценки долговечности технических изделий и сокращает время на проведение эксперимента.

**Список используемых источников**

1. Указ Президента Российской Федерации от 5 марта 2020 года № 164 «Об Основах государственной политики Российской Федерации в Арктике на период до 2035 года». URL: http://www.kremlin.ru/acts/bank/45255. Дата обращения: 25.05.2026.

2. Климат Арктики. Пастухова О. // Polar Travel Club. URL: https://polartravelclub.ru/info-for-travelers/articles/klimat-arktiki/. Дата обращения: 30.05.2026.

3. ГОСТ 15150-69. Машины, приборы и другие технические изделия. Исполнения для различных климатических районов. Категории, условия эксплуатации, хранения и транспортирования в части воздействия климатических факторов внешней среды. Москва: Стандартинформ, 2010. 58 с.

4. Исследование свойств параарамидных нитей под воздействием эксплуатационных факторов с использованием современного программного обеспечения. Лебедева Н. П., Степанова А. Б. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2025). Сборник научных статей XIV Международной научно-технической и научно-методической конференции. В 2-х томах. Санкт-Петербург, 2025. С. 705-709.

5. Обзор исследований свойств параарамидных нитей при воздействии низких температур. Степанова А. Б. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2025). Сборник научных статей XIV Международной научно-технической и научно-методической конференции. В 2-х томах. Санкт-Петербург, 2025. С. 720-724.

# SOFTWARE FOR STUDYING THE PROPERTIES OF MATERIALS OF TECHNICAL PRODUCTS OPERATED IN THE ARCTIC REGION

**Stepanova A.**
Peter the Great Saint Petersburg Polytechnic University

*Since 2020, Russia's interests have been focused on actively developing the Arctic region, expanding its socio-economic influence, and strengthening its position in the region. The unique climate conditions require specific materials for technical products that are best suited for this region. MATLAB can help in designing and analyzing the behavior of technical materials under various factors.*

***Key words:*** *technical textiles, MATLAB environment, data processing*

# РЕЗУЛЬТАТЫ НАУЧНЫХ ИССЛЕДОВАНИЙ

**УДК 654.026**
**ГРНТИ 49.33.01**

## ФОРМИРОВАНИЕ АРХИТЕКТУРНЫХ ПАРАМЕТРОВ СЕРВЕРНЫХ СИСТЕМ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ РАСПРЕДЕЛЕНИЯ НАГРУЗКИ

**Д. С. Алленов, В. Г. Иванов, В. В. Чабаненко**

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

*Рассмотрена задача формирования архитектурных примеров серверных систем, обеспечивающих эффективное распределение вычислительной нагрузки. Описан подход к решению двуединой задачи: обработка вычислительных запросов от должностных лиц, и размещение статистических ресурсов в виде формализованной модели состояния серверного комплекса с использованием средств встроенного мониторинга и векторного описания серверов.*

***бинарная переменная выбора сервера, пространственная составляющая серверного комплекса, оптимальный выбор сервера***

### Введение

Современные информационные системы, функционирующие в условиях интенсивной нагрузки и ограниченности вычислительных ресурсов, требуют высокой устойчивости, скорости обработки данных и способности эффективно масштабироваться [1].

### Задача

Решение задачи – распределение данных и рациональное размещение по вычислительным ресурсам серверного оборудования таких объектов, как текстовые документы, графические файлы, видеофайлы и иные информационные ресурсы, предназначенные для хранения и последующего предоставления по запросу пользователей.

Для постановки математической задачи балансировки введем следующие обозначения параметров, характеризующих работу серверов [2]:

$D_s$ – расстояние от должностного лица до сервера пункта управления (км);

$U_{cpu}$ – загруженность центрального процессора (отн. ед.);

$U_{ram}$ – загруженность оперативной памяти (отн. ед.);

$B_{ch}$ – доступная пропускная способность канала передачи данных, Кбит/с;

$C_{sdr}$ – стоимость затрат на хранение, доставку и репликацию данных, ден. ед.

В статье рассматривается задача балансировки для двух случаев.

В первом случае для задачи распределения вычислительной нагрузки следует учитывать следующие параметры: $D_s$, $U_{ram}$, $U_{cpu}$.

Во втором случае ставится задача распределения статических данных, $D_s$, $B_{ch}$, $C_{sdr}$.

Совокупность серверов зададим множеством

$$S = \{S_1, S_2, S_3\}, \qquad i = \overline{1,3}.$$

Пусть $l = \overline{1, q}$ – номер запроса пользователя, $q$ – общее количество запросов. Для каждого запроса необходимо выбрать один сервер, обеспечивающий наилучшее значение заданного критерия балансировки.

Введем бинарную переменную выбора сервера

$$x_i^l = \begin{cases} 1, & \text{если } l\text{-й запрос направлен на сервер } S_i; \\ 0, & \text{в противном случае.} \end{cases}$$

Для каждого запроса должно выполняться условие однозначного выбора сервера:

$$\sum_{i=1}^{3} x_i^l = 1, \qquad l = \overline{1, q}.$$

Поскольку рассматриваемые параметры имеют разные единицы измерения, далее используются их нормированные значения, обозначенные знаком «~» и принадлежащие интервалу $[0; 1]$.

**Задача распределения вычислительной нагрузки**

Вектор параметров состояния для $l$-го запроса относительно $i$-го сервера имеет вид

$$\mathbf{X}_i^l = \left(\widetilde{D}_{s,i}^l,\ \widetilde{U}_{ram,i}^l,\ \widetilde{U}_{cpu,i}^l\right).$$

Требуется найти распределение запросов $X^* = \{x_i^l\}$, минимизирующее расстояние до сервера и его текущую загрузку:

$$X^* = \underset{x_i^l}{\operatorname{argmin}}\ F_1(X),$$

$$F_1(X) = \sum_{l=1}^{q}\sum_{i=1}^{3} x_i^l \left(\alpha_D \widetilde{D}_{s,i}^l + \alpha_{ram}\widetilde{U}_{ram,i}^l + \alpha_{cpu}\widetilde{U}_{cpu,i}^l\right),$$

при ограничениях

$$\sum_{i=1}^{3} x_i^l = 1, \qquad x_i^l \in \{0,1\}, \qquad l = \overline{1,q},$$

$$U_{ram,i}^l \le U_{ram}^{\max}, \qquad U_{cpu,i}^l \le U_{cpu}^{\max}.$$

Здесь $\alpha_D, \alpha_{ram}, \alpha_{cpu} \ge 0$ – весовые коэффициенты, причем

$$\alpha_D + \alpha_{ram} + \alpha_{cpu} = 1.$$

**Задача распределения статических данных**

Вектор параметров состояния для $l$-го запроса относительно $i$-го сервера имеет вид

$$\mathbf{Y}_i^l = \left(\widetilde{D}_{s,i}^l,\ \tilde{B}_{ch,i}^l,\ \tilde{C}_{sdr,i}^l\right).$$

Требуется найти распределение запросов $Y^* = \{x_i^l\}$, обеспечивающее минимальные расстояние и стоимость при максимальной доступной пропускной способности канала:

$$Y^* = \underset{x_i^l}{\operatorname{argmin}}\ F_2(X),$$

$$F_2(X) = \sum_{l=1}^{q}\sum_{i=1}^{3} x_i^l \left[\beta_D \widetilde{D}_{s,i}^l + \beta_B\left(1 - \tilde{B}_{ch,i}^l\right) + \beta_C \tilde{C}_{sdr,i}^l\right],$$

при ограничениях

$$\sum_{i=1}^{3} x_i^l = 1, \qquad x_i^l \in \{0,1\}, \qquad l = \overline{1,q},$$

$$B_{ch,i}^l \ge B_{ch}^{\min}.$$

Здесь $\beta_D, \beta_B, \beta_C \ge 0$ – весовые коэффициенты, причем

$$\beta_D + \beta_B + \beta_C = 1.$$

Таким образом, решением каждой задачи является отображение множества запросов на множество серверов, при котором каждый запрос назна-

чается ровно одному допустимому серверу, а соответствующий интегральный критерий принимает минимальное значение.

При распределении вычислительной нагрузки ключевыми факторами являются вычислительная сложность обрабатываемых задач и производительность серверных узлов, тогда как при распределении статических данных необходимо учитывать объем передаваемой информации, степень загруженности каналов связи и расстояние до конечного должностного лица, что в оперативной обстановке очень важно.

## Заключение

Для обеспечения принятия обоснованного управленческого решения по выбору узла серверной инфраструктуры, предназначенного для выполнения вычислительных задач, необходимо сформировать и формализовать совокупность входных параметров, характеризующих текущее состояние вычислительных средств пунктов управления и разработать аналитико-имитационный метод распределения вычислительной нагрузки между серверами, отражающего логику функционирования автоматизированных систем военного назначения.

**Список используемых источников**

1. Алленов Д. С., Курбанов С. Н. Распределение нагрузки в информационных системах военного назначения // Телекоммуникации и связь. 2026. № 1(10). С. 8-15.

2. Иванов В. Г., Алленов Д. С., Чабаненко В. В., Михайлов В. П. К вопросу возрастания нагрузки между вычислительными ресурсами в информационных системах отображения роев БПЛА // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2025). Сборник научных статей. 2025. С. 150-154. EDN: XHZRDR.

## FORMATION OF ARCHITECTURAL PARAMETERS OF SERVER SYSTEMS TO IMPROVE LOAD DISTRIBUTION EFFICIENCY IN MILITARY INFORMATION SYSTEMS

**Allenov D., Ivanov V., Chabanenko V.**
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

*The article addresses the problem of designing architectural models of server systems that ensure efficient distribution of computational load. It describes an approach to solving a dual task at control points: processing computational requests from officials and allocating statistical resources in the form of a formalized model of the server system state, using built-in monitoring tools and a vector-based description of servers.*

***Key words:*** *residual computational capacity of servers, spatial component of the server complex, optimal server selection*

**УДК 7.012(062)**
**ГРНТИ 81.95**

# АНАЛИЗ СООТВЕТСТВИЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ СТАНДАРТАМ ДОСТУПНОСТИ

**Б. А. Аль-Нами, О. А. Шурухина**

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

*В статье рассматривается проблема доступности государственных информационных систем для лиц с ограниченными возможностями здоровья и людей пожилого возраста. Изучена история внедрения стандартов и методы тестирования. Проведен анализ соответствия сайта «Здоровье петербуржца» требованиям международного стандарта WCAG 2.1. Исследование включало автоматизированное тестирование с использованием расширения WAVE и ручную экспертизу, в том числе проверку с клавиатуры, масштабирование страницы и тестирование с помощью программы экранного доступа NVDA. Выявлены критические нарушения: низкий цветовой контраст, отсутствие меток у элементов форм, отсутствие альтернативного текста, проблемы с видимостью фокуса и масштабированием при 400 %. В результате исследования и на основе зарубежных практик сформулированы рекомендации по внедрению со-дизайна, обучению разработчиков и институционализации требований доступности. Результаты могут быть использованы для приведения портала в соответствие с национальным стандартом.*

***доступность, WCAG 2.1, ГОСТ Р 52872-2019, государственные информационные системы, инклюзивный дизайн, со-дизайн, ГИС «Здоровье петербуржца», WAVE***

В 1997 году Всемирный консорциум Всемирной паутины (W3C) объявил о запуске Инициативы по обеспечению доступности веб-сайтов (WAI). В 1999 году WAI опубликовала первую версию стандарта веб-доступности WCAG 1.0. На данный момент самой актуальной является версия WCAG 2.2, разрабатывается WCAG 3.0. В основе стандартов WCAG лежат четыре принципа доступности: воспринимаемость, управляемость, понятность и надежность. Для них существуют критерии успеха, которые подразделяются на три уровня: A, AA и AAA. Они определяют «соответствие» стандартам WCAG [1].

В 2016 году странами Европейского союза была принята Директива ЕС 2016/2102. Она обязывает государственные органы стран-членов ЕС обеспечить соответствие своих веб-сайтов и мобильных приложений стандарту

EN 301 549 (гармонизированный стандарт, включающий требования WCAG 2.1), внедрить требования доступности в законы [2].

В 2020 году в Словении было опубликовано исследование доступности веб-сайтов муниципалитетов до и после принятия EN 301 549. Результаты показали улучшение соответствия веб-сайтов стандартам, причем для некоторых требований улучшение оказалось значительным после принятия Директивы. Доля доступных сайтов среди проверенных увеличилась с 0 % до 33 % [3].

В ходе исследования венгерских авторов (2025 год) были изучены 25 веб-сайтов государственных органов. Из 25 доступными признаны 4. В некоторых сегментах наблюдалось улучшение, но многие недостатки так и не были исправлены [4].

В России в 2020 году вступил в силу ГОСТ Р 52872-2019 – национальный стандарт цифровой доступности, адаптирующий требования WCAG 2.1 к российской системе стандартизации [5]. В его разработке принимали участие четыре тотально слепых независимых эксперта [6].

В 2021 году Анатолий Попко, один из разработчиков ГОСТа, представил доклад, посвященный анализу цифровой доступности в России после внедрения стандарта. По оценке Попко, национальный стандарт «становится ориентиром и набирает популярность». Однако крупнейшие технологические компании России «не проявляют интереса к систематическому подходу к цифровой доступности». Исключениями являются некоторые банки [6].

Помимо ГОСТ Р 52872-2019, в России действуют также ГОСТ Р 70186-2022 – требования к инструментам разработки, ГОСТ Р 70177-2022 – требования к браузерам и медиаплеерам, ГОСТ Р 70176-2022 – требования к доступности PDF-документов. Однако все национальные стандарты являются лишь рекомендациями. Исследование Федерального ресурсного центра по формированию доступной среды (в 2022-2023 годах) не выявило ни одного сайта органов власти в четырех субъектах РФ, соответствующего международному стандарту доступности [7].

В 2022 году Ольга Долганова и Людмила Василевская опубликовали статью «Доступность и удобство использования веб-ресурсов электронного правительства: проблемы и решения». Российская научная литература по проблематике доступности государственных веб-ресурсов, отмечают Долганова и Василевская, характеризуется значительным дефицитом эмпирических исследований. Авторами проанализирован зарубежный опыт

и проведена оценка портала «Госуслуги» на соответствие WCAG 2.1: сайт «частично отвечает данным требованиям, однако есть параметры, которые можно существенно улучшить» [8].

В 2025 году Алексей Кудрявцев защитил дипломную работу на тему «Совершенствование применения цифровых платформ при оказании государственных услуг населению в Российской Федерации». Согласно аннотации, по результатам работы были предложены меры по развитию инклюзивных интерфейсов [9].

Методы оценки соответствия стандартам можно разделить на автоматизированные и ручные. С помощью автоматизированного тестирования можно проверить наличие альтернативного текста, цветовой контраст, корректность HTML / CSS, уникальность идентификаторов, семантическую разметку, понятность текста и полей ввода.

Ручное (экспертное) тестирование проверяет отсутствие «клавиатурных ловушек» (возможность перемещения с помощью клавиш Tab и Enter), видимость фокуса, корректность работы скринридеров и вспомогательных технологий, отсутствие потери контента или необходимости двухмерной прокрутки при масштабе 200 % и 400 %, понятность текста и полей ввода.

Автоматизированную проверку можно осуществить с помощью расширения WAVE. После его подключения на тестируемом сайте будут показаны результаты, отмеченные разными цветами: красным – ошибки, желтым – предупреждения (возможные проблемы), зеленым – особенности (элементы доступности), синим – структурные элементы, фиолетовым – атрибуты ARIA (информация для скринридеров). Также желательно отключить стили для проверки логичности структуры HTML-кода.

Для данной статьи был выбран государственный портал с отсутствующими данными о проверках доступности. ГИС «Здоровье петербуржца» – критически важный ресурс. Через портал можно записаться к врачу, получить данные из медицинской книжки, найти информацию о здоровье и предоставляемых услугах, контактные данные. По данным сайта, более 3 миллионов пользователей записались к врачу на портале в 2024 году и более 2 миллионов человек пользуются личным кабинетом.

484 тысяч жителей Санкт-Петербурга имеют инвалидность, включая 373 тысяч граждан пожилого возраста, 8 тысяч – с нарушениями зрения и 80 тысяч – с нарушениями опорно-двигательного аппарата [10].

Они представляют собой потенциальную аудиторию различных информационных систем, в том числе сайт «Здоровье петербуржца».

Применение расширения WAVE на главной странице сайта «Здоровье петербуржца» дало следующие результаты (рис. 1).

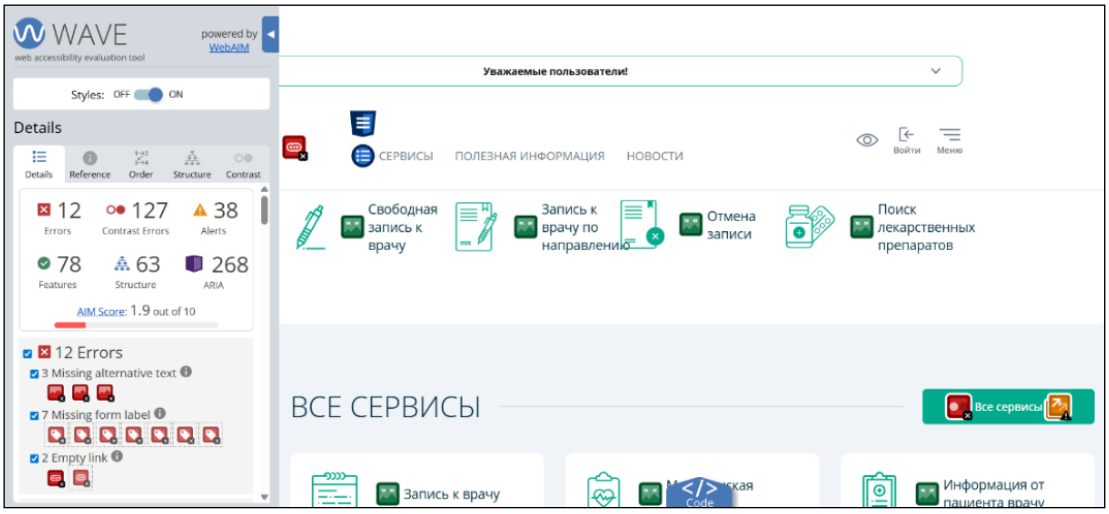



Рис. 1. Результаты автоматизированной проверки сайта

«Красные» ошибки: 2 ссылки без текстового наполнения, 7 элементов управления формой без текстовой метки, 3 изображения без альтернативного текста, 127 отметок о недостаточном контрасте.

«Желтые» предупреждения: отсутствие легенды у поля ввода, отсутствие заголовка первого уровня (<h1>), недостаток семантической разметки списков, наличие 10 избыточных ссылок, присутствие элемента <noscript>, 16 случаев выравнивания текста по ширине, 8 «очень маленьких» текстовых элементов.

«Зеленые» особенности: 5 случаев наличия альтернативного текста и 66 случаев его отсутствия, 3 метки формы (подсказки для поля ввода). 4 рисунка требуют ручной проверки доступности. Язык страницы может быть четко определен программными средствами.

К «синим» элементам относятся заголовок третьего уровня (<h3>), нумерованный и маркированный списки, встроенный фрейм (<iframe>), элементы <head>, <nav>, <footer> (или роли contentinfo), <aside> (или дополнительный ориентир).

«Фиолетовая» категория насчитывает 272 позиции.

Наличие вспомогательных элементов можно обнаружить и без вспомогательных технологий. При нажатии на значок «глаз» появляется возможность выбрать размер шрифта, цветовую гамму и включить/отключить подсказки для ссылок.

Навигация с помощью Tab и фокусировка работают, однако с нарушениями: черный контур отображается не всегда. В таких случаях ориентироваться возможно лишь по ссылке в левом нижнем углу.

При масштабе 200 % значительную площадь экрана занимает шапка сайта. При увеличении до 400 % заголовочная область практически полностью вытесняет содержательную часть страницы. Горизонтальная прокрутка не требуется.

Для проверки с помощью скринридера была использована программа чтения с экрана NVDA. На сайте «Здоровье петербуржца» программа функционировала, но при клавиатурной навигации зафиксировала отсутствие заголовков. Интерактивная карта выбора района оказалась недоступной: отдельные области не озвучивались. Изображения без альтернативного текста также не были восприняты программой.

Для отладки интерфейса можно обратиться к зарубежным практикам. В качестве примера внедрения доступности выделены следующие ресурсы.

1. Официальный портал штата Нью-Джерси, созданный для людей с инвалидностью. По отчетам разработчика, модель базируется на методологии со-дизайна с итеративным тестированием.

2. Портал правительства штата Мэриленд – результат внедрения требований доступности на уровне законодательства и контрактов, обязывающих закупать только доступные цифровые инструменты и предоставлять формальный отчет о соответствии каждому критерию.

3. Официальный сайт Blauer Engel. Характеризуется одной из наиболее прозрачных деклараций доступности, соответствующей немецкому законодательству. В ней подтверждено соответствие WCAG 2.1 Level AA, перечислены сохраняющиеся проблемы.

На основе полученных данных можно сформулировать следующий вывод. Портал «Здоровье петербуржца» требует комплексной доработки интерфейса в соответствии с ГОСТ Р 52872-2019 и WCAG 2.2. Проведенное тестирование выявило множественные нарушения международного стандарта, которые требуют верификации квалифицированными экспертами, в том числе с привлечением экспертов и пользователей с инвалидностью. Эти нарушения затрагивают принципы воспринимаемости и управляемости, что может сделать портал недоступным для лиц с нарушениями зрения и пожилых пользователей. Положительным аспектом является наличие базовой семантической структуры и использование ARIA-атрибутов, однако их корректность требует проверки.

В международной практике стандарты доступности активно развиваются уже несколько десятилетий. В России действует ГОСТ Р 52872-2019,

основанный на WCAG 2.1. Однако, поскольку стандарт носит добровольный характер, механизмы принудительного контроля и ответственности отсутствуют. Зарубежный опыт предлагает работающие модели, на которые можно ориентироваться при улучшении доступности дизайна.

Проблема недостаточной инклюзивности интерфейсов требует повышенного внимания, что подтверждает необходимость дальнейших исследований и публикаций.

По итогам исследования можно составить рекомендации. Внедрение совместного дизайна (co-design) – привлечения экспертов и пользователей с инвалидностью на всех этапах разработки – от сбора требований до приемочного тестирования. Обучение разработчиков основам WCAG 2.2 и ARIA, правилам создания доступного контента. Проведение обязательного комплексного тестирования всех крупных сайтов. Оно должно включать в себя автоматизированное и ручное экспертное тестирование, а также тестирование с участием реальных пользователей. И на этапе экспертного, и на этапе пользовательского тестирования необходимо привлекать людей с инвалидностью. Внедрение в нормативные акты требований доступности, обязывающих закупать только доступные цифровые инструменты и предоставлять формальный отчет о соответствии каждому критерию. Предоставление прозрачных деклараций доступности с перечислением реализованных критериев доступности и существующих барьеров. Проведение независимых аудитов доступности не реже одного раза в год с публикацией результатов. Внедрение автоматизированного тестирования при каждом изменении кода. Создание экспертного совета пользователей с инвалидностью для постоянной обратной связи.

**Список используемых источников**

1. World Wide Web Consortium. Web Content Accessibility Guidelines (WCAG) 2.1. 2018. URL: https://www.w3.org/TR/WCAG21/ (дата обращения: 11.05.2026).

2. European Parliament, Council of the European Union. Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies // Official Journal of the European Union. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L2102 (дата обращения: 26.04.2026).

3. Kous K., Kuhar S., Pušnik M., et al. Web accessibility investigation of Slovenian municipalities' websites before and after the adoption of European Standard EN 301 549 // Universal Access in the Information Society. 2021. Vol. 20. DOI: 10.1007/s10209-020-00732-9.

4. Csontos B., Heckl I. Five years of changes in the accessibility, usability, and security of Hungarian government websites // Universal Access in the Information Society. 2025. DOI: 10.1007/s10209-025-01223-5.

5. Косова Е. А. Стандартизация доступности веб-контента // Открытое образование. 2020. Т. 24, № 3. DOI: 10.21686/1818-4243-2020-3-12-23.

6. Popko A. D. G3ict/Smart Cities for All Country Advisory Network: Update from Russia. 2021. 2 Feb. URL: https://smartcities4all.azurewebsites.net/update-from-russia/ (дата обращения: 11.05.2026).

7. Федеральный ресурсный центр по формированию доступной среды. Опубликованы результаты исследования цифровой доступности. 2023. 20 июля. URL: https://www.frcds.ru/wp-content/uploads/2023/07/Cifrovay-dostupnost.pdf (дата обращения: 11.05.2026).

8. Долганова О. И., Василевская Л. И. Доступность и удобство использования веб-ресурсов электронного правительства: проблемы и решения // Вестник университета. 2022. № 7. URL: https://www.elibrary.ru/item.asp?id=49365659 (дата обращения: 11.05.2026).

9. Кудрявцев А. С. Совершенствование применения цифровых платформ при оказании государственных услуг населению в Российской Федерации: выпуск. квалиф. работа. СПб.: НИУ ВШЭ, 2025. URL: https://www.hse.ru/edu/vkr/1047501560 (дата обращения: 11.05.2026).

10. Управление по организации и проведению конкурсных процедур и обеспечению деятельности учреждений здравоохранения. Все идет по плану: Петербург готовится к нововведениям в системе реабилитации инвалидов. 2025. 4 июня. URL: https://upchspb.ru/news/vse-idet-po-planu-peterburg-gotovitsya-k-novovvedeniyam-v-sisteme-reabilitatsii-invalidov/ (дата обращения: 11.05.2026).

## ANALYSIS OF COMPLIANCE WITH GOVERNMENT INFORMATION SYSTEMS ACCESSIBILITY STANDARDS

**Al-Nami B., Shurukhina O.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article examines the accessibility of government information systems for individuals with disabilities and the elderly. It explores the history of accessibility standards and relevant testing methods. The study analyzes the compliance of the "Health of St. Petersburg" website with the international WCAG 2.1 standard. The assessment included automated testing using the WAVE extension and manual examination, such as keyboard navigation testing, page scaling, and evaluation with the NVDA screen reader. Critical violations were identified: low color contrast, missing labels on form elements and alternative text, issues with focus visibility, and content loss at 400 % zoom. Based on international best practices, the study formulates recommendations for implementing co-design, providing developer training, and adopting mandatory accessibility requirements. The results can be used to bring the portal into compliance with the national standard.*

***Key words:*** *accessibility, WCAG 2.1, GOST R 52872-2019, government information systems, inclusive design, co-design, GIS "Health of St. Petersburg Residents", WAVE*

**УДК 004.896:629.735**
**ГРНТИ 28.23.15**

# МОДИФИЦИРОВАННАЯ НЕЙРОСЕТЕВАЯ АРХИТЕКТУРА DCE-YOLOv8 ДЛЯ АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ МАЛОРАЗМЕРНЫХ ЦЕЛЕЙ НА ИЗОБРАЖЕНИЯХ БПЛА

**К. С. Бабич, С. П. Кузнецов, А. И. Попов**

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

*В работе представлена оптимизированная архитектура нейронной сети, предназначенная для автоматизированного обнаружения малоразмерных и слабоконтрастных целей на оптико-электронных снимках беспилотных авиационных систем. Предложены четыре модификации базовой архитектуры: эффективный остаточный модуль, блок дифференцированного извлечения контекста на основе частичных сверток, исключение вычислительно избыточного блока и замена понижающей дискретизации на повышающую для увеличения чувствительности к микромасштабным объектам. Экспериментальная верификация на наборах данных продемонстрировала прирост точности на 43 % относительно базовой архитектуры при сокращении количества параметров на пятьдесят три процента и сохранении темпа обработки не менее ста восемнадцати кадров в секунду. Результаты подтверждают пригодность архитектуры для бортового развертывания в составе разведывательно-ударных контуров и систем технического зрения тактических беспилотных авиационных систем.*

***компьютерное зрение, обнаружение объектов, беспилотные авиационные системы, малоразмерные цели, бортовые вычислительные платформы, оптимизация нейронных сетей***

## Введение

Автоматизированное обнаружение и классификация объектов на оптико-электронных снимках является критически важной компонентой современных разведывательно-ударных контуров. В условиях динамичной оперативно-тактической обстановки данная задача выступает базовым элементом систем машинного зрения, обеспечивающих целеуказание, корректировку огня, ситуационную осведомленность и противодействие средствам воздушного нападения.

Современные алгоритмические комплексы глубокого обучения преимущественно верифицируются на общедоступных эталонных выборках. Указанные наборы данных характеризуются съемкой с уровня наблюдателя и обладают тактико-техническими ограничениями для боевого применения: малое количество объектов в кадре, минимальное перекрытие, доминирование объектов по площади, преобладание ближней дистанции съемки, статичный фон и оптимальные условия освещенности.

В современных конфликтах беспилотные авиационные системы различных классов выступают основным средством воздушной разведки и ударного применения. Традиционные алгоритмы обнаружения сталкиваются с деградацией точности из-за малого углового размера целей, маскировки, динамического фона и ограниченных вычислительных ресурсов бортовых микрокомпьютеров. Алгоритм YOLOv8 демонстрирует снижение точности при обнаружении малоразмерных и слабоконтрастных объектов, а также нестабильность при одновременном присутствии целей различных масштабов.

Целью настоящей работы является разработка модифицированной архитектуры DCE-YOLOv8, оптимизированной под тактико-технические требования обнаружения малоразмерных целей в полевых условиях при сохранении совместимости с бортовыми вычислительными платформами.

## Материалы и методы

Архитектура базовой сети включает три функциональных блока: Backbone (извлечение признаков), Neck (многоуровневая агрегация) и Head (регрессия ограничивающих рамок и классификация). Базовая часть опирается на модули C2f, представляющие эволюцию модуля C3 с оптимизированным градиентным потоком. Модуль C2f обеспечивает гибкое масштабирование карт признаков посредством чередования сверток 1×1 и 3×3 с шунтирующими соединениями.

Анализ штатной конфигурации показал, что блок B5 содержит около 60 % параметров базовой архитектуры, что создает вычислительную избыточность для задач обнаружения малоразмерных целей на снимках беспилотных авиационных систем.

Для повышения точности и снижения вычислительной нагрузки предложены четыре структурные оптимизации:

*1. Оптимизация глубины сети (удаление блока B5)*

Путем исключения избыточного слоя удалось уменьшить количество параметров до 1 360 064 (что составляет порядка 27 % от базовой версии). Данная мера необходима для корректной работы модели на вычислительных мощностях Jetson Orin Nano и Xavier NX.

*2. Внедрение модуля ERB (Efficient Residual Bottleneck)*

Нами был разработан блок на основе архитектур C3 и C2f, направленный на минимизацию вычислительных затрат при сохранении целостности градиентных потоков.

Принцип работы: за счет уменьшения числа сверточных слоев и использования операции сложения достигается более эффективное взаимо-

действие признаков. Интеграция функций активации SiLU и алгоритмов пакетной нормализации позволяет избежать проблемы затухания градиента.

*3. Модуль DCE (Differential Context Extraction)*

Для снижения интенсивности операций с памятью стандартные свертки были заменены на технику Partial Conv (PConv). Алгоритм обработки входной карты X следующий: 75 % объема данных проходит через цепочку сверточных преобразований, в то время как оставшиеся 25 % сохраняются для последующей агрегации. Такой подход способствует выделению ключевых признаков цели при сохранении высокой детализации изображения.

*4. Модификация системы дискретизации*

Классический подход с понижающей дискретизацией был дополнен повышающей. Введены новые типы карт признаков (микро-, малые и средние), что позволило эффективно распознавать объекты размерностью менее 30×30 пикселей. Детекция подобных целей осуществляется путем объединения данных из модуля DCE с картой, полученной в результате повышающей дискретизации.

*Функционал потерь*

Итоговая функция была настроена с учетом специфических тактических задач:

– BCE – отвечает за точность классификации.
– CIoU – корректирует показатели перекрытия и соотношения геометрических параметров сторон.
– DFL – необходима для стабилизации процесса регрессии, особенно в условиях нечетких границ целевых объектов.

## Результаты и обсуждение

Верификация проводилась на платформе Ubuntu 20.04 (CPU: AMD EPYC 7302, GPU: NVIDIA Tesla A30 24G, фреймворк: PyTorch 3.10). Размер пакета: 2, входное разрешение: 640×640, оптимизатор: SGD (скорость обучения 0,01, коэффициент импульса 0,937, три эпохи прогрева, общее количество эпох 200).

Обучение и тестирование выполнены на наборах данных VisDrone [1], TT100K [2] и AFO [3]. VisDrone имитирует типовые условия тактической разведки в городской и сельской инфраструктуре. TT100K содержит сто тысяч изображений с сорока классами объектов для оценки устойчивости к плотной застройке и динамическому освещению. AFO ориентирован

на мониторинг акваторий и отражает изменчивость водной поверхности, блики и частичное затенение целей.

Распределение параметров в базовой архитектуре представлено в таблице 1. Удаление блока B5 снижает общий объем модели на семьдесят три процента без потери темпа обработки.

ТАБЛИЦА 1. Распределение параметров в базовой архитектуре

| Блок | Позиция | Параметры | Доля, % |
|---|---|---|---|
| B1 | № 1–2 | 125 440 | 2,5 |
| B2 | № 3–4 | 312 896 | 6,2 |
| B3 | № 5–6 | 689 152 | 13,6 |
| B4 | № 7–8 | 933 472 | 18,4 |
| B5 | № 9–10 | 3 018 752 | 59,4 |
| Всего | – | 5 079 712 | 100,0 |

Структура оптимизированной сети извлечения признаков приведена в таблице 2.

ТАБЛИЦА 2. Структура сети извлечения признаков

| Слой | Операция | Ядро | Фильтры | Параметры |
|---|---|---|---|---|
| 1 | Conv | 3×3 | 32 | 896 |
| 2 | ERB | – | 64 | 12 544 |
| 3 | DCE | 3×3 | 128 | 36 992 |
| 4 | ERB | – | 128 | 49 664 |
| 5 | DCE | 3×3 | 256 | 147 712 |
| 6 | ERB | – | 256 | 197 632 |
| 7 | DCE | 3×3 | 512 | 590 336 |
| 8 | ERB | – | 512 | 324 288 |
| Итого | – | – | – | 1 360 064 |

Сравнительные результаты на наборе данных VisDrone приведены в таблице 3. Модифицированная архитектура демонстрирует прирост точности на сорок три процента относительно базовой при сохранении темпа обработки не менее ста восемнадцати кадров в секунду.

ТАБЛИЦА 3. Сравнение производительности на VisDrone

| Модель | Точн. % | Точн. расш. % | Парам. млн | GFLOPs | FPS |
|---|---|---|---|---|---|
| Базовая малая | 48,3 | 29,1 | 1,9 | 4,5 | 142 |
| Базовая малая v8 | 51,2 | 30,8 | 3,0 | 8,1 | 135 |
| Базовая средняя v8 | 55,4 | 34,2 | 11,2 | 28,6 | 87 |
| Предложенная | 73,2 | 45,8 | 1,4 | 6,3 | 118 |

Время логического вывода и производительность на едином графическом процессоре приведены в таблице 4.

ТАБЛИЦА 4. Время логического вывода и производительность

| Модель | Время, мс | FPS (GPU) | FPS (CPU) | Парам. млн | Размер, МБ |
|---|---|---|---|---|---|
| Базовая малая | 7,2 | 139 | 28 | 1,9 | 3,8 |
| Базовая малая v8 | 7,5 | 133 | 26 | 3,0 | 6,2 |
| Базовая средняя v8 | 11,8 | 85 | 18 | 11,2 | 22,5 |
| Предложенная | 8,5 | 118 | 25 | 1,4 | 2,9 |

Кросс-валидация на наборах TT100K и AFO (таблица 5) подтверждает универсальность архитектуры.

ТАБЛИЦА 5. Результаты на TT100K и AFO

| Модель | TT100K % | AFO % | Парам. млн | FPS |
|---|---|---|---|---|
| Базовая средняя | 68,4 | 62,7 | 7,2 | 98/96 |
| Базовая средняя v8 | 71,3 | 65,3 | 11,2 | 87/85 |
| Faster R-CNN | 69,8 | 64,1 | 41,0 | 23/21 |
| Предложенная | 76,9 | 71,8 | 1,4 | 115/112 |

Предложенная архитектура интегрируется в бортовые и наземные вычислительные контуры систем технического зрения беспилотных авиационных систем. Основные сценарии: целеуказание для барражирующих боеприпасов; корректировка артиллерийского огня (задержка <40 мс); обнаружение замаскированных огневых точек; мониторинг акваторий; учет логистических колонн; интеграция с системами РЭБ и ПВО. Обработка на борту обеспечивает автономность в условиях радиоэлектронного подавления при энергопотреблении <10 Вт.

## Заключение

Разработана оптимизированная нейросетевая архитектура для обнаружения малоразмерных целей на снимках БПЛА. Достигнуто повышение точности на 43 % при сокращении параметров на 53 % и темпе обработки ≥118 кадров в секунду. Интеграция в разведывательно-ударные контуры позволяет сократить цикл «обнаружение–целеуказание–поражение». Перспективы: мультисенсорная обработка, адаптация к состязательным атакам, роевое взаимодействие.

**Список используемых источников**

1. Du D., Qi Y., Yu H., et al. The Unmanned Aerial Vehicle Benchmark: Object Detection and Tracking // Proceedings of the European Conference on Computer Vision (ECCV). 2018. P. 370–386.

2. Lin T. Y., Maire M., Belongie S., et al. Microsoft COCO: Common Objects in Context // Proceedings of the European Conference on Computer Vision (ECCV). 2014. P. 740–755.

3. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement // arXiv preprint. 2018. arXiv:1804.02767.

4. Zhu Z., Liang D., Zhang S., Huang X., Li B., Hu S. Traffic-Sign Detection and Classification in the Wild // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). 2016. (TT100K dataset)

5. Zhang Y., Wang L., Chen S. Floating Objects Dataset // Remote Sensing. 2023. Vol. 15, N 12. P. 3012.

## MODIFIED DCE-YOLOV8 NEURAL NETWORK ARCHITECTURE FOR AUTOMATED DETECTION OF SMALL-SIZED TARGETS IN UAV IMAGES

**Babich K., Kuznetcov S., Popov A.**
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

*The paper presents an optimized neural network architecture designed for automated detection of small-sized and low-contrast targets in optoelectronic images of unmanned aerial systems. Four modifications of the basic architecture are proposed: an efficient residual module, a differentiated context extraction block based on partial convolutions, the elimination of a computationally redundant block, and the replacement of downsampling with upsampling to increase sensitivity to microscale objects. Experimental verification on data sets demonstrated a forty-three percent increase in accuracy relative to the base architecture, while reducing the number of parameters by fifty-three percent and maintaining a processing rate of at least one hundred eighteen frames per second. The results confirm the suitability of the architecture for onboard deployment as part of reconnaissance-strike circuits and technical vision systems of tactical unmanned aerial systems.*

***Key words:*** *computer vision, object detection, unmanned aerial systems, small-sized targets, onboard computing platforms, and neural network optimization*

**УДК 621.395.7**
**ГРНТИ 49.33.29, 50.41.31**

# ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ В УСЛОВИЯХ ОТКАЗОВ КРИТИЧЕСКИ ВАЖНЫХ УЗЛОВ

**Д. К. Баразенко, О. И. Пантюхин, А. С. Саврасов, Н. Э. Хрусталев**
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича

*Современные телекоммуникационные сети функционируют в условиях постоянно возрастающих требований к надежности и непрерывности предоставления услуг. Высокая степень распределенности инфраструктуры, увеличение объемов передаваемых данных и сложность маршрутизации делают сети уязвимыми к отказам отдельных компонентов. Наиболее опасными являются сбои критически важных узлов, поскольку их отказ способен привести к нарушению связности сети, росту задержек или полной недоступности сервисов. В данной работе рассматривается концепция интеграции топологического анализа сети, методов машинного обучения и автоматизированных систем управления для повышения устойчивости телекоммуникационной инфраструктуры. Основное внимание уделяется теоретическим аспектам построения архитектуры отказоустойчивых сетей без рассмотрения конкретных экспериментальных реализаций.*

***отказоустойчивость, телекоммуникационные сети, машинное обучение, автоматизация, критические узлы, интеллектуальный мониторинг***

Современные телекоммуникационные сервисы предъявляют высокие требования к непрерывности функционирования инфраструктуры и скорости восстановления после возникновения сбоев. Традиционные подходы к эксплуатации сетевой инфраструктуры, опирающиеся в основном на ручное администрирование и статическое конфигурирование оборудования, в условиях постоянно меняющейся сетевой среды, становятся недостаточно эффективными. Наиболее заметно данная проблема виднеется в распределенных сетях операторского уровня, облачных инфраструктурах и центрах обработки данных. Работа подобных систем определяется не отдельными устройствами, а согласованным взаимодействием большого количества компонентов. Отказ даже одного компонента увеличивает нагрузку на соседние участки и приводит к развитию цепочки последующих отказов.

