

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ЛЕСОТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ Г.Ф. МОРОЗОВА»

Институт цифровых и интеллектуальных систем

Факультет компьютерных наук и технологий

ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ:
ОТ ТЕОРИИ К ПРАКТИКЕ – 2026

Материалы Международной научно-практической конференции

Воронеж, 02 июля 2026 г.

MINISTRY OF SCIENCE AND HIGHER EDUCATION
OF THE RUSSIAN FEDERATION
FEDERAL STATE BUDGET EDUCATIONAL INSTITUTION
OF HIGHER EDUCATION
«VORONEZH STATE UNIVERSITY OF FORESTRY AND TECHNOLOGIES
NAMED AFTER G.F. MOROZOV»

Institute of Digital and Intelligent Systems

Faculty of Computer Science and Technology

INTELLECTUAL INFORMATION SYSTEMS:
FROM THEORY TO PRACTICE – 2026

Proceedings of the International Scientific and Practical Conference

Voronezh, July 02, 2026

Voronezh 2026

И73 Интеллектуальные информационные системы: от теории к практике – 2026 : материалы Международной научно-практической конференции, Воронеж, 02 июля 2026 г. / отв. ред. В. К. Зольников, И. Н. Занин ; М-во науки и высшего образования РФ, ФГБОУ ВО «ВГЛТУ». – Воронеж, 2026. – 124 с. – URL: <https://vgltu.ru/nauka/konferencii/2026/intelektualnye-informacionnye-sistemy-ot-teorii-k-praktike-2026/>.– Текст: электронный.

ISBN 978-5-7994-1266-1

В сборнике представлены материалы Международной научно-практической конференции, проведенной Воронежским государственным лесотехническим университетом 02 июля 2026 г., разбитые на секции: «Системный анализ, управление, обработка информации»; «Системы автоматизации проектирования»; «Современная электронная компонентная база», «Искусственный интеллект, беспилотные летательные аппараты и роботизированные системы.». Целью конференции является ознакомление с результатами новейших научных достижений, обмен знаниями и передовым опытом в области моделирования информационных систем и процессов, привлечение наиболее способных студентов к выполнению научных исследований.

Материалы конференции предназначены для широкого круга специалистов промышленности и образования, научных работников, аспирантов и студентов высших учебных заведений, специализирующихся в вопросах информатизации, моделирования систем и процессов, автоматизированного проектирования.

УДК 004

ПРОГРАММНЫЙ КОМИТЕТ

Драпалюк Михаил Валентинович, ректор ФГБОУ ВО «ВГЛТУ», д.т.н., профессор.

Куцько Павел Павлович, Генеральный директор АО «НИИЭТ», к.т.н.

Морковина Светлана Сергеевна, проректор по науке и инновациям ФГБОУ ВО «ВГЛТУ», д.т.н., профессор.

Зольников Владимир Константинович, директор Института цифровых и интеллектуальных систем ФГБОУ ВО «ВГЛТУ», д.т.н., профессор.

Скворцова Татьяна Владимировна, декан факультета компьютерных наук и технологий, к.т.н., доцент.

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ

Кравченко Андрей Сергеевич, заведующий кафедрой вычислительной техники и информационных систем ФГБОУ ВО «ВГЛТУ», к.т.н., доцент.

Аникеев Евгений Александрович, заведующий кафедрой компьютерных технологий и микроэлектронной инженерии ФГБОУ ВО «ВГЛТУ», к.т.н., доцент.

Ягодкин Александр Сергеевич, заведующий кафедрой информационных технологий ФГБОУ ВО «ВГЛТУ», к.ф.-м.н., доцент.

Заревич Антон Иванович, доцент базовой кафедры технического и программного обеспечения вычислительных и информационных систем ФГБОУ ВО «ВГЛТУ», к.т.н.

Смерек Владимир Андреевич, начальник отдела проектирования СБИС АО «НИИЭТ», к.т.н.

Макаренко Филипп Владимирович, доцент базовой кафедры технического и программного обеспечения вычислительных и информационных систем, к.ф.-м.н.

Потапов Игорь Петрович, главный научный сотрудник отдела проектирования СБИС АО «НИИЭТ», к.т.н.

Зольников Константин Владимирович, ведущий инженер отдела проектирования СБИС АО «НИИЭТ», д.т.н.

Таперо Константин Иванович, заместитель генерального директора по науке и инновациям АО «НИИП», д.т.н.

Бойко Владимир Иванович, заместитель генерального директора по развитию АО «ВЗПП-сборка», к.т.н.

Занин Иван Николаевич, преподаватель кафедры компьютерных технологий и микроэлектронной инженерии ФГБОУ ВО «ВГЛТУ».

РЕЦЕНЗЕНТЫ

Смерек Владимир Андреевич – к.т.н., начальник дизайн-центра проектирования ИМС АО «Научно-исследовательский институт электронной техники».

Потапов Игорь Петрович – к.т.н., главный научный сотрудник АО «Научно-исследовательский институт электронной техники».

СОДЕРЖАНИЕ

СЕКЦИЯ 1. СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ, ОБРАБОТКА ИНФОРМАЦИИ

Авилов Ю.О., Аникеев Е.А., Занин И.Н.	
Анализ цепочек атак (Kill Chain) с применением AI.....	7
Авилов Ю.О., Аникеев Е.А., Занин И.Н., Осипов М.А.	
AI-агенты как цифровые ассистенты преподавателя	14
Буздин В.Э., Аникеев Е.А.	
Обнаружение аномалий в потоке метрик информационной системы на основе адаптивных порогов	19
Новикова Т.П.	
Разработка информационной системы для подбора структуры машинно-тракторного парка и комплекса лесных орудий для лесовосстановительных работ с учётом природно-климатических ограничений.....	26
Поляков К.М., Заревич А.И.	
Алгоритмы скрытой и надёжной передачи информации в беспроводных сетях на основе корреляционного анализа и маскировки во временной области	33
Хуссейн М., Аникеев Е.А.	
Кибербезопасность в эпоху цифровой трансформации	44

СЕКЦИЯ 2. СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ

Буздин В.Э., Аникеев Е.А.	
Конвейер развёртывания и мониторинга моделей машинного обучения с контролем дрейфа данных	51
Завьялова М.Е., Волкова С.Н.	
Анализ методов автоматизации мониторинга кормления на животноводческих предприятиях	59

Занин И.Н., Аникеев Е.А., Мельникова П.А.