Одни из способов повышения отказоустойчивости сети является автоматизация процессов управления инфраструктурой. Современные средства управления позволяют описывать параметры сетевой среды в декларативном виде. Это упрощает воспроизведение конфигураций на различных элементах инфраструктуры и уменьшает количество ошибок, возникающих при ручной

настройке. Также автоматизированное управление позволяет быстрее реагировать на изменения нагрузки и перераспределять вычислительные ресурсы, масштабировать сервисы и изменять маршруты передачи данных, исходя из текущего состояния сети. Особое значение в данном направлении занимают самоисцеляющиеся системы. Их принцип работы заключается в том, что часть действий по восстановлению выполняется автоматически, без непосредственного вмешательства оператора. При обнаружении признаков деградации такая система может начать перезапуск сервисов, задействовать резервный канал или изменить параметры маршрутизации [1].

Но одной автоматизации недостаточно для устойчивой работы инфраструктуры. Существенное влияние на последствия отказа оказывает топология сети. В распределенных системах имеются узлы, которые обрабатывают или пропускают через себя значительную часть трафика. К таким элементам относятся узлы концентрации трафика и устройства выполняющие функции централизованной маршрутизации. Их отказ может иметь значительно более серьезные последствия, чем отказ периферийного оборудования. Такие элементы принято называть критически важными узлами [1, 2]. Обнаружение критически важных узлов представляет собой одну из задач анализа отказоустойчивости. Определение таких элементов позволяет определить участки инфраструктуры, отказ которых потенциально способен оказать наибольшее воздействие на сеть. Эта информация должна использоваться при проектировании механизмов резервирования и мер для повышения общей надежности системы.

При определении значимости узлов сети лучше всего использовать метод теории графов. Основным показателем является степень вершины, то есть число непосредственных связей узла с другими элементами сети. Но одной степени узла недостаточно для оценки реальной роли узла. Из-за этого применяются дополнительные характеристики, такие как центральность по посредничеству. Данная характеристика показывает, насколько часто узел оказывается участником кратчайших маршрутов, соединяющих другие вершины графа. Если значение показателя велико, то узел имеет существенное значение для передачи трафика между различными частями сети. Его отказ может сопровождаться перераспределением значительных объемов данных. Помимо этого, рассматривается центральность по близости и центральность по собственному вектору. Центральность по близости позволяет оценить положение узла относительно других элементов сети, а центральность по собственному вектору учитывает не только количество связей, но и значимость узлов, с которыми он взаимодействует. Использование сразу нескольких характеристик вместе дает более полное представление о топологии. Это позволяет обнаруживать уязвимые участки, которые не

всегда очевидны при использовании только одного показателя, а также оценивать потенциальные направления распространения отказов.

Отказ одного из критически важных узлов вызывает перераспределение трафика между оставшимися элементами инфраструктуры. В результате перераспределения может получить дополнительную нагрузку. Если такая нагрузка превышает допустимый уровень или сохраняется продолжительное время, первоначальный отказ способен сопровождаться постепенным ухудшением состояния других компонентов. В магистральных сетях и распределенных сетях центрах обработки данных риск развития подобных сценариев особенно высок вследствие большого количества взаимосвязанных элементов [3]. По этой причине обеспечение отказоустойчивости невозможно свести исключительно к применению высоконадежного оборудования. Не менее важным является и предварительный анализ топологии сети и моделирования возможных сценариев распространения отказов, что позволяет заранее предусмотреть необходимые механизмы защиты (рис. 1).

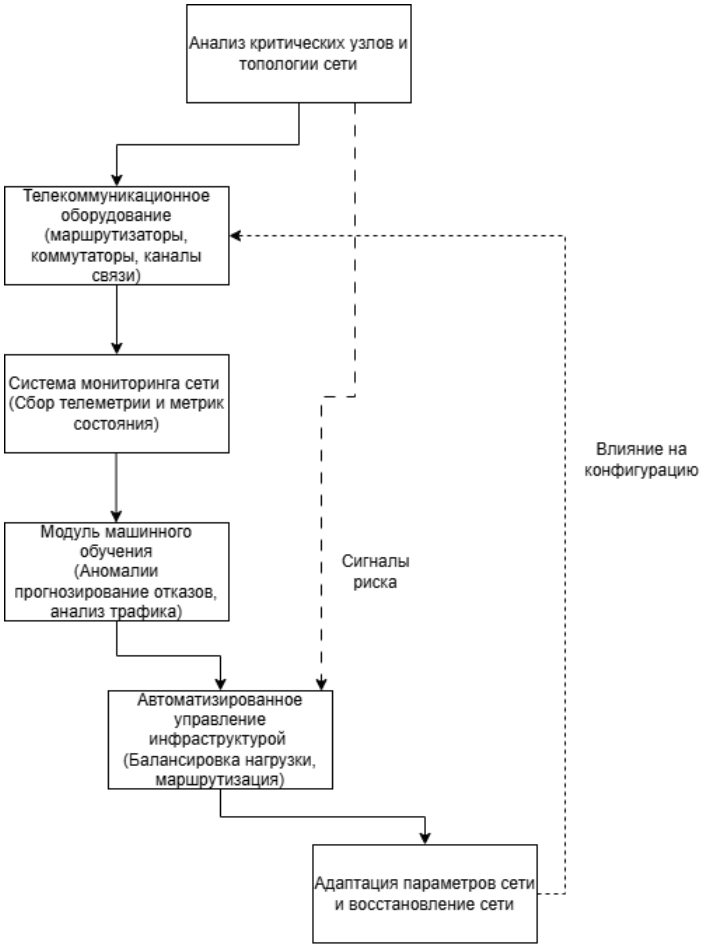



Рис. 1. Архитектура интеллектуального управления устойчивостью телекоммуникационной сети

Важную роль в обеспечении устойчивости телекоммуникационных сетей играют методы машинного обучения, позволяющие анализировать большие объемы данных, поступающих от сетевого оборудования и систем мониторинга. Современная инфраструктура генерирует значительное количество телеметрической информации, включающей показатели загрузки каналов связи, задержек передачи данных, состояния маршрутизаторов и серверных компонентов. Обработка подобных данных традиционными методами становится затруднительной вследствие их высокой динамики и сложности взаимосвязей между параметрами. Использование алгоритмов машинного обучения позволяет автоматизировать процесс анализа состояния сети и выявлять закономерности, недоступные для обнаружения при ручной обработке информации [4].

Одним из наиболее востребованных направлений применения машинного обучения является обнаружение аномалий в поведении инфраструктуры. Алгоритмы обучения без учителя позволяют выявлять отклонения от нормального состояния сети даже в тех случаях, когда характер потенциальной неисправности заранее неизвестен. Подобные методы особенно эффективны для обнаружения скрытых перегрузок, постепенной деградации оборудования и признаков сетевых атак. Дополнительное значение имеют модели прогнозирования, основанные на анализе исторических данных и временных рядов. Применение таких моделей позволяет заранее оценивать вероятность отказа из строя отдельных элементов сети и заранее активировать резервные ресурсы [5].

Возможности использования методов машинного обучения не ограничиваются прогнозированием неисправностей и поиском аномального поведения. Одной из важных задача является автоматическая оценка текущего состояния сетевой инфраструктуры. Алгоритмы обучения с учителем способны классифицировать наблюдаемое состояние сети, относя его к одному из заранее определенных режимов, например к штатному функционированию, деградации или аварийной ситуации. Автоматическая классификация позволяет сократить время обнаружения инцидента и уменьшить объем операций, которые необходимо выполнять специалисту вручную.

Эффективность подобных моделей зависит от качества исходной информации. Если телеметрия собирается неполно, содержит ошибки, либо обучающая выборка недостаточно представляет отдельные классы состояний, точность получаемых результатов может существенно снижаться. Из-за этого интеллектуальный анализ нельзя рассматривать отдельно от си-

стемы мониторинга. Для эффективной работы необходим постоянный сбор и передача актуальных показателей состояние сетевой архитектуры.

Одним из перспективных направлений развития отказоустойчивых телекоммуникационных сетей является объединение нескольких подходов в рамках единой системы. В такой архитектуре топологический анализ используется для определения наиболее значимых узлов, средства машинного обучения для обработки телеметрии и выявления признаков возможных проблем, а автоматизированная система для выполнения корректирующих действия. На основании полученной информации система управления может изменять маршруты передачи данных, корректировать параметры функционирования сети или переводить нагрузку на резервные компоненты. Это позволяет реализовать проактивный подход к обеспечению надежности, при котором предотвращающие меры принимаются до возникновения критического отказа.

Концепция интеллектуальной отказоустойчивой сети включает несколько взаимодополняющих уровней. На первом этапе выполняется исследование топологии сети и определение наиболее значимых узлов. Второй уровень отвечает за мониторинг инфраструктуры и прогнозирование возможных неисправностей с использованием методов машинного обучения. Третий уровень предназначен для автоматизированного управления и восстановления работоспособности системы при возникновении сбоев. Совместная работа указанных подсистем формирует непрерывный контур управления, обеспечивающий адаптацию сети к изменяющимся условиям эксплуатации в режиме реального времени.

**Список используемых источников**

1. Барабаши А.-Л., Пошфаи М. Сетевая наука. М.: ДМК Пресс, 2016. 474 с.

2. Ньюман М. Сети: введение. Оксфорд: Oxford University Press, 2010. 784 с.

3. Sterbenz J. P. G., Hutchison D., Çetinkaya E.K., Jabbar A., Rohrer J.P., Schöller M., Smith P. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines // Computer Networks. 2010. Vol. 54, N 8. P. 1245–1265.

4. Boutaba R., Salahuddin M.A., Limam N., Ayoubi S., Shahriar N., Estrada-Solano F., Caicedo O.M. A Comprehensive Survey on Machine Learning for Networking: Evolution, Applications and Research Opportunities // Journal of Internet Services and Applications. 2018. Vol. 9. Article 16.

5. Kreutz D., Ramos F.M.V., Verissimo P.E., Rothenberg C.E., Azodolmolky S., Uhlig S. Software-Defined Networking: A Comprehensive Survey // Proceedings of the IEEE. 2015. Vol. 103, N 1. P. 14–76.

# INTELLIGENT METHODS FOR ENSURING FAULT TOLERANCE OF TELECOMMUNICATION NETWORKS UNDER FAILURES OF CRITICALLY IMPORTANT NODES

**Barazenko D., Pantyukhin O., Savrasov A., Khrustalev N.**
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

*Modern telecommunication networks operate under constantly increasing requirements for reliability and continuity of service provision. The high degree of infrastructure distribution, increasing volumes of transmitted data, and routing complexity make networks vulnerable to failures of individual components. The most dangerous are failures of critically important nodes, since their failure can lead to disruption of network connectivity, increased latency, or complete unavailability of services. This paper considers the concept of integrating network topology analysis, machine learning methods, and automated control systems to increase the resilience of telecommunication infrastructure. The main focus is on theoretical aspects of building fault-tolerant network architectures without considering specific experimental implementations.*

***Key words:*** *fault tolerance, telecommunication networks, machine learning, automation, critical nodes, intelligent monitoring*

**УДК 004.896:616-056.26**
**ГРНТИ 76.29.55**

# БИОНИЧЕСКИЙ ПРОТЕЗ ГОЛЕНИ С ПОДСВЕТКОЙ ДЛЯ СОЦИАЛЬНОЙ АДАПТАЦИИ РЕБЕНКА

**Е. С. Бедикян, И. С. Жуков, А. И. Камардин, Н. С. Литусов, В. М. Лопашенко**

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

*В статье представлен проект бионического протеза голени с декоративной светодиодной подсветкой для ребенка с отсутствием нижней конечности. Работа связана не только с восстановлением двигательных функций, но и с психологической адаптацией детей, которые могут испытывать стеснение, снижение самооценки и чувство собственной неполноценности. Основная идея проекта заключается в том, чтобы ребенок воспринимал протез не просто как вынужденную замену конечности, а как индивидуальную технологичную особенность, способную вызывать интерес и положительную реакцию окружающих. Для этого предлагается использовать элементы бионического управления и встроенную светодиодную подсветку, которая выполняет не только декоративную, но также эмоциональную и социально-коммуникативную функцию. В работе рассматриваются конструкция протеза, система управления, питание и вопросы безопасности. Предполагается, что такое решение поможет уменьшить психологический дискомфорт, повысить уверенность ребенка в себе и облегчить общение со сверстниками.*

***бионический протез, детское протезирование, LED-подсветка, психологическая адаптация, самооценка, инклюзивный дизайн, реабилитационные технологии, социальная адаптация***

Проблема детской инвалидности, связанной с отсутствием конечностей, имеет не только медицинскую, но и выраженную социально-психологическую сторону [1, 2]. Дети, которые пользуются протезами, нередко чувствуют дискомфорт из-за реакции сверстников и собственного ощущения, что они отличаются от окружающих. При этом внешний вид устройства, которым ребенок пользуется каждый день, может влиять на его самооценку и поведение в обществе.

При разработке протезов основное внимание традиционно уделяется функциональности и биомеханической эффективности [3]. Эстетические и психологические особенности часто остаются на втором плане. Для ребенка это особенно значимо, поскольку в период взросления восприятие

собственного тела и своих особенностей напрямую связано с психологическим благополучием [4].

В рамках проекта предлагается по-другому взглянуть на роль протеза в жизни ребенка. Он должен восприниматься не как медицинское изделие, которого приходится стесняться, а как персонализированное технологичное устройство, способное стать частью образа ребенка. Для этого в корпус протеза встраивается светодиодная подсветка, выступающая одним из элементов инклюзивного дизайна.

Дети особенно чувствительны к оценке сверстников. Исследования в области детской психологии показывают, что в школьном возрасте активно формируются отношение к собственному телу и самовосприятие [1, 5]. Ребенок со стандартным протезом может сталкиваться с вопросами, насмешками или нежелательным вниманием. В результате он может становиться более замкнутым, избегать общения, а в отдельных случаях это отражается и на учебной деятельности.

Инклюзивный дизайн предполагает создание продуктов с учетом потребностей разных групп пользователей, в том числе людей с ограниченными возможностями здоровья [6]. В детском протезировании такой подход означает, что при проектировании необходимо учитывать не только физиологические, но и психологические потребности ребенка.

Необычный и привлекательный внешний вид может изменить характер внимания со стороны окружающих. Вместо жалости или излишнего любопытства протез способен вызывать интерес и положительную реакцию. Сам ребенок при этом может воспринимать его не только как напоминание об отсутствии конечности, но и как собственную необычную особенность, своеобразную «суперспособность». Подсветка делает устройство более заметным и подчеркивает его технологичный характер.

Поэтому одна из основных идей проекта состоит в том, чтобы протез стал для ребенка не источником стеснения, а предметом, который он может воспринимать положительно. Светодиодные элементы интегрируются непосредственно в корпус и позволяют менять внешний вид устройства.

Подсветка выполняет несколько функций. Ребенок может самостоятельно выбирать цвет, режим свечения и визуальный стиль, настраивая протез под свои предпочтения. Предусмотрены статичный, пульсирующий и динамический режимы. Кроме того, подсветка может привлекать к протезу позитивное внимание и переносить акцент с отсутствия конечности на технологические особенности устройства. Возможность самостоятельно

управлять оформлением также дает ребенку больше контроля и повышает его вовлеченность в использование протеза.

В таком варианте подсветка становится не только декоративной деталью. Она используется как инструмент инклюзивного дизайна, который может влиять на восприятие протеза как самим ребенком, так и окружающими. Устройство начинает восприниматься не только как «замена», но и как необычная индивидуальная особенность владельца.

Конструкция бионического протеза голени состоит из нескольких основных элементов (рис. 1). Посадочное место, или гильза, представляет собой индивидуально изготовленный приемник культи и обеспечивает фиксацию протеза и комфорт при ношении. Защитные щитки закрывают несущую конструкцию и одновременно служат основой для размещения светодиодной подсветки. Упругий элемент в виде пружины отвечает за амортизацию и накопление энергии во время ходьбы. Протезная стопа изготавливается из полимерных материалов и имитирует биомеханику естественной стопы. Кольца, болтовые соединения и другие крепежные элементы обеспечивают фиксацию отдельных модулей конструкции.

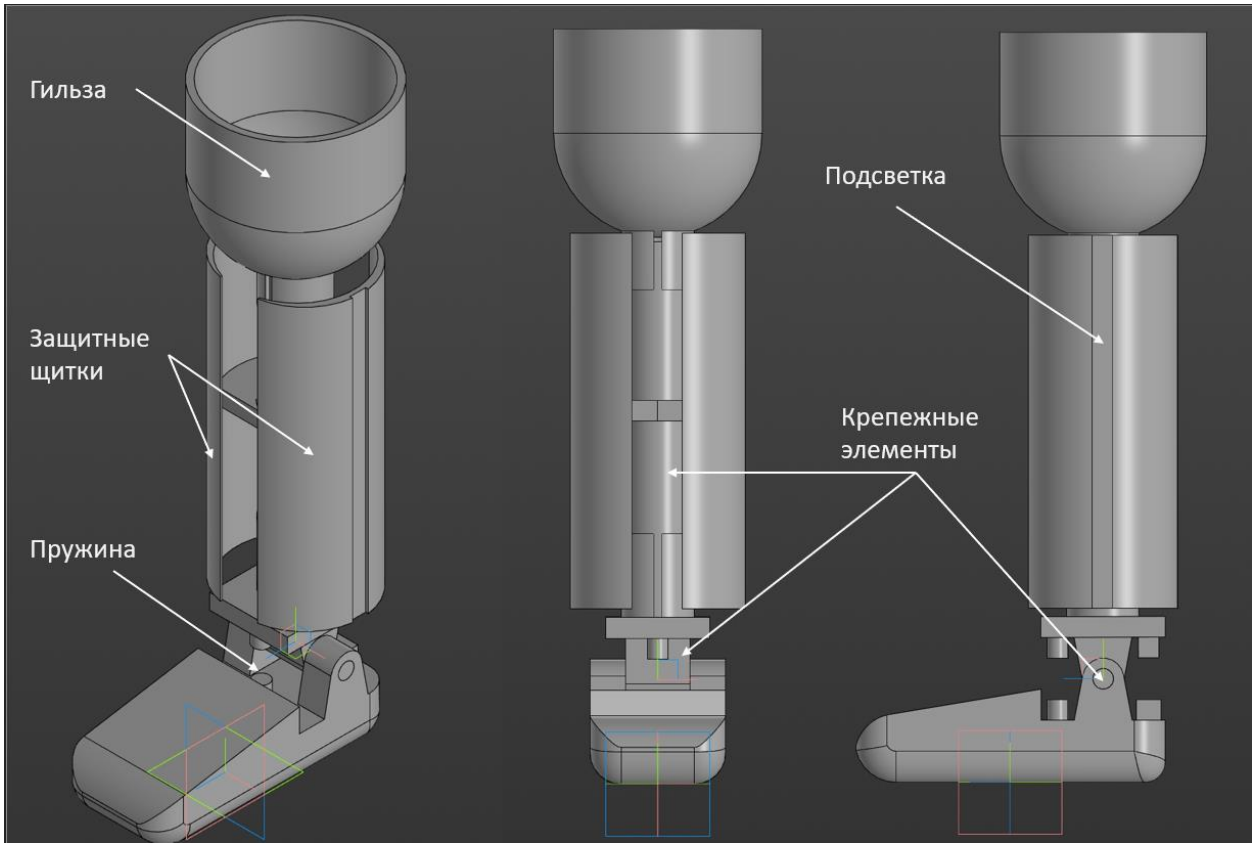



Рис. 1. Конструкция бионического протеза

Работой функций протеза управляет встроенный микроконтроллер. Он обрабатывает сигналы датчиков и формирует команды для системы подсветки. Датчики положения отслеживают отдельные фазы шага, благодаря чему свечение можно синхронизировать с движением.

Система подсветки включает светодиодную ленту, размещенную по контуру защитных щитков. Предусмотрено несколько вариантов работы: постоянное свечение выбранным цветом, пульсация с синхронизацией по шагу, динамическая смена цветов и тематические настраиваемые режимы.

Для автономной работы используется встроенный литий-ионный аккумулятор. Заявленное время работы составляет не менее 8–10 часов в активном режиме. Зарядка выполняется через разъем USB-C. Также предусмотрена защита от перегрева, перегрузки и глубокого разряда аккумулятора.

Предлагаемая концепция может использоваться в нескольких направлениях. В детском протезировании она рассматривается как вариант устройства, в котором наряду с функциональными характеристиками учитываются психологические потребности ребенка. В реабилитационных центрах такой протез может стать частью комплексной работы, связанной с самооценкой и социальной адаптацией. Проект также подходит для образовательных инженерных задач как пример сочетания технических решений и принципов инклюзивного дизайна.

В дальнейшем эту концепцию можно адаптировать для других типов протезов и возрастных групп. Отдельные использованные в ней принципы могут быть применены и при разработке других вспомогательных устройств, включая слуховые аппараты.

Результатом проекта должен стать прототип бионического протеза голени со встроенной светодиодной подсветкой. Предполагается, что устройство будет обеспечивать базовые биомеханические функции при ходьбе и обычной повседневной активности. Ребенок сможет самостоятельно настраивать внешний вид протеза. Ожидается также снижение стеснения и тревожности, связанных с его использованием, более положительная реакция со стороны сверстников и улучшение социальных взаимодействий. В этом случае протез может восприниматься ребенком как собственная особенность, а не только как недостаток.

Авторы предполагают, что регулярное использование такого устройства может положительно влиять на психологическое состояние ребенка и его адаптацию в социальной среде.

Проект бионического протеза голени со встроенной светодиодной подсветкой предлагает подход, при котором реабилитационное устройство рассматривается не только с технической точки зрения. Его отличие заключается в целенаправленном учете психологической стороны реабилитации. Протез должен не просто компенсировать утраченную функцию, но и помогать ребенку увереннее чувствовать себя среди окружающих.

Подсветка как часть инклюзивного дизайна меняет внешний вид устройства и может сделать его объектом интереса вместо источника стеснения. Возможность персонализации, по замыслу проекта, должна помочь ребенку сформировать более положительное отношение к протезу и повысить мотивацию к активному образу жизни.

Следующий этап работы предполагает изготовление физического прототипа и его тестирование с участием детей-пользователей. Планируется оценить психологический эффект с помощью стандартизированных методик, разработать приложение для управления подсветкой и доработать конструкцию по результатам испытаний. Проект рассматривается как одно из направлений детской реабилитационной инженерии, в котором техническая разработка сочетается с задачами психологической и социальной адаптации.

**Список используемых источников**

1. Баранов А. А., Намазова-Баранова Л. С., Терлецкая Р. Н., Антонова Е. В. Проблемы детской инвалидности в современной России // Вестник РАМН. 2017. № 4. URL: https://cyberleninka.ru/article/n/problemy-detskoy-invalidnosti-v-sovremennoy-rossii (дата обращения: 30.08.2026).

2. Афонькина Ю. А., Лапина А. С. Детская инвалидность как комплексная проблема современности // Проблемы современного педагогического образования. 2018. № 61-2. URL: https://cyberleninka.ru/article/n/detskaya-invalidnost-kak-kompleksnaya-problema-sovremennosti (дата обращения: 30.08.2026).

3. Шибкова Д. З., Эрлих В. В. Теоретико-методическое обоснование выбора новых подходов к созданию функциональных протезов нижних конечностей // Человек. Спорт. Медицина. 2024. № 4. URL: https://cyberleninka.ru/article/n/teoretiko-metodicheskoe-obosnovanie-vybora-novyh-podhodov-k-sozdaniyu-funktsionalnyh-protezov-nizhnih-konechnostey (дата обращения: 30.08.2026).

4. Ионина О. С. Факторы, определяющие психологическое здоровье ребенка // Вестник ШГПУ. 2017. № 1 (33). URL: https://cyberleninka.ru/article/n/faktory-opredelyayuschie-psihologicheskoe-zdorovie-rebenka (дата обращения: 30.08.2026).

5. Наберушкина Э. К., Радченко Е. А., Мирзаева Е. Р. Инклюзивный дизайн (Обзор зарубежных концепций) // Теория и практика общественного развития. 2023. № 2 (180). URL: https://cyberleninka.ru/article/n/inklyuzivnyy-dizayn-obzor-zarubezhnyh-kontseptsiy (дата обращения: 30.08.2026).

# BIONIC PROSTHESIS OF THE SHIN WITH BACKLIGHT FOR THE SOCIAL ADAPTATION OF A CHILD

**Bedikyan E., Zhukov I., Kamardin A., Litusov N., Lopashenko V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article discusses the project of developing a bionic leg prosthesis with decorative LED backlighting for a child with absence of the lower limb. The relevance of the work is due not only to the need to restore lost motor functions, but also to the acute problem of psychological adaptation of children who experience embarrassment, low self-esteem and a sense of inferiority. The key idea of the project is to create a device that is perceived by the child not as a forced replacement of a limb, but as an individual technological feature that can arouse interest and a positive reaction from others. The paper proposes to use elements of bionic control and built-in LED backlighting that performs an emotional and socio-communicative function. Technical solutions for the design of the prosthesis, control system, power supply and safety are presented. It is substantiated that such a solution can reduce the level of psychological discomfort, increase the child's self-confidence and promote more successful interaction with peers.*

***Key words:*** *bionic prosthesis, pediatric prosthetics, LED backlight, psychological adaptation, self-esteem, inclusive design, rehabilitation technologies, social adaptation*

**УДК 004.72**
**ГРНТИ 47.47.17**

# ТРЕБОВАНИЯ К КАЧЕСТВУ ОБЪЕКТОВ ЗНАНИЙ В ПЛОСКОСТИ ЗНАНИЙ СЕТЕЙ, ОПРЕДЕЛЯЕМЫХ ЗНАНИЯМИ (KDN)

**Ф. С. Блан**

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

*В статье предложена система требований к качеству объектов знаний в плоскости знаний сетей, определяемых знаниями. Для трех типов объектов (необработанной телеметрии, сгенерированных и сформированных знаний) определены критические атрибуты качества. Показано, что достоверность является основным критерием для сгенерированных знаний, а происхождение – для сформированных, при этом оба атрибута отсутствуют в стандарте МСЭ-Т М.3351. Предложен шаблон спецификации качества для применения в программно-определяемых сетях.*

***сети, определяемые знаниями, плоскость знаний, объекты знаний, качество данных, машинное обучение, достоверность, происхождение знаний***

Появление сетей, определяемых знаниями (Knowledge-Defined Networking, KDN), знаменует парадигмальный сдвиг в управлении сетями: в архитектуру вводится выделенная плоскость знаний (Knowledge Plane), предназначенная для генерации, обработки и распространения знаний, извлеченных из сетевых данных. Концепция KDN, впервые предложенная в [1] и формализованная в [2], предполагает введение плоскости знаний как когнитивного ядра сети, обеспечивающего автономное принятие решений посредством непрерывного применения методов машинного обучения (МО) и искусственного интеллекта. Архитектурная реализация данной концепции включает пять логических плоскостей: передачи данных, управления, мониторинга, знаний и приложений [3-6]. Плоскость знаний, в свою очередь, можно разделить на три функциональных подуровня: генерации, формирования, а также управления и распространения.

Каждый подуровень формирует качественно различные объекты знаний. Подуровень генерации знаний получает дескриптивные выходные данные из необработанной телеметрии с использованием моделей МО и выделяет из них контекст. Подуровень композиции синтезирует эти данные в структурированные правила и политики посредством редакторов онтологий и генераторов правил. Подуровень управления и распространения хранит и распределяет все объекты знаний в рамках архитектуры.

Несмотря на растущий массив работ по архитектуре и применению KDN, требования к качеству объектов знаний в плоскости знаний остаются недостаточно специфицированными. Рекомендация МСЭ-Т M.3351 рассматривает построение, хранение и распределение знаний на высоком уровне абстракции, однако ее положения о качестве ограничены структурированными и необработанными данными и не охватывают объекты, сгенерированные методами машинного обучения или скомпонованные онтологически. В частности, M.3351 не рассматривает достоверность и провенанс (происхождение) – атрибуты, критически важные для производных и составных знаний соответственно. Данная статья восполняет этот пробел, определяя пять атрибутов качества и устанавливая их дифференцированную значимость для трех типов объектов знаний в текущих развертываниях SDN.

Три типа объектов знаний, формируемых подуровнями плоскости знаний, занимают различные позиции в пайплайне машинного обучения, что лежит в основе дифференциации требований к их качеству. Необработанная телеметрия, принимаемая подуровнем управления и распространения, выполняет функцию обучающих выборок и входных признаков. Сгенерированные знания, создаваемые подуровнем генерации, представляют собой предсказания моделей, потребляемые плоскостью управления. Сформированные знания, синтезируемые подуровнем композиции, соответствуют структурированным политикам и правилам высшего порядка. Данная трехуровневая структура обобщена в таблице 1.

ТАБЛИЦА 1. Значения времени передачи кадра при различных соотношениях параметров

| Тип объекта знаний | Подуровень плоскости знаний | Эквивалент в ML-пайплайне | Пример |
|---|---|---|---|
| Необработанная телеметрия | Управление и распространение | Обучающие выборки, входные признаки | Утилизация каналов, глубина очереди, потери пакетов |
| Необработанная телеметрия | Генерация | Выходные данные, предсказания моделей | «Прогнозируется перегрузка», оценка аномалии |
| Скомпонованные знания | Формирование | Априорные знания, ограничения, правила политик | Политики маршрутизации, правила онтологий, SLA |

Каждый тип деградирует качественно по-разному: устаревший образец необработанной телеметрии искажает обучающее окно; предсказание с завышенной достоверностью провоцирует ошибочное решение о маршрутизации;

политика с неустановленным провенансом не может быть безопасно отменена в сценарии отказа. Эти различия в характере деградации обусловливают необходимость дифференцированной системы атрибутов качества для каждого типа объектов.

Атрибуты качества объектов знаний определяются здесь с точки зрения их операционной значимости в рамках плоскости знаний. Используемая терминология основана на модели качества данных ISO/IEC 25012 [7], расширенной с учетом ML-семантики, специфичной для KDN. Выделяются пять атрибутов, необходимых и достаточных для спецификации качества объектов знаний на уровне плоскости знаний:

– Своевременность: степень, в которой объект знаний отражает текущее состояние сети в пределах операционно допустимого возраста. Для необработанной телеметрии своевременность определяется интервалами сбора и экспорта, установленными в фреймворке сетевой телеметрии; для сгенерированных знаний она дополнительно включает устарелость обучающих данных, на которых последний раз обновлялась порождающая модель.
– Полнота: доля необходимых элементов знаний, присутствующих и доступных для потребления в точке использования. Для необработанной телеметрии это соответствует доле ожидаемых образцов, полученных в пределах окна сбора; для сгенерированных и сформированных знаний – охвату входного пространства, в отношении которого применялся порождающий процесс.
– Согласованность: отсутствие логических противоречий между объектами знаний, поступающими из нескольких источников или цепочек деривации. Согласованность приобретает особую критичность для сформированных знаний, где политики, синтезированные на основе независимо сгенерированных выходных данных, могут конфликтовать при отсутствии проверки относительно общего онтологического референса.
– Достоверность: количественная оценка корректности или надежности объекта знаний, применимая в случаях, когда объект является результатом вероятностного или обученного процесса. Достоверность значима только для сгенерированных и, в меньшей степени, сформированных знаний. Необходимость явной квантификации достоверности для принимаемых сетевых решений на основе МО была эмпирически продемонстрирована в контексте предоставления услуг, управляемого трафиком [8].
– Провенанс: прослеживаемая запись происхождения объекта знаний, его цепочки деривации и преобразований. Провенанс необходим для сформированных знаний, где политика маршрутизации или правило онтологии, источник которых не установлен, не может быть проверена, отменена или признана достоверной в многодоменных сценариях. Он также имеет высокую значимость

для сгенерированных знаний, где идентичность порождающей модели и ее обучающего корпуса составляют минимальную запись провенанса.

Достоверность и провенанс отсутствуют в системе качества МСЭ-Т М.3351. Их введение в качестве атрибутов качества первого класса составляет основное расширение настоящей работы относительно действующего стандарта.

Значимость каждого атрибута неодинакова для различных типов объектов знаний. В таблице 2 представлена структурированная оценка, в которой уровни значимости (критический, высокий, средний, желательный и неприменимо) отражают операционные последствия деградации атрибута для каждого типа.

ТАБЛИЦА 2. Значимость атрибутов качества по типам объектов знаний

| Атрибут качества | Необработанная телеметрия | Сгенерированные знания | Сформированные знания |
|---|---|---|---|
| Своевременность | **Критический** | Высокий | Низкий |
| Полнота | Высокий | Средний | Средний |
| Согласованность | Средний | Средний | **Критический** |
| Достоверность | Неприменимо | **Критический** | Низкий |
| Провенанс | Желательный | Высокий | **Критический** |

Достоверность для сгенерированных знаний и провенанс для сформированных представляют первоочередной теоретический интерес. Выходные данные модели без оценки неопределенности не могут быть безопасно применены плоскостью управления: предсказание с низкой достоверностью должно инициировать переход на резервный маршрут, а не немедленное перенаправление трафика. Для сформированных знаний провенанс вытесняет достоверность как доминирующий атрибут: правило политики с неизвестной цепочкой деривации не может быть безопасно применено там, где проверяемость и обратимость являются операционными требованиями. Атрибуты качества не функционируют независимо: нарушение своевременности необработанной телеметрии снижает полноту обучающего окна, что, в свою очередь, снижает достоверность сгенерированных знаний. Данная каскадная деградация не охвачена положениями М.3351 и является одним из обоснований шаблона спецификации, представленного ниже.

Матрица атрибутов качества определяет отдельную спецификацию для каждого типа объектов. Для необработанной телеметрии – SLA своевременности и порог полноты, регулируемые подуровнем управления и распростране-

ния плоскости знаний. Для сгенерированных знаний – порог достоверности, ниже которого активируется резервный механизм, и граница устарелости обучающих данных. Для сформированных знаний – проверка согласованности с базой знаний и требование к глубине провенанса, определяющее обратимость изменений политик в многодоменных развертываниях.

**Список используемых источников**

1. Clark D.D., Partridge C., Ramming J.C., Wroclawski J.T. A Knowledge Plane for the Internet // Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03). ACM, 2003. PP. 3–10. DOI: 10.1145/863955.863957.

2. Mestres A., Rodriguez-Natal A., Carner J., Barlet-Ros P., Alarcón E., Solé-Simó M., et al. Knowledge-Defined Networking // ACM SIGCOMM Computer Communication Review. 2017. Vol. 47. № 3. С. 2–10. DOI: 10.1145/3138808.3138810.

3. Блан Ф. С. Архитектура и применение сетей, определяемых знаниями // Студенческая весна – 2025: сб. науч. тр. СПб.: СПбГУТ, 2025. С. 16–21.

4. Блан Ф. С., Елагин В. С. Перспективная архитектура сетей, определяемых знаниями (KDN) // Труды учебных заведений связи. 2025. Т. 11. № 2. С. 67–82. DOI: 10.31854/1813-324X-2025-11-2-67-82. EDN: QCIUMV.

5. ITU-T Recommendation M.3351. Framework of knowledge management for telecom operation and management. International Telecommunication Union, 2024.

6. Wijesekara P.A.D.S.N., Gunawardena S. A Comprehensive Survey on Knowledge-Defined Networking // Telecom. 2023. Vol. 4. № 3. С. 385–423. DOI: 10.3390/ telecom4030025.

7. Hafsa M., Panayiotou T., Ellinas G. Uncertainty quantification and consideration in ML-aided traffic-driven service provisioning // Computer Networks. 2023. Vol. 202; DOI: 10.1016/j.comcom.2023.02.007.

8. ISO/IEC 25012:2008. Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model. ISO/IEC, 2008.

## QUALITY REQUIREMENTS FOR KNOWLEDGE OBJECTS IN THE KNOWLEDGE PLANE OF KNOWLEDGE-DEFINED NETWORKS

**Blan F.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper proposes a quality requirements framework for knowledge objects in the Knowledge Plane of Knowledge-Defined Networks. For three knowledge object types – raw telemetry, derived knowledge, and composed knowledge – critical quality attributes are identified. It is shown that confidence is the primary quality attribute for derived knowledge, while provenance is dominant for composed knowledge; neither attribute is addressed in ITU-T Recommendation M.3351. A quality specification template is proposed for application in current software-defined network deployments.*

***Key words:*** *knowledge-defined networking, knowledge plane, knowledge objects, data quality, machine learning, confidence, knowledge provenance*

**УДК 535.14**
**ГРНТИ 29.05.15**

# МОДЕЛИРОВАНИЕ ПОЛЯРИЗАЦИОННЫХ СОСТОЯНИЙ В ИМИТАТОРЕ КРК

**Г. Р. Бразовский, А. А. Шевцова, А. Е. Яцкова**

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

*Обеспечение лабораторного практикума в рамках дисциплин обеспечивающих подготовку кадров для квантовых коммуникаций является сложной задачей. Использование реального оборудования затруднено его стоимостью и редкостью. Существует два варианта решения данной проблемы: создание физических имитаторов и виртуальных лабораторий. В работе проведено моделирование поляризационных состояний света в создаваемой сейчас лаборатории имитаторе системы КРК.*

***квантовые коммуникации, квантовое распределение ключей***

В настоящее время квантовые технологии являются одной из наиболее развиваемых областей науки и техники во всем мире. Выделяют 3 основных направления квантовых технологий: квантовые коммуникации, квантовые вычисления и квантовая сенсорика. Считается, что квантовые коммуникации позволят в будущем строить абсолютно защищенные от перехвата информации системы передачи данных.

Основным направлением квантовых коммуникаций, на данный момент, считается квантовое распределение ключей шифрования (КРК). Основанные на теореме о запрете клонирования, такие системы позволят обеспечить потоковую генерацию гарантированно секретных ключей шифрования.

Предполагается, что в ближайшем будущем, развитие и массовое внедрение систем КРК потребует большого количества подготовленных кадров. Для полноценного обучения профессионалов требуется как теоретическая, так и практическая подготовка.

Обеспечение практической подготовки составляет значительную трудность для большинства образовательных организаций ввиду высокой стоимости и низкой доступности оборудования КРК. Для преодоления этой трудности могут быть использованы лабораторные установки, основанные на имитации систем КРК. Такие установки могут быть виртуальными [1]

и математически моделировать процессы, происходящие в системах КРК, или физическими использующими схожие процессы для моделирования систем КРК. Создание такой физической имитационной лабораторной установки происходит в настоящее время на кафедре оптических и квантовых систем связи в СПБГУТ.

Разрабатываемая лабораторная установка предполагается для имитации систем КРК с поляризационным кодированием. Схема установки состоит из лазера (ЛД), 3 четвертьволновых пластин (ЧВ) на поворотных установках, поляризационный светоделитель (ПС) и два фотодетектора (ФД). На рисунке 1 приведена структурная схема разрабатываемой установки.

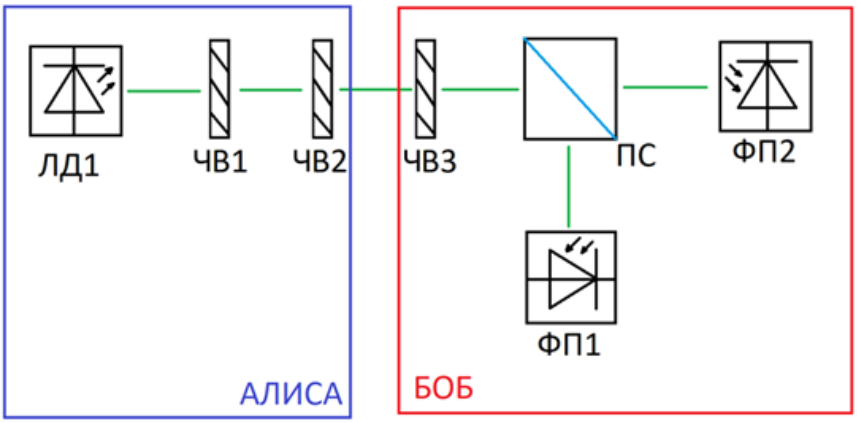



Рис. 1. Схема разрабатываемой установки имитатора КРК

Излучение от лазера поступает на две четвертьволновых пластины (ЧВ1 и ЧВ2), относящихся к блоку Алисы. При помощи данных двух пластин производится преобразование поляризации излучения лазера, имитирующее выбор квантового состояния на выходе Алисы.

При помощи четвертьволновой пластины ЧВ3 производится имитация выбора Бобом базиса, в котором происходит прием фотона, а поляризационный светоделитель и два фотоприемника позволяют имитировать работу однофотонных детекторов. Данная установка позволяет имитировать множество различных протоколов КРК, но в основу работ по разработке положен протокол ВВ-84.

Протокол ВВ84, предложенный Беннеттом и Брассаром в 1984 году [2], использует два неортогональных базиса: прямоугольный базис с горизонтальной и вертикальной поляризациями и диагональный базис с диагональной и антидиагональными поляризациями.

Алиса случайным образом выбирает базис и состояние, кодируя бит. Боб случайным образом выбирает базис измерения. После передачи по от-

крытому каналу сравниваются базисы, и совпавшие позиции образуют секретный ключ. Физической основой стойкости протокола является принцип неопределенности Гейзенберга и теорема о запрете клонирования.

Основные этапы взаимодействия Алисы и Боба в протоколе BB-84 представлены на рисунке 2.

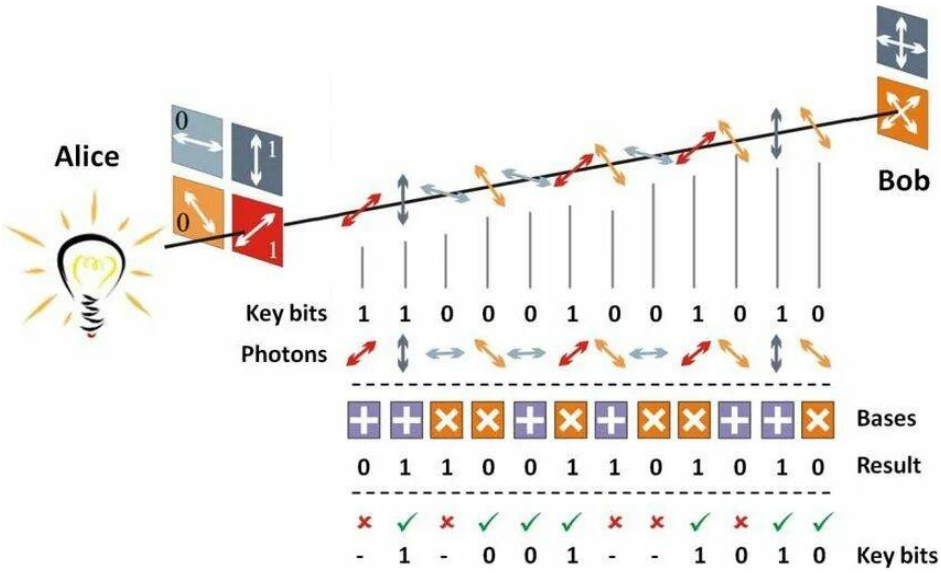



Рис. 2. Описание протокола BB-84

В разрабатываемой установке предполагается возможность использования как базисов, основанных как на ортогональных линейных поляризациях, так и на круговых поляризациях.

Для подтверждения работоспособности схемы разрабатываемой установки было произведено математическое моделирование ее работы. Основой математической модели стали вектора и матрицы Джонса.

Вектор Джонса для линейно поляризованного излучения имеет следующий вид [3]:

$$L(\alpha) = \begin{pmatrix} \sin(\alpha) \\ \cos(\alpha) \end{pmatrix}, \quad (1)$$

где $\alpha$ – азимут поляризации излучения.

Четвертьволновая пластина может быть описана следующей матрицей Джонса:

$$QWP(\gamma) = \begin{pmatrix} \cos^2(\gamma) + i\sin^2(\gamma) & (1-i)\sin(\gamma)\cos(\gamma) \\ (1-i)\sin(\gamma)\cos(\gamma) & \sin^2(\gamma) + i\cos^2(\gamma) \end{pmatrix}, \quad (2)$$

где $\gamma$ – угол поворота быстрой оси четвертьволновой пластины от вертикальной оси.

Блок Алисы состоит из двух четвертьволновых пластин, следовательно излучение на его выходе может быть вычислено по формуле 3.

$$L_{Aout}(\gamma_1, \gamma_2, \alpha) = QWP(\gamma_2) * QWP(\gamma_1) * L(\alpha), \quad (3)$$

где $L_{Aout}$ – вектор Джонса для излучения на выходе Алисы, $\alpha$ – азимут поляризации на выходе лазера, а $\gamma_1$ и $\gamma_2$ – углы поворота четвертьволновых пластин ЧВ1 и ЧВ2 соответственно.

Для каждого состояния поляризации на выходе блока Алисы, требуемого для имитации системы КРК, были эмпирически подобраны углы поворота четвертьволновых пластинок. Результаты представлены в таблице 1.

ТАБЛИЦА 1. Результаты расчетов углов поворота пластинок для Алисы

| Базис Алисы | Бит Алисы | Поляризация на выходе | Угол поворота ЧВ1 | Угол поворота ЧВ2 |
|---|---|---|---|---|
| Линейный | 0 | Линейная, азимут 90° | 22.5° | 22.5° |
| | 1 | Линейная, азимут 0° | 67.5° | 67.5° |
| Круговой | 1 | Круговая по часовой | 135° | 90° |
| | 0 | Круговая против часовой | 135° | 0° |

Результаты эмпирического подбора были проверены с использованием формулы 3. Пример проверочного расчета для имитации передачи бита 0 в круговом базисе приведено в формуле 4.

$$L_{Aout}(135°, 0°) = QWP(0°) * QWP(135°) * \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = e^{i*\frac{\pi}{2}}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}. \quad (4)$$

Данный вектор Джонса соответствует круговой поляризации против часовой стрелки, а множитель $e^{i*\frac{\pi}{2}}$ показывает, что излучение приобрело дополнительную фазу $\frac{\pi}{2}$, которой можно пренебречь в рассматриваемой схеме.

Аналогично углам поворота четвертьволновых пластин Алисы, эмпирически были найдены углы поворота ЧВ3 Боба. Данные углы поворота представлены в таблице 2.

ТАБЛИЦА 2. Результаты расчетов углов поворота пластинок для Боба

| Базис Боба | Угол поворота ЧВ2 |
|---|---|
| Линейный | 0° |
| Круговой | 45° |

Для подтверждения правильного определения углов поворота ЧВ3, были вычислены векторы Джонса для излучения, поступающего на поляризационный светоделитель при каждом состоянии Алисы. Расчет производился по формуле 5.

$$L_{Bout}(\gamma_3) = QWP(\gamma_3) * L_{Aout}, \quad (5)$$

где $L_{Aout}$ – вектор Джонса для излучения на выходе Алисы, $L_{Bout}$ – вектор Джонса для излучения, поступающего на поляризационный светоделитель, а $\gamma_3$ – угол поворота четвертьволновой пластины ЧВ3.

При правильном выборе углов поворота ЧВ3 и совпадении базисов Алисы и Боба излучение, поступающее на поляризационный светоделитель, должно иметь линейную поляризацию с азимутом 0° или 90° (в зависимости от бита Алисы). При несовпадении базисов на поляризационный светоделитель должно поступать излучение, имеющее либо круговую поляризацию, либо линейную с азимутом 45° или 135°.

Пример расчета вектора Джонса для излучения, поступающего на поляризационный светоделитель при совпадении базисов (излучение на выходе Алисы соответствует таковому из формулы (4):

$$Lout(45°) = QWP(45°) * e^{i*\frac{\pi}{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = e^{i*\frac{\pi}{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (6)$$

Пример вычисления вектора Джонса для излучения, поступающего на поляризационный светоделитель при несовпадении базисов:

$$Lout(0°) = QWP(0°) * e^{i*\frac{\pi}{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} e^{i*\frac{\pi}{2}} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad (7)$$

Как видно из результатов расчета формул 6 и 7, углы поворота четвертьволновой пластины ЧВ3 были определены верно.

Приведенное в статье математическое моделирование поляризационных состояний в разрабатываемой лабораторной установке имитаторе КРК подтвердило правильность выбранной схемы.

**Список используемых источников**

1. Бразовский Г. Р., Исупов А. И., Былина М. С. Лабораторная работа по исследованию влияния поляризаторов на одиночные фотоны в интерферометре Маха-Цендера // 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. 454–458. EDN: KPKBYS.

2. Bennett C. H. and Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984. PP. 175–179.

3. Аззам Р., Башара Н. Эллипсометрия и поляризованный свет / Пер. с англ. под ред. А. В. Ржанова, К. К. Свиташева. Москва: Мир, 1981. 583 с.

*Статья представлена научным руководителем, доцентом кафедры ОКСС СПбГУТ, кандидатом технических наук М. С. Былиной.*

## SIMULATION OF POLARIZATION STATES IN THE QKD SIMULATOR

***Brazovsky G., Shevtsova A., Yatskova A.***
*The Bonch-Bruevich Saint Petersburg State University of Telecommunications*

*Providing laboratory practice in the framework of disciplines providing training for quantum communications is a difficult task. Using real hardware is hampered by its cost and rarity. There are two possible solutions to this problem: the creation of physical simulators and virtual laboratories. The paper simulates the polarization states of light in a simulator of the QKD system currently being created in the laboratory.*

***Key words:*** *Quantum communications, quantum key distribution*

**УДК 621.391**
**ГРНТИ 49.43.31**

# ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПОЛОСЫ ПРОПУСКАНИЯ ФИЛЬТРА НА Q-ФАКТОР В СИСТЕМАХ КОГЕРЕНТНОЙ ОПТИЧЕСКОЙ СВЯЗИ С МОДУЛЯЦИЕЙ M-QAM

**М. С. Былина, Л. А. Гнедов, М. В. Никитин**

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

*В статье рассмотрено влияние полосы пропускания фильтра на качество передачи сигнала в волоконно-оптических системах связи с использованием квадратурно-амплитудной модуляции и когерентного приема. Актуальность исследования обусловлена необходимостью повышения пропускной способности современных магистральных линий связи и обеспечения высокой спектральной эффективности при передаче больших объемов данных.*

*Целью работы является исследование зависимости Q-фактора от ширины полосы пропускания фильтра в когерентной многопролетной ВОСС при использовании различных форматов модуляции M-QAM. моделирование проводилось в программной среде OptiSystem. Модель включает оптический передатчик с DP-QAM модуляцией, волоконно-оптическую линию связи с оптическими усилителями EDFA, а также когерентный приемник с цифровой обработкой сигнала (DSP).*

*В работе проведен сравнительный анализ характеристик систем с различными форматами модуляции, определены оптимальные полосы пропускания фильтров, обеспечивающие наилучшее качество передачи сигнала.*

***волоконно-оптическая система связи, ВОСС, когерентный прием, квадратурно-амплитудная модуляция, M-QAM, Q-фактор, BER, OptiSystem, цифровая обработка сигнала, полоса пропускания фильтра, OSNR, оптические усилители, DP-QAM***

В современных волоконно-оптических системах связи (ВОСС) для повышения пропускной способности и спектральной эффективности широко применяются когерентный прием и многоуровневые форматы квадратурной амплитудной модуляции (QAM – Quadrature Amplitude Modulation). Использование данных технологий позволяет передавать большие объемы информации на высоких скоростях при ограниченной полосе частот [1].

QAM представляет собой метод модуляции, при котором передача информации осуществляется символами, характеризующиеся определенными значениями амплитуды и фазы оптического излучения. Одним символом может быть закодировано от 2 до 8 бит информации [2]. QAM сигнал принято представлять на фазовой плоскости, образованной синфазной (I) и квадратурной (Q) осями, в виде так называемого сигнального созвездия

В данной работе рассматриваются форматы модуляции 16QAM, 32QAM, 64QAM и 128QAM (рис. 1).

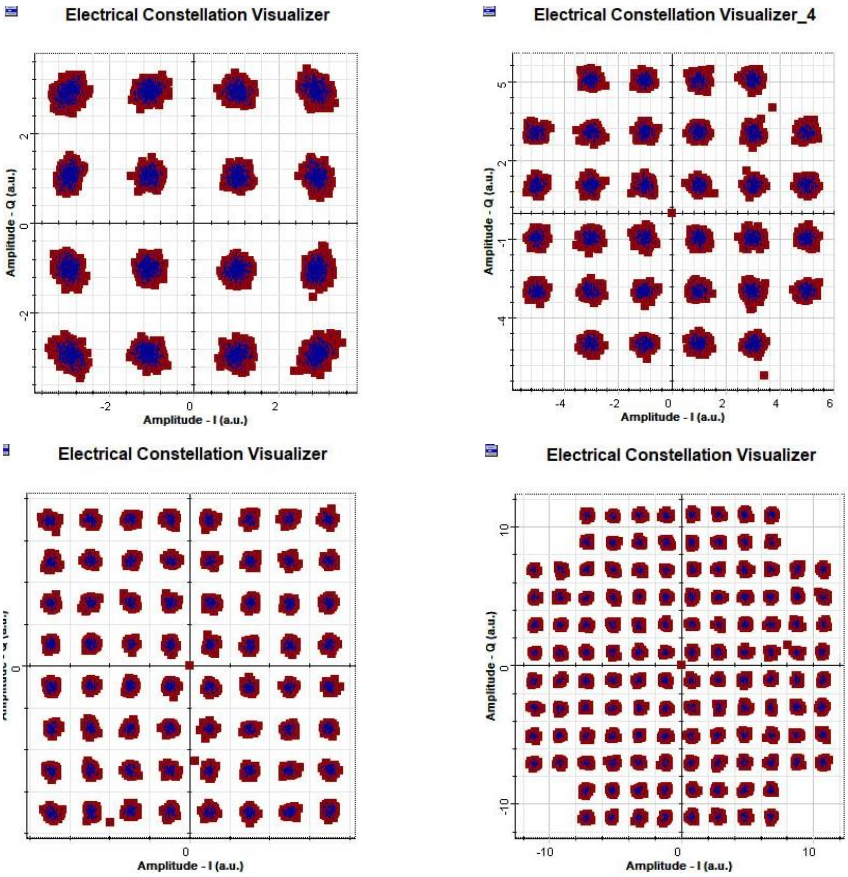



Рис. 1. Сигнальные созвездия QAM16, QAM32, QAM64, QAM128

Увеличение порядка модуляции позволяет повысить спектральную эффективность системы связи, однако приводит к уменьшению расстояния между символами в сигнальном созвездии и повышению чувствительности системы к шумам и искажениям [3].

Схема, моделируемой ВОСС в программе OptiSystem [4], представлена на рис. 2. Она содержит: передатчик M-QAM сигнала, где M-количество разных символов, усилители мощности, волоконно-оптический линейный тракт, содержащий два пролета длиной 80 километров с линейными усилителями, гауссовский фильтр, когерентный приемник и измерительные приборы.

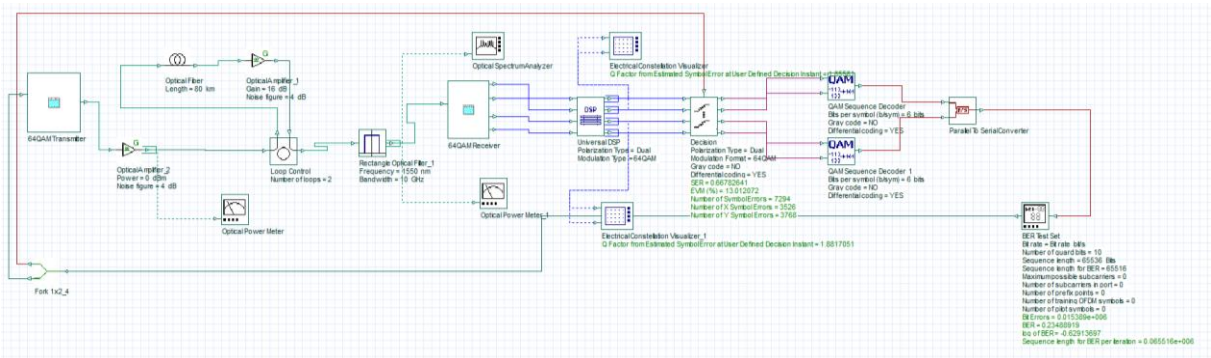


Рис. 2. Исследуемая схема ВОСС

Принцип когерентного приема основан на интерференции принимаемого оптического сигнала с излучением локального лазера. Это позволяет восстановить амплитудную и фазовую информацию сигнала, необходимую для корректного приема многоуровневых форматов модуляции. Когерентный прием обеспечивает высокую чувствительность системы и возможность применения цифровой обработки сигнала (DSP-расшифровка), используемой для компенсации шумов и искажений, возникающих в процессе передачи, усиления и приема сигнала.

Для оценки качества связи используется символьный Q-фактор – параметр, показывающий, насколько хорошо принимаемые символы отделены друг от друга на сигнальном созвездии [5]. Из-за шумов и искажений точки символов начинают «размываться» и могут попадать в соседние области созвездия, что приводит к ошибкам распознавания. Чем больше Q-фактор, тем меньше пересечение соседних символов и тем выше качество связи.

Q-фактор связан с вероятностями символьных и битовых ошибок (BER):

$$p_{e\_m,k} = \frac{1}{2} \cdot \mathrm{erfc}\left(\frac{Q_{\mathrm{m,k}}}{\sqrt{2}}\right); \quad (1)$$

где $p_{e(m,k)}$ – вероятность ошибки при приеме, когда символ $m$ был ошибочно распознан как символ $k$; $Q_{(m,k)}$ – $Q$-фактор для пары символов $m$ и $k$, характеризующий степень разделения этих символов на сигнальном созвездии; erfc() – дополнительная функция ошибок, используемая для расчета вероятности ошибок при гауссовском шуме; $\sqrt{2}$ – нормирующий коэффициент.

Для получения вероятности ошибок не более $10^{-12}$ необходимо обеспечить значение Q-фактора не менее 3 до исправления ошибок помехоустойчивыми кодами.

Очень важную роль в формировании Q-фактора играет OSNR (Optical Signal-to-Noise Ratio), то есть отношение оптической мощности сигнала к мощности шума в полосе принятого сигнала. При низком OSNR значительный уровень шумов приводит к падению Q-фактора [6].

В работе проведено исследование зависимости Q-фактора от ширины полосы пропускания гауссовского фильтра. Параметры исследуемой ВОСС представлены в таблице 1.

ТАБЛИЦА 1. Параметры исследуемой ВОСС

| | | | |
|---|---|---|---|
| Скорость передачи данных | 112e009 бит/с | Скорость передачи символов (QAM64) | 9.33e009 символ/с |
| Длина последовательности | 65536 бит | Скорость передачи символов (QAM128) | 8e009 символ/с |
| Отсчетов на бит | 4 | OSNR(QAM32) | 18 dB |
| Защитные биты | 10 | OSNR(QAM128) | 18 dB |
| Скорость передачи символов (QAM16) | 14e009 символ/с | Мощность сигнала | 0 dBm |
| Скорость передачи символов (QAM32) | 11e009 символ/с | Длина волны канала | 1550 нм |
| Коэффициент дисперсии | 16.75 пс/нм×км | Длина линии | 160 км |
| Коэффициент шума усилителя | 4 dB | Мощность накачки усилителя | 16 dB |

Основные результаты исследования представлены на графиках (рис. 3).

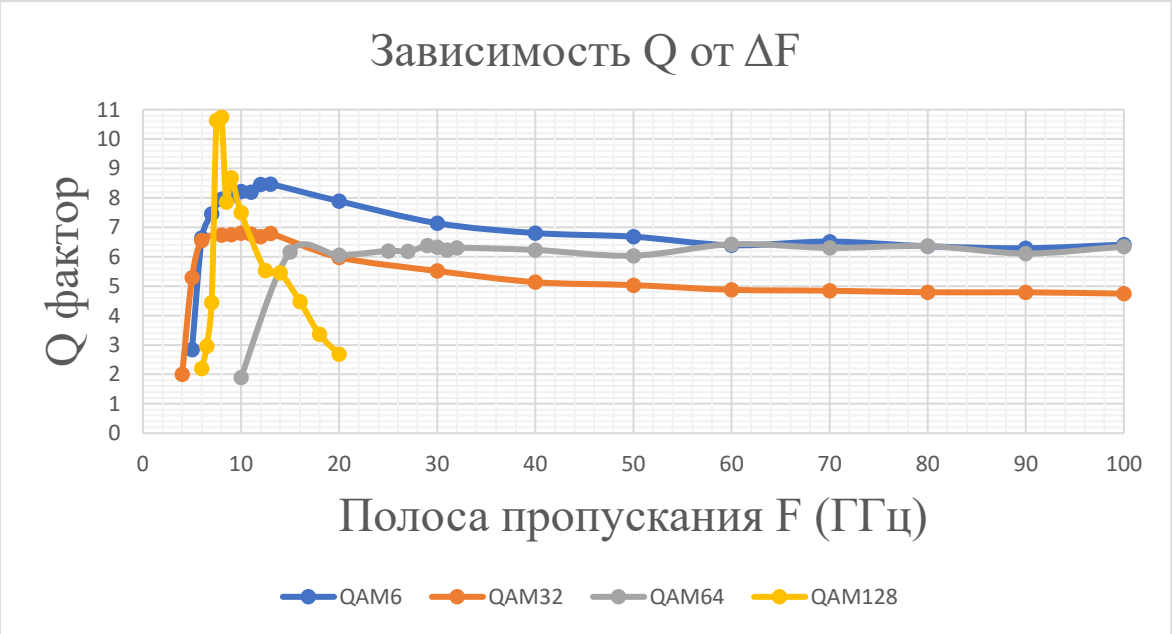



Рис. 3. Результаты исследования

Из графиков видно, что для каждого из рассмотренных форматов модуляции существует оптимальное значение полосы пропускания фильтра, при котором обеспечивается наилучшее качество передачи. Ухудшение качества при расширении сверх оптимального значения обусловлено попаданием в полосу приема шумов усилителей. Из графиков также видно, что модуляция QAM128 наиболее чувствительна к настройкам фильтрации.

## Список используемых источников

1. Трещиков В. Н., Листвин В. Н. DWDM – системы. М.: Техносфера, 2021. 420 с.

2. Былина М. С., Глаголев С. Ф. Обзор методов оценки качества связи и современных транспортных высокоскоростных волоконно-оптических систем связи // Современные средства связи 2025. С. 166-168.

3. Величко М. А., Наний О. Е., Сусьян А. А. Новые форматы модуляции в оптических системах связи // LIGHTWAVE Russian Edition. 2005. № 4. С. 21-36.

4. OptiSystem. Tutorial – Volume 1. Version 14. URL:http://optiwave.com (дата обращения 10.05.2026).

5. Леонов А., Наний О. Е., Трещиков В. Н. Совершенствование форматов модуляции в оптических системах связи DWDM // Первая миля. 2019. № 8. С. 30-36.

6. Былина М. С., Глаголев С. Ф. Оценка качества связи в современных высокоскоростных волоконно-оптических системах // Актуальные проблемы инфотелекоммуникаций в науке и образовании. XII Международная научно-техническая и научно-методическая конференция (АПИНО-2023); сб. науч. ст. в 4 т. С. 209-214.

## INVESTIGATION OF THE EFFECT OF FILTER BANDWIDTH ON THE Q-FACTOR IN COHERENT OPTICAL COMMUNICATION SYSTEMS WITH M-QAM MODULATION

**Bylina M., Gnedov L., Nikitin M.**
The Bonch-Bruevich Saint-Petersburg State University of Telecommunication

*The article examines the effect of the filter bandwidth on the quality of signal transmission in fiber-optic communication systems (VOSS) using quadrature amplitude modulation (QAM) and coherent reception. The relevance of the study is due to the need to increase the throughput of modern backbone communication lines and ensure high spectral efficiency when transmitting large amounts of data. One of the key factors affecting the quality of signal transmission is the choice of the filter bandwidth, which determines the level of intersymbol and noise distortion in the system.*

*The aim of the work is to study the dependence of the Q-factor on the filter bandwidth in a coherent multi-span VOSS using various M-QAM modulation formats). The scheme of a coherent optical transmission system implemented in the OptiSystem software environment is chosen as the object of modeling. The model includes an optical transmitter with DP-QAM modulation, a fiber-optic communication line with EDFA optical amplifiers, as well as a coherent receiver with digital signal processing (DSP).*

*In the course of the work, the system was modeled when changing the bandwidth of the Gaussian filter and different QAM modulation orders. Special attention is paid to the study of changes in the Q-factor with varying filtration parameters. A comparative analysis of the characteristics of systems with different modulation formats has been performed, and the bandwidth ranges ensuring optimal signal transmission quality have been determined.*

***Key words:*** *fiber-optic communication system, VOSS, coherent reception, quadrature amplitude modulation, M-QAM, Q-factor, BER, OptiSystem, digital signal processing, Gaussian filter, filter bandwidth, OSNR, optical amplifiers, DP-QAM,OSNR*

**УДК 681.518.5**
**ГРНТИ 50.47.31**

# РАЗРАБОТКА БЛОКА УПРАВЛЕНИЯ ОСВЕЩЕНИЕМ СОВРЕМЕННОГО ЛОГИСТИЧЕСКОГО ЦЕНТРА

**А. В. Ваганов, С. А. Чистый**

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

*В данной работе рассматриваются вопросы разработки блока управления для автоматизированной системы освещения промышленных помещений на базе программируемых логических интегральных схем. Обоснована актуальность внедрения автоматизированных систем управления освещением, позволяющих минимизировать энергетические затраты для предприятий в соответствии с нормами энергосбережения. Приведено описание структурной схемы системы, а также обобщенного алгоритма ее работы. Представлен пример расчета тракта предварительной обработки сигналов от первичного измерительного преобразователя (датчика) и обоснован выбор элементной базы для реализации устройства. Продемонстрирован пример моделирования работы фотометрического датчика в специализированных программных средах, позволяющий осуществлять предварительную настройку и отладку системы.*

***программируемые логические интегральные схемы, автоматизированная система освещения, энергосбережение, логистический центр, датчики, блок управления***

## Введение

Эффективным способом снижения расходов электроэнергии промышленными предприятиями является минимизация ее затрат на освещение помещений. В соответствии с законодательством об энергосбережении, внедрение автоматизированных систем позволяет оптимизировать расход ресурсов при сохранении комфортных условий труда [1-4]. Существующие готовые решения часто отличаются избыточной сложностью, громоздкостью структуры и высокой стоимостью эксплуатации, что делает их труднодоступными для небольших организаций. Целью данной работы является разработка бюджетного и гибкого блока управления на базе программируемых логических интегральных схем (ПЛИС), адаптированного под нужды современного логистического центра.

## Обоснование выбора элементной базы

Для реализации логики управления была выбрана ПЛИС типа CPLD семейства MAX II (модель EPM570). Данный выбор обусловлен тем, что

CPLD лучше подходят для схем управления с комбинационной логикой и начинают работу мгновенно после подачи питания, в отличие от FPGA.

Для определения уровня внешней освещенности в системе используются специализированные датчики – фотодиоды. В ходе проектирования был проведен сравнительный анализ доступных компонентов, представленных в таблице 1.

ТАБЛИЦА 1 – Основные характеристики используемых фотодиодов

| Параметр | SFH 203 FA | BPW20RF | BPV10NF |
|---|---|---|---|
| Длина волны (максимальная чувствительность), нм | 900 | 1040 | 940 |
| Темновой ток, нА | 1 | 2 | 1 |
| Угловая апертура, град | +/- 20 | +/- 50 | +/- 20 |

На основании анализа был выбран фотодиод SFH 203 FA, обладающий достаточной чувствительностью в видимой области, а также в ближнем инфракрасном диапазоне оптического излучения.

## Структурная схема системы

Кроме датчика освещенности, автоматизированная система включает в себя также датчики присутствия, движения и освещенности, блок управления и терминал мониторинга. Блок управления является центральным узлом, осуществляющим сбор данных с периферийных устройств и формирование управляющих сигналов. На рисунке 1 представлена общая структура блока управления освещением с учетом взаимодействия его компонентов.

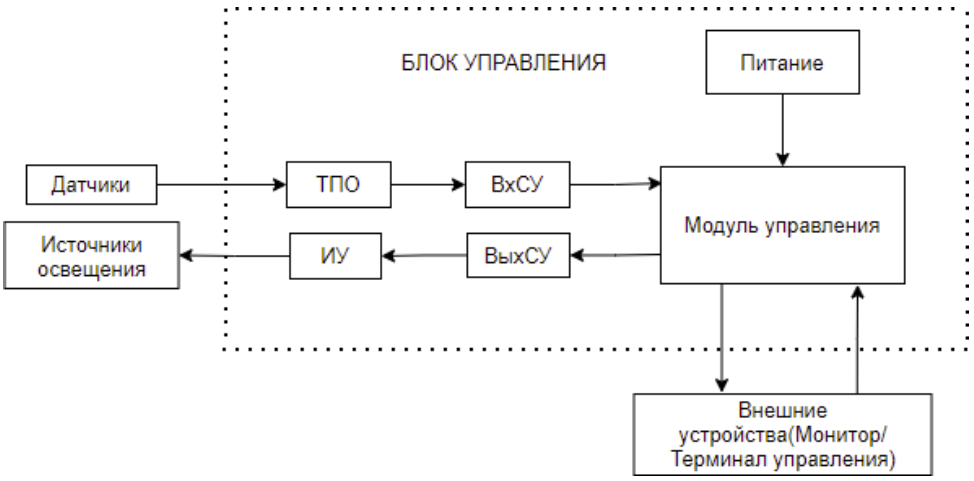



Рис. 1. Структурная схема блока управления автоматизированной системы освещения

**Упрощенный расчет тракта предварительной обработки сигнала**

Для усиления малого тока фотодиода (порядка микроампер) используется трансимпедансный усилитель (TIA). Выходное напряжение TIA определяется выражением:

$$U_{\text{вых}} = -I_{\text{вых}} R_{\text{ос}},$$

где $I_{\text{вых}}$ – ток фотодиода, $R_{\text{ос}}$ – сопротивление обратной связи.

При условии, что $R_{\text{ос}}$ = 10 кОм и уровне максимальной внешней освещенности (солнечный день): 750 лк (ток 50 мкА), выходное напряжение составит 0,5 В.

Для минимизации помех, присутствующих в сигнале от фотоприемника, применен активный фильтр нижних частот (ФНЧ) второго порядка Саллена-Ки с частотой среза равной 10 Гц (верхний порог частоты полезного сигнала). Расчет номиналов его элементов производится по следующей зависимости:

$$\tau = R \cdot C = \frac{1}{2\pi f_{\text{в}}} = \frac{1}{2*3{,}14*10} = 0{,}016 \text{ с},$$

где τ = R·C – постоянная времени фильтра.

Таким образом, при величине $R$ = 10 кОм значение $C$ составит около 1 мкФ.

**Алгоритмы функционирования системы**

Логика работы блока управления адаптирована под три типа зон.

1. Рабочие места (АРМ): освещение включается при наличии персонала или по расписанию. При уровне ниже 750 лк активируется основной свет, ниже 500 лк – дополнительный.

2. Складские секции: реализовано дежурное фоновое освещение (50 лк). При срабатывании датчиков движения освещение переходит в основной режим (200 лк).

3. Коридоры: используется алгоритм плавного включения и выключения светильников по ходу движения человека с использованием широтно-импульсной модуляции.

На рисунке 2 представлен обобщенный алгоритм работы устройства.

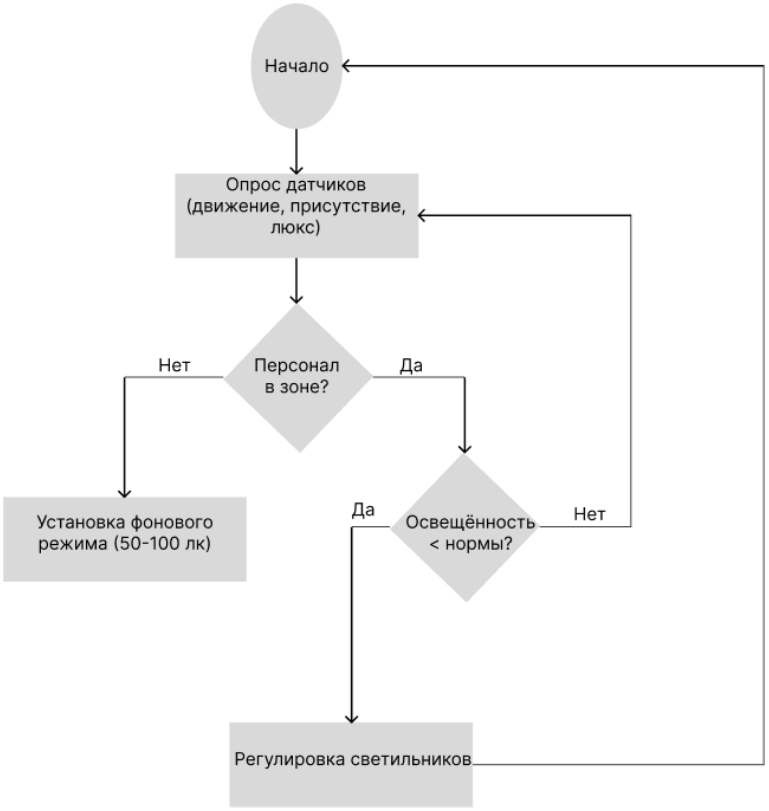



Рис. 2. Обобщенный алгоритм работы системы

## Пример моделирования фотометрического датчика системы

Моделирование элементов ТПО осуществлялось в специализированной среде Multisim. На рисунке 3 показан результат эмулирования работы датчика SFH 203 FA для трех вариантов его освещенности: 200; 500 и 750 лк.

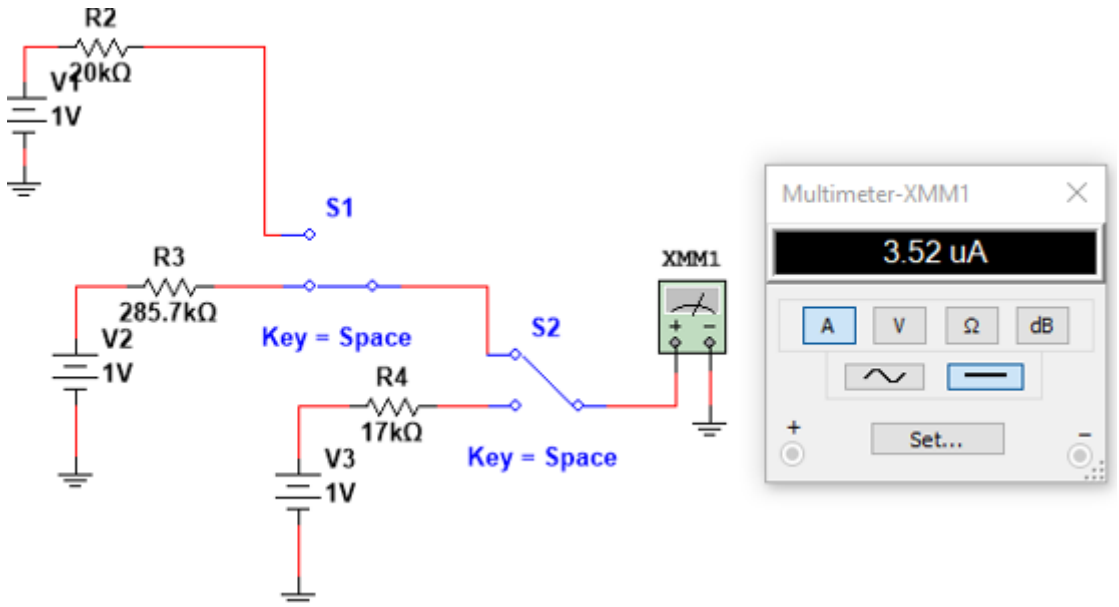



Рис. 3. Эмуляция показаний датчика при уровне его освещенности равной 500 лк

Глобальное исследование ТПО подтвердило эффективное подавление высокочастотных помех (более 100 Гц), а также корректность функционирования всей системы в целом. Функциональное моделирование цифровой части блока управления освещением выполнялось в среде Quartus II и Vector Waveform File.

## Заключение

Описанный в статье блок управления обеспечивает эффективное управление системой освещения предприятия благодаря развитой системе сенсоров, а также адаптивных алгоритмов анализа и управления источниками освещения рабочих мест персонала. Такое сочетание позволяет существенно снизить энергопотребление и эксплуатационные расходы, обеспечивая высокую надежность и ремонтопригодность системы.

Концепция построения блока управления, выбор элементной базы, а также рекомендации к его моделированию могут найти применение при разработке различных автоматизированных систем современного предприятия.

**Список используемых источников**

1. СП 52.13330.2016 «Естественное и искусственное освещение». М.: Стандартинформ, 2018. 121 с.

2. Алейник А. С., Востриков Е. В. Основы схемотехники приемопередающих электронных устройств. СПб: Университет ИТМО, 2021. 149 с.

3. Акчурин А. Д., Юсупов К. М., Колчев А. А. Основы работы в среде Quartus II. Казань: КФУ, 2017. 49 с.

4. ГОСТ Р 55710-2013 «Освещение рабочих мест внутри зданий. Нормы и методы измерений».

## DEVELOPMENT OF A LIGHTING CONTROL UNIT FOR A MODERN LOGISTICS CENTER

**Vaganov A., Chistiy S.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper explores the design and implementation of a control unit for an automated lighting system in industrial premises based on programmable logic integrated circuits. The relevance of adopting automated lighting control systems to minimize enterprise energy consumption in compliance with energy-saving regulations is substantiated. The structural diagram of the system, including motion, presence, and light intensity sensors, is described. Mathematical calculations for the analog signal preprocessing path and operational algorithms for various functional zones of a logistics center are presented. Modeling of the developed units in specialized software environments was conducted, confirming the effectiveness of the proposed technical solutions.*

***Key words:*** *programmable logic integrated circuits, automated lighting system, energy saving, logistics center, sensors, control unit*

**УДК 621.311.24**
**ГРНТИ 49.33.29**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕД СХЕМОТЕХНИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ ПРОЕКТИРОВАНИЯ ГИБРИДНЫХ СИСТЕМ ЭЛЕКТРОПИТАНИЯ ОБЪЕКТОВ РАДИОСВЯЗИ

**П. Ю. Виноградов, Р. А. Михайлов**

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

*Внедрение перспективных сетей подвижной радиосвязи пятого поколения сопровождается существенным ростом энергопотребления базовых станций и ужесточением требований к их отказоустойчивости. Для автономных и удаленных объектов радиосвязи безальтернативным решением становится применение гибридных систем электропитания, сочетающих возобновляемые источники энергии, накопители и резервные генераторы. Проектирование таких комплексов требует высокоточного схемотехнического моделирования силовых преобразователей, алгоритмов отбора мощности и переходных процессов. В статье представлен обзор и сравнительный анализ систем автоматизированного проектирования для моделирования электрических цепей. Рассматриваются классические зарубежные симуляторы, а также отечественные программные продукты, включая среды динамического моделирования. Проведена оценка их функциональных возможностей и адекватности решателей для обоснования выбора инструментария при проектировании энергоэффективной инфраструктуры телекоммуникаций.*

***гибридные системы электропитания, базовая станция, схемотехническое моделирование, силовая электроника, программа моделирования, программное обеспечение***

Масштабное развертывание сетей 5G привело к резкому скачку плотности мощности радиооборудования. Если в сетях LTE потребление макроплощадки редко превышало 3-4 кВт, то современные блоки Massive MIMO и активные антенные системы AAU поднимают планку пиковой нагрузки до 12-15 кВт [1, 2]. В таких условиях шина питания испытывает серьезный динамический стресс при колебаниях трафика.

Для площадок без доступа к центральным сетям единственным выходом остаются гибридные системы электропитания (ГСЭП). Проектировщик сталкивается с задачей: как объединить солнце, ветер и АКБ так, чтобы оборудование не отключилось в момент резкого роста нагрузки. Статичного расчета баланса мощностей здесь уже недостаточно – нужны динамические

модели, способные предсказать поведение токов и напряжений за доли миллисекунд. Сегодня перед российскими инженерами стоит дополнительная преграда: необходимость быстрого перехода с привычного западного софта на отечественные платформы.

## 1. Инструментарий схемотехнического уровня

Проектирование силовой части ГСЭП традиционно начинается на уровне SPICE-моделей. Здесь критически важна точность отображения пульсаций и фронтов переключения транзисторов.

Признанным стандартом считается LTspice [3]. Программа подкупает скоростью и обширной базой компонентов, позволяя детально анализировать потери в узлах преобразования. Однако закрытость исходного кода и отсутствие официальной поддержки в РФ вынуждают искать замену.

Российским аналогом в области анализа систем силовой электроники выступает программный комплекс Fastmean. Его отличительной особенностью является использование оригинальных численных методов («метод быстрых средних»), оптимизированных для расчета установившихся режимов в преобразователях напряжения. Fastmean позволяет значительно сократить время анализа переходных процессов в импульсных схемах по сравнению с классическими SPICE-решателями, что делает его эффективным инструментом для оперативной отладки алгоритмов управления силовыми каскадами ГСЭП [4].

## 2. Системный анализ и цифровые двойники

Когда фокус смещается со схемы на анализ всей системы (энергобаланс за сутки, нагрев АКБ), требуются среды мультифизичного моделирования. Эталоном здесь выступает связка MATLAB/Simulink и библиотеки Simscape. Она позволяет моделировать батарею не как «черный ящик», а как живой химический объект с учетом температуры и износа.

В рамках импортозамещения авторы изучили платформу Engee. Это российское облачное решение, которое повторяет логику блочного моделирования MATLAB. Важно, что Engee позволяет использовать готовые наработки и библиотеки физических блоков, обеспечивая независимость от зарубежных лицензионных серверов и сохраняя высокую точность прогнозирования суточной автономности объекта [5].

### 3. Сравнительная характеристика программного обеспечения

Для выбора оптимального инструментария на различных этапах проектирования ГСЭП необходимо учитывать специфику решаемых задач. Сравнение рассмотренных программных сред представлено в таблице 1.