Интеграция генеративного дизайна и параметрического моделирования в САПР для оптимизации конструкций аэрокосмических компонентов 67

СЕКЦИЯ 3. СОВРЕМЕННАЯ ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА

Занин И.Н., Аникеев Е.А., Авилов Ю.О.

Применение глубокого обучения с подкреплением для управления манипуляторами сервисных роботов в неструктурированных средах 73

Хуссейн М., Акименко А.В.

Искусственные разумы в человеческом облике: эволюция гуманоидных роботов на основе искусственного интеллекта 80

Шхагор Мд.Ш.И., Аникеев Е.А., Акименко А.В.

Постквантовая блокчейн-платформа для подключенных интеллектуальных транспортных средств 88

СЕКЦИЯ 4. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ И РОБОТИЗИРОВАННЫЕ СИСТЕМЫ

Давиденко Д.Н., Ачкасов А.В.

Критериальная систематизация методов машинного обучения для адаптивного светофорного управления 96

Давиденко Д.Н., Ачкасов А.В.

Трехконтурная модель обучаемого управления светофорным объектом: ранжирование, сервисный долг и фазовый допуск 103

Занин И.Н., Аникеев Е.А., Акименко А.В.

Гибридная система навигации БПЛА в условиях отказа GNSS: комбинация визуальной одометрии и инерциальных измерений 111

Рахман Дж., Акименко А.В.

Влияние искусственного интеллекта на повседневную жизнь 117

СЕКЦИЯ 1
СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ,
ОБРАБОТКА ИНФОРМАЦИИ

DOI: 10.58168/IntInfSys2026_7-13

УДК: 004.056.5:004.85

АНАЛИЗ ЦЕПОЧЕК АТАК (KILL CHAIN) С ПРИМЕНЕНИЕМ AI

Ю.О. Авилов¹, Е.А. Аникеев¹, И.Н. Занин¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье предложен подход к автоматизации анализа кибератак на базе модели Cyber Kill Chain с применением методов искусственного интеллекта. Проведена формализация семи этапов kill chain через наблюдаемые индикаторы компрометации. Подчёркнута роль ИИ как вспомогательного инструмента. Обозначены направления дальнейшего развития. Результаты работы применимы как в индустриальной практике кибербезопасности, так и в подготовке специалистов по информационной безопасности.

Ключевые слова: Cyber Kill Chain, искусственный интеллект в кибербезопасности, автоматизация анализа кибератак, машинное обучение для ИБ, MITRE ATT&CK, детектирование этапов атаки.

ANALYSIS OF ATTACK CHAINS (KILL CHAIN) USING AI

Yu.O. Avilov, E.A. Anikeev, I.N. Zanin

Voronezh State University of Forestry and Technologies named after
G.F. Morozov

Abstract. The article proposes an approach to automating the analysis of cyber attacks based on the Cyber Kill Chain model using artificial intelligence methods. The seven stages of the kill chain were formalized through the observed indicators of compromise. The role of AI as an auxiliary tool is emphasized. The directions of further development are outlined. The results of the work are applicable both in the industrial practice of cybersecurity and in the training of information security specialists.

Keywords: Cyber Kill Chain, artificial intelligence in cybersecurity, automation of cyberattack analysis, machine learning for information security, MITRE ATT&CK, detection of attack stages.

Современная кибербезопасность сталкивается с нарастающей сложностью и скоростью кибератак: злоумышленники применяют изощрённые тактики и автоматизацию, быстро адаптируясь к защитным мерам. Традиционные методы расследования инцидентов, основанные на ручном анализе и экспертной интерпретации данных, недостаточно эффективны: они трудоёмки, субъективны и плохо масштабируются при больших объёмах телеметрии. Важна своевременная реконструкция цепочки действий атакующего – она позволяет выявить критические точки, где можно прервать атаку до достижения целей злоумышленника [1].

Модель Cyber Kill Chain (Lockheed Martin) – распространённый инструмент структурирования этапов кибератаки: от разведки и доставки вредоносного инструментария до эксплуатации уязвимостей, закрепления в инфраструктуре и реализации целевых действий. На практике её применение часто сводится к экспертному сопоставлению индикаторов с этапами, что затрудняет оперативное выявление многоэтапных атак. Технологии искусственного интеллекта (ИИ) открывают возможности для автоматизации: методы машинного обучения, NLP и графового анализа помогают выявлять закономерности, классифицировать события по стадиям атаки и восстанавливать последовательности действий с меньшими временными затратами.

Цель работы – разработать подход к автоматизированному анализу цепочек кибератак на основе ИИ в соответствии с моделью kill chain. Задачи: формализовать критерии отнесения событий к этапам kill chain, выбрать и адаптировать алгоритмы машинного обучения для классификации и восстановления последовательностей, экспериментально оценить эффективность подхода. Практическая значимость – повышение оперативности и точности выявления атак, оптимизация реагирования в SOC, применение методик в учебных курсах по информационной безопасности.

Cyber Kill Chain декомпозирует атаку на семь этапов: разведка (Reconnaissance), вооружение (Weaponization), доставка (Delivery), эксплуатация (Exploitation), установка (Installation), управление и контроль (C2), действия по достижению целей (Actions on Objectives). Модель популярна благодаря нагляд-

ности и совместимости с threat hunting, но её линейная структура не всегда отражает динамику современных атак (например, параллельные векторы или возврат к предыдущим этапам).

В качестве альтернативы используют матрицу MITRE ATT&CK – каталог техник и тактик злоумышленников, удобный для сопоставления событий с конкретными TTP и обогащения правил корреляции. Ещё одно развитие концепции – Unified Kill Chain: она включает боковое перемещение и эскалацию привилегий, повышая релевантность для сложных атак, но усложняя автоматизацию из-за большого числа техник и отсутствия жёсткой последовательности.

Исследования последних лет активно применяют машинное обучение и NLP для анализа кибератак: классифицируют инциденты по этапам kill chain, извлекают TTP из отчётов и публикаций, строят таймлайны атак с помощью графовых моделей. Однако многие решения разрабатываются в изолированных средах и слабо привязаны к реальным процессам SOC [2].