ТАБЛИЦА 1. Сравнительные характеристики программных комплексов

| Критерий оценки | LTspice | Fastmean | MATLAB | Engee |
|---|---|---|---|---|
| Уровень моделирования | Схемотехнический | Схемотехнический | Системный | Системный |
| Объект моделирования | Компонент (SPICE) | Электрическая цепь | Цифровой двойник | Цифровой двойник |
| Мультифизика | Ограничена | Нет | Полная поддержка | Полная поддержка |
| Правовой статус | Зарубежное ПО | Отечественное ПО | Зарубежное ПО | Отечественное ПО |
| Среда запуска | Локальное прил. | Локальное прил. | Локальное прил. | Облачная (Web) |

Как показано в таблице 1, для детальной отладки силовых преобразователей целесообразно использование Fastmean, тогда как для комплексного анализа поведения ГСЭП в течение длительных интервалов времени и внедрения алгоритмов управления оптимальным выбором является платформа Engee.

### Заключение

В ходе проведенного обзора показано, что современный рынок программного обеспечения предоставляет широкий спектр инструментов для проектирования систем электропитания объектов радиосвязи. Выявлено, что переход от зарубежных продуктов (LTspice, MATLAB) к отечественным аналогам (Fastmean, Engee) технически оправдан и позволяет решать задачи проектирования без потери точности и функциональности. Применение двухуровневого подхода – от схемотехнической оптимизации узлов в Fastmean к системному анализу в Engee – позволяет создавать эффективные и надежные гибридные системы электропитания в рамках реализации стратегии технологической независимости телекоммуникационной отрасли.

**Список используемых источников**

1. Михайлов Р. А. Исследование эффективности солнечных батарей в качестве источника электропитания для базовых станций. ВКР бакалавра. СПбГУТ. СПб, 2023.
2. Михайлов Р. А. Разработка и исследование системы электропитания на альтернативных источниках для объекта радиосвязи. Магистерская диссертация. СПбГУТ. СПб, 2025.
3. Simulation Program with Integrated Circuit Emphasis (SPICE) // Документация LTspice. URL: https://www.analog.com/en/design-center/design-tools-and-calculators/ltspice-simulator.html (дата обращения: 12.05.2026).
4. Амелин С. А. Моделирование систем силовой электроники в программе Fastmean. Смоленск: Изд-во СмолГУ, 2011. 144 с.
5. Платформа математического моделирования Engee // Engee: официальный сайт. URL: https://engee.com/ (дата обращения: 12.05.2026).

## COMPARATIVE ANALYSIS OF CIRCUIT SIMULATION ENVIRONMENTS FOR DESIGNING HYBRID POWER SUPPLY SYSTEMS FOR RADIO COMMUNICATION FACILITIES

**Vinogradov P., Mikhailov R.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The implementation of advanced fifth-generation (5G) mobile networks is accompanied by a significant increase in base station power consumption and more stringent reliability and fault tolerance requirements. For autonomous and remote radio communication sites, the use of hybrid power supply systems–combining renewable energy sources, energy storage units, and backup generators–is becoming an indispensable solution. Designing such systems requires high-precision circuit-level simulation of power converters, maximum power point tracking algorithms, and transient processes. This article provides an overview and comparative analysis of computer-aided design (CAD) systems for electric circuit simulation. Both classic foreign simulators and domestic software products, including dynamic simulation environments, are examined. The study evaluates their functional capabilities and solver adequacy to justify the selection of software tools for designing energy-efficient telecommunications infrastructure.*

***Key words:*** *hybrid power supply systems, base station, circuit simulation, power electronics, simulation software, software*

**УДК 004.8**
**ГРНТИ 20.51.19**

# ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЭКСПЛУАТАЦИОННОГО УПРАВЛЕНИЯ СЕТЯМИ ПЯТОГО ПОКОЛЕНИЯ

**А. Б. Гольдштейн, А. Р. Камаев, Р. Ф. Рафикова**

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

*В статье рассматривается применение методов искусственного интеллекта для эксплуатационного управления сетями пятого поколения. Актуальность темы связана с ростом сложности 5G/IMT-2020, внедрением программно-конфигурируемых сетей, виртуализацией сетевых функций и необходимостью обработки больших объемов телеметрии. На основе анализа отечественных и зарубежных публикаций рассматриваются задачи мониторинга, прогнозирования трафика, выявления аномалий, управления ресурсами и поддержки качества обслуживания. Показано, что искусственный интеллект целесообразно рассматривать не как отдельную надстройку над сетью, а как часть контура эксплуатационного управления, связанного с системами OSS/BSS, SDN/NFV, MEC и оркестрацией сетевых функций.*

***искусственный интеллект, сети 5G, эксплуатационное управление, машинное обучение, SDN, NFV, прогнозирование трафика, QoS***

## Введение

Переход к сетям пятого поколения изменил представление об эксплуатации телекоммуникационной инфраструктуры. Если в сетях предыдущих поколений значительная часть задач управления могла решаться на основе заранее заданных правил и регламентов, то для 5G такой подход становится недостаточным. Это связано не только с ростом скорости передачи данных, но и с появлением принципиально разных классов услуг: высокоскоростного мобильного доступа, массового интернета вещей, сервисов с ультрамалыми задержками и повышенными требованиями к надежности. В результате оператору необходимо одновременно контролировать состояние радиодоступа, транспортной сети, ядра, виртуализированных сетевых функций, вычислительных ресурсов и пользовательских сервисов.

В работах, посвященных искусственному интеллекту в сетях связи, подчеркивается, что функциональная сложность сетей 5G возрастает на порядок по сравнению с существующими сетями, а эффективная эксплуатация

такой инфраструктуры требует применения методов машинного и глубокого обучения [1].

Общетеоретическая основа такого подхода связана с тем, что искусственный интеллект применяется для решения задач, где заранее неизвестен полный алгоритм решения или где традиционные математические методы становятся недостаточно эффективными из-за объема данных, неопределенности и большого числа ограничений [2].

При этом усложнение эксплуатационного управления связано не только с ростом объема данных, но и с изменением самой природы инфокоммуникационных сетей. В современных сетях связи одновременно проявляются мультисервисность, гетерогенность и клиентоцентричность, что приводит к росту событийности и ситуативности управления [3]. Изменение нагрузки в одном сегменте способно влиять на состояние других сегментов сети, а разнообразие пользовательских сценариев требует все более гибкой адаптации сетевых политик и параметров обслуживания.

В этих условиях традиционные OSS/BSS-системы и классические механизмы мониторинга уже не обеспечивают необходимой скорости реакции и адаптивности. Как отмечается в работе Б. С. Гольдштейна и А. Б. Гольдштейна [3], сети Beyond 5G требуют перехода к когнитивному управлению, основанному на принципах самоорганизации, автоматизации и использовании методов искусственного интеллекта и машинного обучения. Таким образом, применение ИИ в сетях 5G связано не только с обработкой телеметрии, но и с трансформацией всей архитектуры эксплуатационного управления.

## Технологические предпосылки внедрения ИИ в управление 5G

Возможность практического применения искусственного интеллекта в сетях связи связана с развитием нескольких технологических направлений. Во-первых, это программно-конфигурируемые сети SDN, которые разделяют плоскость управления и плоскость передачи данных. Благодаря этому появляется возможность централизованно получать информацию о потоках, маршрутах и состоянии сетевых элементов, а также программно воздействовать на поведение сети. Во-вторых, это виртуализация сетевых функций NFV, позволяющая разворачивать сетевые функции в виде программных компонентов, масштабировать их и переносить между вычислительными узлами. В-третьих, это развитие систем сбора данных, включая

DPI, мониторинг ресурсов, журналы событий, данные OSS/BSS и телеметрию виртуальной инфраструктуры.

В статье И. Г. Малыгина, А. А. Тарабаева и М. Ю. Аванесова предложена архитектура интеллектуальной сети связи, включающая интеллектуальную, агентскую и бизнес-плоскости [4]. Интеллектуальная плоскость отвечает за анализ данных и выработку управляющих решений, агентская плоскость обеспечивает обмен информацией между интеллектуальными модулями и сетевыми компонентами, а бизнес-плоскость включает реальные сети, сервисы и системы управления.

Данный подход соответствует современным концепциям автоматизированного управления сетями связи, в том числе ETSI Zero-touch Service Management. В таких системах методы искусственного интеллекта и машинного обучения используются как элементы замкнутого цикла управления [3]. Эксплуатационная система при этом не ограничивается наблюдением за состоянием сети, а может формировать и выполнять корректирующие действия.

В работе А. С. Бородина, А. Н. Волкова, А. С. Мутханны и А. Е. Кучерявого рассматривается применение машинного обучения в перспективных сетях связи, включая IMT-2020 [5]. Авторы обращают внимание на представленный в рекомендациях МСЭ-Т конвейер машинного обучения. Он охватывает сбор и обработку данных, обучение и применение модели, а также оркестрацию соответствующих функций.

**Направления применения в эксплуатационном управлении**

Одной из основных областей применения искусственного интеллекта является мониторинг состояния сети. Традиционный мониторинг обычно основан на проверке отдельных пороговых значений, например загрузки интерфейсов, процессоров и памяти, уровня задержек или потерь пакетов. Вместе с тем неисправность не всегда сопровождается резким изменением одного показателя. Нередко ее развитию предшествуют несколько незначительных отклонений, которые по отдельности не воспринимаются как критические. Методы машинного обучения позволяют анализировать такие комбинации признаков и выявлять отклонения раньше, чем они приведут к заметному ухудшению качества обслуживания.

Особую актуальность это приобретает для систем Fault Management и Assurance. В современных сетях связи требования к эксплуатационному управлению включают минимизацию времени обнаружения неисправности

(MTTD) и времени восстановления (MTTR), а также автоматизированный поиск корневой причины инцидента (Root Cause Analysis) [3].

Второе направление связано с прогнозированием трафика и нагрузки. Для сетей 5G эта задача имеет не только исследовательский, но и практический характер. Оператору необходимо заранее понимать, где может возникнуть перегрузка, какие сегменты требуют масштабирования, когда нужно перераспределить ресурсы между сетевыми срезами или перенести часть функций ближе к пользователю. В работе Р. Абделлаха Али и А. Е. Кучерявого отмечается, что прогнозирование трафика с использованием нейронных сетей, включая NARX, RNN и LSTM, может применяться для повышения эффективности QoS и планирования ресурсов [1]. Для эксплуатационного управления это означает переход от реакции на уже возникшую проблему к предупреждающим действиям.

Третье направление – обнаружение аномалий и инцидентов безопасности. В условиях 5G сеть обслуживает большое число устройств и сервисов, в том числе IoT-устройств, которые могут генерировать нестандартные или вредоносные потоки данных. В источниках по теме подчеркивается, что ИИ может применяться для распознавания атак, анализа поведения и формирования опережающей реакции [4]. На практике это может выражаться в выявлении DDoS-активности, нетипичного поведения пользовательского оборудования, аномальной сигнализации или подозрительных изменений в управляющем трафике.

Четвертое направление связано с управлением ресурсами. В сетях 5G эксплуатационное управление должно учитывать не только физические ресурсы, но и виртуальные: вычислительные мощности, ресурсы хранения, пропускную способность, сетевые функции и срезы сети. Использование ИИ позволяет строить более гибкие механизмы балансировки нагрузки, выбора места размещения виртуальных сетевых функций и распределения ресурсов MEC. При этом важным становится не только само решение модели, но и возможность его выполнения через существующие системы оркестрации.

В перспективе такие механизмы могут развиваться в сторону сетей, основанных на намерениях (Intent-Based Networking, IBN), где оператор задает не конкретные параметры конфигурации, а требуемый результат функционирования сети [3]. В рамках IBN интеллектуальная система получает описание требуемого состояния сети и на его основе выбирает необходимые управляющие действия.

Не менее важной задачей является обеспечение качества обслуживания и качества восприятия услуги пользователем. Контроля отдельных технических показателей для этого недостаточно, так как одинаковое значение одной и той же метрики может по-разному влиять на различные приложения. Например, определенный уровень задержки может не оказывать заметного влияния на передачу файлов, но быть неприемлемым для сервисов реального времени. По этой причине при анализе состояния сети необходимо учитывать не только значения технических параметров, но и требования конкретных услуг, условия SLA и фактическое качество, воспринимаемое пользователем.

**Ограничения и проблемы внедрения**

Несмотря на широкие возможности искусственного интеллекта, его внедрение не отменяет существующие средства мониторинга и администрирования. Интеллектуальные алгоритмы должны дополнять эксплуатационные системы и использовать данные, поступающие из них.

Одним из основных ограничений остается качество исходных данных. Точность моделей машинного обучения напрямую зависит от полноты и достоверности телеметрии. На практике часть показателей может поступать с задержкой, отсутствовать либо представляться в разных форматах, поскольку оборудование и системы управления различных производителей используют собственные способы сбора и описания данных. Поэтому до внедрения моделей необходимо нормализовать данные и приводить их к единому формату.

Еще одна сложность связана с объяснением решений, которые сформировала модель. Оператору необходимо понимать, на основании каких данных и признаков система предлагает решение. Это особенно важно в случаях, когда предполагается изменение маршрутов, масштабирование виртуальных функций или перераспределение ресурсов. Возможность проверить логику принятого решения позволяет снизить риск ошибочного воздействия на сеть и повышает доверие эксплуатационного персонала к автоматизированным механизмам.

Необходимо учитывать и дрейф данных. Состав абонентов, топология сети, программное обеспечение и структура трафика постоянно меняются. В результате модель, которая демонстрировала достаточную точность в момент внедрения, позднее может начать выдавать менее надежные резуль-

таты. По этой причине требуется регулярно оценивать качество ее работы, обновлять обучающие выборки и выполнять переобучение.

Отдельная группа рисков связана с информационной безопасностью. Злоумышленник может попытаться изменить входные данные таким образом, чтобы система зафиксировала несуществующую аномалию либо не распознала реальную угрозу. Дополнительную опасность создает включение модели непосредственно в контур управления, ошибочное решение в этом случае может автоматически применяться сразу к нескольким сетевым элементам. Для снижения подобных рисков необходимо ограничивать перечень действий, доступных интеллектуальной системе, проверять сформированные команды перед их выполнением и сохранять возможность вмешательства со стороны оператора.

Дополнительной проблемой является необходимость интеграции интеллектуальных алгоритмов с существующей инфраструктурой OSS/BSS. В монолитных системах эксплуатационного управления многие процессы выполняются относительно медленно и ориентированы на статическую инфраструктуру. Однако в среде SDN/NFV жизненный цикл виртуальных сетевых функций измеряется секундами, а ресурсы могут динамически переноситься между вычислительными узлами [3].

**Заключение**

Применение искусственного интеллекта для эксплуатационного управления сетями пятого поколения является закономерным этапом эволюции инфокоммуникационных систем. Рост масштабов телеметрии, виртуализация сетевых функций, распределенная облачная инфраструктура и высокая динамика сервисов делают невозможным эффективное управление сетью исключительно на основе статических правил и ручного администрирования. В этих условиях ИИ становится не вспомогательным инструментом анализа, а частью архитектуры управления сетями 5G/B5G.

Проведенный анализ показывает, что наибольшую практическую значимость ИИ приобретает в задачах мониторинга, прогнозирования трафика, обнаружения аномалий, управления ресурсами SDN/NFV и поддержки качества обслуживания. При этом ключевым эффектом внедрения интеллектуальных механизмов является переход от реактивной модели эксплуатации к проактивному управлению, при котором система способна выявлять потенциальные проблемы до возникновения деградации сервиса и автоматически адаптировать параметры сети.

Дальнейшее развитие эксплуатационного управления, вероятно, будет связано не с изолированным применением отдельных AI/ML-моделей, а с их включением в единую систему управления сетью. Такая система должна объединять сбор и анализ телеметрии, автоматизацию эксплуатационных процессов, оркестрацию сетевых функций и механизмы адаптации к изменяющимся условиям. Для сетей 5G и Beyond 5G данный подход представляется более практичным, поскольку позволяет использовать результаты интеллектуального анализа непосредственно при принятии и выполнении управляющих решений.

**Список используемых источников**

1. Abdellah Ali R., Koucheryavy A.: Artificial Intelligence Driven 5G and Beyond Networks // Telecom IT. 2022. Vol. 10. Iss. 2. PP. 1–13. DOI: 10.31854/2307-1303-2022-10-2-1-13.

2. Соколов И. А. Теория и практика применения методов искусственного интеллекта // Вестник Российской академии наук. 2019. Т. 89. № 4. С. 365–370. DOI: 10.31857/S0869-5873894365-370.

3. Гольдштейн Б. С., Гольдштейн А. Б. Управление инфокоммуникациями. СПб.: БХВ-Петербург, 2026. 224 с. ISBN 978-5-9775-2127-7

4. Малыгин И. Г., Тарабаев А. А., Аванесов М. Ю. Интеграция искусственного интеллекта в коммуникационные сети и услуги // Информация и космос. 2019. № 4. С. 6–11.

5. Бородин А. С., Волков А. Н., Мутханна А. С., Кучерявый А. Е. Искусственный интеллект в сетях связи пятого и последующих поколений // Электросвязь. 2021. № 1. С. 17-22. EDN: JDHISS

## APPLICATION OF ARTIFICIAL INTELLIGENCE FOR OPERATIONAL MANAGEMENT OF FIFTH-GENERATION NETWORKS

**Goldstein A., Kamaev A., Rafikova R.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article discusses the use of artificial intelligence and machine learning methods in the operational management of 5G networks. The study considers network monitoring, traffic prediction, anomaly detection, resource allocation, and service quality assurance. Particular attention is given to the integration of AI technologies with SDN/NFV architectures, OSS/BSS systems, MEC platforms, and network orchestration mechanisms.*

***Key words:*** *artificial intelligence, 5G, machine learning, network management, SDN, NFV, traffic prediction, anomaly detection, QoS*

**УДК 621.397.7-182.3**
**ГРНТИ 47.51.31**

# ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ «УМНОГО ДОМА» В РАМКАХ СИСТЕМЫ ВИДЕОКОНТРОЛЯ НА ПРОМЫШЛЕННЫХ ОБЪЕКТАХ

**А. А. Горынцев, С. Л. Фёдоров**

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

*Сегодня системы видеонаблюдения активно используются для защиты жилых и промышленных объектов. Однако их проектирование часто осложняется трудностью прокладки кабелей. Использование систем видеонаблюдения на базе «умного дома» позволяют избежать этого, но стандарты технологии имеют ограничения по дальности связи или пропускной способности канала. В связи с этим сохраняется высокая потребность в оптимальном решении, способное одновременно поддерживать объединение устройств в единую сеть, высокую скорость передачи видео и большую дальность связи. В данной работе проведен анализ и сравнение технологий «умного дома» для решения задачи обеспечения видеоконтроля на промышленных объектах.*

***Wi-Fi, Wi-Fi Halow, LTE, технология, система, видеонаблюдение***

Обеспечение безопасности на объектах жилого и промышленного комплексов до сих пор остается важной задачей. Внедрение систем видеонаблюдения облегчает контроль объектов и снижает человеческий фактор неверной интерпретации ситуаций, связанных с безопасностью охраняемых комплексов. Однако огромные площади больших предприятий и разветвленные коридоры жилых помещений не всегда позволяют разместить оборудование системы. Проблема заключается в невозможности или сложности выполнения прокладки кабеля для подключения устройств к общей сети.

Как вариант решения – организация беспроводного радиоканала передачи данных между устройствами системы видеоконтроля. Качество и дальность связи может быть ограничена выбранным стандартом передачи, расстоянием между объектами. Дополнительными факторами, ограничивающими дальность передачи видеопотока, выступают физические препятствия, а также помехи различной природы: техногенные (вызванные работой электроустановок и радиоэлектронных средств) и природные (атмосферные явления и возмущения магнитосферы Земли). Как по отдельности, так и в совокупности эти явления оказывают негативное влияние на эффективный радиус связи системы [1].

Организация систем видеоконтроля по беспроводной сети может быть осуществлена через протоколы передачи систем «умного дома». Однако не

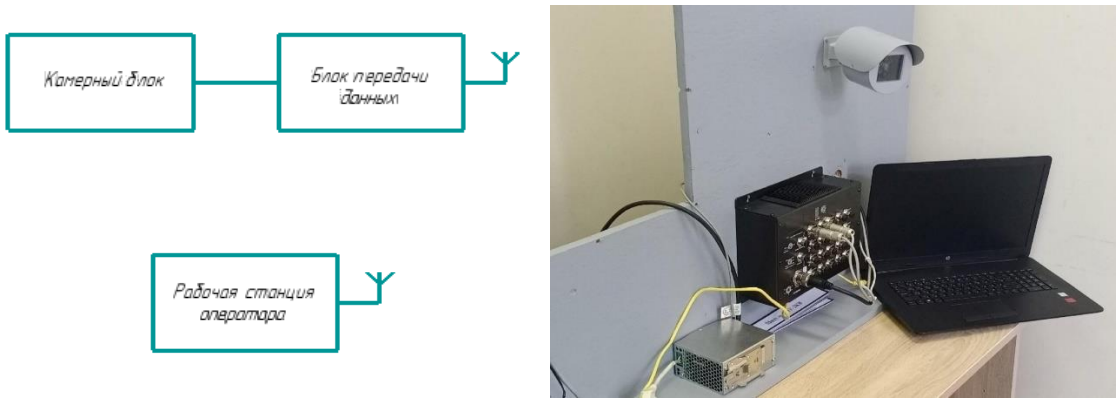
все протоколы подходят именно для передачи видеопотока, так как часть из них задумывалась, как передача простых команд состояния или функций управления. Далее рассмотрены технологии, которые рассчитаны на передачу видеопотока.

Один из распространенных протоколов – это Wi-Fi в наборе стандартов IEEE 802.11: 4 (802.11n), 5 (802.11ac), 6 (802.11ax). Преимуществами выбора данного протокола является высокая скорость передачи данных (до 9,6 Гбит/с), удобство использования и доступность оборудования на рынке. Недостатками выбора является дальность передачи сигнала (не более 300 м), что требует установку ретрансляторов сигнала [2].

Стандарт IEEE 802.11ah Wi-Fi HaLow разработан для работы на частотах ниже 1 ГГц, что дает существенный прирост в энергоэффективности и дальности связи. Благодаря использованию узкополосных сигналов радиус его действия достигает 3 км, что более чем в 10 раз превосходит показатели классических сетей на 2,4 и 5 ГГц. Основной минус – ограничение по максимальной скорости передачи данных, составляющее 40 Мбит/с [3].

Технология LTE – стандарт беспроводной связи для сетей мобильной связи. Преимуществами данной технологии является высокая пропускная способность (до 300 Мбит/с), гибкость в режиме работы (использование частот 800, 1800, 2600 МГц) и широко развернутая сеть базовых станций на территории страны. Недостатками являются зависимость от инфраструктуры базовых станций, ограниченная проницаемость сигнала и уязвимость к перехвату информации [4].

Для экспериментального исследования применимости вышеуказанных технологий к системе видеонаблюдения была разработана так называемая мобильная система видеонаблюдения (МСВ) (рис. 1), составляющие которой являются: камерный блок, блок передачи данных, рабочая станция оператора.




а) б)

Рис. 1. а) структурная схема системы МСВ, б) внешний вид системы МСВ

Камерный блок формирует цифровой несжатый сигнал изображения (разрешение 1080pi) и со скоростью 100 Мбит/с передает его в блок передачи данных. Блок передачи данных состоит из нескольких модулей: Wi-Fi (частота 2,4 ГГц), Wi-Fi HaLow и 4G LTE. Рабочая станция оператора выполняет функцию контроля состояния, а также фиксирования результатов исследования.

Экспериментальные исследования проводились на контрольных дистанциях 10 м (эталон), 50 м, 100 м, 250 м, 500 м и 1 км. Поверка выполнялась в двух типах условий:

– на открытой местности в условиях условной прямой видимости с естественными преградами (деревья, кустарники);
– внутри здания (в закрытых коридорах, комнатах и межэтажных перекрытиях).

По результатам работы системы МСВ (рис. 2) на станцию оператора по радиосвязи было транслировано видео с камерного модуля. В ходе эксперимента зафиксированы результаты перемещения объекта в кадре в режиме реального времени, представленные в табл. 1, 2.



а) б)

Рис. 2. а) изображения с рабочей станции на открытом, б) изображения с рабочей станции на закрытом участке

ТАБЛИЦА 1. Результаты экспериментальной проверки на открытой местности

| Расстояние, м | Wi-Fi | | Wi-Fi HaLow | | 4G LTE | |
|---|---|---|---|---|---|---|
| | Скорость, Мбит/с | Оценка* | Скорость, Мбит/с | Оценка* | Скорость, Мбит/с | Оценка* |
| 10 | 98 | 5 | 11 | 5 | 30 | 5 |
| 50 | 75 | 5 | 10 | 5 | 32 | 5 |
| 100 | 39 | 4 | 8,5 | 4 | 31 | 5 |
| 250 | 8 | 2 | 8 | 4 | 30 | 4 |
| 500 | 1 | 1 | 7,5 | 3 | 31 | 5 |
| 1000 | 0 | 1 | 7 | 3 | 30 | 4 |

ТАБЛИЦА 2. Результаты экспериментальной проверки на закрытой местности

| Расстояние, м | Wi-Fi | | Wi-Fi HaLow | | 4G LTE | |
|---|---|---|---|---|---|---|
| | Скорость, Мбит/с | Оценка* | Скорость, Мбит/с | Оценка* | Скорость, Мбит/с | Оценка* |
| 10 | 92 | 5 | 10 | 5 | 17 | 4 |
| 50 | 32 | 3 | 9 | 4 | 16 | 3 |
| 100 | 3 | 1 | 7 | 4 | 15 | 3 |
| 250 | 0 | 1 | 5 | 3 | 16 | 4 |
| 500 | 0 | 1 | 3,5 | 2 | 18 | 4 |
| 1000 | 0 | 1 | 2 | 1 | 14 | 3 |

(* 1 – нет видеопотока, 2 – видеопоток представлен отдельными редкими кадрами, 3 – видеопоток представлен длительными задержками и артефактами на изображении, 4 – видеопоток представлен короткими периодическими задержками, и редкими проявлениями артефактов на изображения, 5 – видеопоток без задержек и артефактов).

Проведенные испытания продемонстрировали работоспособность системы и позволили оценить влияние условий на качество видеопотока.

В ходе экспериментов была установлена зависимость качества видеопотока – в частности, возникновения задержек, искажений и артефактов изображения – от дистанции и характера преград. Наряду с естественными помехами, на передачу данных влияла специфика промышленной зоны: наличие высоковольтных линий, трансформаторных подстанций и иного индустриального оборудования.

Полученные результаты доказали целесообразность применения данной технологии при построении комплексов видеонаблюдения. Однако каждый из исследованных способов имеет ряд своих ограничений, исходя из которых выбор оборудования под стандарт передачи беспроводного сигнала должен производиться по месту установки. Оборудование на основе стандартов Wi-Fi IEEE 802.11: 4 (802.11n), 5 (802.11ac), 6 (802.11ax) на большой территории требует развертывания большой сети ретрансляторов для эффективной и стабильной передачи видеопотока с камер на пункты оператора. Система на основе стандарта 4G LTE требует наличие рядом с контролируемым объектом сети базовых станций, так как связь проходит через них. Система с использованием технологии Wi-Fi HaLow требует большие затраты на внедрение, так как оборудование не имеет широкого распространения в стране. Но независимость оборудования от общих сетей, высокая дальность и перспективность развития данной технологии, предпочтительно для решения задачей организацией видеоконтроля на промышленных объектах.

**Список используемых источников**

1. Горынцев А. А, Фёдоров С. Л. Применение технологии Wi-Fi Halow для передачи видеопотока // 66-я Научно-техническая конференции профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2026). Сб. науч. статей. СПб.: СПбГУТ, 2026. Т. 1. с. 167-171.
2. Основные стандарты беспроводных локальных сетей. Сайт «ZSC». URL: https://zscomp.ru/news/Standarti_besprovodnih_lokalnih_setei_text_/ (дата обращения 20.04.2026).
3. HaLow: дальнобойный Wi-Fi, который работает на расстоянии в несколько километров // Сайт «Хабр». Блог компании МТС. URL: https://habr.com/ru/companies/ru_mts/articles/791858/ (дата обращения 21.04.2026).
4. Умнова А. Lte – что такое. Сайт «SKYENG». URL: https://skyeng.ru/magazine/wiki/it-industriya/chto-takoe-lte/ (дата обращения 20.04.2026).

## APPLICATION OF SMART HOME TECHNOLOGIES WITHIN THE FRAMEWORK OF VIDEO SURVEILLANCE SYSTEMS AT INDUSTRIAL FACILITIES

**Gorincev A., Fedorov S.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*It's now common knowledge that residential and industrial buildings are equipped with video surveillance systems to ensure security and monitor the environment. Often, when designing such systems, cabling for connectivity is challenging. One solution is to implement systems based on smart home technologies; however, depending on the chosen standard, there are limitations on the effective communication range or channel capacity. Therefore, devices based on technologies with sufficient bandwidth to support video stream transmission, long-range communication, and network connectivity are required. This paper analyzes and compares smart home technologies for solving the problem of video surveillance at industrial facilities.*

***Key words:*** *Wi-Fi, Wi-Fi Halow, LTE, technology, system, video surveillance*

**УДК: 617.7-77**
**ГРНТИ 76.09.35**

# РАЗРАБОТКА ПРОТОТИПА БИОУПРАВЛЯЕМОГО ГЛАЗНОГО ПРОТЕЗА С ИНТЕГРИРОВАННОЙ СИСТЕМОЙ АДАПТИВНОЙ ФОНОВОЙ ПОДСВЕТКИ

**И. С. Жуков, Я. С. Лихачев, М. А. Мансуров, Я. К. Тесслер**

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

*У пациентов с анофтальмом после ретинобластомы или механической травмы косметические протезы восстанавливают внешний вид, но функциональная ограниченность остается нерешенной клинической проблемой. Цель работы – создание масштабируемого прототипа, который дополняет эстетическую функцию индивидуальной подсветкой, активируемой без помощи рук, путем тройного быстрого моргания.*

***протезно-ортопедические изделия, бионический протез глаза, ассистивные технологии, интерфейс «глаз-компьютер», Arduino Nano, компаратор LM393, детекция моргания, помехозащищенность***

Развитие технологий биомедицинской инженерии и микроэлектроники предопределяет переход от пассивного (косметического) протезирования к созданию активных экзопротезов и ортезов, способных частично компенсировать утраченные функции поврежденных органов. У пациентов с дефектами орбитальной области стандартные глазничные протезы успешно восстанавливают симметрию лица, но остаются функционально статичными. Интеграция дополнительных электронных узлов в ограниченный объем конъюнктивальной полости представляет актуальную научно-практическую задачу.

Анализ современного мирового опыта проектирования интерфейсов «глаз-компьютер» (Eye-Computer Interface, ECI) показывает, что ключевым барьером является выбор физиологического метода съема управляющего биосигнала. Применение поверхностной электромиографии (миографических датчиков круговой мышцы глаза m. orbicularis oculi) ограничено из-за высокого уровня артефактов движения: при жевании, глотании или мимической активности точность распознавания управляющих команд снижается до 40–50 %. Использование миниатюрных видеокамер для трекинга

зрачка и века технически избыточно, энергозатратно и нарушает конфиденциальность пациента [1]. Наиболее перспективным и инвариантным к внешним помехам решением является метод оптической ближней инфракрасной детекции, фиксирующий изменение коэффициента отражения светового потока при перемещении кожных покровов века [2].

Цель настоящей работы – создание масштабируемого прототипа биоуправляемого глазного протеза с функцией адаптивной фоновой подсветки, активируемой без помощи рук путем тройного быстрого моргания, с обеспечением высокой помехозащищенности и инвариантности к рефлекторным морганиям.

Реализация бесконтактного управления бионическим протезом требует четкого сопряжения программных алгоритмов микроконтроллера с физиологическими параметрами биомеханики века человека. В качестве управляющего паттерна выбрано намеренное тройное последовательное смыкание век. Временные параметры регистрации поступающих оптических импульсов жестко ограничены в коде максимальным интервалом ожидания, что позволяет отсекать естественное рефлекторное моргание. Техническая последовательность прохождения и преобразования сигналов в рамках интерфейса представлена на рисунке 1.

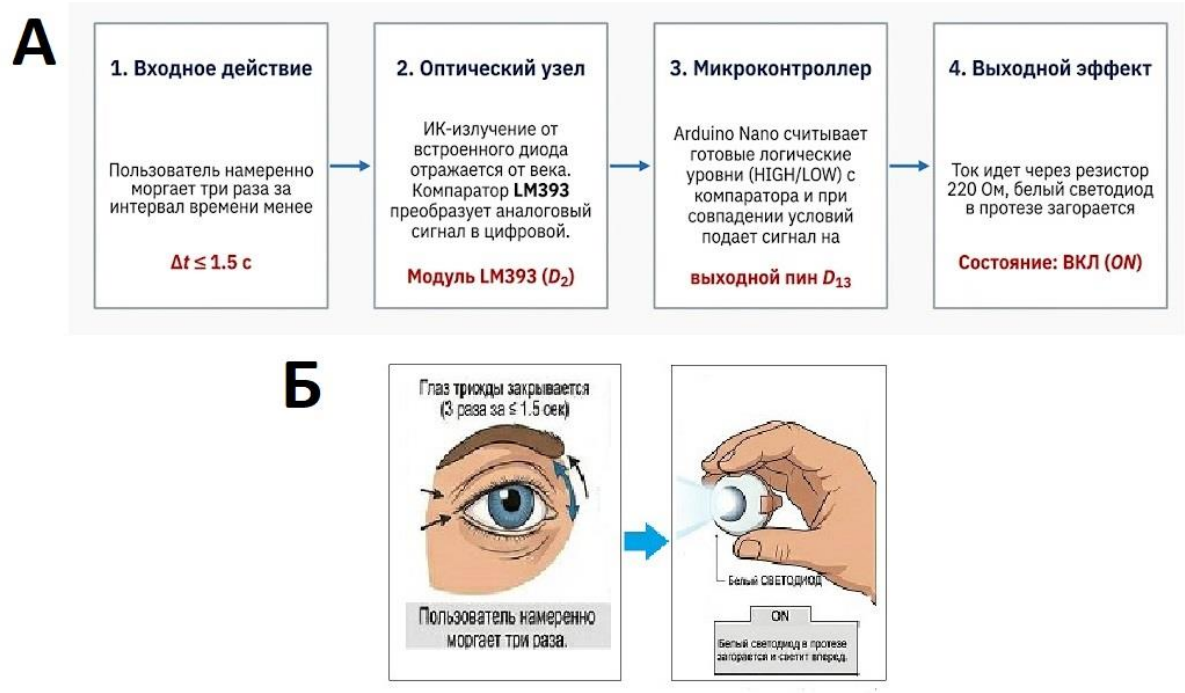



Рис. 1. А – структурно-функциональная схема биоуправляемого глазного протеза, Б – итоговый вид проекта

Условие программной верификации осознанной команды и последующего переключения триггера питания описывается выражением:

$$\lim(t_3 - t_1) \leq \Delta t_{max}$$

где $t_1$ – временная метка фиксации первого импульса, мс;

$t_3$ – временная метка третьего последовательного импульса, мс;

$\Delta t_{max}$ – программный тайм-аут, составляющий в текущей конфигурации устройства 1500 мс.

Если интервал времени между крайними импульсами превышает установленный лимит $\Delta t_{max}$ [3], программная логика интерпретирует серию как случайную и сбрасывает внутренний счетчик в исходное нулевое состояние. Дополнительно в цикле обработки данных заложена программная задержка опроса портов длительностью не менее 10 мс, обеспечивающая подавление динамического «дребезга» сигналов, возникающего в моменты частичного перекрытия оптического канала кожными покровами в процессе движения века. Принципиальная схема изображена на рисунке ниже (рис 2).

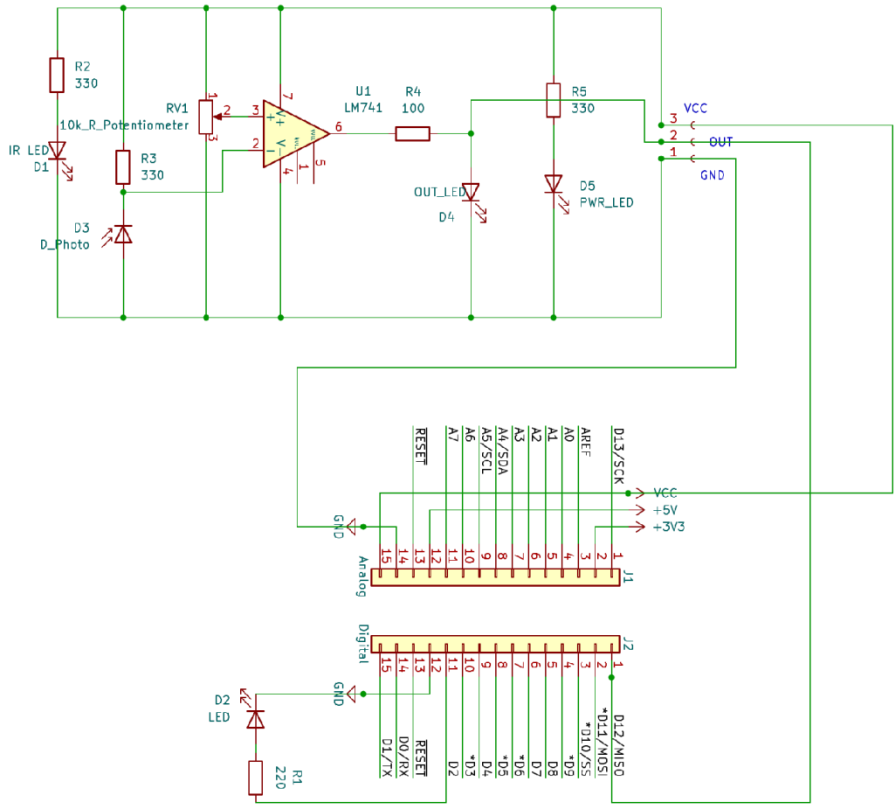



Рис. 2. Принципиальная схема биоуправляемого глазного протеза

Измерительный ИК-модуль построен на базе микросхемы компаратора U1 (LM393), соединенной по дифференциальной схеме сравнения сигналов.

Задание опорного порогового напряжения осуществляется посредством прецизионного подстроечного потенциометра RV1 номиналом 10 кОм, включенного в плечо делителя напряжения параллельно фиксированному резистору R2 (330 Ом). Оптический канал детекции формируется за счет инфракрасного излучающего диода D6 (IR LED) и приемного фотодиода D3 (IR Photo) [2]. Для стабилизации работы полупроводниковых структур излучателя в схему интегрирован ограничительный резистор R3 (330 Ом). Светодиод D5 (Power_LED) выполняет функцию визуального контроля подачи питания по шине VCC (5 В), а светодиод D4 (OUT_LED) отображает состояние логического выхода компаратора в реальном времени.

Выходной информационный интерфейс датчика OUT подключен к цифровому порту ввода D2 микроконтроллера, аппаратно поддерживающему обработку внешних прерываний. Исполнительный узел направленного освещения на базе белого сверхъяркого светодиода D2 (LED) подключен к цифровому выходу D13 последовательно через токоограничивающий резистор R1 номиналом 220 Ом, стабилизирующий номинальный рабочий ток элемента на уровне 8 мА.

Для обеспечения долговечности полупроводниковых структур расчет балластного сопротивления R1 (Ом) выполнялся по закону Ома:

$$R_1 = \frac{\left(U_{\text{пит}} - U_{\text{диод}}\right)}{I_{\text{ном}}}$$

где $U_{\text{пит}}$ – стабильное напряжение питания логики микроконтроллера (5,0 В);

$U_{\text{диод}}$ – прямое падение напряжения на переходе белого светодиода в номинальном режиме (3,2 В);

$I_{\text{ном}}$ – номинальный рабочий ток, установленный для обеспечения энергоэффективности.

Сводные верифицированные параметры электрических режимов компонентов приведены в таблице 1.

ТАБЛИЦА 1. Номинальные электрические параметры компонентов оптического и исполнительного узлов

| Наименование компонента | Рабочее напряжение U, В | Номинальный ток I, А | Длина волны / Цветовая температура |
|---|---|---|---|
| ИК-передатчик (светодиод) | 5,0 | 0,021 | 940 нм |
| Белый светодиод (фонарик) | 3,2 | 0,0081 | 6000K |

Интеграция готового модуля компаратора LM393 позволила перенести процедуру фильтрации входного шума из программного кода в аппаратную среду [4]. Дифференциальный каскад микросхемы LM393 обладает собственным током потребления не более 0,4–1,0 мА, что минимизирует общую энергоемкость оптического узла (21 мА в номинальном режиме с учетом подсветки) и делает систему перспективной для автономного питания от миниатюрных Li-Po аккумуляторов.

Главным преимуществом разработанного паттерна тройного моргания перед стандартными бинарными датчиками является полная инвариантность к неосознанным физиологическим реакциям. Одиночные и двойные случайные смыкания полностью отсекаются предложенным алгоритмом временного окна, поскольку вероятность случайного рефлекторного воспроизведения трех быстрых осознанных морганий подряд крайне мала.