Ключевые проблемы внедрения автоматизации: слабая интеграция с потоками данных SIEM-систем (в реальности телеметрия шумная, неполная, разнородная), дефицит воспроизводимых бенчмарков для сравнения алгоритмов, низкая интерпретируемость моделей ИИ – это снижает доверие аналитиков и вынуждает полагаться на ручной анализ. Устранение этих ограничений необходимо для перехода к устойчивым и доверенным инструментам.

Методология исследования основана на формализации этапов kill chain в терминах наблюдаемых технических индикаторов: каждый этап соотносится с конкретными артефактами. Например, разведка фиксируется через аномальные DNS-запросы и сканирование портов; вооружение и доставка – через подозрительные вложения и хеши вредоносных файлов; эксплуатация – через ошибки, вызовы API и аномалии приложений; установка и закрепление – через изменения реестра и создание автозагружаемых сервисов; C2 – через устойчивые исходящие соединения и нестандартные протоколы; действия по целям — через доступ к конфиденциальным данным и попытки горизонтального перемещения. Это создаёт основу для классификации с помощью ИИ [3].

Источники данных – разнородные телеметрические потоки: системные логи (Windows Event Log, Sysmon, EDR), сетевой трафик (pcap, NetFlow), внешние данные Threat Intelligence (IoC-базы, STIX, отчёты). Комбинирование источников даёт многомерный взгляд на инцидент: локальные артефакты дополняют сетевую картину, внешние индикаторы ускоряют идентификацию угроз.

Эффективность методологии оценивают по количественным и качественным метрикам: точность, полнота и F1-мера [4] – по каждому этапу kill chain; доля правильно восстановленных переходов между этапами; время обработки потока событий. Такой набор метрик позволяет комплексно оценить качество классификации и пригодность решения для работы в реальном времени.

Практическая реализация – proof of concept на публичных датасетах (MITRE Engenuity ATT&CK Evaluations, наборы логов, имитирующие инциденты). Экспериментальная среда включает конвейер предобработки: нормализацию форматов, приведение событий к единой схеме, обогащение IoC, ручную разметку по этапам kill chain для обучающей выборки. Сравнивают классические ML-алгоритмы (Random Forest, XGBoost), трансформерные модели для текстовых описаний событий и графовые методы для восстановления последовательностей. Результаты показывают: классические ML-модели эффективны на структурированных логах, трансформеры лучше работают с неструктурированными отчётами, графовые подходы дают наиболее достоверную реконструкцию цепочек, но требуют значительных вычислительных ресурсов [5].

Анализ результатов выявляет зоны ошибок: этапы разведки и доставки часто смешиваются из-за схожести сетевых паттернов, этап установки может пропускаться при слабой телеметрии EDR. Примеры реконструированных цепочек представляют в виде таймлайнов с маппингом на техники MITRE ATT&CK. Ложные срабатывания и пропущенные этапы обусловлены неполнотой данных и поведением легитимных процессов, имитирующих вредоносные действия. Это определяет направления доработки – от расширения набора признаков до уточнения правил корреляции.

Сценарии применения подхода: в SOC – приоритизация алертов по стадии kill chain (C2 и действия по целям получают высший приоритет, разведка – обрабатывается в плановом порядке); в threat hunting – генерация гипотез о незавершённых атаках (например, при наличии разведки и доставки, но отсутствии эксплуатации, система рекомендует проверить следы закрепления); в образовании – автоматическая генерация сценариев атак для учебных полигонов и отработки навыков расследования. При этом качество выводов зависит от полноты телеметрии, критические гипотезы требуют ручной валидации, чрезмерная уверенность в автоматике может привести к пропуску нетипичных атак.

Интерпретируемость выводов важна для доверия аналитиков: нужно не просто отнести событие к этапу, но и объяснить, какие признаки повлияли на решение модели. Это реализуют с помощью методов объяснимого ИИ (XAI:

SNAP, LIME) и прозрачных правил корреляции. Интеграция с SIEM/SOAR предполагает стандартизацию форматов передачи гипотез (правила Sigma, API-интерфейсы). В перспективе – переход к мультимодальным моделям (одновременная обработка логов, трафика и текстовых отчётов) и внедрение адаптивного обучения с учётом обратной связи от экспертов.

Исследование показывает, что ИИ позволяет ускорить и стандартизировать анализ цепочек атак в рамках kill chain: автоматизация снижает временные затраты и субъективность оценок. При этом ИИ не заменяет аналитика, а выступает инструментом поддержки принятия решений, требующим обязательной валидации – особенно в критических или нетипичных инцидентах. Экспериментальная проверка подтвердила работоспособность методологии: гибридное использование ML, NLP и графовых методов обеспечило приемлемую точность классификации и достоверную реконструкцию последовательностей, хотя разведка и доставка остаются сложными для однозначного разделения из-за схожести паттернов и неполноты телеметрии.

Практическая ценность методики: в SOC – для приоритизации алертов, автоматизации классификации инцидентов и формирования гипотез; в криминалистическом анализе – для быстрого восстановления хронологии атаки и сопоставления артефактов с техниками MITRE ATT&CK, что сокращает время локализации угрозы; в образовании – для создания реалистичных сценариев киберучений и отработки навыков анализа инцидентов.

В качестве дальнейших шагов по развитию исследования планируется расширить область применения подхода на сценарии внутренних атак и горизонтального перемещения (lateral movement), которые слабо покрываются классической моделью kill chain и требуют учёта специфики поведения злоумышленника внутри периметра. Перспективным направлением также является создание открытого бенчмарка на базе репрезентативных наборов данных с размеченными цепочками атак — такой ресурс позволит стандартизировать оценку эффективности различных ИИ-решений и обеспечит воспроизводимость результатов в академической и индустриальной среде. Кроме того, целесообразно проработать интеграцию методики с распространёнными SIEM/SOAR-платформами и внедрить механизмы адаптивного обучения, которые будут учитывать обратную связь от аналитиков и оперативно адаптироваться к новым тактикам злоумышленников.

Список литературы

1. Джафарли, В. Ф. Криминологическая кибербезопасность: теоретические, правовые и технологические основы: монография / В. Ф. Джафарли; под редакцией С. Я. Лебедева. – 2-е изд. – Москва: Проспект, 2024. – 480 с. – ISBN 978-5-392-40599-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/463901> (дата обращения: 27.06.2026). – Режим доступа: для авториз. пользователей.