Использование подстроечного элемента RV1 частично решает проблему ложных срабатываний при саккадических движениях глазных яблок (взгляд вниз-вбок), описанную в обзорах интерфейсов «глаз-компьютер». [2]. Ограничением текущей версии прототипа является фиксированный шаг временного окна в коде, что в будущих итерациях проекта потребует внедрения адаптивного алгоритма самообучения под индивидуальную скорость моргания конкретного пациента.

В данном исследовании спроектирован масштабируемый прототип биоуправляемого глазного протеза с функцией направленного освещения, была достигнута высокая стабильность детекции оптического сигнала отражения в ближнем ИК-диапазоне (940 нм). Программный алгоритм временной сепарации импульсов обеспечивает надежное разделение осознанных команд управления от естественного рефлекторного моргания. Полученные электротехнические и конструктивные параметры создают прочный базис для последующей миниатюризации устройства и его интеграции в реальные полимерные глазные протезы.

**Список используемых источников**

1. Frigerio A., Hadlock T. A., Murray E. H., Heaton J. T. Infrared-based blink-detecting glasses for facial pacing: toward a bionic blink // JAMA Facial Plastic Surgery. 2014. Vol. 16. N 3. P. 211–218. DOI: 10.1001/jamafacial.2014.1.

2. Marin M., Negoiaș M., Marin F. B. Development of a Real-Time Eye Blink Monitoring System Using an IR Sensor and Arduino Microcontroller // The Annals of “Dunarea de Jos” University of Galati. Fascicle IX, Metallurgy and Materials Science. 2025. Vol. 48. N 2. P. 49–55.

3. Shafi R., Musthafa R. P., Anto R., Suresh S., Prem R. Arduino Based Assistance Model for Paralysed Patients Using Blink Detection // Proceedings of International Conference. 2019.
4. LM393 Dual Differential Comparators Datasheet. – Dallas, Texas: Texas Instruments Publishing, 2020.

## DEVELOPMENT OF A BIO-CONTROLLED EYE PROSTHESIS PROTOTYPE WITH AN INTEGRATED ADAPTIVE BACKGROUND LIGHTING SYSTEM

**Zhukov I., Likhachev Ya., Mansurov M., Tessler Ya.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In patients with anophthalmos after retinoblastoma or mechanical trauma, cosmetic prostheses restore appearance, but their functional limitations remain an unsolved clinical problem. The aim of this work is to create a scalable prototype of a bio-controlled eye prosthesis that complements the aesthetic function with individual adaptive lighting activated hands-free by triple rapid blinking. The article describes the block diagram, operating principle, electrical parameters, and software algorithm for conscious command verification. The proposed solution provides high noise immunity and invariance to reflex blinks.*

***Key words:*** *prosthetic and orthopaedic devices, bionic eye prosthesis, assistive technologies, eye-computer interface, Arduino Nano, LM393 comparator, blink detection, noise immunity*

**УДК 004.932**
**ГРНТИ 28.23.15**

# АНАЛИЗ ТЕХНОЛОГИИ КОНТРОЛЯ СИТУАЦИОННОЙ ОБСТАНОВКИ МЕСТНОСТИ С ПРОГНОЗИРОВАНИЕМ РАЗВИТИЯ УГРОЗ РАЗЛИЧНОГО ТИПА С ИСПОЛЬЗОВАНИЕМ СИСТЕМ ТЕХНИЧЕСКОГО ЗРЕНИЯ С ИНТЕРАКТИВНЫМ ПОЛЬЗОВАТЕЛЬСКИМ ИНТЕРФЕЙСОМ

**Р. Р. Зайдуллин, Е. И. Туманова**

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

*В данной работе проводится исследование технологий автоматизированного контроля за состоянием местности с применением интеллектуальных алгоритмов анализа видеопотока. Основное внимание уделяется переходу от систем пассивного видеонаблюдения к комплексам, способным осуществлять прогнозирование развития опасных ситуаций в реальном времени. В статье рассматриваются современные методы обнаружения объектов, алгоритмы сопровождения целей и модели предсказания их дальнейшего поведения на основе рекуррентных нейронных сетей. В рамках исследования проведен эксперимент по моделированию мониторинга воздушного пространства, в ходе которого выполнено сравнение различных конфигураций программного обеспечения. Оценка эффективности производилась по метрикам точности распознавания, стабильности идентификации объектов и скорости обработки данных. Результаты анализа позволяют обосновать выбор наиболее подходящих алгоритмических решений для построения систем безопасности с интерактивным пользовательским интерфейсом.*

***системы технического зрения, ситуационный мониторинг, распознавание объектов, нейронные сети, прогнозирование угроз, трекинг объектов***

Рост численности техногенных и антропогенных рисков в современном мире заставляет создавать повышенные требования к системам, которые отвечают за обеспечение безопасности объектов и территорий. Традиционные методы наблюдения, ориентированные на фиксацию уже произошедших событий, перестают быть эффективными в условиях, в которых динамично меняются угрозы. Необходимость повышать скорость принятия мер по безопасности обуславливает актуальность разработки новых технологий, способных не только обнаруживать потенциальную опасность, но и прогнозировать ее развитие на ранних этапах [1].

Интеграция методов, которые используют в сфере машинного обучения и компьютерного зрения, позволяет автоматизировать процесс анализа

в определенной ситуационной обстановке. При этом критически важным аспектом является использование интерактивных пользовательских интерфейсов, которые позволяют оператору достаточно быстро взаимодействовать с системой, допуская меньшее кол-во ошибок, визуализируя не только текущее положение объектов, но и векторы их предполагаемого движения. Целью данной работы является комплексный анализ существующих технологий и методов контроля местности на основе систем технического зрения и выявить наиболее перспективные комбинаций алгоритмов для прогнозирования угроз.

## 1. Теоретические основы и этапы работы систем технического зрения

Работа современной системы технического зрения представляет собой многоэтапный процесс преобразования первичных данных, полученных с сенсоров в смысловую модель описанной сцены. К основным источникам данных для мониторинга местности относятся: камеры, тепловизоры, беспилотные летательные аппараты (БПЛА), лидары и спутниковые камеры [2].

Процесс обработки информации ситуационного контроля, как правило, разделяется на следующие ключевые стадии:

1. Предобработка: подавление шумов и нормализация изображения для повышения точности работы нейронных сетей.

2. Извлечение признаков: использование сверточных нейронных сетей для идентификации границ, текстур и форм объектов.

3. Семантическая интерпретация: этот этап описывает как система отвечает на вопросы о типе объекта и его состоянии.

4. Динамический анализ: отслеживание траектории перемещения (трекинг) через последовательность кадров.

5. Прогнозирование: вероятностная оценка будущих состояний системы на основе накопленной информации [3].

## 2. Методы детекции и классификации потенциальных угроз

На этапе семантического анализа система должна не только выявить наличие объектов в наблюдаемой области, но и определить их принадлежность к определенному классу угроз: техногенным, природным или антропогенным. Для реализации данных функций в современных системах технического зрения широко используются сверточные нейронные сети (CNN), способные эффективно извлекать характерные признаки из изображений. В

рамках исследования были рассмотрены три архитектуры, которые получили широкое распространение при решении задач обнаружения объектов: YOLOv8, Faster R-CNN и Mask R-CNN.

YOLOv8 представляет собой одностадийный алгоритм детекции, в котором процесс поиска и классификации объектов выполняется одновременно. Такой подход обеспечивает высокую скорость обработки данных (примерно 0,304 с на кадр), что делает модель востребованной при построении систем наблюдения, работающих в режиме реального времени. Вместе с тем при анализе сложных сцен с большим количеством объектов или их частичным перекрытием может наблюдаться снижение точности распознавания [4].

Архитектура Faster R-CNN работает в 2 этапа: сначала нейронная сеть формирует области возможного расположения объектов (Region Proposal Network), после чего выполняет их классификация. Данный метод позволяет достичь высокой точности для обнаружения объектов, достигающей 98 %, что делает его эффективным инструментом для именно детального анализа видеоданных. Правда повышение качества распознавания приводит к увеличению вычислительной нагрузки и, соответственно, снижению скорости обработки до 8,421 с. Следующем развитием данного подхода стала модель Mask R-CNN, в которую была добавлена возможность построения попиксельной маски объекта. Исходя из этой маски, система получает возможность определять не только координаты объекта, но и его точные границы, что особенно важно при работе с объектами, которые тяжело обнаружить, и сложными визуальными сценами [5].

## 3. Сопровождение объектов и прогнозирование развития ситуаций

Для анализа развития событий недостаточно только обнаруживать объекты в отдельные моменты времени – необходимо учитывать их перемещение и изменение положения в пространстве. Решение этой задачи обеспечивается с помощью алгоритмов сопровождения объектов (Tracking), которые позволяют формировать и обновлять траектории движения на последовательности кадров.

Одним из распространенных методов является алгоритм SORT (Simple Online and Realtime Tracking), в основе которого лежит использование фильтра Калмана для оценки текущего положения объекта и прогнозирования его координат на следующем кадре. Более расширенный подход реализован в алгоритме DeepSORT, где к анализу движения добавляются признаки

внешнего вида объекта. Это позволяет системе сохранять корректный идентификатор цели даже в ситуациях временного перекрытия несколькими объектами [6].

Определение возможного развития угроз выполняется на основе обработки временных последовательностей координат, полученных в процессе сопровождения объектов. Для построения прогностических моделей могут использоваться различные методы:

1. Рекуррентные нейронные сети (RNN/LSTM) – применяются для анализа последовательностей данных и позволяют учитывать предыдущие состояния объекта при прогнозировании его дальнейшего поведения.

2. Трансформерные модели (Transformer) – используются для выявления сложных зависимостей в траекториях движения и эффективны при обработке длительных временных последовательностей.

3. Стохастические модели (Particle Filter) – обеспечивают вероятностную оценку будущего состояния системы, что особенно актуально при наличии шумов в данных и высокой степени неопределенности [7].

Дополнительным этапом работы современных систем мониторинга является объединение результатов прогнозирования и модель описываемой сцены. Такой подход дает оценку характеру движения объекта и позволяет выявить потенциально опасные исходы. Например, приближение к охраняемой зоне. При обнаружении подобных ситуаций информация передается оператору через пользовательский интерфейс для последующего анализа и принятия того или иного решения.

## 4. Эксперимент и сравнительный анализ результатов.

На данном этапе исследования была выполнена имитация мониторинга воздушного пространства с ограниченной зоной для доступа. Это позволило оценить работу выбранных методов. В качестве сценария исследования рассматривалось движение трех объектов, имитирующих беспилотные летательные аппараты (БПЛА), с различными траекториями и скоростью. В ходе эксперимента ставилась задача прогнозирования траектории движения на интервал в $N$ кадров вперед и оценка вероятности нарушения объектами границ запретной зоны. Пересечение зоны классифицировалось системой как реализация потенциальной угрозы. Для обнаружения объектов использовался известный детектор YOLOv8, а для анализа динамики – связки различных трекеров с моделью предсказывания на базе рекуррентной нейронной сети LSTM.

Результаты сравнительного анализа трех различных конфигураций программно-алгоритмического комплекса представлены в таблице 1.

ТАБЛИЦА 1. Сравнительные характеристики исследуемых комбинаций алгоритмов

| Конфигурация ПО (Трекер + Детектор) | mAP, % | IDF1, % | MOTA, % | Точность прогноза угрозы, % | Скорость обработки (кадры/сек) |
|---|---|---|---|---|---|
| YOLOv8 + SORT + LSTM | 65 | 75 | 78 | 80 | 45 |
| YOLOv8 + DeepSORT + LSTM | 65 | 90 | 87 | 85 | 28 |
| YOLOv8 + Particle Filter + LSTM | 65 | 80 | 79 | 82 | 22 |

Анализ данных таблицы 1 позволил сделать вывод – выбор технологии напрямую зависит от приоритетов конкретной системы безопасности. Комбинирование YOLOv8 + SORT + LSTM дает увидеть наивысшую скорость обработки (45 кадров в секунду), что делает ее оптимальной для мониторинга «in-real time» на скромных, на 2026 год, вычислительных мощностях. Однако использование DeepSORT в составе исследуемой системы позволило значительно повысить стабильность идентификации (метрика IDF1 достигла 90 %) и общую точность многообъектного трекинга (MOTA = 87 %), что в итоге привело к росту точности предсказания опасных событий до 85 %.

Связка с использованием фильтра частиц (Particle Filter) показала хорошие результаты в условиях зашумленности видеопотока, но из-за высокой вычислительной сложности алгоритма скорость обработки снизилась до 22 кадров в секунду, что может быть критичным для систем оперативного реагирования.

## Заключение

Результаты исследования подтверждают, что применение современных систем технического зрения позволяет расширить возможности классического в нашем понимании наблюдения за счет автоматизированного анализа данных и прогнозирования возможного развития ситуаций. Совместное использование алгоритмов обнаружения объектов и методов прогнозирования (ИИ) способствует более раннему выявлению потенциальных угроз, что очень важно для обеспечения безопасности контролируемых территорий.

Одним из актуальных направлений дальнейшего развития подобных систем является разработка адаптивных моделей, способных изменять пара-

метры обработки информации в зависимости от внешних условий, включая уровень освещенности и количество объектов в зоне наблюдения. Перспективным также является применение гибридных архитектур, сочетающих возможности нейронных сетей при извлечении признаков с вероятностными методами оценки будущего состояния системы. Такой подход может повысить устойчивость работы комплексов мониторинга, снизить количество ошибочных срабатываний и обеспечить их эффективное функционирование в сложных условиях эксплуатации.

**Список используемых источников**

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. ЛитРес, 2014.
2. Визильтер Ю. В. и др. Обработка и анализ изображений в задачах машинного зрения. 2010.
3. Хайкин С. Нейронные сети: полный курс, 2-е издание. Издательский дом Вильямс, 2008.
4. Redmon J., Divvala S., Girshick R., Farhadi A. You only look once: Unified, real-time object detection // Proceedings of the IEEE conference on computer vision and pattern recognition. 2016. С. 779-788.
5. He K., Gkioxari G., Dollár P., Girshick R. Mask R-CNN // Proceedings of the IEEE international conference on computer vision. 2017. С. 2961-2969.
6. Wojke N., Bewley A., Paulus D. Simple online and realtime tracking with a deep association metric // IEEE international conference on image processing (ICIP). 2017. С. 3645-3649.
7. Hochreiter S., Schmidhuber J. Long short-term memory // Neural computation. 1997. Т. 9. № 8. С. 1735-1780.

## ANALYSIS OF A TERRAIN SITUATIONAL AWARENESS MONITORING TECHNOLOGY WITH PREDICTION OF THE DEVELOPMENT OF VARIOUS TYPES OF THREATS USING COMPUTER VISION SYSTEMS WITH AN INTERACTIVE USER INTERFACE

**Zaidullin R., Tumanova E.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper investigates technologies for automated terrain monitoring using intelligent video stream analysis algorithms. Particular attention is given to the transition from passive video surveillance systems to integrated solutions capable of predicting the development of hazardous situations in real time. The article examines modern object detection methods, target tracking algorithms, and models for predicting future behavior based on recurrent neural networks. As part of the study, an experiment was conducted to simulate airspace monitoring, during which various software configurations were compared. Performance was evaluated using metrics such as recognition accuracy, object identification stability, and data processing speed. The analysis results provide a basis for selecting the most suitable algorithmic solutions for developing security systems with an interactive user interface.*

***Key words:*** *computer vision systems, situational monitoring, object recognition, neural networks, threat prediction, object tracking*

**УДК 004.72:004.032.26**
**ГРНТИ 49.33.29; 28.23.37**

# ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОГО УПРАВЛЕНИЯ ТРАФИКОМ И МАРШРУТИЗАЦИИ В СЕТЯХ 5G/6G

**В. К. Мавричев**

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

*В статье рассматриваются подходы к применению нейронных сетей для интеллектуальной маршрутизации и управления трафиком в сетях 5G/6G. Особое внимание уделяется возможностям адаптивного распределения сетевых ресурсов, снижению задержек, повышению пропускной способности и обеспечению качества обслуживания в условиях динамически изменяющейся нагрузки. Анализируются преимущества использования моделей машинного обучения для прогнозирования трафика, выбора оптимальных маршрутов и автоматизации принятия решений в инфокоммуникационных системах. Подчеркивается, что интеллектуальные методы управления позволяют повысить эффективность работы сетевой инфраструктуры и создать основу для развития сетей следующего поколения.*

***нейронные сети; интеллектуальная маршрутизация; управление трафиком; сети 5G; сети 6G; адаптивное распределение ресурсов; качество обслуживания (QoS); снижение задержек; повышение пропускной способности; прогнозирование сетевого трафика; машинное обучение; автоматизация принятия решений***

## Введение

Развитие сетей пятого и шестого поколений сопровождается ростом требований к задержке, пропускной способности, надежности и адаптивности сетевой инфраструктуры. Современные инфокоммуникационные системы должны обрабатывать неоднородный трафик, поддерживать большое число подключенных устройств и обеспечивать стабильное качество обслуживания даже в условиях быстро меняющейся нагрузки. Традиционные алгоритмы маршрутизации и статического распределения ресурсов уже не всегда способны своевременно реагировать на изменения сетевого состояния, что делает особенно актуальным использование интеллектуальных методов управления [1].

Одним из наиболее перспективных направлений является применение нейронных сетей и других методов машинного обучения для анализа тра-

фика, прогнозирования нагрузки, выбора оптимальных маршрутов и автоматизации принятия решений в реальном времени [2]. В сетях 5G такие методы уже демонстрируют практическую эффективность в задачах предсказания трафика и балансировки нагрузки, а в концепциях 6G искусственный интеллект рассматривается как встроенный элемент самой сетевой архитектуры [3].

Цель работы заключается в анализе подходов к применению нейронных сетей для интеллектуальной маршрутизации и управления трафиком в сетях 5G/6G, а также в выявлении их преимуществ, ограничений и перспектив дальнейшего развития. Основное внимание уделяется вопросам адаптивного распределения ресурсов, снижению задержек, повышению пропускной способности и обеспечению качества обслуживания в условиях динамически изменяющейся сетевой нагрузки.

Сети 5G ориентированы на поддержку широкополосной мобильной связи, массового машинного взаимодействия и сервисов со сверхнизкой задержкой. При переходе к 6G эти требования усиливаются: ожидается дальнейшее увеличение плотности устройств, появление нативных AI-функций в сети и еще более жесткие требования к интеллектуальному управлению ресурсами.

В таких условиях маршрутизация перестает быть исключительно задачей поиска кратчайшего пути. Она превращается в многокритериальную проблему, где одновременно учитываются задержка, перегрузка каналов, надежность маршрута, доступность полосы пропускания и требования приложений к качеству обслуживания. Это особенно важно для сервисов реального времени, промышленного интернета вещей, автономного транспорта и распределенных вычислений на периферии сети.

К ключевым задачам управления трафиком в сетях 5G/6G относятся [4]:

– прогнозирование объема и структуры трафика;
– раннее обнаружение перегрузок и аномалий;
– адаптивное распределение полосы пропускания и вычислительных ресурсов;
– выбор маршрутов с учетом QoS/QoE;
– автоматизация переключения между режимами обслуживания и сетевыми политиками.

Основные требования к интеллектуальному управлению трафиком представлены в таблице 1.

ТАБЛИЦА 1. Основные требования к интеллектуальному управлению трафиком

| Параметр | Сети 5G | Сети 6G | Практическое значение |
|---|---|---|---|
| Задержка | Низкая, критична для URLLC | Еще более жесткие требования, вплоть до субмиллисекундного уровня | Необходимость быстрого выбора маршрута и перераспределения ресурсов |
| Пропускная способность | Высокая | Сверхвысокая, с учетом новых сервисов | Нужны прогнозирование нагрузки и балансировка трафика |
| Управление ресурсами | Частично интеллектуализированное | AI-ориентированное и глубже интегрированное в архитектуру | Требуется автоматизация принятия решений |
| Характер нагрузки | Динамический и разнородный | Еще более сложный, многосервисный и контекстно-зависимый | Повышается роль предиктивных моделей |

Так, одной из базовых задач является прогнозирование трафика, от которого зависит эффективность интеллектуальной маршрутизации [5]. Если система способна заранее оценить рост нагрузки, она может заблаговременно перераспределить потоки, изменить приоритеты и выделить дополнительные ресурсы, не допуская деградации качества обслуживания.

Для этих целей эффективнее всего применять рекуррентные нейронные сети, LSTM- и GRU-модели, поскольку они хорошо работают с временными рядами и позволяют учитывать временную зависимость сетевого трафика [6]. Вместе с тем в современных исследованиях активно используются сверточные и графовые нейронные сети, позволяющие выявлять пространственно-временные корреляции между различными узлами, сотами или сегментами сети [7].

Исследования по 5G-трафику подтверждают, что усовершенствованные LSTM-подходы обеспечивают более высокую точность прогноза по сравнению с рядом классических методов, что делает их полезными для задач динамической маршрутизации и резервирования ресурсов [8].

Обучение рекуррентных или сверточных нейронных сетей (LSTM/CNN) для предсказания нагрузки сводится к минимизации функции потерь, например, среднеквадратичной ошибки (MSE) между реальным и спрогнозированным объемом трафика:

$$L(\theta) = \frac{1}{T}\sum_{t=1}^{T}\left(V_t - \mathrm{f}_\theta(X_{t-k:t-1})\right)^2]$$

где $\theta$ – матрица весов нейронной сети, $V_t$ – фактический объем трафика в момент $t$, а $f_\theta(X_{t-k:t-1})$ – объем трафика, предсказанный моделью на основе исторического окна данных длиной $k$. Чем ниже значение $L(\theta)$, тем точнее сеть резервирует ресурсы, не допуская перегрузок.

Интеллектуальный контур управления трафиком представлен на рис. 1.

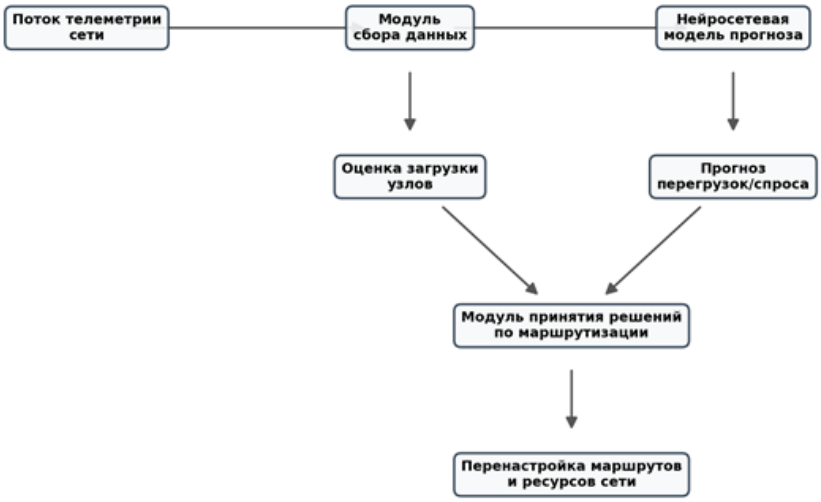



Рис. 1. Интеллектуальный контур управления трафиком

Предиктивный характер таких моделей особенно важен для сетей следующего поколения, где реактивное управление уже недостаточно. Чем раньше система обнаруживает тенденцию к перегрузке, тем эффективнее она может перераспределить трафик, снизить задержки и предотвратить потерю пакетов.

Интеллектуальная маршрутизация в сетях 5G/6G основана на переходе от фиксированных или слабо адаптивных алгоритмов к системам, которые выбирают маршрут с учетом текущего и прогнозируемого состояния сети [9]. В этом случае нейронная сеть выступает не только как инструмент анализа, но и как компонент системы поддержки или автоматизации принятия решений.

Особую роль здесь играют методы глубокого и усиленного обучения [10]. В задачах управления ресурсами такие подходы могут динамически выбирать параметры распределения полосы, мощности, каналов и других сетевых ресурсов в зависимости от условий среды и текущих целевых показателей.

В задачах управления трафиком с помощью глубокого обучения с подкреплением агент максимизирует функцию вознаграждения $R_t$, которая отражает соответствие текущим требованиям качества обслуживания (QoS) [11]:

$$R_t = \alpha \cdot Th_t - \beta \cdot D_t - \gamma \cdot P_t],$$

где в момент времени $t$: $Th_t$– общая пропускная способность, $D_t$ – задержка передачи, $P_t$ – коэффициент потери пакетов, а $\alpha$, $\beta$ и $\gamma$ – настраиваемые весовые коэффициенты. Такая целевая функция позволяет гибко адаптировать сеть 5G/6G: для URLLC-трафика увеличиваются веса $\beta$ и $\gamma$, а для eMBB в приоритете коэффициент $\alpha$.

В таблице 2 рассмотрены нейросетевые подходы и области их применения.

ТАБЛИЦА 2. Нейросетевые подходы и области их применения

| Подход | Основная задача | Преимущества | Ограничения |
|---|---|---|---|
| LSTM / GRU | Прогнозирование временных рядов трафика | Учет временной динамики, хорошая точность прогноза | Требовательность к качеству обучающих данных |
| CNN | Пространственно-временной анализ нагрузки | Выявление локальных структур и повторяющихся паттернов | Менее естественна для сложных графовых топологий |
| GNN / GCN | Анализ связности узлов и маршрутов | Учет топологии сети и взаимосвязей между узлами | Сложность построения графовой модели |
| DRL | Динамическое распределение ресурсов и выбор действий | Адаптация к изменяющейся среде, оптимизация политики управления | Высокая вычислительная сложность и сложность обучения |

С практической точки зрения интеллектуальная маршрутизация дает несколько важных эффектов. Во-первых, повышается устойчивость сети к пиковым нагрузкам, так как система способна заранее подготовить альтернативные пути передачи. Во-вторых, становится возможной более точная настройка QoS для различных классов трафика. В-третьих, уменьшается доля ручного управления.

К основным преимуществам применения нейронных сетей для управления трафиком относятся повышение точности прогнозирования, более эффективное распределение ресурсов, снижение задержек и рост пропускной способности сети при сложной и переменной нагрузке.

Для количественной оценки выигрыша в эффективности маршрутизации можно ввести метрику эффективности сети $E$, определяемую как отношение успешно доставленного объема данных к суммарной задержке:

$$E = \frac{1}{N}\sum_{i=1}^{N}\frac{S_i}{T_{prop,i} + T_{queue,i}}]$$

где $N$ – количество переданных пакетов, $S_i$– размер $i$-го пакета, $T\_\{prop, i\}$ – физическая задержка распространения сигнал, а T_{queue, i}

$T\_\{queue, i\}$ – задержка в очереди узла. Классические алгоритмы маршрутизируют трафик реактивно, что приводит к росту $T\_\{queue\}$ в моменты пиковых нагрузок. Использование предиктивных нейросетей позволяет перенаправлять потоки до возникновения затора, сводя $T\_\{queue\}$ к минимуму.

Относительный прирост эффективности при внедрении интеллектуального управления вычисляется по формуле:

$$\Delta E = \frac{E_{NN} - E_{trad}}{E_{trad}} \cdot 100\backslash\ \%],$$

где $E_{NN}$– эффективность сети под управлением ИИ, а $E_{trad}$ – эффективность со стандартными протоколами.

Вместе с тем внедрение нейросетевых методов связано с рядом ограничений. Среди них можно выделить высокие требования к объему и качеству данных, вычислительную сложность обучения, чувствительность моделей к изменению условий эксплуатации и необходимость обеспечения интерпретируемости решений, особенно в критически важных сетевых сценариях. С инженерной точки зрения перспективным представляется гибридный подход, при котором нейронные сети дополняют классические алгоритмы маршрутизации, а не полностью заменяют их [12].

## Заключение

Применение нейронных сетей в задачах интеллектуальной маршрутизации и управления трафиком становится одним из ключевых факторов эволюции сетей 5G/6G. Предиктивные и адаптивные модели позволяют более

эффективно распределять ресурсы, уменьшать задержки, повышать пропускную способность и поддерживать требуемое качество обслуживания в условиях сложной и динамической нагрузки.

Развитие этого направления связано с переходом от отдельных ML-модулей к глубокой интеграции искусственного интеллекта в сетевую архитектуру. В перспективе это формирует технологическую основу для построения самонастраивающихся сетей следующего поколения, способных автономно анализировать состояние среды, прогнозировать изменения трафика и оптимизировать маршрутизацию в реальном времени.

**Список используемых источников**

1. A Survey on 6G Networks: State of the Art, Challenges, and Future Directions [Text] // IEEE Access. 2023. С. 45–48.

2. Tang F., Mao B., Kawamoto Y., Kato N. A Survey on Machine Learning for End-to-End Intelligent Networking in 6G: From Network Access and Routing to Traffic Management and Flow Adaptation [Text] // IEEE Communications Surveys & Tutorials. 2021. Vol. 23. С. 682–685.

3. AI-based Technologies and Network Layers for 6G [Text] // Expert Systems with Applications (ScienceDirect). 2024. С. 22–25.

4. A Survey on Deep Learning for Cellular Traffic Prediction [Text] // IEEE Communications Surveys & Tutorials. 2024. С. 10–12.

5. Gao Z. 5G Traffic Prediction Based on Deep Learning [Text] // Computational Intelligence and Neuroscience. 2022. Vol. 2022. Article ID 3174530. С. 4–7.

6. Traffic Prediction for 5G: A Deep Learning Approach Based on Lightweight Hybrid Attention Networks [Text] // Physical Communication (ScienceDirect). 2024. С. 118–120.

7. Spatio-Temporal Graph Neural Networks for Traffic Prediction and Optimization in 6G Networks [Text] // Nature Scientific Reports. 2026. С. 2–5.

8. Development and Implementation of a Neural Network Model for Traffic Prediction in 5G Networks [Text] // European Journal of Applied Sciences, Engineering and Technology (EJASET). 2025. С. 55–58.

9. AI-enabled routing in next generation networks: A survey [Text] // Journal of Network and Computer Applications (ScienceDirect). 2025. С. 112–115.

10. AI-driven Dynamic Resource Allocation for ISAC Systems in 6G Networks [Text] // Nature Scientific Reports. 2026. С. 7–9.

11. AI-based Multiple Access for 6G Networks [Text] // arXiv preprint. 2024. С. 3–4.

12. Goal-Oriented Network Architecture for 6G with Embedded AI [Text] // DSG TU Wien Publications. 2024. С. 12–14.

*Статья представлена научным руководителем, доцентом кафедры ИУС СПбГУТ, кандидатом технических наук, старшим научным сотрудником Ф. В. Филипповым.*

# APPLICATION OF NEURAL NETWORKS FOR INTELLIGENT TRAFFIC MANAGEMENT AND ROUTING IN 5G/6G NETWORKS

**Mavrichev V.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This article explores approaches to applying neural networks for intelligent routing and traffic management in 5G/6G networks. Particular attention is paid to the potential for adaptive network resource allocation, latency reduction, throughput enhancement, and ensuring quality of service (QoS) under dynamically changing loads. The study analyzes the advantages of using machine learning models for traffic prediction, optimal route selection, and decision-making automation in infocommunication systems. It emphasizes that intelligent management methods can improve the efficiency of network infrastructure and lay the groundwork for developing next-generation networks.*

***Key words:*** *neural networks; intelligent routing; traffic management; 5G networks; 6G networks; adaptive resource allocation; quality of service (QoS); latency reduction; throughput enhancement; network traffic prediction; machine learning; decision-making automation*

**УДК 004.7:004.422.8**
**ГРНТИ 28.29.01**

# МЕТОД СТАБИЛИЗАЦИИ ОБУЧЕНИЯ ГЛУБОКОЙ НЕЙРОННОЙ СЕТИ В ЗАДАЧАХ СЛАЙСИНГА 5G НА ОСНОВЕ МОДИФИЦИРОВАННОЙ МОДЕЛИ ЗАДЕРЖКИ M/M/1

**Н. Н. Мошак, Н. Эль Сабаяр Шевченко**

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

*Обучение нейросетевых контроллеров для распределения канального ресурса в сетях 5G осложняется численной нестабильностью при обработке входной телеметрии, вызванной сингулярностью классической модели задержки M/M/1 в режимах перегрузки. Цель работы: разработка метода стабилизации глубоких нейронных сетей путем модификации модели задержки, используемой в качестве параметра входного сигнала. Используемые методы: аппарат теории массового обслуживания, методы глубокого обучения. Новизна: предложена кусочно-заданная аппроксимация модели M/M/1 для формирования вектора состояний сети, ограничивающая рост входных признаков в области насыщения радиоканала. Результат: показано, что использование модифицированной задержки на входном слое предотвращает подачу аномальных значений в нейронную сеть, исключая проблему «взрыва градиентов» и гарантируя успешную сходимость алгоритма оптимизации. Практическая значимость: метод позволяет создавать надежные нейросетевые системы управления радиоресурсами 5G, обеспечивая вычислительную стабильность для безопасного исследования пространства состояний среды в режимах критических перегрузок.*

***5G сети, QoS, Network Slicing, модель задержки M/M/1, глубокие нейронные сети, взрыв градиентов***

Развитие сетей мобильной связи от архитектуры LTE к 5G характеризуется экспоненциальным ростом плотности абонентских устройств и гетерогенности трафика [1]. В сетях LTE статические алгоритмы диспетчеризации (например, Round Robin, Proportional Fair) успешно решали задачу распределения радиоресурсов. В условиях 5G, где обслуживаются разнородные сетевые срезы, требуется адаптивное выделение квот канального ресурса, что делает актуальным применение контроллеров на основе глубоких нейронных сетей. Нейросетевые контроллеры показывают высокую эффективность, выявляя зависимости между состоянием радиосреды и оптимальным планом распределения квот канального ресурса. Однако процесс обучения контроллеров может сталкиваться с проблемой численной нестабиль-

ности, возникающей при подаче на входной слой признаков, полученных из классических инфокоммуникационных моделей в режимах перегрузки.

Анализируемая инфокоммуникационная среда 5G рассматривается как совокупность логически изолированных сетевых срезов $\boldsymbol{I} = \{\mathbf{eMBB}, \mathbf{URLLC}, \mathbf{mMTC}\}$, совместно использующих общий ресурс радиоинтерфейса. В рамках концепции «Network Slicing» процесс диспетчеризации трафика на MAC-уровне для каждого *i*-го сетевого среза аппроксимируется независимой одноканальной системой массового обслуживания (СМО) типа *M*/*M*/1 с собственной буферной очередью [2]. Функционирование очереди задается базовыми параметрами для *i*-го среза: интенсивность входящего потока $\boldsymbol{\lambda}$ и интенсивность обслуживания $\boldsymbol{\mu}$, которая детерминируется выделенной квотой канального ресурса.

Критическим элементом вектора состояния среды, определяющим качество принятия решений, служит расчет среднего времени пребывания заявки $T$ в системе. Для расчета данного показателя QoS применяется классическая модель массового обслуживания M/M/1, подробно описанная в контексте вычислительных систем в [3]:

$$T = \frac{1}{\mu_i - \lambda_i}, \tag{1}$$

где $i$ – индекс сетевого среза, $\mu_i$ – интенсивностью обслуживания, $\lambda_i$ – интенсивность входящего потока. Формула (1) может быть представлена с учетом коэффициента удельной загрузки $\rho_i$:

$$T = \frac{1}{\mu_i(1-\rho_i)}. \tag{2}$$

В классической модели M/M/1 стационарное распределение существует при $\rho_i < 1$ [2, 3], однако с приближением $\rho_i$ к единице среднее время пребывания заявки асимптотически стремится к бесконечности. Прямая подстановка таких аномальных значений в среду обучения приводит к вычислительной неустойчивости, вызывая хорошо известную проблему «взрыва градиентов» на этапе обратного распространения ошибки. Это блокирует сходимость алгоритма оптимизации именно в той фазе, которая наиболее важна для оперативного управления – при переходе сети в состояние критической перегрузки, когда происходит нарушение соглашений об уровне обслуживания (SLA). Для предотвращения подачи аномально больших значений определяется порог $\rho_{thr}$. В целях обеспечения устойчивости процесса обучения нейросетевого аппроксиматора в области $\rho_i \geq \rho_{thr}$ вво-

дится модифицированная модель задержки $M/M/1$ в виде кусочно-заданной функции:

$$T(\rho_i) = \begin{cases} \frac{1}{\mu_i(1-\rho_i)}, \text{при } \rho_i < \rho_{thr} \\ T_{base} + \tau \cdot (\rho_i - \rho_{thr}), \text{при } \rho_i \geq \rho_{thr} \end{cases}, \quad (3)$$

где $T_{base}$ – базовая задержка согласно SLA $i$-го сетевого среза, $\tau$ – коэффициент интенсивности штрафа за перегрузку, аппроксимирующий рост задержки в нестабильном режиме, значение которого вычисляется как первая производная базовой функции задержки в пороговой точке.

Графическая интерпретация классической и модифицированной моделях представлены на рисунке 1. В ходе имитационного моделирования, установлено значение порога удельной загрузки $\rho_{thr} = 0.95$. Показано, что при $\rho_i < \rho_{thr}$ обе модели демонстрируют стабильные значения с одинаковыми результатами. Однако выявлено, что при переходе в режим перегрузки $\rho_i \geq \rho_{thr}$ классическая модель $M/M/1$ генерирует гиперболический выброс, стремящийся к бесконечности. В то же время, введенная кусочно-заданная функция (3) стабилизирует рост значения задержки $T$, сохраняя предсказуемую динамику вычислений на этапе обучения.

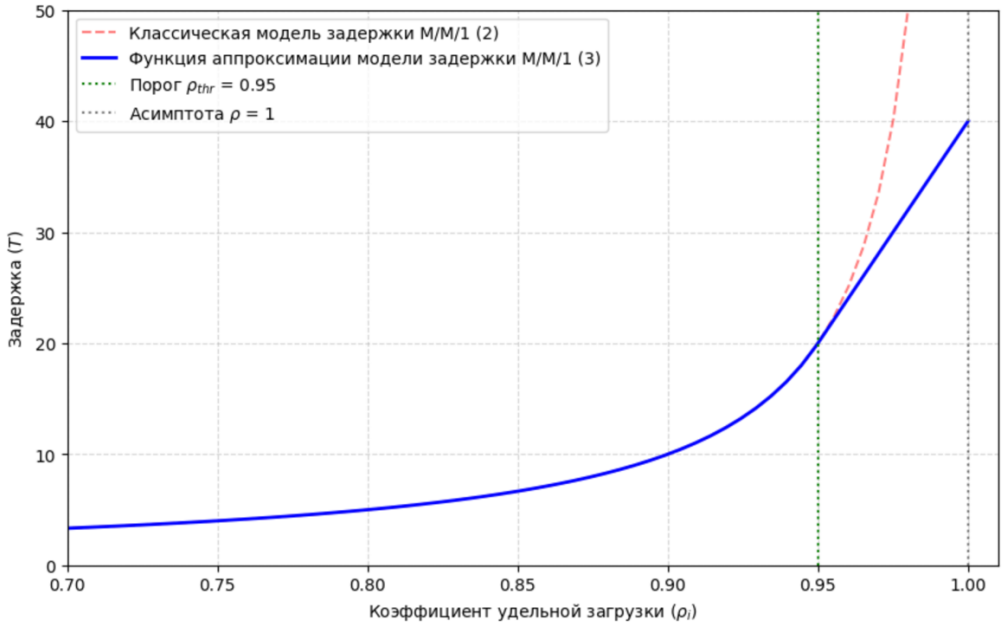



Рис. 1. Зависимость нормированной задержки от коэффициента удельной загрузки для исследуемых моделей

Предложенная кусочно-заданная функция сохраняет аналитический вид классической формулы среднего времени пребывания пакета в системе в стационарной области $\rho_i < \rho_{thr}$, а при переходе в область перегрузки, за-

меняет ее функцией при $\rho_i \geq \rho_{thr}$, рост которой остается предсказуемым, что предотвращает появление аномально больших значений. Такой подход, в отличие от простого отсечения выбросов, позволяет нейросетевому контроллеру выполнять безопасное исследование пространства состояний инфокоммуникационной среды, получая количественную меру глубины перегрузки без потери вычислительной устойчивости во время градиентного шага. Разработанный метод обеспечивает сходимость глубоких нейронных сетей в режимах критических перегрузок радиоканала, что открывает путь к созданию надежных и отказоустойчивых систем управления радиоресурсами 5G.

**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. Клейнрок Л. Теория массового обслуживания. Пер. с англ. М.: Машиностроение, 1979. 432 с.

3. Клейнрок Л. Вычислительные системы с очередями. М.: Мир, 1979. 600 с.