2. Трансграничные отношения в киберпространстве: правовое регулирование, кибербезопасность, разрешение споров: монография / В. А. Канашевский, Б. А. Шахназаров, Л. В. Терентьева, О. Ф. Засемкова. – Москва: Проспект, 2024. – 136 с. – ISBN 978-5-392-39596-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/491291> (дата обращения: 27.06.2026). – Режим доступа: для авториз. пользователей.

3. Джафарли, В. Ф. Криминология кибербезопасности: монография / В. Ф. Джафарли; под редакцией С. Я. Лебедева. – Москва: Проспект, 2022 – Том 5: Криминологическая кибербезопасность: перспективы развития – 2022. – 272 с. – ISBN 978-5-392-36256-1. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/280301> (дата обращения: 27.06.2026). – Режим доступа: для авториз. пользователей.

4. Кибербезопасность в условиях электронного банкинга: практическое пособие: учебное пособие / А. В. Наваленный, А. Б. Дудка, С. В. Конявская [и др.]; под редакцией П. В. Ревенкова. – Москва: ЦИПСИР, 2020. – 522 с. – ISBN 978-5-907244-61-0. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/161659> (дата обращения: 27.06.2026). – Режим доступа: для авториз. пользователей.

5. Ревенков, П. В. Кибербезопасность в условиях электронного банкинга: Практическое пособие: учебное пособие / П. В. Ревенков; под редакцией П. В. Ревенкова. – Москва: Прометей, 2020. – 522 с. – ISBN 978-5-907244-61-0. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/book/166805> (дата обращения: 27.06.2026). – Режим доступа: для авториз. пользователей.

References

1. Jafarli, V. F. Criminological Cybersecurity: Theoretical, Legal, and Technological Foundations: monograph / V. F. Jafarli; edited by S. Ya. Lebedev. - 2nd ed. - Moscow: Prospect, 2024. - 480 p. - ISBN 978-5-392-40599-2. - Text: electronic // Lan: electronic library system. - URL: <https://e.lanbook.com/book/463901> (date accessed: 06/27/2026). - Access mode: for authorized users.
2. Cross-border relations in cyberspace: legal regulation, cybersecurity, dispute resolution: monograph / V. A. Kanashevsky, B. A. Shakhnazarov, L. V. Terentyeva, O. F. Zasemkova. - Moscow: Prospect, 2024. - 136 p. - ISBN 978-5-392-39596-5. - Text: electronic // Lan: electronic library system. - URL: <https://e.lanbook.com/book/491291> (date of access: 06/27/2026). - Access mode: for authorized users.
3. Jafarli, V. F. Criminology of cybersecurity: monograph / V. F. Jafarli; edited by S. Ya. Lebedev. – Moscow: Prospect, 2022 – Volume 5: Criminological Cybersecurity: Development Prospects – 2022. – 272 p. – ISBN 978-5-392-36256-1. – Text: electronic // Lan: electronic library system. – URL: <https://e.lanbook.com/book/280301> (accessed: 06/27/2026). – Access mode: for authorized users.
4. Cybersecurity in the Context of Electronic Banking: A Practical Guide: A Tutorial / A. V. Navalny, A. B. Dudka, S. V. Konyavskaya [et al.]; edited by P. V. Revenkov. – Moscow: TsIPSiR, 2020. – 522 p. – ISBN 978-5-907244-61-0. – Text: electronic // Lan: electronic library system. – URL: <https://e.lanbook.com/book/161659> (date of access: 06/27/2026). – Access mode: for authorized users.
5. Revenkov, P. V. Cybersecurity in the Context of Electronic Banking: A Practical Guide: a tutorial / P. V. Revenkov; edited by P. V. Revenkov. – Moscow: Prometheus, 2020. – 522 p. – ISBN 978-5-907244-61-0. – Text: electronic // Lan: electronic library system. – URL: <https://e.lanbook.com/book/166805> (date of access: 06/27/2026). – Access mode: for authorized users.

AI-АГЕНТЫ КАК ЦИФРОВЫЕ АССИСТЕНТЫ ПРЕПОДАВАТЕЛЯ

Авилов Ю.О.¹, Аникеев Е.А.¹, Занин И.Н.¹, Осипов М.А.¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В статье рассматривается потенциал AI агентов и раскрыты их ключевые характеристики и технологические основы. Проведён анализ практических кейсов внедрения в российских и зарубежных вузах. Особое внимание уделено этическим и правовым вызовам. Обсуждены технологические барьеры и организационные аспекты. В заключении обозначены перспективы развития.

Ключевые слова: AI агенты, образование, высшее образование, персонализация обучения, машинное обучение, этика ИИ, образовательные технологии, виртуальные наставники, академическая честность.

AI AGENTS AS DIGITAL TEACHING ASSISTANTS

Yu.O. Avilov¹, E.A. Anikeev¹, I.N. Zanin¹, M.A. Osipov¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article examines the potential of AI agents and reveals their key characteristics and technological foundations. The analysis of practical cases of implementation in Russian and foreign universities is carried out. Special attention is paid to ethical and legal challenges. Technological barriers and organizational aspects were discussed. In conclusion, the prospects for development are outlined.

Keywords: AI agents, education, higher education, personalization of learning, machine learning, AI ethics, educational technologies, virtual mentors, academic integrity.

Внедрение AI-агентов – перспективное направление развития образования. Это автономные или полуавтономные системы, способные анализировать данные, принимать решения и адаптироваться к условиям; их ключевое преимущество перед традиционными решениями – способность к самообучению.

Актуальность темы связана с запросом вузов на персонализацию обучения, автоматизацию рутины и рост вовлечённости студентов. Цель публикации – рассмотреть принципы работы AI-агентов, их характеристики и технологии, изучить кейсы внедрения в российских и зарубежных вузах, а также осветить этические и правовые аспекты интеграции.

Ключевые характеристики AI-агентов: автономность (действия в рамках целей без постоянного контроля), адаптивность (корректировка стратегий по обратной связи), целеориентированность (фокус на конкретных образовательных результатах) и интерактивность (взаимодействие через разные каналы). В образовании агенты выступают как виртуальные наставники, инструменты персонализации, аналитики и средства автоматизации административных процессов.