## METHOD FOR STABILIZING DEEP NEURAL NETWORK TRAINING IN 5G NETWORK SLICING BASED ON A MODIFIED M/M/1 DELAY MODEL

**Moshak N., El Zabayar Shevchenco N.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*Training neural network controllers for channel resource allocation in 5G networks is complicated by numerical instability when processing input telemetry, caused by the singularity of the classical M/M/1 delay model under overload conditions. The aim of this work is to develop a method for stabilizing deep neural networks by modifying the delay model used as an input signal parameter. Methods employed: queuing theory apparatus, deep learning methods. Novelty: a piecewise-defined approximation of the M/M/1 model is proposed to form the network state vector, limiting the growth of input features in the radio channel saturation region. Result: it is shown that using the modified delay at the input layer prevents anomalous values from being fed into the neural network, eliminating the "exploding gradient" problem and guaranteeing successful convergence of the optimization algorithm. Practical significance: the method enables the creation of reliable neural network-based radio resource management systems for 5G, providing computational stability for safe exploration of the environment's state space under critical overload conditions.*

***Key words:*** *5G networks, QoS, Network Slicing, M/M/1 delay model, deep neural networks, exploding gradients*

**УДК 007.52**
**ГРНТИ 28.19**

# БАЙЕСОВСКИЙ АЛГОРИТМ КОЛЛЕКТИВНОГО ВОСПРИЯТИЯ СРЕДЫ ПРИ РАЗЛИЧНЫХ ТИПАХ ДИНАМИЧЕСКИХ ИЗМЕНЕНИЙ СРЕДЫ

**Е. А. Новиков**

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

*Исследуется байесовский алгоритм коллективного восприятия в роевой робототехнике при статической среде, перестановке клеток и стохастической генерации цвета. Моделирование на Python показало, что динамика ускоряет сходимость в 1,5–2 раза без потери точности. Наибольший эффект – для равномерного распределения признаков. Алгоритм рекомендуется для нестационарных сред.*

***групповая робототехника, коллектив роботов, роевой интеллект, мультиагентные робототехнические системы, коллективное восприятие, байесовское решающее правило***

Роевая робототехника использует децентрализованное взаимодействие агентов [1, 2]. Ключевая задача – групповое восприятие (определение глобальных характеристик среды по локальным наблюдениям) [3, 4]. Байесовский алгоритм [5] вычисляет вероятности гипотез о состоянии среды, что дает ему преимущества перед частотными методами. Однако его поведение в динамических средах (перемещение объектов, флуктуации признаков) изучено недостаточно.

Цель работы – оценить влияние двух типов динамики (перестановка клеток, стохастическая генерация цвета) на скорость сходимости и точность байесовского алгоритма по сравнению со статическим случаем.

Сцена – сетка 40×40 клеток (1600), 5 цветов. Рой – 20 агентов. На каждом шаге агент перемещается, определяет цвет, обменивается данными. Глобальная характеристика – распределение цветов. Три альтернативы: $A_1$ (доминирование 60 %), $A_2$ (40 %), $A_3$ (равномерное, по 20 %).

Рассматриваются три типа динамики. Статическая – фиксированное распределение, приведенное в таблице 1. Перестановка клеток – обмен 800 пар клеток на каждом шаге (глобальное распределение сохраняется). Стоха-

стическая генерация – цвет каждой клетки пересчитывается по вероятностям из таблицы 1 [6].

Доля исправных агентов – 100 %, 100 итераций. Оценивалась вероятность правильного выбора (апостериорная).

ТАБЛИЦА 1. Распределение вероятностей цветов для рассматриваемых сцен

| | $A_1$ | $A_2$ | $A_3$ |
|---|---|---|---|
| $p(a_{желтый} / A_i)$ | 0,6 | 0,15 | 0,2 |
| $p(a_{синий} / A_i)$ | 0,1 | 0,4 | 0,2 |
| $p(a_{зеленый} / A_i)$ | 0,1 | 0,15 | 0,2 |
| $p(a_{фиолетовый} / A_i)$ | 0,1 | 0,15 | 0,2 |
| $p(a_{голубой} / A_i)$ | 0,1 | 0,15 | 0,2 |

На рисунках 1-3 приведены результаты моделирования для сцен $A_1$-$A_3$ соответственно.

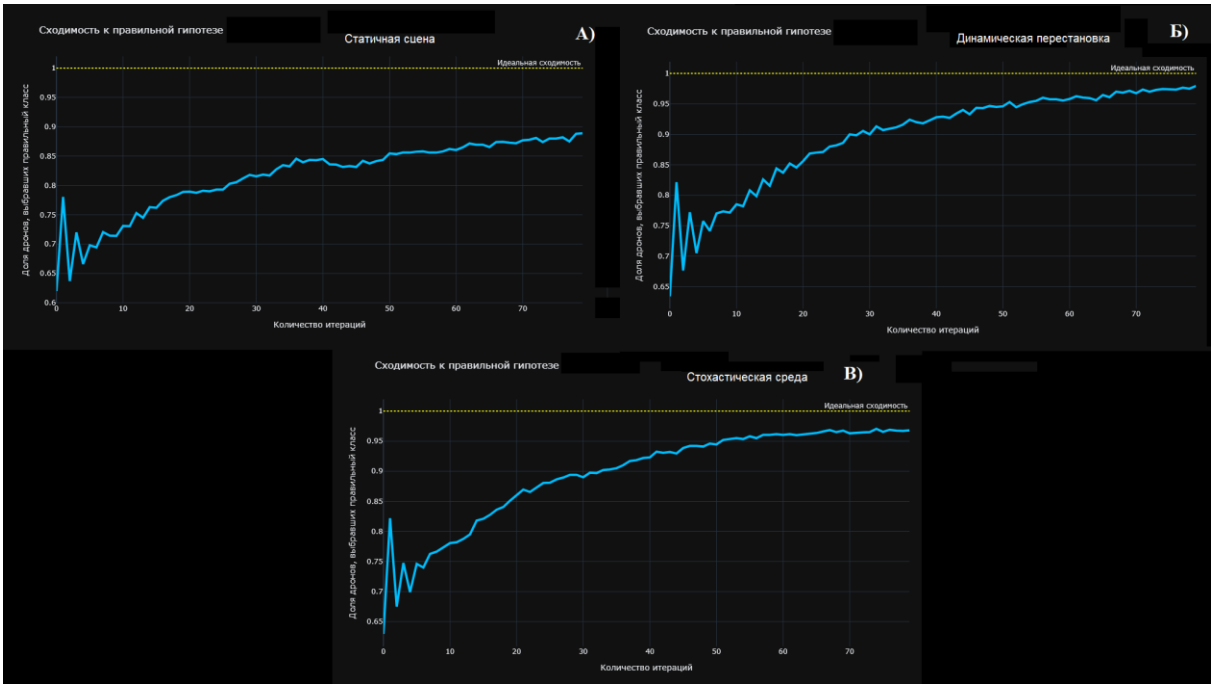



Рис. 1. Моделирование для сцены $A_1$

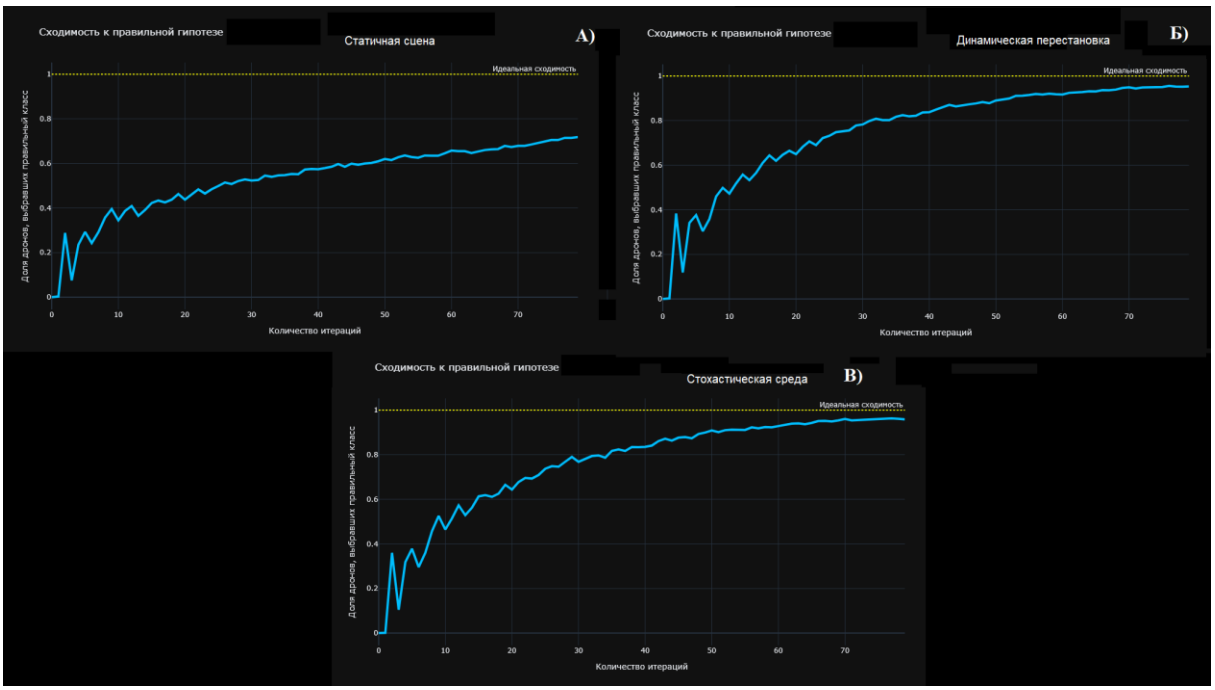



Рис. 2. Моделирование для сцены $A_2$

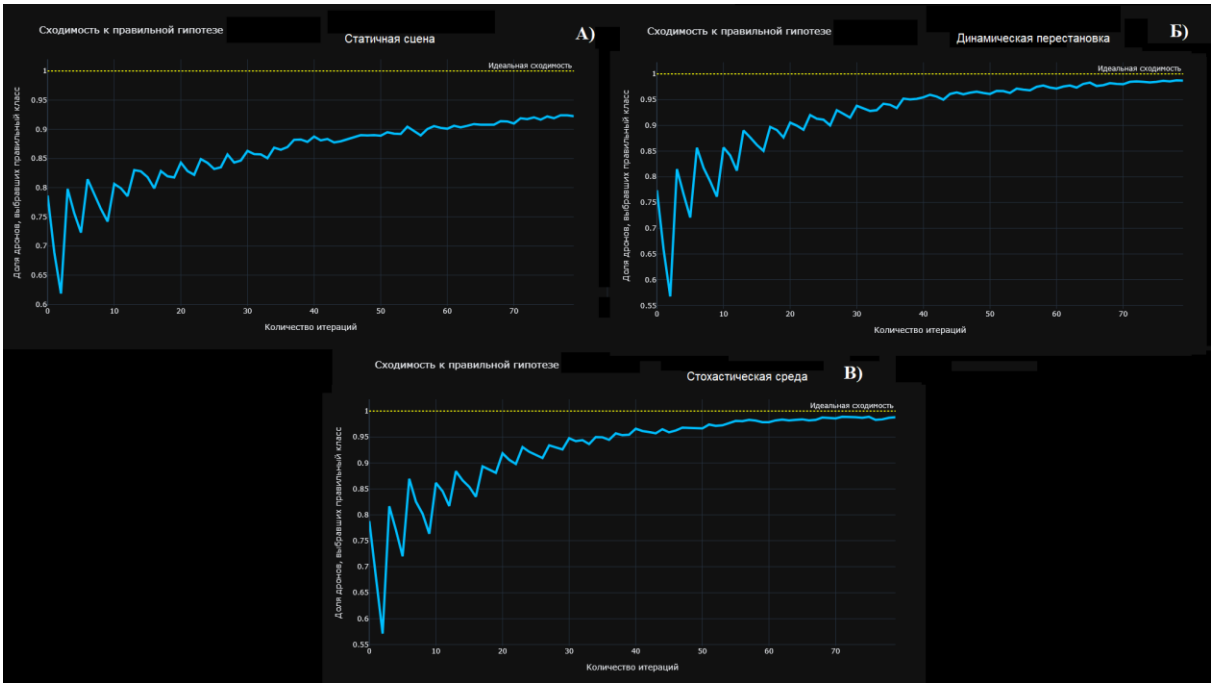



Рис. 3. Моделирование для сцены $A_3$

В сцене $A_1$ (с сильным доминированием одного цвета) имеем следующие результаты. Для статичной сцены имеем сходимость к 90 % корректно принимающих решение дронов роя за 80 итераций. Для динамических сред (как для перестановочной, так и стохастической) сходимость к тому же зна-

чению происходит за 30 шагов итераций, что в 2,3 раза быстрее. За 80 шагов итераций в динамических средах имеем итоговое значение точности 97 %.

В сцене $A_2$ (с умеренным доминированием одного цвета) имеем следующие результаты. Для статичной сцены имеем сходимость значения точности к 70 % (за 80 итераций). Для динамических сред сходимость к тому же значению происходит за 45 итераций, итоговое ускорение – в 1,6 раз. За 80 шагов итераций в динамических средах итоговое значение точности – 95 %.

В сцене $A_3$ (с равномерным распределением цветов) имеем следующие результаты. Для статичной сцены имеем сходимость значения точности к 95 % (за 80 итераций). Для динамических сред сходимость к тому же значению происходит за 40 итераций, итоговое ускорение – в 2 раз. За 80 шагов итераций в динамических средах итоговое значение точности – 98 %, незначительность увеличения итогового значения связана с большим исходным значением точности (в статичном случае).

На основании проведенного анализа можно сделать вывод, что в динамических средах байесовский алгоритм значительно увеличивает скорость сходимости для всех типов сцен (в 1,5 – 2 раза) без уменьшения точности. При этом характер динамики влияет на увеличение скорости работы алгоритма незначительно: наибольшее ускорение наблюдается для сцен с равномерным распределением ($A_3$) и с сильным превалированием одного цвета ($A_1$).

## Заключение

На основании проведенного исследования можно видеть, что байесовский алгоритм группового восприятия успешно может использоваться для работы в динамических средах, поскольку скорость его сходимости не только не уменьшается, а даже увеличивается по сравнению со статичной средой. Исходя из этого, можно говорить о возможности практического применения данного алгоритма для работы в нестационарных средах, например мониторинг подвижных объектов или поиск объектов в изменяющихся условиях. Дальнейшими направлениями исследования можно назвать учет отказов сенсоров при исследовании работы алгоритма в динамических средах, а также разработка адаптивного критерия остановки для более точного и детального анализа работы предложенного алгоритма и для выработки критерия принятия решения роем роботов.

**Список используемых источников**

1. Dorigo M., et al.: Swarm robotics. Scholarpedia. 2014. N 9(1). P. 1463/

2. Каляев И. А., Гайдук А. Р., Капустян С. Г. Модели и алгоритмы коллективного управления в группах роботов. М.: ФИЗМАТЛИТ, 2009. 280 с.

3. Valentini G., et al.: Efficient decision-making in a self-organizing robot swarm: On the speed versus accuracy trade-o // Proc. of the 14th Int. Conf. on Autonomous Agents and Multiagent Systems. 2015. PP. 1305.

4. Valentini G., Hamann H., Dorigo M.: Self-organized collective decision making: The weighted voter model // Proc. of the 13th Int. Conference on Autonomous Agents and Multiagent Systems. 2014. PP. 45.

5. Новиков Е. А. Алгоритм коллективного восприятия сцены на основе байесовского решающего правила // Молодой исследователь Дона. 2026; № 7(4).

6. Зикратов И. А., Зикратова Т. Н., Новиков Е. А. Реализация стратегии коллективного восприятия в самоорганизующейся роевой системе с использованием байесовского решающего правила. Труды учебных заведений связи, 2025. Т. 11. № 3. С. 108-118. DOI:10.31854/1813-324X-2025-11-3-108-118. EDN: XTDMRI.

*Статья представлена научным руководителем, профессором кафедры ИУС СПбГУТ, доктором технических наук, профессором И. А. Зикратовым.*

## BAYESIAN ALGORITHM FOR COLLECTIVE PERCEPTION UNDER VARIOUS TYPES OF DYNAMIC ENVIRONMENT CHANGES

**Novikov E. A.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The Bayesian collective perception algorithm is studied under static, cell-permutation, and stochastic color generation environments. Python simulations show that dynamics accelerates convergence 1.5–2 times without accuracy loss. The greatest effect is for uniform feature distribution. The algorithm is recommended for non-stationary environments.*

***Key words:*** *swarm robotics, robot collective, swarm intelligence, multi-agent robotic systems, collective perception, Bayesian decision rule*

**УДК 621.391**
**ГРНТИ 49.33.29**

# ОБНАРУЖЕНИЕ МНОЖЕСТВА СОТ В 5G NR ПРИ НАЧАЛЬНОМ ПОИСКЕ В УСЛОВИЯХ ШУМА И ВЗАИМНЫХ ПОМЕХ

**В. О. Орехова, И. Ф. Павлюк, Г. А. Фокин**

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

*В сетях 5G NR пользовательское оборудование находится в зоне действия большого количества базовых станций. Основной задачей начального доступа является не только обнаружение обслуживающей соты, но и идентификация соседних базовых станций для выбора соты с наилучшим уровнем сигнала и подготовки процедуры хэндовера. В статье решается задача идентификации нескольких базовых станций 5G NR при начальном поиске в условиях аддитивного белого гауссовского шума и взаимного влияния сигналов. Предложен алгоритм, обнаруживающий не один, а несколько идентификаторов сот, в отличие от известных методов, ориентированных на выделение единичного глобального максимума корреляции. С помощью имитационного моделирования в среде MATLAB получены количественные оценки вероятности правильного обнаружения нескольких Cell ID в зависимости от отношения сигнал/шум и разницы уровней мощности сигналов.*

***генерация сигналов, 5G NR, MATLAB, SSB, PCI, PSS, SSS.***

В реальных условиях абонентские терминалы находятся в зоне действия не одной, а нескольких базовых станций. Однако алгоритмы начального поиска, реализованные в симуляционных средах, таких как MATLAB, ориентированы на выделение одного максимума корреляции сигналов синхронизации PSS/SSS и не рассчитаны на одновременное обнаружение множества идентификаторов сот. Реальная радиообстановка осложняется воздействием шума, а также различный уровнем мощности передатчиков. Это приводит к тому, что сигнал соседней соты может быть подавлен более сильным.

Таким образом, возникает необходимость в модификации алгоритма поиска для идентификации заданного количества сот и в исследовании его помехоустойчивости в условиях шума и разницы уровней мощности сигналов.

## Стандартный алгоритм поиска

В сетях 5G NR процедура начального доступа опирается на обнаружение блока сигналов синхронизации (SSB), который передается базовой стан-

цией с определенной периодичностью. SSB включает в себя первичный (PSS) и вторичный (SSS) сигналы синхронизации, а также физический широковещательный канал (PBCH). Идентификатор физической соты определяется по формуле:

$$PCI = 3 \times N_{ID}^{1} + N_{ID}^{2},$$

где $N_{ID}^{1} \in \{0, 1, \dots, 335\}$ – идентификатор сигнала *SSS*, $N_{ID}^{2} \in \{0, 1, 2\}$ идентификатор сигнала *PSS* [1].

В рассматриваемом сценарии абонентское устройство находится в зоне действия K базовых станций. Принятый сигнал во временной области $y(n)$ представлен как суперпозиция сигналов от множества сот:

$$y(n) = \sum_{k=1}^{K} \sqrt{P_k} s_k(n - \tau_k) e^{j2\pi\Delta f_k n} + \omega(n).$$

Стандартный алгоритм 5G Toolbox вычисляет взаимную корреляцию y(n) с эталонными последовательностями PSS и SSS и оценивает временное смещение и индекс PSS поиском единственного максимума корреляционной функции [2]. После временной и частотной синхронизации, индекс SSS определяется поиском глобального максимума в частотной области. Главный недостаток подхода в том, что операция argmax выделяет только сигнал с максимальным значением корреляции. Для устранения этого недостатка предложен модифицированный алгоритм.

**Модифицированный алгоритм**

Блок схема алгоритма представлена на рис. 1. Входными данными являются принятый сигнал y(n) и его параметры: частота дискретизации, шаблон SSB, Lmax, минимальная ширина канала. Алгоритм не использует функцию cellSearch и реализован с помощью функций: nrPSS, nrSSS, nrTimingEstimate, nrOFDMDemodulate, findpeaks.

На первом этапе формируются три опорные ресурсные сетки SSB размером 240×4 элемента. В позициях PSS занесены последовательности nrPSS для $N_{ID}^{2}$. Сетки используются как эталоны для вычисления корреляции с принятым сигналом функцией nrTimingEstimate. Результатом являются три массива корреляций на каждое значение $N_{ID}^{2}$.

Далее реализуется многопиковый детектор. Для каждой корреляции функция findpeaks ищет локальные максимумы, превышающие амплитудный порог $\eta_{\text{p}} \times R_n(\tau)$ и разнесенные между собой не менее чем на $0{,}85 \times T_{SSB}$, где $T_{SSB}$ – период следования SSB, $\eta_p$ – безразмерный коэффициент.

Найденные пики объединяются в единый массив. Главное отличие от стандартного коррелятора в том, что вместо одного глобального максимума возвращается множество локальных пиков, каждый из которых соответствует кандидату на одну физическую соту.

После кандидаты упорядочиваются по убыванию амплитуды PSS, и из них формируется массив фиксированного размера. Запас по числу кандидатов необходим, поскольку один SSB-burst может порождать несколько локальных максимумов, подлежащих объединению.

Для каждого кандидата выполняется внутренний цикл проверки. Принятый сигнал смещается на временной сдвиг и демодулируется функцией nrOFDMDemodulate.

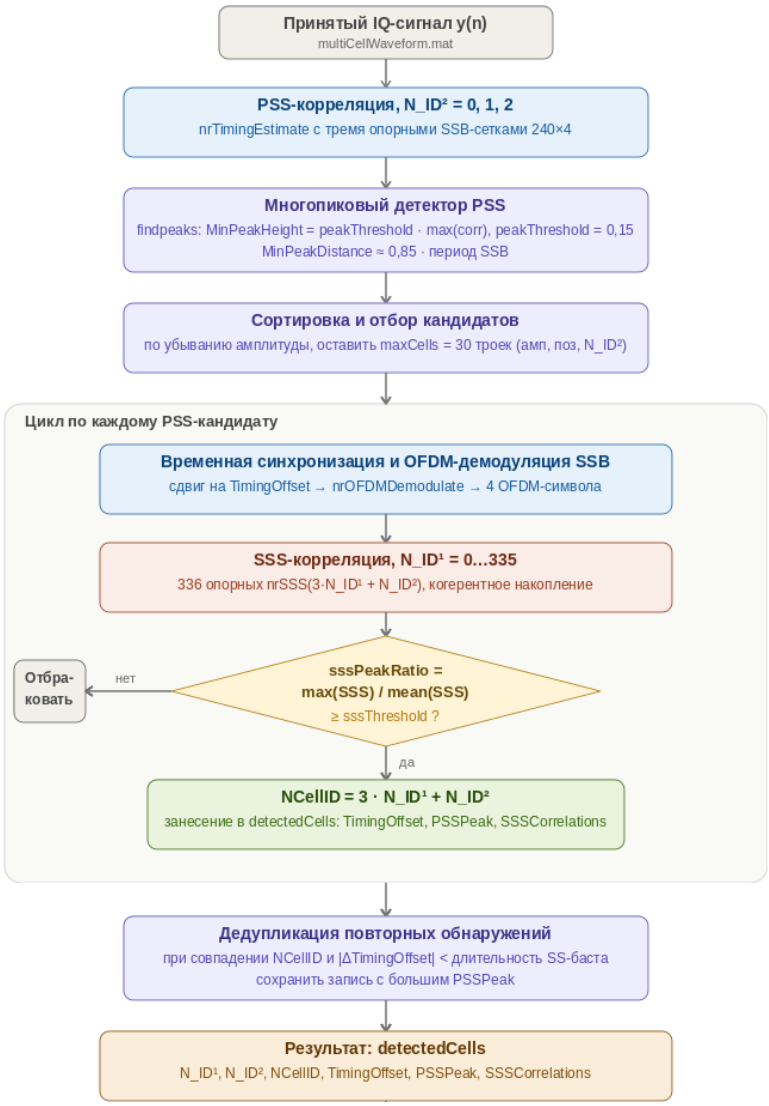



Рис. 1. Блок-схема алгоритма

Из ресурсной сетки извлекаются первые четыре OFDM-символа SSB. Затем выполняется корреляция SSS для всех $N_{ID}^{1}$ , а также проверяется отно-

шение пиковой величины корреляции SSS к ее среднему уровню (pSSS). Если pSSS ниже порога, то кандидат отбраковывается. Иначе фиксируется $N_{ID}^{1}$ и вычисляется $PCI$.

Завершающий блок выполняет дедупликацию повторных обнаружений одной и той же соты. Результатом будет массив detectedCells, содержащий для каждой обнаруженной соты поля $N_{ID}^{1}$, $N_{ID}^{2}$, $PCI$, TimingOffset, PSSPeak и вектор корреляций SSS.

**Имитационное моделирование**

Параметры трех передающих базовых станций приведены в таблице 1. Сигналы передаются в шаблоне SSB Case B [3]. Принятый сигнал y(n) сформирован как суперпозиция временных реализаций сот с амплитудным масштабированием и временны́ми сдвигами при SNR = 25 дБ. Параметры детектора: maxCells = 30, $\eta_p$ = 0,15, $\eta_s$ = 5.

ТАБЛИЦА 1. Параметры сценария

| Сота | *PCI* | $N_{ID}^{1}$ | $N_{ID}^{2}$ | Мощность, дБ | Задержка, семпл |
|---|---|---|---|---|---|
| 1 | 102 | 34 | 0 | 0 | 0 |
| 2 | 277 | 97 | 1 | -4 | 1 500 |
| 3 | 300 | 100 | 0 | -3 | 12 000 |

На корреляциях PSS на рис. 2 для $N_{ID}^{2}$ = 0 выделены пики сот 102 и 300, для $N_{ID}^{2}$ = 1 – пики соты 277, для $N_{ID}^{2}$ = 2 пики отсутствуют. На корреляциях SSS (рис. 3) для подтвержденных кандидатов наблюдаются единственные пики при $N_{ID}^{1}$ = 34, 92 и 100; pSSS превышает 100, что выше порога $\eta_s$ = 5. Три соты восстановлены корректно с подтверждением SSS.

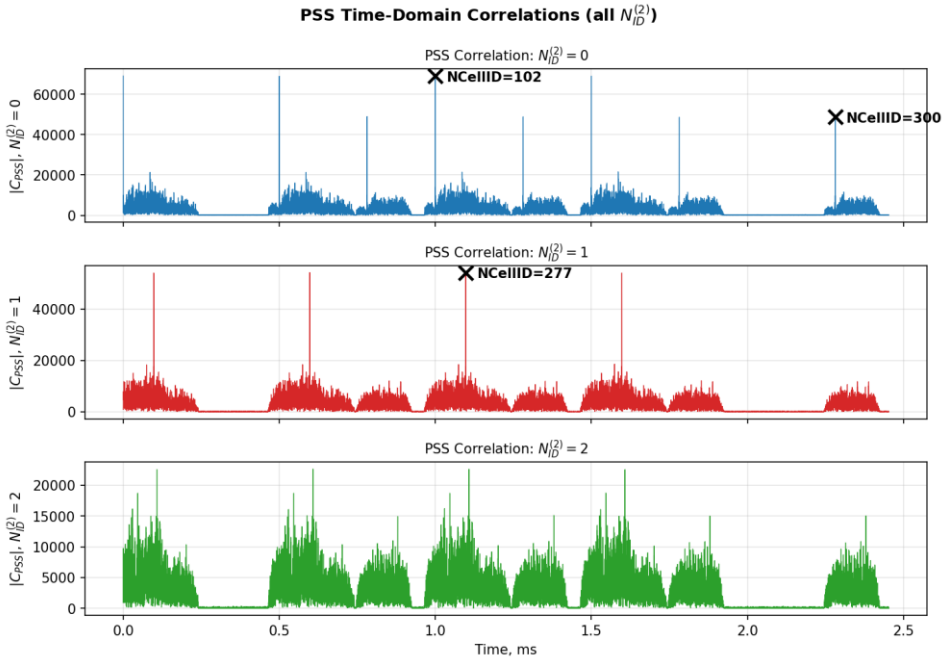



Рис. 2. Корреляции PSS во временной области для трех значений $N_{ID}^{2}$

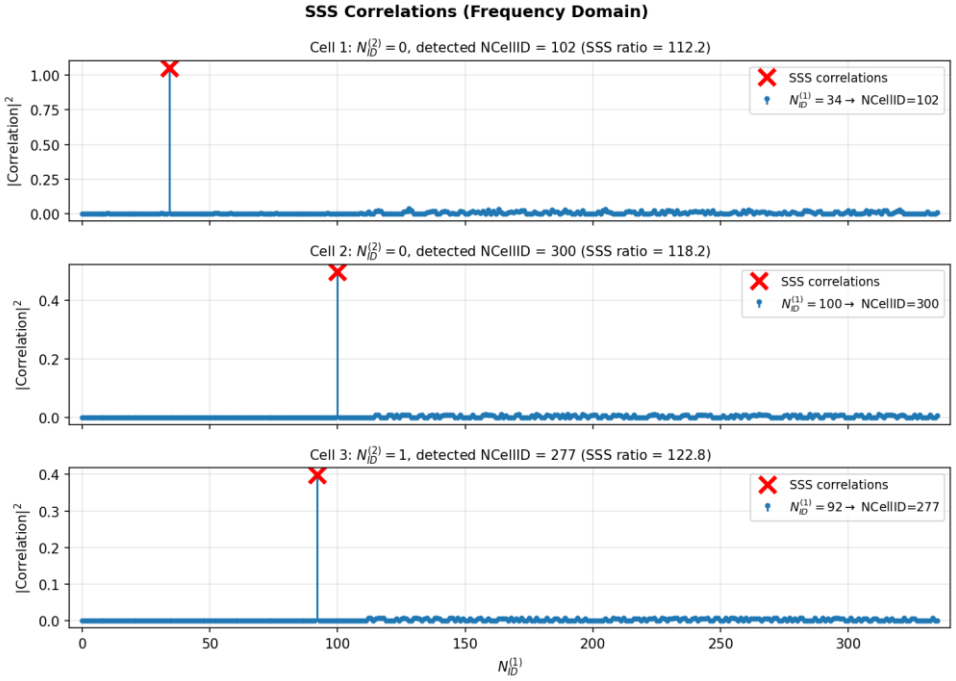



Рис. 3. Корреляции SSS в частотной области для подтвержденных сот

Стандартная процедура *cellSearch* возвращает соту 102, поскольку оперирует глобальным максимумом корреляции и игнорирует пики меньшей амплитуды. При разнице уровней мощности до 4 дБ предложенный алгоритм идентифицирует все три соты, что подтверждает применимость метода для измерения соседних сот и подготовки процедуры хэндовера.

## Заключение

Предложен алгоритм многопикового обнаружения нескольких сот 5G NR в условиях шума и взаимных помех. В отличие от штатной процедуры, основанной на поиске единственного глобального максимума корреляции, алгоритм возвращает множество локальных пиков PSS и подтверждает их по корреляции SSS, что позволяет идентифицировать одновременно несколько идентификаторов Cell ID.

**Список используемых источников**

1. 3GPP TS 36.101. Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Radio Transmission and Reception // 3rd Generation Partnership Project; Technical Specification Group Radio Access Network V11.4.0 (2013-03) С. 293-297. URL: https://www.arib.or.jp/english/html/overview/doc/STD-T104v2_00/5_Appendix/Rel11/36/36101-b40.pdf (дата обращения: 23.04.2026).

2. MathWorks. 5G Toolbox. "NR Cell Search and MIB and SIB1 Recovery" // MATLAB Documentation. URL: https://www.mathworks.com/help/5g/ug/nr-cell-search-and-mib-and-sib1-recovery.html (дата обращения: 23.04.2026).

3. Павлюк И. Ф., Орехова В. О. Генерация LTE, 5G NR спектрограмм для обучения сети семантической сегментации // Подготовка профессиональных кадров в магистратуре в эпоху цифровой трансформации (ПКМ-2024). V Всероссийская научно-техническая и научно-методическая конференция магистрантов и их руководителей: сб. науч. ст. в 2-х т. СПб.: СПбГУТ, 2025. Т. 3. С. 142-147. EDN: DSBBIZ.

## DETECTION OF A MULTIPLE OF CELLS IN 5G NR DURING INITIAL SEARCH IN NOISE AND INTERFERENCE CONDITIONS

**Orekhova V., Pavlyuk I., Fokin G.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*In 5G NR networks, user equipment is located within the coverage area of a large number of base stations. The primary task of initial access is not only to detect the serving cell but also to identify neighboring base stations in order to select the cell with the best signal level and prepare for the handover procedure. This paper addresses the problem of identifying multiple 5G NR base stations during the initial search under conditions of additive white Gaussian noise and signal interference. An algorithm is proposed that detects not one but several cell identifiers, unlike known methods focused on identifying a single global correlation maximum. Using simulation modeling in the MATLAB environment, quantitative estimates of the probability of correctly detecting multiple Cell ID were obtained depending on the signal-to-noise ratio and the difference in signal power levels.*

***Key words:*** *signal generation, 5G NR, MATLAB, SSB, PCI, PSS, SSS*

**УДК 654.739**
**ГРНТИ 49.33.29**

# АРХИТЕКТУРА БОРТОВОЙ МОНОКУЛЯРНОЙ ВИДЕОСИСТЕМЫ И МЕТОДЫ ОБРАБОТКИ ВИДЕОИНФОРМАЦИИ ДЛЯ ОБЛЕТА ПРЕПЯТСТВИЙ

**А. А. Павловская, М. В. Павловский, С. Л. Фёдоров**

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

*Предлагается архитектура бортовой монокулярной видеосистемы БПЛА, объединяющая классический оптический поток с легкой нейросетевой моделью глубины для автономного облета препятствий. Экспериментально показано, что гибридный алгоритм снижает количество ложных срабатываний на 28 % на слаботекстурированных поверхностях по сравнению с чистым оптическим потоком при сохранении частоты обработки 16 кадров в секунду на модуле NVIDIA Jetson Nano. Система работоспособна при скоростях полета до 8 м/с и предназначена для использования в условиях отсутствия GPS.*

***монокулярное зрение, избегание препятствий, оптический поток, нейросетевая оценка глубины, БПЛА, встраиваемые системы, видеотракт***

Автономное пилотирование БПЛА в условиях отсутствия или недоступности сигналов ГНСС – внутри помещений, в лесных массивах или узких городских «каньонах» – требует альтернативных методов пространственной ориентации [1]. Использование стереопар или лидаров увеличивает массу, стоимость и энергопотребление, что критично для малых беспилотных аппаратов. Монокулярная камера легка и компактна, однако задача оценки расстояний по одному изображению является некорректно поставленной и нуждается в специальных алгоритмических решениях [2]. Целью настоящей работы является разработка архитектуры бортовой монокулярной видеосистемы и методов обработки видеоинформации [3], обеспечивающих обнаружение препятствий и формирование управляющих сигналов для их облета в реальном времени.



Рис. 1. Вычислительный модуль NVIDIA Jetson Nano

В состав разработанной архитектуры входят видеодатчик с глобальным затвором, специализированный процессор обработки изображений (ISP), вычислительный модуль для выполнения алгоритмов компьютерного зрения и интерфейс связи с полетным контроллером. Ключевым требованием к видеосенсору является минимальная задержка (менее 20 мс) и отсутствие искажений типа «желе» при резких перемещениях, что обеспечивается использованием матрицы с глобальным затвором [4]. В задачи ISP входит декейеринг, коррекция дисторсии объектива и шумоподавление; на выходе формируется видеопоток в формате YUV. Вычислительное ядро построено на модуле NVIDIA Jetson Nano (Рис. 1) и способно параллельно обрабатывать кадры с частотой 15–20 fps при энергопотреблении 5–7 Вт. Функциональная схема взаимосвязи блоков показана на Рис. 2.

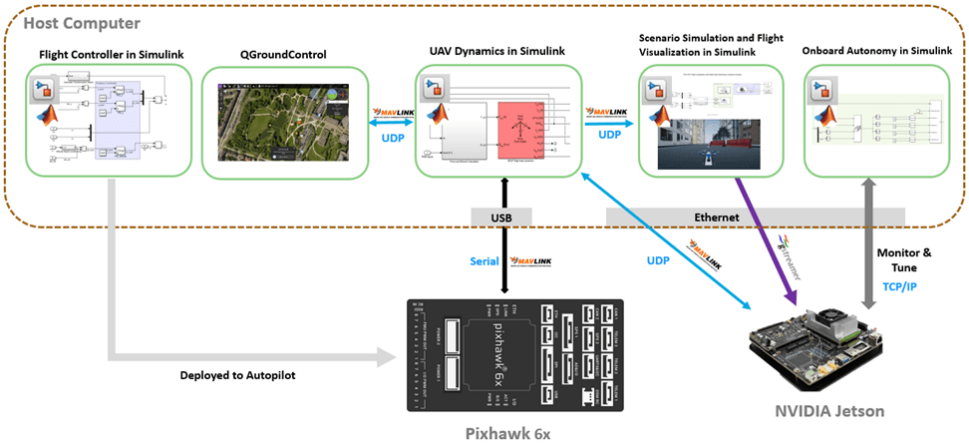



Рис. 2. Функциональная схема бортовой монокулярной видеосистемы

Традиционный способ оценки глубины по данным движущейся монокулярной камеры – анализ оптического потока [5], то есть поля векторов смещения пикселей между соседними кадрами. Для вычисления плотного оптического потока используется метод Farneback, реализованный в библиотеке OpenCV. Время до столкновения с препятствием (Time-to-Contact, TTC) оценивается по формуле:

$$TTC = \frac{f}{v} \cdot \frac{d}{dx}, \quad (1)$$

где $f$ – фокусное расстояние камеры в пикселях, $v$ – скорость сближения, $d$ – текущее расстояние до объекта в условных единицах, определяемое по величине расхождения оптического потока. При значении TTC менее 0,5 секунды полетный контроллер получает команду на торможение или изменение курса. Достоинство метода заключается в низкой вычислительной

сложности [6]. Недостатком является низкая эффективность на сценах со слабой текстурой (однотонная стена, небо, гладкая поверхность), где оптический поток не формируется из-за отсутствия различимых признаков.

Для сцен с недостатком текстур применяется легкая нейросетевая модель на основе архитектуры MobileNetV3 в качестве энкодера и мелкого декодера с крестовыми связями. Модель обучена на наборе данных NYU Depth V2 с приведением входного кадра к разрешению 224×224 пикселя. На выходе формируется карта глубины, нормализованная к диапазону от 0 (ближний объект) до 1 (дальний объект). Инференс модели выполняется на GPU модуля Jetson Nano за 25–30 мс. Чтобы снизить вычислительную нагрузку, нейросеть вызывается не на каждом кадре, а с шагом в 5 кадров (то есть 3–4 раза в секунду). Для сцен, где оптический поток дает надежные значения, нейросеть не запускается. Решающее правило комбинирования имеет следующий вид:

$$d_{final} = \begin{cases} d_{OF}, & \text{если дисперсия текстур} > T_{var} \\ d_{CNN}, & \end{cases}. \quad (2)$$

Здесь $T_{var}$ – экспериментально подобранный порог, разделяющий текстурные и слаботекстурированные сцены. Такой гибридный подход позволяет сохранить высокую частоту обработки при гарантированном обнаружении препятствий даже на однородных поверхностях.

На основе полученной карты глубины выделяются коллизионно-опасные зоны – области, для которых значение глубины оказывается меньше критического порога $D_{cr}$. Далее вычисляется вектор отклонения как смещение центра масс опасной зоны относительно оптического центра кадра. Управляющий сигнал на полетный контроллер формируется в виде нормализованных приращений по углам рыскания и тангажа. Алгоритм уклонения от препятствия стремится удерживать опасную зону вне центральной области кадра [7]. Для предотвращения осцилляций и рывков в управлении применяется низкочастотная фильтрация управляющих сигналов с постоянной времени 0,2 секунды.

Экспериментальная проверка выполнялась на лабораторном стенде, состоящем из квадрокоптера собственной сборки с камерой IMX219 (глобальный затвор, разрешение 640×480 пикселей, фокусное расстояние 2,1 мм) и вычислителем Jetson Nano. Тесты проводились в трех типовых сценариях: коридор с хорошо выраженной текстурой стен, помещение с гладкими

окрашенными поверхностями и смешанный случай. Итоговые данные сведены в таблицу 1.

В текстурированном коридоре гибридный алгоритм успешно обнаруживал и облетал препятствия в 94 % случаев. Для сравнения, метод, основанный только на оптическом потоке, показал 92 %, а нейросетевой подход – 88 %. При испытаниях в помещении с гладкими стенами результативность классического метода резко падала до 34 %, тогда как гибридный вариант сохранил высокий уровень в 93 %, практически не уступив нейросетевому (91 %). Средняя скорость обработки у гибридного решения составила 16 кадров в секунду. Это несколько ниже, чем у оптического потока (18 fps), но выше, чем у чисто нейросетевого подхода (12 fps). Таким образом, использование гибридной схемы позволило уменьшить количество ложных срабатываний на 28 % в слаботекстурированных сценах ценой потери всего двух кадров в секунду.