Основу функционирования AI-агентов составляют: машинное обучение (выявление закономерностей, прогнозирование результатов, персонализированные решения), NLP (понимание и генерация речи для диалогов и оценки работ), анализ цифрового следа (отслеживание действий учащихся для корректировки материалов) и адаптивные алгоритмы (настройка параметров обучения под текущее состояние студента).

AI-агенты классифицируют по уровню автономности: простые чат-боты (работа по жёстким сценариям), системы с элементами адаптивности (персонализация с периодическим вмешательством человека), самообучающиеся агенты (непрерывное улучшение стратегий) и интегрированные экосистемы (координация нескольких агентов для комплексных задач). Классификация отражает эволюцию от инструментов автоматизации до интеллектуальных систем.

Этические и правовые вызовы включают: конфиденциальность данных (защита персональных сведений учащихся методами анонимизации и шифрования), прозрачность алгоритмов (необходимость Explainable AI для доверия пользователей), распределение ответственности за решения и предотвращение предвзятости алгоритмов (регулярная проверка и корректировка обучающих данных).

За рубежом AI-агенты активно применяют в вузах [1]: Университет Карнеги – Меллон адаптирует материалы под студентов, MIT использует виртуального тьютора по техническим дисциплинам, Университет Торонто автоматизирует формирование групп, Лондонский университет мониторит вовлечённость в онлайн-курсах [2].

В России практики также развиваются: МФТИ генерирует индивидуальные задачи по физике и математике, НИТУ «МИСиС» поддерживает студентов

инженерных специальностей инструкциями и прогнозированием трудностей, СПбГУ помогает в организации междисциплинарных проектов, ТГУ анализирует эффективность программ и формирует рекомендации по учебным планам.

Преимущества внедрения: персонализация обучения, автоматизация рутинных задач, рост вовлечённости, прогнозная аналитика для корректировки программ. Вызовы: потребность в качественной и регулярно обновляемой базе знаний, соблюдение норм конфиденциальности, преодоление сопротивления изменениям со стороны участников процесса.

Технологические ограничения связаны с качеством и фрагментарностью обучающих данных – это может приводить к «галлюцинациям» и недостоверным выводам, особенно в фундаментальных дисциплинах. Решение требует создания специализированных баз знаний и механизмов верификации результатов ИИ [3].

Перспективы связаны с развитием ML и NLP: появятся агенты, способные генерировать учебные материалы, модерировать дискуссии и оценивать творческие работы [4]. Важное направление – методические стандарты и этические нормы, обеспечивающие баланс между использованием ИИ и сохранением академических ценностей (критическое мышление, исследовательская самостоятельность, академическая честность).

Социальный аспект интеграции значим: студенты воспринимают AI как естественный элемент обучения, тогда часть преподавателей испытывает недоверие. Успешная интеграция требует стратегии: тренинги для педагогов, разъяснительная работа со студентами, создание сообществ практики для обмена опытом.

В перспективе AI-агенты станут частью цифровой образовательной экосистемы вуза, формируя у студентов компетенции будущего – работу с данными, критическую оценку результатов ИИ, применение технологий для междисциплинарных задач. Реализация потенциала возможна только при комплексном подходе: технологическое развитие, педагогическая рефлексия и этическое регулирование.

Таким образом, AI-агенты способны трансформировать высшее образование, сделав его гибче и эффективнее. Их потенциал раскрывается при условии преодоления технологических, педагогических и организационных барьеров [5]. Дальнейшие исследования должны фокусироваться на методах повышения доверия к агентам, их интеграции в существующие системы и стратегиях преодоления барьеров внедрения.

Список литературы

1. Юньчжун, Ц. Агенты искусственного интеллекта. Руководство по разработке: руководство / Ц. Юньчжун; переводчик И. Л. Люско. — Москва: ДМК Пресс, 2025. — 502 с. — ISBN 978-5-93700-410-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/521206> (дата обращения: 25.06.2026). — Режим доступа: для авториз. пользователей.
2. Бахтеев, Д. В. Искусственный интеллект: этико-правовые основы: монография / Д. В. Бахтеев. — Москва: Проспект, 2021. — 176 с. — ISBN 978-5-392-33413-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/227240> (дата обращения: 25.06.2026). — Режим доступа: для авториз. пользователей.
3. Фундаментальные и прикладные исследования в информатике и цифровизации: материалы симпозиума XX (LII) Международной научной конференции студентов, аспирантов и молодых ученых «Образование, наука, инновации: вклад молодых исследователей», посвященной 80-й годовщине Победы в Великой Отечественной войне (24 апреля 2025): материалы конференции / редактор Е. С. Чернова. — Кемерово: КемГУ, 2025. — 203 с. — ISBN 978-5-8353-3369-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/507593> (дата обращения: 25.06.2026). — Режим доступа: для авториз. пользователей.
4. Гуманитарные проблемы искусственного интеллекта и его применения: монография / А. Б. Гехт, Р. В. Душкин, А. В. Неровный [и др.]. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 267 с. — ISBN 978-5-89160-320-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/426152> (дата обращения: 25.06.2026). — Режим доступа: для авториз. пользователей.
5. Ручкина, Г. Ф. Правовое регулирования искусственного интеллекта, роботов и объектов робототехники как условие формирования экономического лидерства в России: монография / Г. Ф. Ручкина, М. В. Демченко; под редакцией Г. Ф. Ручкиной. — Москва: Прометей, 2021. — 350 с. — ISBN 978-5-00172-197-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/189730> (дата обращения: 25.06.2026). — Режим доступа: для авториз. пользователей.

References

1. Yunzhong, C. Artificial Intelligence Agents. A Development Guide / C. Yunzhong; translator I.L. Lyusko. — Moscow: DMK Press, 2025. — 502 p. — ISBN 978-5-93700-410-9. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/521206> (date of reference: 25.06.2026). — Access mode: for authorized users.
2. Bakhteev, D.V. Artificial Intelligence: Ethical and Legal Foundations: monograph / D.V. Bakhteev. — Moscow: Prospekt, 2021. — 176 p. — ISBN 978-5-392-33413-1. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/227240> (date of reference: 25.06.2026). — Access mode: for authorized users.
3. Fundamental and Applied Research in Informatics and Digitalization: proceedings of the symposium of the XX (LII) International Scientific Conference of Students, Postgraduates and Young Scientists "Education, Science, Innovation: Contribution of Young Researchers", dedicated to the 80th Anniversary of the Victory in the Great Patriotic War (April 24, 2025): conference materials / editor E.S. Chernova. — Kemerovo: KemSU, 2025. — 203 p. — ISBN 978-5-8353-3369-1. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/507593> (date of reference: 25.06.2026). — Access mode: for authorized users.
4. Humanitarian Problems of Artificial Intelligence and Its Applications: monograph / A.B. Gecht, R.V. Dushkin, A.V. Nerovny [et al.]. — Saint Petersburg: SPbSUT named after M.A. Bonch-Bruевич, 2024. — 267 p. — ISBN 978-5-89160-320-2. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/426152> (date of reference: 25.06.2026). — Access mode: for authorized users.
5. Ruchkina, G.F. Legal Regulation of Artificial Intelligence, Robots and Robotics Objects as a Condition for Forming Economic Leadership in Russia: monograph / G.F. Ruchkina, M.V. Demchenko; edited by G.F. Ruchkina. — Moscow: Prometheus, 2021. — 350 p. — ISBN 978-5-00172-197-0. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/189730> (date of reference: 25.06.2026). — Access mode: for authorized users.

ОБНАРУЖЕНИЕ АНОМАЛИЙ В ПОТОКЕ МЕТРИК ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ АДАПТИВНЫХ ПОРОГОВ

В.Э. Буздин¹, Е.А. Аникеев¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. Рассмотрена задача обнаружения аномалий в потоке эксплуатационных метрик информационной системы. Предложен адаптивный порог на основе экспоненциально взвешенного скользящего среднего и текущей оценки разброса, подстраивающийся под суточные изменения нагрузки. На реальных данных показано, что адаптивный порог по сравнению с фиксированным повышает полноту обнаружения при меньшем числе ложных срабатываний и сокращает время до обнаружения инцидента.

Ключевые слова: обнаружение аномалий, мониторинг, временные ряды, адаптивный порог, наблюдаемость, обработка информации, метрики, информационная система, надёжность.

ANOMALY DETECTION IN THE METRIC STREAM OF AN INFORMATION SYSTEM BASED ON ADAPTIVE THRESHOLDS

V.E. Buzdin¹, E.A. Anikeev¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The problem of detecting anomalies in the stream of operational metrics of an information system is considered. An adaptive threshold based on an exponentially weighted moving average and the current spread estimate is proposed, which adjusts to daily load variations. Using real data, it is shown that the adaptive threshold, compared to a fixed one, increases the detection recall with fewer false alarms and reduces the time to detect an incident.

Key words: anomaly detection, monitoring, time series, adaptive threshold, observability, information processing, metrics, information system, reliability.

Эксплуатация информационной системы немыслима без мониторинга: непрерывно собираются метрики – время ответа, частота запросов, доля ошибок, загрузка ресурсов. Главная задача мониторинга – вовремя заметить, что система перешла в нештатное состояние, и оповестить дежурного до того, как сбой почувствуют пользователи. Поэтому от качества обнаружения аномалий напрямую зависят надёжность и время восстановления сервиса.

Самый распространённый способ – фиксированный порог: оповещение срабатывает, когда метрика превышает заранее заданное значение. Он прост, но плохо работает с метриками, у которых есть выраженный суточный ритм. Если порог задать высоким, чтобы не реагировать на дневные пики, то ночью реальная аномалия его не достигнет и останется незамеченной. Если задать низким, то каждый дневной пик нагрузки будет давать ложное срабатывание. В обоих случаях дежурный либо пропускает инциденты, либо перестаёт доверять оповещениям из-за их обилия.

Выход – порог, который подстраивается под текущее поведение метрики: днём поднимается, ночью опускается, следуя естественному ритму нагрузки. Решение о том, считать ли отклонение аномалией, по сути принимается в условиях шума и неопределённости, что роднит задачу с известными подходами к принятию решений [1]. Цель работы – предложить адаптивный порог для обнаружения аномалий в потоке метрик и сравнить его с фиксированным по полноте обнаружения, числу ложных срабатываний и времени до обнаружения инцидента.

Источником данных служил поток эксплуатационных метрик веб-сервиса за 30 суток с шагом в одну минуту: время ответа по 95-му перцентилю, частота запросов и доля ошибочных ответов. Эти ряды имеют выраженную суточную периодичность — днём значения закономерно выше, ночью ниже, — а также редкие настоящие аномалии: всплески времени ответа при деградации, провалы частоты запросов при недоступности, скачки доли ошибок.

Задача формулируется так: по поступающим значениям метрики в реальном времени относить каждую точку к норме или к аномалии, не имея заранее размеченных примеров. Это задача обработки информации в условиях, когда «норма» сама по себе меняется во времени. Качество решения оценивалось тремя величинами: полнота (доля выявленных настоящих аномалий), точность (доля настоящих среди всех срабатываний) и время до обнаружения – задержка между началом инцидента и оповещением. Перечень контролируемых показателей и эталонные интервалы их значений задавались на основе модели нормального функционирования системы [2, 3].

Схема обработки потока метрик показана на рисунке 1. Метрики снимаются с узлов и сервисов агентом сбора, складываются в хранилище временных рядов, откуда поступают на детектор аномалий. Детектор сравнивает каждое значение с адаптивным порогом и при выходе за его границы формирует оповещение дежурному инженеру. Такая организация отделяет сбор данных от логики обнаружения: правило выявления аномалий можно менять, не затрагивая остальные звенья.

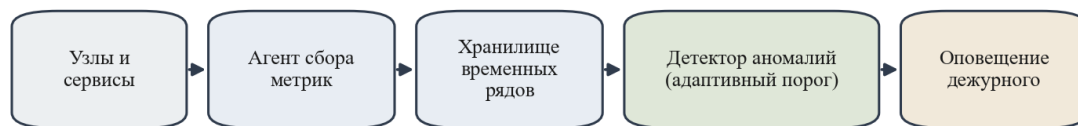


Рисунок 1 – Схема обнаружения аномалий в потоке метрик информационной системы

Ключевое звено — детектор с адаптивным порогом. В отличие от фиксированного значения, его границы пересчитываются на каждом шаге по недавней истории метрики, поэтому порог «дышит» вместе с нагрузкой. Контроль штатности функционирования по непрерывно наблюдаемым показателям характерен для управления высоконадёжными системами, где отклонение требуется обнаружить как можно раньше [4].