ТАБЛИЦА 1. Сравнение монометодных и гибридного подходов

| Сценарий | Чистый оптический поток | Только нейросеть | Гибридный метод |
|---|---|---|---|
| Текстурный коридор, % успеха | 92 | 88 | 94 |
| Гладкая стена, % успеха | 34 | 91 | 93 |
| Средняя частота обработки, fps | 18 | 12 | 16 |

По итогам исследования была спроектирована бортовая монокулярная видеосистема для автономного облета препятствий, объединяющая алгоритм оптического потока с нейросетевой оценкой глубины. Эксперименты показали, что предложенный подход обеспечивает надежное обнаружение препятствий на поверхностях с низкой текстурной информативностью, где классические методы часто оказываются неэффективными. При этом сохраняется высокая скорость обработки видео, достаточная для работы в реальном времени. Работоспособность системы подтверждена при полетах со скоростью до 8 м/с. В перспективе целесообразно перенести нейросетевой модуль на специализированные аппаратные ускорители ИИ (например, Google Coral Edge TPU или аналоги). Это позволит снизить энергопотребление вычислительной части и поднять производительность обработки видеопотока примерно до 30 кадров в секунду.

**Список используемых источников**

1. Форсайт Д., Понс Ж. Компьютерное зрение. Современный подход. М.: Вильямс, 2020. 928 с.

2. Szeliski R. Computer Vision: Algorithms and Applications. 2nd ed. Springer, 2022. 925 p.

3. Павловская А. А., Павловский М. В., Фёдоров С. Л. Методы слияния данных с сенсоров видимого и инфракрасного диапазонов, установленных на беспилотном летательном аппарате // 66-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2026); сб. науч. ст. СПб.: СПбГУТ, 2026. Т. 1. С. 291-296.

4. Badrinarayanan V., Kendall A., Cipolla R. SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2017. Vol. 39. N 12. PP. 2481-2495. DOI: 10.1109/TPAMI.2016.2644615.

5. Павловская А. А., Павловский М. В., Фёдоров С. Л. Оценка качества закодированных видеоизображений // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС 2026); сб. науч. ст. СПб.: СПбГУТ, 2025. Т. 3. С. 485-490.

6. Farneback G. Two-Frame Motion Estimation Based on Polynomial Expansion // Scandinavian Conference on Image Analysis. 2003. PP. 363-370. DOI: 10.1007/3-540-45103-X_50.

7. Ranftl R., Lasinger K., Hafner D. et al. Towards Robust Monocular Depth Estimation: Mixing Datasets for Zero-Shot Cross-Dataset Transfer // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2022. Vol. 44. N 3. P. 1623–1637. DOI: 10.1109/TPAMI.2020.3019967.

## ARCHITECTURE OF AN ONBOARD MONOCULAR VIDEO SYSTEM AND VIDEO INFORMATION PROCESSING METHODS FOR OBSTACLE AVOIDANCE

**Pavlovskaya A., Pavlovsky M., Fedorov S.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article proposes an architecture of an onboard monocular video system for UAVs, combining classical optical flow with a lightweight neural network depth model for autonomous obstacle avoidance. It is experimentally shown that the hybrid algorithm reduces the number of false positives by 28 % on low-textured surfaces compared to pure optical flow while maintaining a processing rate of 16 frames per second on an NVIDIA Jetson Nano module. The system is operational at flight speeds up to 8 m/s and is intended for use in GPS-denied conditions.*

***Key words:*** *monocular vision, obstacle avoidance, optical flow, neural network depth estimation, UAV, embedded systems, video path*

**УДК 654.739**
**ГРНТИ 49.33.29**

# ДЕТЕКТИРОВАНИЕ ТЕПЛОВЫХ АНОМАЛИЙ ПОСРЕДСТВОМ БОРТОВОГО ТЕПЛОВИЗОРА БПЛА

**А. А. Павловская, М. В. Павловский, С. Л. Фёдоров**

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

*В статье рассматривается метод автоматического детектирования тепловых аномалий по видеопотоку с бортового тепловизора беспилотного летательного аппарата. Описан двухэтапный алгоритм, включающий гистерезисную пороговую сегментацию, морфологическую фильтрацию и адаптивную модель фона на основе экспоненциального скользящего среднего. Экспериментальная верификация на задаче мониторинга линий электропередачи показала повышение полноты детектирования до 92 процентов при снижении ложных срабатываний до 5 процентов.*

***беспилотный летательный аппарат, тепловизор, детектирование аномалий, инфракрасная съемка, пороговая сегментация, морфологическая фильтрация***

Современные беспилотные летательные аппараты все чаще оснащаются тепловизионными камерами длинноволнового инфракрасного диапазона (8–14 мкм). В отличие от традиционных RGB-сенсоров, тепловизор регистрирует собственное излучение объектов, что позволяет вести наблюдение в полной темноте, в условиях дыма, тумана, а также выявлять скрытые дефекты по аномальному нагреву [1]. Тепловизионное изображение представляет собой карту распределения температуры, где различные объекты (люди, техника, элементы ландшафта, дефектные соединения) отображаются в виде контрастных областей. Переход от регистрируемого термографического распределения к формализованному акту обнаружения аномалии сопряжен с необходимостью применения вычислительных схем, компенсирующих как дискретность пространственной выборки, так и вариативность коэффициента спектральной излучательности, вносящую систематическую погрешность в показания.

В формальной постановке задача выявления тепловых отклонений сводится к сегментации кадрового потока с выделением областей, чей температурный профиль демонстрирует статистически значимые расхождения с модельным представлением о фоновом поле. В числе детектируемых ти-

пов фигурируют локальные перегревы, характеризующиеся точечной пространственной локализацией (неисправные контактные соединения, опорные узлы), протяженные зоны с повышенной теплоотдачей, типичные для ландшафтных возгораний, а также низкоконтрастные сигнатуры, например, биологические объекты на подстилающей поверхности, аккумулировавшей солнечную радиацию [2, 3]. Существенным дестабилизирующим фактором выступает нестационарность теплового фона, обусловленная суточным ходом метеорологических параметров и перераспределением тепла в конструкционных элементах.

Принципиальное различие между тепловизионным и оптическим каналами регистрации заключается в критериальной базе: в первом случае решающее правило опирается не на морфологические или фактурные признаки, а на величину абсолютной температуры и характер ее изменения в пространственно-временном континууме, что требует учета градиентных характеристик как по координатам, так и по времени. Это позволяет использовать относительно простые пороговые методы, но накладывает жесткие требования к калибровке сенсора и учету коэффициента эмиссии.

Предлагаемая схема обработки тепловизионных данных предусматривает последовательное выполнение нескольких операций, объединенных в два основных этапа. Сначала выполняется выделение потенциально аномальных областей на основе гистерезисной пороговой обработки, после чего сформированные области проходят пространственную и временную фильтрацию.

Пусть *T(x,y,t)* – обозначает температуру, зарегистрированную в пикселе с координатами (*x,y*) в момент времени *t*. Перед использованием в алгоритме температурные значения подвергаются калибровке и коррекции с учетом излучательной способности исследуемой поверхности. Для формирования первичной бинарной маски вводится двухуровневый пороговый критерий:

$$M(x,y,t) = \begin{cases} 1, \text{если } T(x,y,t) \geq \theta_{high} \\ 1, \text{если } T(x,y,t) \geq \theta_{low} \text{ и существует соседний пиксель с } M = 1, \\ 0, \text{в остальных случаях} \end{cases} \quad (1)$$

Здесь $\theta_{high}$ соответствует верхнему порогу температуры (например, 80 °C для перегретых соединений ЛЭП), а $\theta_{low}$ – нижнему. Для рассматриваемой задачи разность между ними может составлять порядка 10–15 °C;

значение верхнего порога, например, может быть принято равным 80 °C при обнаружении перегрева контактных соединений ЛЭП. При проверке пространственной связанности используется 8-связная окрестность.

Введение двухуровневой системы отсчета позволяет нивелировать эффект фрагментации выделяемой области, возникающий при флуктуациях измеряемых значений в окрестности единственного порогового уровня. Пиксели, чьи температурные показатели локализуются в интервале между нижней $\theta_{low}$ и верхней $\theta_{high}$ границами, подвергаются ретенции в бинарном представлении исключительно при условии их пространственной сопряженности с зоной, превосходящей верхний порог. Подобный подход обеспечивает подавление изолированных шумовых артефактов и снижает долю дискретных включений, не обладающих статистической устойчивостью.

Полученное бинарное поле в дальнейшем пропускается через этап морфологической фильтрации. В целях ликвидации микродизъюнкций и упорядочения граничных контуров реализуется оператор замыкания: композиция дилатационного и эрозионного преобразований с применением структурирующего ядра размерностью 3×3 пикселя. Заключительным этапом выступает процедура трассировки связных областей, позволяющая перейти к количественному анализу выявленных тепловых неоднородностей на уровне отдельных объектов. Компоненты, площадь которых не достигает заданного минимального значения $S_{\min}$, исключаются из рассмотрения как потенциальные шумовые образования. Для условий съемки с высоты 30–50 м и использования тепловизионной матрицы 640×512 значение $S_{\min}$ может находиться в диапазоне 5–10 пикселей [4].

Пространственных признаков недостаточно для однозначного отделения развивающихся температурных аномалий от объектов, которые имеют стабильно повышенную температуру. Поэтому дополнительно учитывается изменение характеристик обнаруженной области во времени. Для каждой связной компоненты анализируется последовательность из K кадров, где (K=5…10). Скорость изменения максимальной температуры оценивается по конечной разности:

$$\frac{dT_{\max}}{dt} \approx \frac{T_{\max}(t)-T_{\max}(t-\Delta t)}{\Delta t}, \quad (2)$$

Для развивающегося горения типично $\frac{dT_{\max}}{dt} > 0$ с положительной второй производной, в то время как термически инертные объекты фона демон-

стрируют квазистационарный режим либо монотонное остывание. В качестве дополнительного критерия используется прирост площади аномальной области $\frac{dS}{dt} > 0$.

Фоновое состояние описывается адаптивной моделью на базе экспоненциального скользящего среднего:

$$\mu(x, y, t) = \alpha \cdot T(x, y, t) + (1 - \alpha) \cdot \mu(x, y, t - 1), (3)$$

где μ – текущая оценка фоновой температуры, α = 0,05…0,1 – коэффициент обновления модели. Тепловая аномалия фиксируется при

$$|T(x, y, t) - \mu(x, y, t)| > \sigma(x, y, t) \cdot k, (4)$$

где σ – оценка среднеквадратического отклонения фона, $k$ – доверительный множитель (как правило, 2–3). Указанный подход обеспечивает компенсацию суточного хода и метеорологической изменчивости без ручной коррекции пороговых значений.

Экспериментальная апробация алгоритма проведена на массиве тепловизионных видеозаписей, полученных с борта беспилотного летательного аппарата DJI Matrice 300 RTK. Для регистрации теплового излучения использовался тепловизионный модуль Zenmuse H20T с матрицей разрешением 640×512 пикселей и частотой съемки 30 кадров/с. В качестве объекта наблюдения был выбран участок воздушной линии электропередачи напряжением 110 кВ (рис. 1). На исследуемом участке присутствовали болтовые контактные соединения с признаками перегрева, наличие которых было подтверждено результатами инструментального контроля.

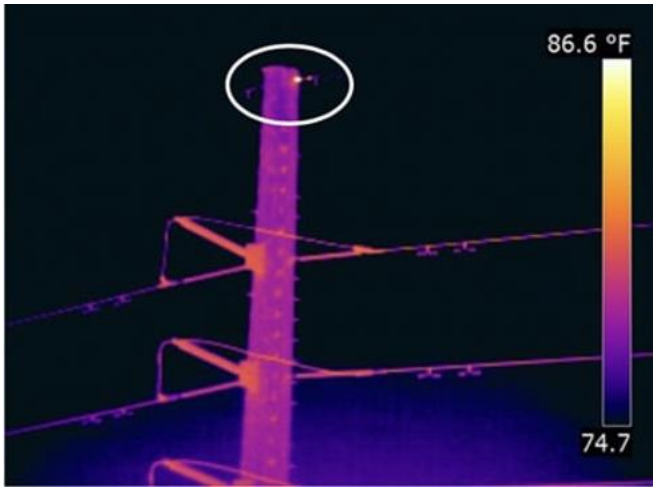



Рис. 1. Термограмма опоры ЛЭП с зоной перегрева, зарегистрированной тепловизором БПЛА

Результаты обработки показывают, что гистерезисная пороговая сегментация с верхним порогом $\theta_{high}$= 75°C и нижним $\theta_{low}$= 60°C позволяет оконтурить компактные связные области, отвечающие перегретым контактам. Исходная термограмма содержит участок опоры с выраженной температурной аномалией в зоне дефекта. На выходе алгоритма формируется бинарная маска: аномальная область маркируется единичным уровнем, фон нулевым. Локальные шумовые артефакты, не коррелирующие с дефектами, подавляются процедурой морфологической фильтрации.

Численные значения показателей достоверности детектирования для трех категорий объектов, полученные как при использовании классического метода с единственным жестким порогом, так и в рамках предлагаемой гистерезисной схемы с адаптивно подстраиваемым фоновым уровнем, сведены в Таблице 1. В качестве референтного критерия истинно-положительного срабатывания выступало подтверждение наличия термического дефекта наземными службами по результатам независимого термографического обследования.

В ходе экспериментальных испытаний верхняя и нижняя границы гистерезисного окна были зафиксированы на отметках $\theta_{high}$= 75°C и $\theta_{low}$= 60°C соответственно. Результирующее бинарное поле, сформированное по итогам двухпороговой фильтрации, демонстрировало образование пространственно-компактных связных кластеров в проекции зон локализации перегретых контактных узлов; при этом на исходном термографическом изображении соответствующий участок характеризовался устойчивым превышением температурных показателей над окружающими элементами несущей конструкции. В бинаризованном представлении аномальным областям присваивалась единица, тогда как фоновой компоненте соответствовали нулевые значения. Обособленные фрагменты, утратившие пространственную корреляцию с основным тепловым контрастом, элиминировались в процессе морфологической постобработки.

Сопоставительная оценка эффективности разработанного алгоритма производилась относительно эталонного варианта, базирующегося на единичном пороговом уровне, не зависящем от локальных особенностей распределения температурного поля. Анализ проводился для трех классов объектов: перегретых болтовых соединений, имитированных очагов возгорания и человека, находящегося на фоне лесного массива. В качестве критерия истинного обнаружения принималось наличие соответствующей аномалии, подтвержденной наземным термографическим контролем.

ТАБЛИЦА 1. Сравнение методов детектирования тепловых аномалий

| Тип объекта | Фиксированный порог | Гистерезис + адаптивный фон |
|---|---|---|
| Перегрев болтового соединения | 74 % / 18 % | 92 % / 5 % |
| Очаг пожара (имитация) | 68 % / 22 % | 89 % / 7 % |
| Человек на фоне леса | 55 % / 30 % | 84 % / 10 % |

Примечание: в каждой ячейке указана полнота (процент истинно обнаруженных аномалий) / частота ложных срабатываний.

Результаты сравнительного эксперимента показывают, что использование гистерезисной обработки совместно с адаптивным моделированием фона улучшает характеристики обнаружения по сравнению с фиксированным порогом. Для рассмотренных классов объектов полнота обнаружения возрастает в среднем на 18-20 процентных пунктов, тогда как частота ложных срабатываний уменьшается приблизительно в 3-4 раза. Наиболее высокие показатели получены при обнаружении перегрева болтовых соединений: полнота составила 92 % при частоте ложных срабатываний 5 %.

Несмотря на полученные результаты, применимость алгоритма зависит от теплофизических характеристик наблюдаемых поверхностей. Дополнительные сложности могут возникать при работе с материалами, излучательная способность которых близка к характеристикам окружающего фона. В качестве примера можно отметить окисленные алюминиевые поверхности. Кроме того, при резком изменении метеорологических условий адаптивная модель может обновляться недостаточно быстро, вследствие чего в переходные периоды возрастает вероятность ошибочного выделения температурных отклонений.

В целом предложенная последовательность обработки обеспечивает выделение температурных аномалий непосредственно из видеопотока бортового тепловизора. Основу вычислительной процедуры составляют гистерезисная сегментация, морфологическая обработка и адаптивное оценивание фоновой температуры с использованием экспоненциального скользящего среднего. Экспериментальные данные, полученные при обследовании участка ЛЭП, показали возможность достижения полноты обнаружения до 92 % при частоте ложных срабатываний около 5 %.

Программная реализация выполнена на языке Python с использованием библиотек OpenCV и NumPy. При испытаниях на вычислительном модуле

NVIDIA Jetson Xavier скорость обработки составляла 25-30 кадров/с. Полученная производительность позволяет использовать предложенный алгоритм в составе бортовых систем, работающих в режиме, близком к реальному времени.

Вектор дальнейшего развития представленной методологии видится во встраивании в вычислительный тракт легких архитектур сверточного типа. Их применение может быть ориентировано как на распознавание категориальной принадлежности выявленных тепловых неоднородностей, так и на нивелирование погрешностей, вносимых вариативностью спектральной излучательности материалов. При такой конфигурации традиционный этап сегментации аномальных областей утрачивает функцию финального классификатора и переходит в ранг препроцессинговой стадии, обеспечивающей пространственную локализацию кандидатов для последующего нейросетевого анализа.

В числе прочих многообещающих траекторий следует отметить интеграцию предложенной схемы с алгоритмическими решениями в области нейросетевого композинга и рендеринга [5]. Подобное объединение создает предпосылки для выхода за рамки двумерной локализации температурных отклонений и восстановления их объемно-пространственных характеристик. Кроме того, ожидаемым сопутствующим эффектом выступает прирост информационной насыщенности термографических данных, получаемых в условиях пониженного пространственного разрешения либо при высоком уровне аддитивных шумовых составляющих.

**Список используемых источников**

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М.: Техносфера, 2012. 688 с. ISBN: 978-5-94836-331-8.

2. Santos T., Dias A., Cerveira T., Moreira A. P., Almeida J. UAV Visual and Thermographic Power Line Detection Using Deep Learning // Sensors. 2024. Vol. 24. N 17. P. 5678. DOI: 10.3390/s24175678.

3. Гришин А. М., Долгов А. А., Зима В. П., Рейно В. В., Цвык Р. Ш. Тепловизионные исследования развития и распространения низового лесного пожара // Оптика атмосферы и океана. 1997. Т. 10. № 10. С. 1139-1146.

4. Bradski G., Kaehler A. Learning OpenCV. Sebastopol: O'Reilly Media, 2008. 293 p.

5. Семенищев Е. А., Толстова И. В. Объединение изображений ближнего инфракрасного и видимого диапазона, полученных с камер БПЛА // Евразийский Союз Ученых (ЕСУ). 2019. № 11 (68). С. 36.

# DETECTION OF THERMAL ANOMALIES USING AN UAV'S ON-BOARD THERMAL IMAGING DEVICE

**Pavlovskaya A., Pavlovsky M., Fedorov S.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The article discusses a method for automatic detection of thermal anomalies based on a video stream from an onboard thermal imager of an unmanned aerial vehicle. A two-stage algorithm is described, which includes hysteresis threshold segmentation, morphological filtering, and an adaptive background model based on an exponential moving average. Experimental verification on the task of monitoring power lines showed an increase in detection completeness to 92 percent while reducing false positives to 5 percent.*

***Key words:*** *unmanned aerial vehicle, thermal imager, anomaly detection, infrared imaging, threshold segmentation, and morphological filtering*

**УДК 37.01:004**
**ГРНТИ 50.43.71, 14.35.07**

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ GOOGLE FORMS И YANDEX FORMS ДЛЯ ПРОВЕДЕНИЯ ПЕДАГОГИЧЕСКОГО ТЕСТИРОВАНИЯ

**Г. Н. Смородин**

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

*Представлены результаты сравнительного анализа двух популярных облачных сервисов Google Forms и Yandex Forms с точки зрения их пригодности для педагогического тестирования в вузах. Рассматриваются ключевые аспекты: функциональные возможности для создания тестов, система оценивания, ограничения, безопасность данных, интеграция с образовательной средой и пользовательский опыт. На основе анализа формулируются практические рекомендации по выбору инструмента в зависимости от конкретных педагогических задач.*

***педагогическое тестирование, Google Forms, Yandex Forms, сравнительный анализ, онлайн-тестирование, цифровые инструменты в образовании.***

## Введение

Цифровизация образования делает онлайн-тестирование не просто удобным дополнением, а неотъемлемой частью учебного процесса. Возможность быстро оценить знания студентов, получить мгновенную обратную связь и автоматизировать рутинную проверку – ключевые преимущества, которые ищут преподаватели в цифровых инструментах. Среди множества решений особое место занимают конструкторы форм – Google Forms и Yandex Forms. Данные сервисы бесплатны, просты в освоении и позволяют создавать тесты без знания языков программирования.

Вместе с тем для проведения педагогического тестирования эти сервисы имеют существенные различия.

Целью данной работы является выявление и классификация возможностей данных сервисов (платформ), что позволит принимать более обоснованные решения при выборе той либо иной платформы для формирования библиотеки тестов, проведения тестирования и обработки полученных результатов.

## 1. Возможности платформ для создания тестов

Google Forms предлагает широкий набор типов вопросов, применимых для тестирования: множественный выбор, раскрывающийся список, сетка выборов, шкала Лайкерта и другие [1]. Использование режима Тест позволяет оценивать в баллах каждых правильный ответ.

Ключевой функцией для преподавателей является режим «Тест». При его активации у создателя появляется возможность назначать баллы за каждый правильный ответ и настраивать автоматическое оценивание.

Сервис Yandex Forms также предоставляет интуитивно понятный интерфейс и подходит для создания тестов [2]. Для этих целей в конструкторе есть специальный раздел «Тесты и квизы». Аналогично Google Forms, сервис позволяет определять правильные ответы, назначать баллы и настраивать автоматический подсчет результатов; результат доступен для анализа после завершения теста.

Сервис имеет много возможностей для настройки внешнего вида, включая изменение цветов и выбор обложек, в том числе и из набора обложек пользователя. Вставка логотипов позволяет следовать корпоративному стилю при создании образовательных материалов.

## 2. Сравнительный анализ по ключевым критериям

Для объективной оценки сервисов их возможности были рассмотрены по нескольким параметрам, наиболее важным с точки зрения педагогического тестирования. Результаты анализа представлены в Таблице 1. Ниже приведен сравнительный анализ ряда других параметров.

*Соответствие законодательству в области хранения данных* Google Forms не гарантирует хранение персональных данных на территории РФ, возможность настройки территории хранения данных отсутствует. Yandex Forms размещает данные на российских серверах, что соответствует требованиям 152-ФЗ.

В случае использования персональных данных при проведении тестов Yandex Forms может быть рекомендован однозначно.

*Совместная работа и администрирование.* С точки зрения взаимодействия разработчиков тестов, сервисы существенно различаются. Для совместного редактирования формы в Google Forms достаточно отправить ссылку коллеге, у которого есть Google аккаунт.

Yandex Forms в этом плане более консервативна: для совместной работы необходим корпоративный аккаунт в Yandex Cloud, частным пользователям доступно только индивидуальное редактирование.

В ином случае придется обсуждать тестовые задания в черновой форме на ином ресурсе с последующим заполнением Yandex Forms одним из авторов.

*Интерфейс пользователя.* Google Forms известен своим минималистичным и интуитивно понятным интерфейсом. Yandex Forms также предоставляет современный и удобный интерфейс, учитывающий особенности русского языка.

ТАБЛИЦА 1. Сравнение функциональности Google Forms и Yandex Forms

| Критерий сравнения | Google Forms | Yandex Forms |
|---|---|---|
| Автоматическое оценивание | Да. Полноценный режим «Тест» с назначением баллов | Да. Специальный раздел «Тесты и квизы» |
| Логика перехода (вопросов) | Да. Можно показывать вопросы в зависимости от предыдущих ответов | Да. Можно показывать или скрывать блоки на основе ответов |
| Интеграция с LMS/экосистемой | Да. Глубокая интеграция с Google Classroom (создание заданий, импорт оценок, режим блокировки на Chromebook | Ограничена. Интеграция с другими сервисами возможна через API, но готовой глубокой интеграции со сторонними LMS нет |
| Работа с мультимедиа | Да. Возможность вставки фото, видео, создания интерактивных заданий | Да. Возможность вставки изображений и логотипов |
| Безопасность и хранение данных | Данные хранятся на серверах Google за пределами РФ. Для образовательных учреждений – специальный Workspace for Education | Данные хранятся на серверах в РФ, что соответствует 152-ФЗ. Важно для гос. проектов и работы с персональными данными |
| Лимиты и ограничения | Бесплатная версия: 15 ГБ дискового пространства, до 300 элементов контента, 2000 вариантов ответов, 75 разделов. До 200 000 ответов на форму | Бесплатная версия: неограниченное количество ответов, максимум 20 загружаемых файлов общим объемом до 20 МБ |
| Цена и модель распространения | Базовый функционал – бесплатно. Расширенные возможности для совместной работы – платно (Google Workspace) | Базовый функционал для личного использования – полностью бесплатен. Корпоративный функционал – платно (Яндекс 360 для бизнеса) |

### 3. AI-инструменты: оптимизация создания контента

Одним из трендов 2025 года стало активное внедрение генеративных нейросетей в офисные инструменты. Оба сервиса не остались в стороне.

Google Forms обладает функцией «Help me create» на базе платформы искусственного интеллекта Gemini. Преподаватель может создать простой текстовый запрос, например, «Викторина по корпоративным информационным технологиям с 10 вопросами» или загрузить файл (Google Doc, PDF) – и Gemini автоматически сгенерирует черновик формы. Это может радикально ускорить подготовку учебных материалов. На момент публикации функция работает только на английском языке.

Относительно Yandex Forms, на данный момент официальная информация о встроенных AI-функциях для создания тестов отсутствует.

### 4. Рекомендации по выбору инструмента

Проведенный анализ позволяет сформулировать следующие рекомендации для авторов педагогических тестов.

Рекомендуется выбрать Google Forms, если вы работаете в образовательной организации, которая использует экосистему Google Workspace for Education; вам важна глубокая интеграция с LMS и возможность автоматического импорта оценок; вам нужен мощный AI-ассистент для быстрой генерации тестов; тестовые задания и ответы не содержат персональных данных.

Следует отдать предпочтение Yandex Forms, если для вашей организации критически важно хранение данных на серверах в РФ; необходимость командной работы по разработке тестовых заданий отсутствует, а гибкая кастомизация внешнего вида тестовых заданий является существенным фактором.

### Заключение

Как Google Forms, так и Yandex Forms предоставляют преподавателям мощный и в основном бесплатный функционал для создания онлайн-тестов, автоматической проверки и анализа результатов.

Google Forms, благодаря глубокой интеграции с образовательной экосистемой Google и внедрению AI-инструментов, выигрывает в сценариях «все-в-одном» при полной лояльности к условиям хранения данных.

Yandex Forms становится более предпочтительным выбором для организаций, в первую очередь озабоченных вопросами безопасности и юридической чистоты работы с данными в соответствии с российским законодательством.

Принятие окончательного решения зависит от приоритетов конкретного учебного заведения и его информационно-технологической инфраструктуры.

**Список используемых источников**

1. Шмотьев А. Ю. Возможности использования Google-сервисов в образовании // Наука и перспективы. 2017. № 3. С. 27-32.

2. Суровцев Д. А. и др. Сравнительный анализ сервисов для создания анкет, опросов и тестов // Научно-методические основы формирования функциональной грамотности: теория и практика современной школы. 2023. С. 207-213.

## COMPARATIVE ANALYSIS OF THE CAPABILITIES OF GOOGLE FORMS AND YANDEX FORMS FOR PEDAGOGICAL TESTING

**Smorodin G.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*The results of a comparative analysis of two popular cloud services Google Forms and Yandex Forms from the point of view of their suitability for pedagogical testing in universities are presented. Key aspects are considered: functionality for creating tests, assessment system, limitations, data security, integration with the educational environment and user experience. Based on the analysis, practical recommendations are formulated for the choice of a tool depending on specific pedagogical tasks.*

***Key words:*** *pedagogical testing, Google Forms, Yandex Forms, comparative analysis, online testing, digital tools in education*

**УДК 621.395.44**
**ГРНТИ 49.03.03**

# РЕАЛИЗАЦИЯ АППАРАТНЫХ МОДУЛЕЙ СИНХРОНИЗАЦИИ ВРЕМЕНИ В СЕТЯХ TSN

**Н. Л. Сторожук**

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

*В докладе рассматриваются принципы работы аппаратных модулей синхронизации в устройствах сетей, чувствительных ко времени, предназначенных для обеспечения предсказуемости параметров передачи данных при пакетной коммутации, чтобы гарантировать своевременную доставку данных с минимальной задержкой и наилучшим образом обеспечить обмен информацией для процессов реального времени.*

***TSN, PTP, BMCA, синхронизация времени, аппаратный модуль синхронизации, процесс реального времени***

## Введение

Современные промышленные технологии выдвигают повышенные требования как к качественным параметрам каналов связи, так и к их пропускной способности. Интеллектуальные производственные системы не могут функционировать без гарантированных ультрамалых задержек передачи данных. Хотя конкретные требования у различным промышленных приложений различаются, они объединяют в себе общую потребность в управлении параметрами каналов передачи данных в режиме реального времени [1].

Таким образом, производственная сеть связи должна гарантировать детерминированные и надежные коммуникационные услуги для критически важных функций, и в то же время обслуживать менее важные сервисы. Для этого в сети используется временное и пространственное разделение коммуникационных ресурсов [2]:

– передача трафиков: с переключением по времени (TT англ. Time Triggered), с ограничением по скорости (RC англ. Rate Constr ained), без гарантии качества и доставки по принципу, приложив максимум усилий (BE, англ. Best Effort);
– настройка и изменение конфигурации сетевых компонентов, таких как коммутаторы и оконечные устройства;
– передача меток времени и синхронизации часов;

– предотвращение, обнаружение и устранение неисправностей.

Технология «Сети, чувствительные ко времени» (TSN, англ. Time-Sensitive Networking, представляющая из себя набор стандартов, преобразующих сети Ethernet в системы передачи данных в реальном времени, обеспечивает гарантированную задержку, предсказуемость доставки кадров и высокую надежность для критически важных потоков данных, что особенно важно в управлении производственными процессами [3].

Фундаментальный принцип технологии TSN, обеспечивающий детерминированную передачу данных и соответствие требованиям к скорости, надежности и предсказуемости в производственных сетях – это точная синхронизация времени на всех сетевых устройствах.

## Характеристики аппаратных модулей TSN

Рассмотрим следующие аспекты взаимодействия устройств синхронизации времени в сетях TSN:

– размещение аппаратных модулей, реализующих функции TSN;
– необходимые дополнительные функции.

С точки зрения проектирования устройств TSN, расположение аппаратных и функциональных элементов в одном модуле позволяет использовать только один общий интерфейс передачи данных, что снижает сложность аппаратной реализации. Как показано на рисунке 1, эти модули сгруппированы в блоке обработки входящего трафика, в то время как фильтрации входящего потока выполняются блоком поискового механизма, управляющего виртуальной очередью вывода (VOQ, англ. Virtual Output Queueing).

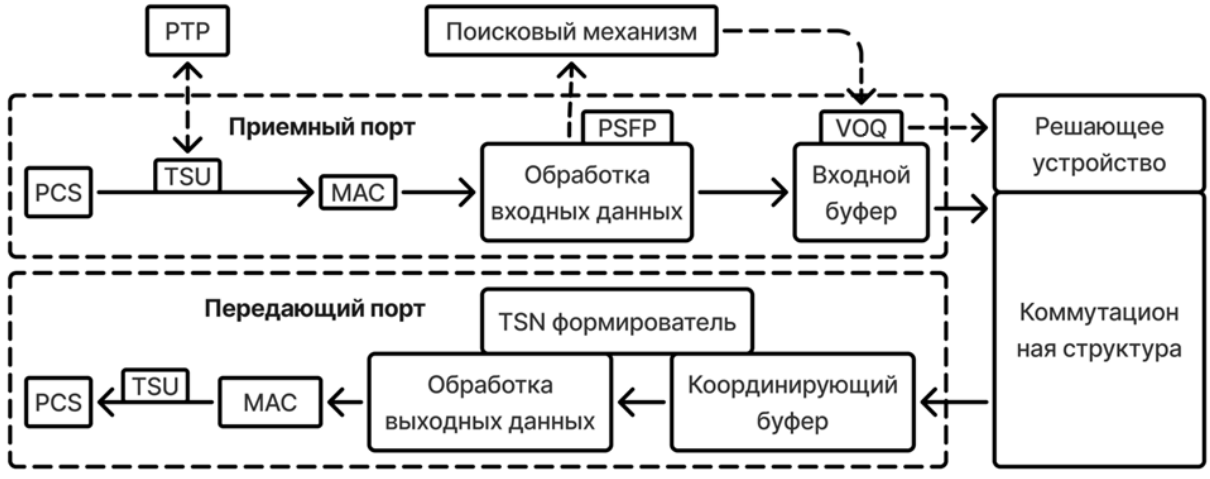



Рис. 1. Размещение аппаратных модулей TSN в системе коммутации

Функции набора инструментов TSN требуют, чтобы каждый узел сети был синхронизирован по времени. Это следующие инструменты:

– планирование с учетом времени (TAS, англ. Time-Aware Scheduler), который определяет для каждой очереди временные ворота и минимизирует задержку для критических потоков времени;
– механизм фильтрации и контроля потоков (PSFP, англ. Per-Stream Filtering and Policing), который улучшает надежность сети за счет фильтрации отдельных потоков трафика.

Кроме того, даже без этих функций некоторые приложения требуют синхронизации времени. Независимо от области применения за синхронизацию времени отвечает протокол точного времени (PTP, англ. Precision Time Protocol), выполняемый подсистемой PTP, как показано на рисунке 2 (сплошные линии представляют потоки данных (пакетов), а пунктирные линии – потоки управления).

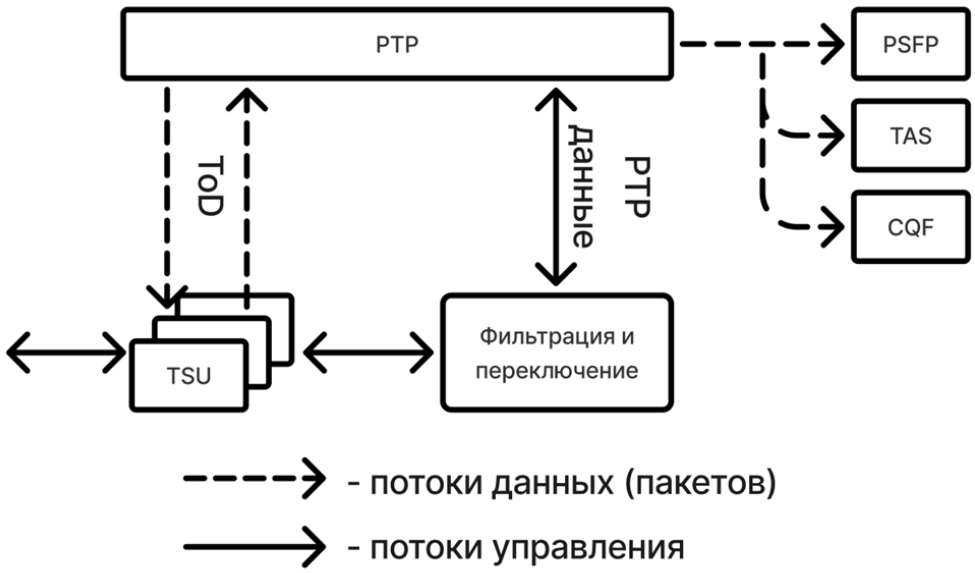



Рис. 2. Подсистема протокола PTP

Подсистема PTP состоит из основного модуля PTP и вспомогательных блоков отметки времени (TSU, англ. Time-Stamping Unit). Когда на конкретном узле сети не требуются данные для записи синхронизированного времени (ToD, англ. Time of Day), модуль PTP не нужен, и TSU работают как прозрачные часы. Режим прозрачных часов используется для коррекции недетерминированного времени, проведенного пакетом в коммутационном узле. Таким образом, коммутационный узел может выглядеть прозрачным для сети PTP, а точность синхронизации повышается по сравнению с сетью без поддержки этой функции. Для этого приемник (RX, англ. Receiver) TSU

сохраняют текущее значение несинхронизированных локальных часов в поле коррекции PTP-пакетов. Когда пакет покидает узел коммутации, передатчик (TX, англ. Transmitter) TSU использует это сохраненное значение и текущее время для внесения коррекции. Все TSU должны иметь доступ к общим локальным часам.

Если на конкретном коммутационном узле требуется синхронизированный ToD, то необходим модуль PTP, и вся система должна работать в режиме граничной синхронизации. В этом режиме коммутаторы TSN генерируют потоки данных PTP. Для этого система коммутации должна отфильтровать PTP-пакеты и доставить их PTP-модулю, который отвечает за выполнение алгоритма выбора лучших главных часов (BMCA, англ. Best Master Clock Algorithm), BMCA описан в стандарте IEEE 1588, а в более новых редакциях стандартов МСЭ-Т он называется − алгоритм выбора лучших часов передатчика времени (BTCA, англ. Best TimeTransmitter Clock Algorithm). TSU больше не модифицируют PTP-пакеты, однако они должны отмечать время приема и передачи PTP-кадров на коммутационном узле. Модуль PTP может быть общим для всей системы коммутации, а его части могут быть реализованы как в программном, так и в аппаратном исполнении.

Независимо от режима работы основным фактором, влияющим на размещение TSU в иерархии уровня передачи регистра, является точность синхронизации. TSU могут корректировать только недетерминированное время, затраченное между RX TSU и TX TSU. Поэтому TSU должны быть размещены так, чтобы охватить как можно большую часть системы между ними, т.е. располагаться близко к каналу связи. Предпочтительное расположение − между блоками управление доступом к среде передачи (MAC, англ. Media Access Control). и физическим подуровнем кодирования (PCS, англ. Physical Coding Sublayer). Это позволяет анализировать и модифицировать кадры PTP, а время их задержки в модулях на стороне канала может быть включено в процесс коррекции в качестве независимой константы, которая предоставляется TSU при загрузке системы.

Модули TSU должны анализировать полученные пакеты, чтобы распознавать PTP-трафик. Кроме того, изменение содержимого кадра подразумевает изменение контрольной последовательности кадра (FCS, англ. Frame Check Sequence), что, в свою очередь, подразумевает, что TSU также должны проверять циклический избыточный код (CRC, англ. Cyclic Redundancy Check), предназначенный для нахождения контрольной суммы

с целью проверки целостности данных. Алгоритма CRC используется для обнаружения ошибок, которые могут возникнуть при передаче данных.

Функция выгрузки кадров позволяет приостанавливать передаваемые кадры во время передачи, чтобы экспресс-кадры могли быть переданы до них. Это возможно за счет «маркировки» передаваемых кадров с помощью специальных полей в преамбуле, а также сигнализации о «паузе» в передаче путем завершения кадра специальной версией FCS. Экспресс-кадры остаются неизменными по сравнению со стандартными кадрами Ethernet.

Так как модуль MAC изначально отвечает за проверку FCS, фильтрацию недопустимых кадров и, возможно, удаление полей преамбулы и FCS, операции выгрузки кадров должны выполняться на стороне канала MAC. Фактическая реализация модуля MAC вытеснения кадров (прерывание передачи низкоприоритетных кадров с возобновлением ее после передачи высокоприоритетных) может выглядеть так, как показано на рисунке 3.

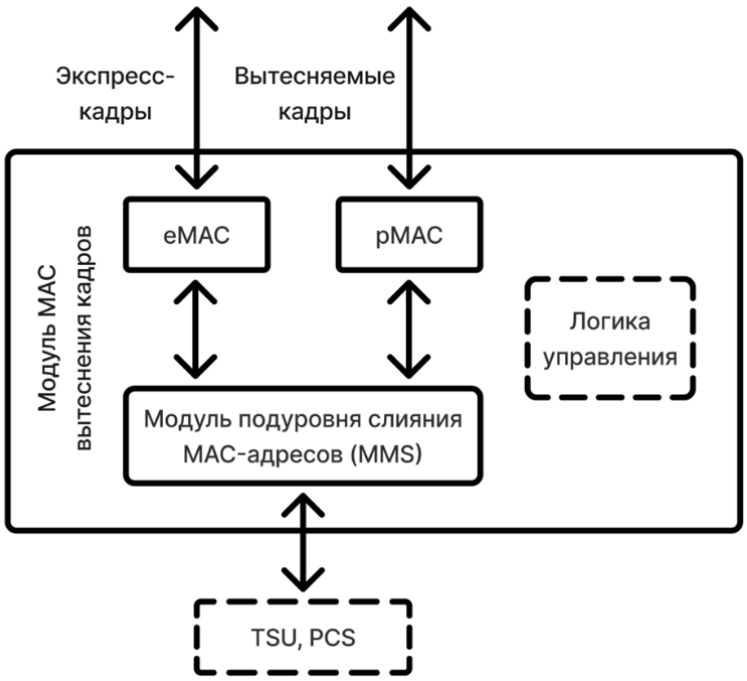



Рис. 3. Пример реализации модуля MAC вытеснения кадров

Единый независимый от среды интерфейс (MII, англ. Medium Independent Interface) на стороне канала, в котором могут присутствовать фрагментированные кадры, подключается к подуровню слияния MAC (MMS, англ. MAC Merge Sublayer). Модуль MMS различает экспресс-кадры и кадры с вытеснением (на основе преамбулы) и направляет экспресс-трафик на экспресс-MAC-адрес (eMAC), а вытесняемый трафик − на вытесняемый MAC-адрес (pMAC). Модуль MMS также отвечает за повторную

сборку фрагментов кадра, что с точки зрения данных означает восстановление стандартной преамбулы (после проверки).