В основу порога положено экспоненциально взвешенное скользящее среднее (exponentially weighted moving average, EWMA). На каждом шаге оценка среднего уровня метрики пересчитывается по правилу:

$$m_t = \alpha \cdot x_t + (1 - \alpha) \cdot m_{t-1}$$

где x_t — текущее значение метрики;

m_t — сглаженная оценка её уровня;

α — коэффициент сглаживания ($0 < \alpha < 1$), задающий, насколько быстро оценка реагирует на изменения.

Аналогично, по экспоненциальному сглаживанию отклонений оценивается текущий разброс σ_t . Границы нормального коридора задаются как $m_t \pm k \cdot \sigma_t$, и значение признаётся аномальным, если выходит за этот коридор. Коэффициент k определяет чувствительность: при $k = 3$ в коридор попадают практически все обычные колебания, а за его пределы — лишь редкие, действительно нетипичные значения.

Поскольку оценки (1) непрерывно следуют за метрикой, коридор автоматически расширяется в часы высокой изменчивости и сужается в спокойные периоды. Благодаря этому один и тот же детектор без перенастройки одинаково корректно работает и днём, и ночью. Параметры α и k подбираются как компромисс: меньшие значения дают более чувствительный, но и более «нервный» детектор, большие – устойчивый, но медленнее реагирующий.

На собранных данных адаптивный порог сравнивался с фиксированным. Фиксированный порог подбирался по обучающему участку так, чтобы не реагировать на типичные дневные пики. Параметры адаптивного детектора приняты равными $\alpha = 0,08$ и $k = 3$. Фрагмент работы детектора показан на рисунке 2: метрика времени ответа колеблется в пределах коридора, а одиночный всплеск около 95-й минуты выходит за верхнюю границу и помечается как аномалия.

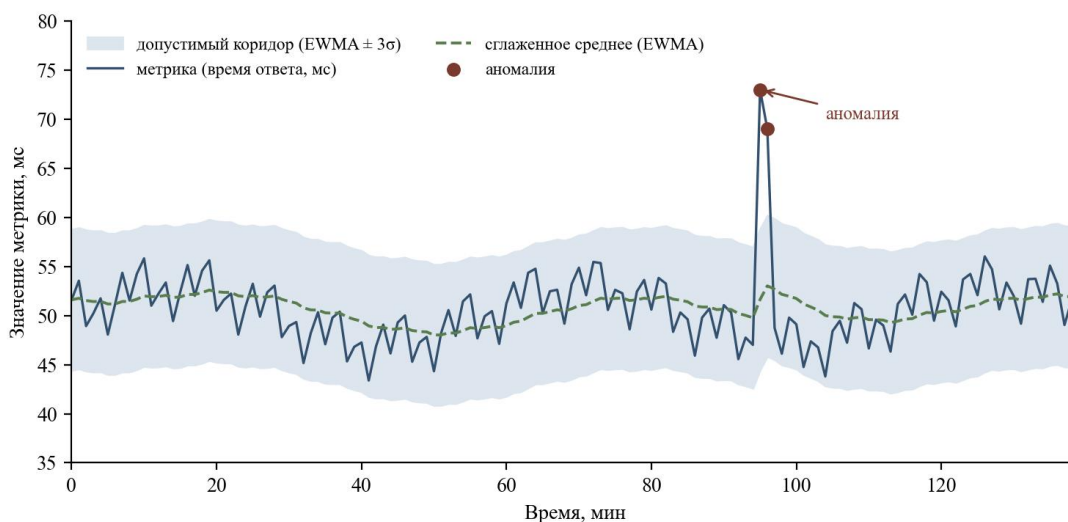


Рисунок 2 – Поток метрики, адаптивный коридор нормы и обнаруженная аномалия

По размеченному вручную набору из 32 настоящих инцидентов за месяц подсчитаны показатели качества обнаружения. Сводное сравнение приведено в таблице 1. Адаптивный порог выявил больше настоящих аномалий при существенно меньшем числе ложных срабатываний, а также раньше реагировал на ночные инциденты, которые фиксированный порог систематически пропускал.

Таблица 1 – Качество обнаружения аномалий

Показатель	Фиксированный порог	Адаптивный порог
Полнота обнаружения, %	72	91
Точность (доля верных тревог), %	63	88
Ложных срабатываний за сутки	11,4	2,3
Среднее время до обнаружения, мин	8,5	3,1

Главная причина различия – суточный ритм. Фиксированный порог приходится ставить выше дневных пиков, и тогда ночные аномалии, не достигающие этого уровня, остаются незамеченными; адаптивный же порог ночью опускается вслед за метрикой и улавливает их. Сокращение времени до обнаружения с 8,5 до 3,1 минуты напрямую уменьшает время восстановления сервиса, поскольку дежурный получает сигнал раньше.

Адаптивный порог переводит обнаружение аномалий из ручной настройки «магического числа» в воспроизводимое правило, которое само следует за поведением метрики. Это снижает нагрузку на дежурного — меньше ложных тревог — и одновременно повышает шансы заметить настоящий инцидент. Решение о тревоге при этом принимается по понятному критерию, что согласуется с подходами к выбору решений в условиях неопределённости и с ситуационным моделированием состояния системы [1, 5].

У метода есть ограничения. Экспоненциальное сглаживание хорошо описывает плавный суточный ритм, но хуже – резкие штатные переходы (например, регламентные работы), которые оно может принять за аномалию; такие периоды разумно пометить отдельно. Кроме того, медленно нарастающая деградация способна «увести» за собой сам порог и остаться незамеченной — против этого помогает контроль и более долгого тренда. Тем не менее даже простой адаптивный порог заметно превосходит фиксированный и не требует обучающей разметки, что делает его удобным средством повышения наблюдаемости информационной системы.

Предложен адаптивный порог обнаружения аномалий в потоке эксплуатационных метрик информационной системы, основанный на экспоненциально взвешенном скользящем среднем и текущей оценке разброса. Коридор нормы по правилу (1) автоматически подстраивается под суточный ритм нагрузки, что позволяет одному детектору одинаково работать в разное время суток. На реальных данных за месяц адаптивный порог по сравнению с фиксированным повысил

полноту обнаружения с 72 % до 91 % и точность с 63 % до 88 %, сократив среднее время до обнаружения инцидента с 8,5 до 3,1 минуты. Метод не требует размеченных данных и применим как практическое средство мониторинга интеллектуальных информационных систем.