Как экспресс-MAC-адрес, так и виртуальный MAC-адрес выполняют стандартные операции MAC независимо друг от друга, что в принципе означает, что MAC с вытеснением кадров разделяет один MII на два (экспресс и вытесняемый) клиентских интерфейса. Кадры на этих интерфейсах могут поступать (или отправляться) в любое время, что дает контроль над их обслуживанием клиентской системе. Однако этот контроль порождает некоторые проблемы интеграции. В худшем случае преимущества, получаемые от вытеснения кадров в канале, могут быть сведены на нет неправильным обслуживанием клиентской системой.

**Фильтрация и применение политик для каждого потока данных**

Фильтрация и применение политик для каждого потока данных использует извлеченную информацию заголовка для идентификации потока, классификации, измерения и, возможно, отбрасывания кадров. Два основных фактора, которые следует учитывать при отбрасывании кадров:

– механизм поиска не должен обновлять базу данных фильтрации, используя исходный адрес отбрасываемых кадров;
– удаленные кадры не должны тратить впустую коммутационные ресурсы системы.

Таким образом, рекомендуется установить модуль PSFP перед фазой переключения. Блок обработки входных данных уже выполняет синтаксический анализ пакетов для запроса к поисковому механизму, поэтому блок PSFP может повторно использовать существующее оборудование. Кроме того, здесь также возможно принимать решения об удалении кадров, поэтому удаляемые кадры не тратят впустую буферную емкость во входном буфере.

Дополнительным фактором, влияющим на размещение и архитектуру модуля PSFP, является то, что считается ли база данных измерений совместно используемой портами. База данных измерений содержит временную информацию о скоростном трафике для каждого потока и влияет на решения о фильтрации [4]. Предполагается, что кадры, принадлежащие одному потоку, классифицированному с помощью функции потока, могут поступать только на один RX-порт в каждый момент времени. Следствием этого предположения является то, что состояние базы данных измерений не

нужно разделять между портами. Таким образом, на каждом порту может присутствовать эксклюзивный экземпляр PSFP-модуля.

### Элементы сетей TSN и управление их работой

Общей темой для всех формирователей TSN, не зависимо от того, запускаются ли они по событию или по времени, является тот факт, что они работают с очередями приоритетов для каждого выхода. На рисунке 4 показан выходной порт с восемью приоритетными очередями, сформированными TAS-планировщиком и формирователем на основе кредитов (CBS англ. Credit-Based Shaper).

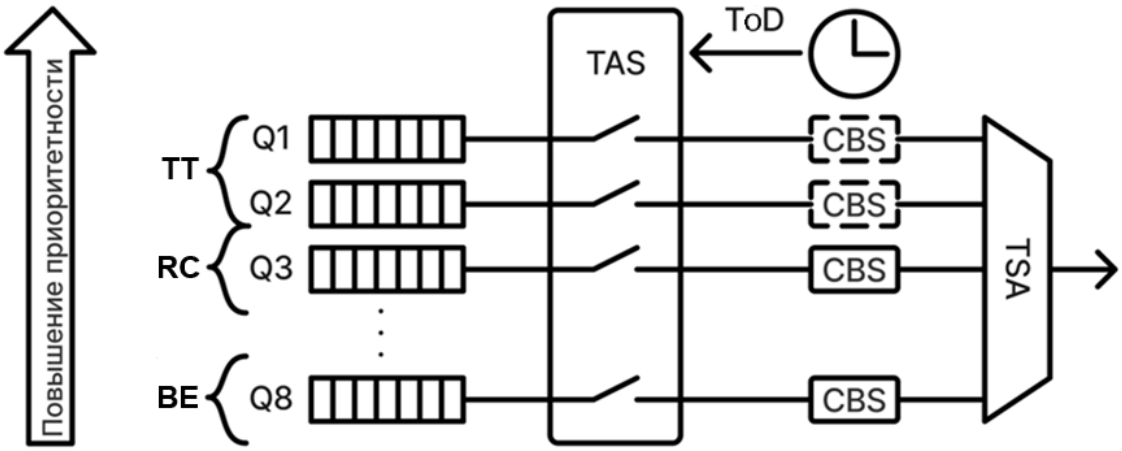



Рис. 4. Функциональное представление системы очередей выходных портов

Если, в конце концов, несколько кадров подходят для передачи, алгоритм выбора передачи (TSA, англ. Transmission Selection Algorithm) выбирает только один из них.

В случае запуска по событию CBS для управления кредитами каждой из этих очередей он должен быть размещен там, где может отслеживать трафик, передаваемый из порта каждой приоритетной очереди.

С другой стороны, TAS-планировщик, запускаемый по времени, не нуждается в мониторинге трафика. Тем не менее, он предназначен для точного указания времени отправления кадра из узла сети. Таким образом, любая задержка, возникающая после того, как TAS-планировщик планирует выход кадра, должна быть в худшем случае детерминированной, а в лучшем − постоянной.

Рассмотрим ситуацию, когда оба механизма применяются одновременно. Чтобы гарантировать, что кадры, запланированные TAS-планировщиком, не будут задерживаться CBS-формирователями, послед-

ние должны быть отключены для очередей TT трафика (изображены пунктиром на рисунке 4).

На практике набор очередей с наивысшим приоритетом будет обозначаться как очереди TT трафика, и TAS будет единственным ограничителем их передачи [5]. Другой набор очередей с более низким приоритетом будет обозначен как RC, и их передача будет ограничена как TAS-планировщиком, так и CBS. Наконец, оставшиеся очереди могут быть обозначены как очереди BE, и им может быть назначена оставшаяся пропускная способность. TSA гарантирует, что очереди RC с более высоким приоритетом будут обслуживаться перед очередями BE с более низким приоритетом в случае конфликта.

Когда TAS и CBS работают совместно, очередь для CBS может накапливаться только тогда, когда шлюз TAS-планировщика открыт и скорость заполнения очереди совместима с рабочим циклом шлюза.

Координационный буфер, отвечающий за повторную сборку ячеек в кадры, уже обеспечивает выходные порты возможностями буферизации. Можно сказать, что кадр поступает на выход, когда его последняя ячейка получена в координационном буфере. Только такие кадры могут быть отправлены на передачу.

Учитывая все вышеперечисленное, любой модуль формирования TSN должен быть размещен на выходном порту после буфера координации.

В системах TSN устройства передают свои атрибуты с помощью объявляющих сообщений. При получении объявляющих сообщений инициализируется BTCA, чтобы указать часы с лучшими атрибутами, а также состояние порта.

**Заключение**

Коммутаторы, поддерживающие стандарт сети, чувствительной ко времени, должны обеспечивать минимальные задержки при работе с сообщениями протоколов синхронизации. Для этого они должны включать блок синхронизации, выполняющий обработку меток времени, внося минимальную задержку при их пересылке. Общая структура блока синхронизации состоит из процессоров приема-передачи, управляющего, дублирующего, прокси- и PTP-процессоров. Поддержка протоколов сети, чувствительной ко времени, обусловливает включение в его состав планировщика, обработчика приоритетов и сдвоенного буфера памяти. Фильтрация и применение политик производится на основе информации, извлеченной из заголовка

кадра для идентификации потока, классификации потока, измерения параметров и, при необходимости, отбрасывания кадров. Синхронизация сетевого оборудования по частоте и времени является одновременно фундаментальной целью и ключевым фактором в выполнении других функций TSN [6].

Данные элементы отвечают за процессы циклической пересылки, разделения кадров и приоритетности их обработки с учетом тэгов и возможности резервирования потоков данных. Все это можно обеспечить только при выполнении всех этих процессов на аппаратном уровне.

**Список используемых источников**

1. Сторожук Н. Л. Применение технологии TSN в промышленных сетях связи Первая миля. 2025. № 2 (126). С. 48-52.

2. Степанов С. В. Синхронизация времени на цифровых подстанциях // Молодой ученый. 2022. № 24 (419). С. 122-126. URL: https://moluch.ru/archive/419/93158/ (дата обращения 10.04.2026).

3. Росляков А. В., Герасимов В. В., Мамошина Ю. С., Сударева М.Е. TSN – сети Ethernet, чувствительные ко времени // Инфокоммуникационные технологии. 2021. Т. 19. № 2. С. 187-201.

4. Рекомендация МСЭ-Т G.8262.1-2022. Временные характеристики усовершенствованного синхронного оборудования ведомых часов.

5. Janssen, Dr. Dirk, Büttner, Holger. EtherCAT – the Ethernet Fieldbus // PC Control Magazine. 2003. № 3.

6. Сторожук М. Н., Киричек Р. В. Обзор систем мониторинга для протокола TSN // Сборник докладов Научно-технической конференции Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященной Дню радио. 2022. № 1. С. 131-132.

## IMPLEMENTATION OF HARDWARE TIME SYNCHRONIZATION MODULES IN TSN NETWORKS

**Storozhuk N.**
The Bonch-Bruevich Saint Petersburg State University of Telecommunications

*This paper examines the operating principles of hardware synchronization modules in devices in time-sensitive networks designed to ensure predictability of data transmission parameters during packet switching, guaranteeing timely data deli very with minimal latency and optimally supporting information exchange for real-time processes.*

***Key words:*** *TSN, PTP, BMCA, time synchronization, hardware synchronization module, real-time process*

**УДК 621.396.94**
**ГРНТИ 47.31.29**

# ВЛИЯНИЕ ДИНАМИЧЕСКОЙ АДАПТАЦИИ МОДУЛЯЦИИ И КОДИРОВАНИЯ В СИСТЕМАХ СПУТНИКОВОЙ СВЯЗИ

**Ф. Д. Хлопунов**

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

*Статья посвящена комплексному анализу влияния механизма адаптивной модуляции и кодирования (АСМ) как одного из наиболее эффективных инструментов компенсации замираний в спутниковых каналах на показатели надежности, пропускной способности и задержки передачи данных в автономных телеметрических сетях. В работе рассматриваются теоретические основы формирования адаптивных символьных потоков, математический аппарат оптимизации режима связи, его соотношение со статическими схемами передачи, а также эмпирические закономерности деградации качества канала при различных параметрах атмосферных возмущений и скорости обратной связи.*

***спутниковая связь, адаптивная модуляция и кодирование, АСМ, надежность передачи, телеметрические сети, задержка сигнала, помехоустойчивость, спутниковые группировки***

Современные низкоорбитальные и геостационарные группировки, опирающиеся на стандарты DVB-S2X, достигают спектральной эффективности 4–6 бит/с/Гц, создавая иллюзию абсолютной связности. Однако в их физическом уровне заложена хрупкость: достаточно тропосферного ливня или ионосферной турбулентности, чтобы отношение сигнал/шум рухнуло, а статический бюджет линии оказался пробит. Судить о надежности спутникового тракта по расчетам для ясной погоды оказалось несостоятельно; индустрия обратилась к механизмам динамической компенсации и минимаксным формулировкам управления ресурсами [1].

Адаптивная модуляция и кодирование (АМК) не «раздувает» запас мощности и не прячет уязвимости за жесткими протоколами ретрансляции. Система работает против наихудшего сценария канала: внутренний контур оценивает мгновенное состояние среды, внешний – жестко переключает связку «созвездие + скорость кода» (от QPSK до 64-APSK). Введение гистерезиса и фильтров прогноза превращает АМК из набора эвристик в строгий инструмент управления. Эмпирика подтверждает: если терминал выдержи-

вает глубокие замирания без разрыва сеанса, это свидетельство подлинной живучести. Метод фактически стал обязательным стресс-тестом; архитектуру, не способную к динамической подстройке, трудно считать пригодной для задач с высокими рисками.

Влияние на доступность структурное. Алгоритм динамически сдвигает рабочую точку: статический терминал с 99,5 % доступности в ясную погоду при ливне теряет связь полностью, тогда как АМК удерживает канал на уровне 90 %, жертвуя скоростью ради выживания. Процедура находит баланс между спектральной отдачей и избыточностью, подавляя лавинообразный рост битовых ошибок [3]. В отличие от пассивного закладывания энергетического запаса, применяемого однократно и бессильного против внезапных градиентов затухания, АМК итеративно отслеживает SNR, формируя глобально устойчивый тракт с минимальными потерями в идеальных условиях.

Вычислительная цена определяется задержкой обратной связи и шириной гистерезиса. Редкие отсчеты не позволяют поймать начало замирания; учащение обновлений повышает робастность, но нагружает бортовые процессоры. Прирост выходит на плато, и основная нагрузка ложится на DSP-модуль. Для строгой проверки применяют адаптивные окна переключения и прогнозирующие фильтры [4]. Выбор семейства кодов и модуляции меняет геометрию помехоустойчивости: АМК на базе QPSK дает широкий отступ, но низкую скорость; 64-APSK максимизирует поток, но требует идеального SNR. Терминалы, оптимизированные под одну схему, не обязательно устойчивы к другой, поэтому сертифицированные комплексы тестируют по всем группам режимов.

АМК перераспределяет нагрузку по лучам: терминалы на границе зоны покрытия или в дождевых облаках потребляют больше корректирующих символов и требуют больших возмущений для перехода в режим телеметрии. Допускается и целевое управление качеством (QoS) – принудительная консервация режима для критических команд, что позволяет точечно контролировать поведение в узких коридорах связи.

В плотных группировках устойчивость к взаимным помехам у АМК-систем имеет свою специфику: алгоритмы фиксируют локальные оптимумы, специфичные для данного распределения. В режиме локального контроля («белый ящик») АМК уверенно отражает деградацию канала, но при массовом развертывании и преднамеренном глушении атакующий спосо-

бен запустить многошаговые процедуры, требуя перебалансировки на межуровневом этапе.

Наибольшую прочность дает связка АМК с распределенной криптозащитой и динамическим частотным планированием. Чистая криптография для спутниковых линков неподъемна из-за задержек, поэтому применяют облегченные протоколы аутентификации на физическом уровне, оставляя тяжелую математику для финального аудита. Альтернативы – статическое частотное планирование, массивные антенные решетки – против динамической атмосферы показали себя слабо: рабочие радиусы CERT-гарантий оказываются меньше необходимых для отражения быстрых фазовых сдвигов, а стохастические ретрансляторы не выдерживают прямой оптимизации границы помехоустойчивости.

Адаптивная модуляция и кодирование остается центральным инструментом исследования устойчивости спутниковых сетей: она выявляет минимально допустимые энергетические отступы, вскрывает ложную надежность статических бюджетов и служит основой для взвешенных решений о развертывании группировок. Дальнейший прогресс потребует междисциплинарных усилий, и АМК в обозримом будущем сохранит свою ключевую роль.

**Список использованных источников**

1. Elsayed E. E. et al. Coding techniques for diversity enhancement of dense wavelength division multiplexing MIMO-FSO fault protection protocols systems over atmospheric turbulence channels // IET Optoelectron., 2024. Vol. 18. N 1-2. PP. 11-31.

2. Kim S.-J. and Han S.-K. Power efficiency analysis of spatial diversity based vertical FSO links with pointing error in multiple beam transmissions // IEEE Access, 2022. Vol. 10. PP. 129925–129931.

3. Kaur S. and Lubana A. Performance investigation of Ro-FSO link under clear and fog conditions employing machine learning // J. Opt., 2024. Vol. 54. PP. 2925.2934.

4. Tang X., Reviriego P., Tang W., Mitchell D. G., Lombardi F., and Liu S. Joint learning and channel coding for error-tolerant IoT systems based on machine learning // IEEE Trans. Artif. Intell., 2024. Vol. 5. N 1. PP. 217-228.

5. Khedhri N. and Najar M. Reinforcement learning-based adaptive modulation systems // in Proc. Adv Inf Netw. Appl. in ser. Lecture Notes on Data Engineering and Communications Technologies, Berlin, Germany, Springer, 2025. Vol. 248. PP. 101-112.

*Статья представлена научным руководителем, профессором кафедры автоматизированных систем специального назначения ВАС, доктором технических наук, профессором И. Б. Саенко.*

# THE IMPACT OF DYNAMIC ADAPTATION OF MODULATION AND CODING IN SATELLITE COMMUNICATION SYSTEMS

**Khlopunov F.**
Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny

*The article is devoted to a comprehensive analysis of the impact of the adaptive modulation and coding (ACM) mechanism as one of the most effective tools for compensating fading in satellite channels for reliability, bandwidth, and data transmission delays in autonomous telemetry networks. The paper examines the theoretical foundations of the formation of adaptive symbolic streams, the mathematical apparatus for optimizing the communication mode, its relationship to static transmission schemes, as well as empirical patterns of degradation of channel quality under various parameters of atmospheric disturbances and feedback rates.*

***Key words:*** *satellite communications, adaptive modulation and coding, ACM, transmission reliability, telemetry networks, signal delay, noise immunity, satellite groupings*

# АВТОРЫ СТАТЕЙ


АЛЕКСАНДРОВ Игорь Николаевич — кандидат экономических наук, доцент, доцент Высшей школы государственного управления Санкт-Петербургского политехнического университета Петра Великого, a78302я98@gmail.com

АЛЕКСЕЕНКО Ирина Альбертовна — кандидат педагогических наук, доцент кафедры социально-политических наук Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ialekseenko@sut.ru

АЛЕШИНА Екатерина Сергеевна — студент группы МЗС-2512 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, aleshina.es@sut.ru

АЛКАТТАН Самех — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, alkattan.s@sut.ru

АЛЛЕНОВ Денис Сергеевич — соискатель, Военная академия связи им. Маршала Советского Союза С. М. Буденного, allenovdenis@yandex.ru

АЛЬ-НАМИ Башер Али — кандидат технических наук, доцент кафедры информатики и компьютерного дизайна Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, al-nami.baa@sut.ru

АШУРКИН Артем Андреевич — студент группы ИКТЗ-25 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ashurkin.aa@sut.ru

БАБИН Николай Николаевич — кандидат технических наук, доцент кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, babin.nn@sut.ru

БАБИЧ Константин Сергеевич — курсант учебной группы 3271 Военной академии связи им. Маршала Советского Союза С. М. Буденного, kostyan_2021@bk.ru

БАЛСА Алдрин Раульевич — кандидат географических наук, доцент кафедры вычислительных систем и информатики Государственного университета морского и речного флота им. адмирала С. О. Макарова, balsaar@gumrf.ru

БАРАЗЕНКО Даниил Кириллович — студент группы МСТ-2561 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, barazenko.dk@sut.ru

БЕДИКЯН Елизавета Сергеевна — студент группы РБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, bedikian.es@sut.ru

БЕЛОВ Вадим Александрович — студент группы ИКБ-32 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, belov.va@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

БИЛАН Виктория Викторовна — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, bilan_vv@bk.ru

БЛАН Филип Сергеевич — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, blan.fs@sut.ru

БРАЗОВСКИЙ Глеб Русланович — ассистент кафедры оптических и квантовых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, brazovskii.gr@sut.ru

БРАНИЦКИЙ Александр Александрович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, branickii1.aa@sut.ru

БРЫДЧЕНКО Александр Владимирович — подполковник, кандидат технических наук, доцент кафедры проводной электросвязи и фельдъегерско-почтовой связи Военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, brydchenko@sut.ru

БУДАРНЫЙ Глеб Сергеевич — ассистент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, budarnyi.gs@sut.ru

БЫЛИНА Мария Сергеевна — кандидат технических наук, доцент, заведующий кафедрой оптических и квантовых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, BylinaMaria@mail.ru

ВАГАНОВ Александр Валерьевич — старший преподаватель кафедры систем автоматизации и робототехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vaganov.av@sut.ru

ВАСИЛЬЕВ Дмитрий Николаевич — начальник кафедры военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vasilev@sut.ru

ВИНОГРАДОВ Пётр Юрьевич — кандидат технических наук, доцент, доцент кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, power@sut.ru

ВОЛЬФСОН Михаил Борисович — кандидат экономических наук, доцент, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, volfson.mb@sut.ru

ВТОРЫГИН Илья Дмитриевич — студент группы ИКПИ-34 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vtorygin.id@sut.ru

ВЯЗЬМИН Алексей Юрьевич — кандидат философских наук, доцент кафедры социально-политических наук Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, vyazmin.au@sut.ru

ГАНИН Даниил Павлович — студент группы ИКТЗ-26 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, daniil.ganin@sut.ru

ГЕЛЬФАНД Артем Максимович — старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gelfand.am@sut.ru

ГЕХТ Антон Борисович — кандидат исторических наук, доцент, заведующий кафедрой истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, geht.ab@sut.ru

ГИЛАВОГИ Мишель — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gilavogi.m@sut.ru

ГЛУШКО Артем Вячеславович — полковник, начальник кафедры проводной электросвязи и фельдъегерско-почтовой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, glushko@sut.ru

ГНЕДОВ Леонид Артемович — студент группа ИКТО-37 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gnedov.la@sut.ru

ГОЛОШУМОВ Борис Романович — курсант Военного университета радиоэлектроники Министерства обороны РФ, miyagggy@mail.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

ГОРДИЙЧУК Руслан Викторович — начальник цикла – старший преподаватель военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gordijchuk@sut.ru

ГОРЫНЦЕВ Андрей Арсеньевич — аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, goryntsev.aa@sut.ru

ГРИГОРЧУК Александр Николаевич — подполковник (запаса), доцент, преподаватель кафедры радиорелейной, тропосферной и спутниковой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, grigorchuk@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

ГРУЗДЕВ Дмитрий Анатольевич — подполковник, заместитель начальника кафедры проводной электросвязи и фельдъегерско-почтовой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gruzdev@sut.ru

ГУДАКОВ Антон Павлович — выпускник Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, сотрудник Digital Design, reall905@mail.ru

ДЕМИДОВ Николай Александрович — кандидат технических наук, старший преподаватель кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, demidov.na@sut.ru

ДЕНИСОВ Роман Сергеевич — студент группы БИБ244 Национального исследовательского университета «Высшая школа экономики», rdenisov@edu.hse.ru

ДОБРОВОЛЬСКИЙ Станислав Леонидович — преподаватель военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, dobrovolskij@sut.ru

ДОКУЧАЕВ Иван Ильич — аспирант кафедры социальной философии и философии истории Санкт-Петербургского государственного университета, ivan.i.dokuchaev@gmail.com

ДРОБОТОВ Андрей Григорьевич — студент группы ИКТЗ-25 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, branickii1.aa@sut.ru

ДРОБЯСКИН Андрей Николаевич — начальник учебной части – заместитель начальника кафедры радио, радиорелейной, тропосферной и спутниковой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, drobyaskin@sut.ru

ДРОЧНЕВ Андрей Александрович — курсант группы 143-25 Военного университета радиоэлектроники Министерства обороны РФ, andy.panda004@mail.ru

ЕГОРОВА Марина Александровна — кандидат экономических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, egorova2.ma@sut.ru

ЖЕЛТОВА Елена Петровна — кандидат педагогических наук, доцент, доцент кафедры иностранных языков Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, elenazheltova@sut.ru

ЖУКОВ Илья Сергеевич — кандидат биологических наук, доцент кафедры конструирования и производства радиоэлектронных средств Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zhukov.is@sut.ru

ЖУРАВЛЁВ Владимир Анатольевич — кандидат сельскохозяйственных наук, старший научный сотрудник научно-технического отдела Белорусской государственной академии связи, zhuravlyov-77@mail.ru

ЗАВАЛИШИН Андрей Юрьевич — доктор социологических наук, профессор кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zavalishin.aiu@sut.ru

ЗАГОРЕЛЬСКИЙ Владимир Валерьевич — преподаватель цикла фельдъегерско-почтовой связи кафедры проводной электросвязи и фельдъегерско-почтовой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zagorelskij@sut.ru

ЗАДБОЕВ Вадим Александрович — младший научный сотрудник Военной академии связи им. Маршала Советского Союза С. М. Буденного, zadboev89@mail.ru

ЗАЙДУЛЛИН Рустем Рамилевич — аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Zaidullin.rr@sut.ru

ЗАЙЦЕВА Екатерина Викторовна — кандидат технических наук, доцент кафедры информатики и компьютерных технологий Санкт-Петербургского горного университета императрицы Екатерины II, zaytseva_ev@pers.spmi.ru

ЗАПАЙЩИКОВ Александр Викторович — аспирант кафедры радиотехники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, zapaishikov.av@sut.ru

ЗНОБИЩЕВ Роман Сергеевич — подполковник, начальник цикла проводной электросвязи кафедры проводной электросвязи и фельдъегерско-почтовой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, znobishchev@sut.ru

ИВАКИНА Мария Дмитриевна — студент группы РИ-331056 института радиоэлектроники и информационных технологий-РТФ Уральского федерального университета им. первого Президента России Б. Н. Ельцина, mashaivakina26@gmail.com

ИВАНОВ Василий Геннадиевич — доктор военных наук, советник Российской академии ракетных и артиллерийских войск, профессор кафедры информатики и вычислительной техники Академии гражданской защиты МЧС России им. генерал-лейтенанта Д. И. Михайлика, wasj2006@yandex.ru

ИВАНОВ Денис Александрович — кандидат технических наук, старший преподаватель кафедры информационной безопасности Военного университета радиоэлектроники Министерства обороны РФ, prosto_deniss@mail.ru

ИВАНОВ Яков Сергеевич — студент группы ИКТЗ-26 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, branickii1.aa@sut.ru

ИКЛЮШИНА Татьяна Александровна — аспирант кафедры государственного и муниципального управления Гатчинского государственного университета, t-iklyushina@yandex.ru

ИЛЬИН Ярослав Александрович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ilin.ya@sut.ru

ИСАКОВ Александр Вячеславович — кандидат экономических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, isakov.av@net.sut.ru

КАЛИМУЛЛИНА Ольга Валерьевна — кандидат экономических наук, доцент, заведующий кафедрой экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kalimullina.ov@sut.ru

КАМАЕВ Артём Русланович — студент группы ИКМ-41з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kamaev.ar@sut.ru

КАМАРДИН Александр Иванович — студент группы РБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kamardin.ai@sut.ru

КОБИЛЬНЯК Арина Алексеевна — студент группы ЗР-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kobilnyak.aa@sut.ru

КОВЦУР Максим Михайлович — кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kovcur.mm@sut.ru

КОСМАЧЕВ Алексей Алексеевич — аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра РАН, преподаватель кафедры информационной безопасности киберфизических систем Национального исследовательского университета «Высшая школа экономики», a.kosmachev@hse.ru

КОТЕНКО Игорь Витальевич — доктор технических наук, профессор, главный научный сотрудник, руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра РАН, ivkote1@mail.ru

КОТОВ Виктор Иванович — кандидат технических наук, доцент, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kafedra-umses@sut.ru

КРАСОВ Андрей Владимирович — кандидат технических наук, доцент, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Krasov.av@sut.ru

КРУГЛОВА Анастасия Владимировна — студент группы МТВ-2531, специалист по учебно-методической работе института магистратуры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kruglova.av@sut.ru

КУДЕСОВ Артём Станиславович — студент группы ИКТЗ-25 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kudesov.as@sut.ru

КУЗНЕЦОВ Семен Павлович — курсант учебной группы 3271 Военной академии связи им. Маршала Советского Союза С. М. Буденного, Sema2003Kuz@yandex.ru

КУЛИКОВ Виктор Владимирович — кандидат технических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Ekon_up@sut.ru

КУЛИЧКИН Артем Александрович — руководитель проектов АО «СОГАЗ», соискатель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, Kubich0055@gmail.com

КУРАНДА Александр Иванович — преподаватель военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, kuranda@sut.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

ЛЕБЕДЕВА Наталья Павловна — кандидат технических наук, доцент кафедры материаловедения и товарной экспертизы Санкт-Петербургского государственного университета промышленных технологий и дизайна, tms@sutd.ru

ЛЕВШУН Дмитрий Сергеевич — кандидат технических наук, доцент кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, levshun.d@sut.ru

ЛЕГКОВ Константин Евгеньевич — кандидат технических наук, доцент, благотворительный фонд «На благо Отечества», constl@mail.ru

ЛЕГКОДЫМОВ Даниил Михайлович — студент группы ИКТЗ-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, legkodymov.dm@sut.ru

ЛИТУСОВ Никита Сергеевич — техник Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, litusov.ns@sut.ru

ЛИХАЧЕВ Ярослав Сергеевич — студент группы РБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, likhachev.ias@sut.ru

ЛОГИНОВСКАЯ Алёна Николаевна — кандидат географических наук, доцент кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, loginovskaya.an@sut.ru

ЛОПАШЕНКО Варвара Михайловна — студент группы РБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lopashenko1.vm@sut.ru

ЛУКОВ Артем Павлович — студент группы МСО-2511 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lukov.ap@sut.ru

ЛЮБАЩЕНКО Тимофей Дмитриевич — аспирант кафедры информационной безопасности компьютерных сетей Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, lyubashchenko.td@sut.ru

МАВРИЧЕВ Вячеслав Константинович — аспирант кафедры инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mavrichevvk@gmail.com

МАГОМЕДОВ Асадула Артурович — студент группы БИБ245 Национального исследовательского университета «Высшая школа экономики», aamagomedov@edu.hse.ru

МАКАРЕНКОВА Екатерина Александровна — студент группы ИКБ-32 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, makarenkova.ea@sut.ru

МАКАРОВ Владимир Васильевич — доктор экономических наук, профессор, академик Международной академии связи, Заслуженный деятель науки РФ, профессор кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, makarov.vv@sut.ru

МАНСУРОВ Мансур Анварович — студент группы РБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mansurov.ma@sut.ru

МАРЧЕНКОВ Алексей Алексеевич — старший преподаватель кафедры проводной электросвязи и фельдъегерско-почтовой связи военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marchenkov@sut.ru

МАРШЕВА Наталия Владимировна — старший преподаватель кафедры иностранных языков Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, marsheva.nv@sut.ru

МЕЛЕШКИН Олег Станиславович — студент группы ИБС-23 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, meleshkin.os@sut.ru

МЕРЗЛИКИН Егор Игоревич — студент группы ПВ-2 Белгородского государственного технологического университета им. В.Г. Шухова, x0djers@yandex.ru

МЕШКОВ Александр Владимирович — кандидат экономических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, meshkov.av@sut.ru

МИНЯЕВ Андрей Анатольевич — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, minyaev1.aa@sut.ru

МИХАЙЛОВ Максим Николаевич — студент группы ПВ-2 Белгородского государственного технологического университета им. В. Г. Шухова, mikhailovmaksim.educational@gmail.com

МИХАЙЛОВ Роман Алексеевич — аспирант кафедры беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mihailov.ra@sut.ru

МИХАЙЛОВА Анна Сергеевна — аспирант кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mihailova1.as@sut.ru

МИХАЙЛЮК Валерия Станиславовна — студент группы ЗР-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, mihailuk.vs@sut.ru

МОЛЧАНОВА Татьяна Вячеславовна — кандидат исторических наук, доцент кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, molchanova.tv@sut.ru

МОШАК Николай Николаевич — доктор технических наук, профессор кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, moshak.nn@sut.ru

МУЗЫКАНТОВ Алексей Николаевич — кандидат педагогических наук, заместитель начальника военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, muzykantov@sut.ru

МУСТАФИН Роман Олегович — студент группы ЭУ-423621 Уральского федерального университета им. первого Президента России Б. Н. Ельцина, roman.mustafin.2004@mail.ru

НГУЕН Хоанг Хиеп — студент группы N4254C Национального исследовательского университета ИТМО, anhhiep04082000@gmail.com

НЕРОВНЫЙ Артем Викторович — старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nerovnyi.av@sut.ru

НИКИТИН Кирилл Никитич — студент Санкт-Петербургского горного университета императрицы Екатерины II, s250727@stud.spmi.ru

НИКИТИН Максим Владимирович — студент группа ИКТР-22 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, nikitin.mv@sut.ru

НИКОЛАЕВА Наталья Александровна — старший преподаватель кафедры вычислительных систем и информатики Государственного университета морского и речного флота им. адмирала С. О. Макарова, nikolaevana@gumrf.ru

НОВИКОВ Егор Анатольевич — аспирант кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, novikov.ea@sut.ru

ОЖЕГОВ Владислав Андреевич — студент группы ЭП-41м Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ogegov.va@sut.ru

ОРЕХОВА Виктория Олеговна — студент группы МБК-2581 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, orehova.vo@sut.ru

ОРУДЖОВА Лейла Сайядовна — студент Санкт-Петербургского горного университета императрицы Екатерины II, s250731@stud.spmi.ru

ПАВЛОВА Елена Васильевна — кандидат экономических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekon_up@sut.ru

ПАВЛОВСКАЯ Анна Александровна — аспирант кафедры цифрового телевидения и метрологии Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavlovskaya.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

ПАВЛЮК Игнат Фёдорович — студент группы МБК-2581 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, pavlyuk.if@sut.ru

ПАНТЮХИН Олег Игоревич — кандидат технических наук, доцент, доцент кафедры сетей связи и передачи данных Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, pantuhin.oi@sut.ru

ПАСКЕНОВА Айлана Улюмджиевна — студент группы ИБС-12 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, paskenova.au@sutkt.ru

ПЕРЯЗЕВА Юлия Валерьевна — кандидат физико-математических наук, доцент кафедры информатики и компьютерных технологий Санкт-Петербургского горного университета императрицы Екатерины II, peryazeva_yuv@pers.spmi.ru

ПЕТРОВСКИЙ Никита Дмитриевич — аспирант кафедры государственного и муниципального управления Гатчинского государственного университета, nikita.ptr@mail.ru

ПЛОТНИКОВ Евгений Павлович — заместитель генерального директора по автоматизации и информационным технологиям АО «Навигатор», eplotnikov@navigat.ru

ПОПОВ Андрей Иванович — кандидат технических наук, доцент Военной академии связи им. Маршала Советского Союза С. М. Буденного Adpopovai@yandex.ru

ПОСОХОВА Ольга Алексеевна — преподаватель кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, posokhova.oa@sut.ru

РАФИКОВА Рада Фануровна — студент группы ИКМ-41з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, rafikova.rf@sut.ru

РУССКИХ Александр Романович — студент группы МЗС-2511 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, russkikh.ar@sut.ru

САВРАСОВ Артём Сергеевич — студент группы МСТ-2561 Санкт-Петербургского государственного университета им. проф. М. А. Бонч-Бруевича, savrasov.as@sut.ru

САГДЕЕВ Александр Константинович — подполковник, кандидат технических наук, доцент 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

САМАРКИН Денис Сергеевич — начальник цикла – старший преподаватель военного учебного центра Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, samarkin@sut.ru

САФИУЛЛИН Матвей Артемович — студент группы ЭМ-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekon_up@sut.ru

СЕМЕНОВ Данил Сергеевич — преподаватель кафедры информационной безопасности Военного университета радиоэлектроники Министерства обороны РФ, prst_danilka@mail.ru

СЕРГЕЕВ Никита Дмитриевич — студент группы ИКПИ-34 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sergeev.nd@sut.ru

СИМОНИНА Анна Александровна — старший преподаватель кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, simonina.aa@sut.ru

СМЕТАНИН Роман Александрович — студент группы МБИ-2511з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, smetanin.ra@sut.ru

СМОРОДИН Геннадий Николаевич — кандидат технических наук, доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, gsmorodin@sut.ru

СПИРИДОНОВ Даниил Петрович — аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, spiridonov.dp@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

СТЕПАНОВ Николай Андреевич — студент группы МБИ-2511з Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, stepanov.na@sut.ru

СТЕПАНОВА Анна Борисовна — кандидат технических наук, старший преподаватель Института энергетики Санкт-Петербургского политехнического университета Петра Великого, stepanova-anna-b@yandex.ru

СТЕЦЕНКО Оксана Николаевна — ассистент кафедры программного обеспечения вычислительной техники и автоматизированных систем Белгородского государственного технологического университета им. В. Г. Шухова, stetsenkoon81@yandex.ru

СТОРОЖУК Николай Леонидович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, storozhuk.nl@sut.ru

СТУРМАН Владимир Ицхакович — доктор географических наук, профессор кафедры экологической безопасности телекоммуникаций Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sturman.vi@sut.ru

СУЗДАЛОВ Дмитрий Станиславович — студент группы ЭМ-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, suzdalov.ds@sut.ru

ТАТАРИНОВ Владимир Иннокентьевич — кандидат технических наук, заместитель начальника отдела научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, tatar271@mail.ru

ТЕРОВЕЦ Алексей Алексеевич — студент группы МЗС-2511 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, terovec.aa@sut.ru

ТЕССЛЕР Ярослав Константинович — студент группы РБ-41 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tessler.iak@sut.ru

ТОКАРЬ Владислав Сергеевич — студент группы ИКТЗ-25 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, tokar.vs@sut.com

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

УХАЛОВ Олег Алексеевич — студент группы ЗР-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, uhalov.oa@sut.ru

ФЕДОРЕНКО Ирина Николаевна — кандидат экономических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fedorenko.in@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

ФЁДОРОВА Марина Юрьевна — старший преподаватель кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. М. А. Бонч-Бруевича, fyodorova.mj@sut.ru

ФОКИН Григорий Алексеевич — доктор технических наук, доцент, заведующий кафедрой беспроводных технологий и систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, fokin.ga@sut.ru

ХАЛАПЯН Алёна Сергеевна — студент группы МСО-2511 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, khalapian.as@sut.ru

ХИТРИН Сергей Ионович — старший преподаватель кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hitrin.si@sut.ru

ХИТРИНА Ирина Юрьевна — кандидат психологических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hitrina.iu@sut.ru

ХЛОПУНОВ Фёдор Дмитриевич — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, xlopunov_fd@mail.ru

ХРУСТАЛЕВ Никита Эдуардович — студент группы МСТ-2561 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, hrustalev.ne@sut.ru

ЦВЕРИАНАШВИЛИ Иван Алексеевич — старший преподаватель кафедры истории и регионоведения Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, cverianashvili.ia@sut.ru

ЧАБАНЕНКО Виктор Вячеславович — соискатель, Военная академия связи им. Маршала Советского Союза С. М. Буденного, flame69rus@yandex.ru

ЧИМИТОВ Дабасамбу Дашицыренович — курсант Военной академии связи им. Маршала Советского Союза С. М. Буденного, dabasambu.chimitov@mail.ru

ЧИСТЫЙ Степан Александрович — студент группы МАП-2611 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, chistyy.sa@sut.ru

ШАРИКОВ Павел Иванович — кандидат технических наук, старший преподаватель кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, sharikov.pi@sut.ru

ШУРУХИНА Олеся Антоновна — студент группы ИСТ-431 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shurukhina.oa@sut.ru

ШАХМОВЕДЕВ Марат Андреевич — студент группы МЗС-2512 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shahmovedev.ma@sut.ru

ШЕВЦОВА Александра Андреевна — студент группы ИКТО-37 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shevtsova.aa@sut.ru

ШЕВЧЕНКО Александр Александрович — кандидат технических наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shevchenko.aa@sut.ru

ШЕВЯКОВ Владислав Денисович — младший научный сотрудник научно-исследовательского центра Военной академии связи им. Маршала Советского Союза С. М. Буденного, Vlad89312239540.la@yandex.ru

ШИЛКОВ Владимир Ильич — кандидат экономических наук, доцент, доцент кафедры экономической безопасности производственных комплексов Уральского федерального университета им. первого Президента России Б. Н. Ельцина, vi.shilkov@urfu.ru

ШИШКОВА Анна Сергеевна — аспирант кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shishkova.as@sut.ru

ШМАТКОВА Ксения Андреевна — студент группы ИКБ-33 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, shmatkova.ka@sut.ru

ЩЕРБАКОВ Игорь Борисович — кандидат технических наук, доцент кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, sherbakov.ib@sut.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

ЮЮКИНА Татьяна Игоревна — кандидат экономических наук, старший преподаватель кафедры экономики данных Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iuiukina.ti@sut.ru

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, yakovlev.vi@sut.ru

ЯНКОВСКИЙ Максим Андреевич — студент группы ЭМ-21 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ekon_up@sut.ru

ЯНЧЕНКО Даниил Леонидович — студент группы ИКПИ-34 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ianchenko.dl@sut.ru

ЯЦКОВА Анастасия Евгеньевна — студент группы ИКТО-37 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, iatskova.ae@sut.ru

# XV МЕЖДУНАРОДНАЯ НАУЧНО-ТЕХНИЧЕСКАЯ И НАУЧНО-МЕТОДИЧЕСКАЯ КОНФЕРЕНЦИЯ

# «АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОТЕЛЕКОММУНИКАЦИЙ В НАУКЕ И ОБРАЗОВАНИИ» (АПИНО 2026)

**Сборник научных статей**

*Научное издание*

Верстка
М. О. Мотыгина
Корректура
Д. Н. Яшугин
Дизайн логотипа Г. И. Юрьев
Подписано в печать 07.09.2026
Объем 40,81 усл.-печ. л.

Объединенная редакция рецензируемых научных изданий СПбГУТ
193232 СПб., пр. Большевиков, 22, корп. 1



АПИНО
ICAIT

APINO.SUT.RU