Список литературы

1. Горбунов, В. Г. Сравнительный анализ методов «Прометей» и нечетких отношений в условиях принятия решений / В. Г. Горбунов, О. Л. Бордюжа, А. А. Пак // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 42-56. – DOI 10.12737/2219-0767-2024-17-1-42-56. – EDN LSMBMD.
2. Морозов, Н. Д. Введение в управление микросервисами / Н. Д. Морозов, Д. Д. Романов, К. В. Пугин // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. – 2022. – № 40. – С. 689-702. – EDN DMLLTW.
3. Системное моделирование и разработка протоколов информационного взаимодействия блоков в программно-аппаратном комплексе САПР / К. В. Зольников, Д. В. Шеховцов, М. А. Махиборода [и др.] // Моделирование систем и процессов. – 2025. – Т. 18, № 2. – С. 53-62. – DOI 10.12737/2219-0767-2025-18-2-53-62. – EDN XKOLNC.
4. Комплексование технического обеспечения в САПР / М. И. Конча, А. С. Мещеряков, М. А. Махиборода [и др.] // Моделирование систем и процессов. – 2025. – Т. 18, № 4. – С. 39-47. – DOI 10.12737/2219-0767-2025-18-4-39-47. – EDN CVAQJW.
5. Сумин, В. И. Использование ситуационного моделирования в разработке систем принятия решений для сложных организационных систем / В. И. Сумин, А. С. Кравченко, А. В. Толкачев // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 71-79. – DOI 10.12737/2219-0767-2024-69-77. – EDN FBBHJO.

References

1. Gorbunov, V. G. Comparative analysis of the PROMETHEE method and fuzzy relations under decision-making conditions / V. G. Gorbunov, O. L. Bordyuzha, A. A. Pak // Modeling of systems and processes. – 2024. – Vol. 17, No. 1. – pp. 42-56. – DOI 10.12737/2219-0767-2024-17-1-42-56. – EDN LSMBMD.
2. Morozov, N. D. Introduction to microservices management / N. D. Morozov, D. N. D. Romanov, K. N. V. N. Pugin // Modern problems of linguistics and methods

of teaching Russian in higher education institutions and schools. – 2022. – No. 40. - St. 689-702. – EDN DMLLTW.

3. System modeling and development of protocols for information interaction of blocks in the CAD software and hardware complex / K. V. Zolnikov, D. V. Shekhovtsov, M. A. Makhaboroda [et al.] // Modeling of systems and processes. – 2025. – Vol. 18, No. 2. – pp. 53-62. – DOI 10.12737/2219-0767-2025-18-2-53-62. – EDN XKOLNC.

4. Integration of technical support in CAD / M. I. Koncha, A. S. Meshcheryakov, M. A. Makhaboroda [et al.] // Modeling of systems and processes. – 2025. – Vol. 18, No. 4. – pp. 39-47. – DOI 10.12737/2219-0767-2025-18-4-39-47. – EDN CVAQJW.

5. Sumin, V. I. The use of situational modeling in the development of decision-making systems for complex organizational systems / V. I. Sumin, A. S. Kravchenko, A. V. Tolkachev // Modeling of systems and processes. – 2024. – Vol. 17, No. 3. – pp. 71-79. – DOI 10.12737/2219-0767-2024-69-77. – EDN FBBHJO.

**РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ
ДЛЯ ПОДБОРА СТРУКТУРЫ МАШИННО-ТРАКТОРНОГО ПАРКА
И КОМПЛЕКСА ЛЕСНЫХ ОРУДИЙ
ДЛЯ ЛЕСОВОССТАНОВИТЕЛЬНЫХ РАБОТ
С УЧЁТОМ ПРИРОДНО-КЛИМАТИЧЕСКИХ ОГРАНИЧЕНИЙ**

Т.П. Новикова¹

¹Санкт-Петербургский государственный лесотехнический университет
имени С.М. Кирова

Аннотация. В работе рассматривается необходимость комплексного учёта факторов, определяющих выбор технических средств, машин и тракторов при лесовосстановлении. Предложена реляционная структура данных, отражающая взаимодействие машинотракторного парка, технологических операций, энергетических средств с учетом почвенных и других природно-климатических характеристик. Приведено описание разработанного программного обеспечения, позволяющего повысить рациональность принятия решений при формировании машинно-тракторного парка в условиях природно-климатических ограничений.

Ключевые слова: программное обеспечение, реляционная модель, база данных, лесовосстановление, машинно-тракторный парк.

**DEVELOPMENT OF AN INFORMATION SYSTEM FOR SELECTION
OF THE STRUCTURE OF THE MACHINE AND TRACTOR PARK AND
THE COMPLEX OF FOREST TOOLS FOR REGENERATION WORKS,
TAKING INTO ACCOUNT NATURAL AND CLIMATIC RESTRICTIONS**

T.P. Novikova¹

¹Saint Petersburg State Forestry Technical University named after S.M. Kirov

Abstract. The paper discusses the need for a comprehensive account of the factors that determine the choice of technical equipment, machines, and tractors for reforestation. A relational data structure is proposed that reflects the interaction of the machine and tractor fleet, technological operations, and energy resources, taking into account soil and other natural and climatic characteristics.

The paper provides a description of the developed software that enhances the rationality of decision-making when forming a machine and tractor fleet in the context of natural and climatic constraints.

Keywords: software, relational model, database, reforestation, machine and tractor fleet.

Восстановление лесных территорий может быть связано с различными причинами: необходимостью возобновления лесного покрова после сплошных или выборочных рубок, ликвидацией последствий лесных пожаров [1], восполнением утраченных насаждений вследствие распространения вредителей или заболеваний, а также реабилитацией территорий после антропогенного воздействия. Каждая из этих ситуаций формирует специфический набор исходных условий, влияющих на технологию работ: наличие пнёвой остаточности, захламлированность порубочными остатками, присутствие жизнеспособного подроста, степень и характер нарушения почвенного покрова (химические изменения при пожарах, физические нарушения при механизированных рубках и т.п.). Кроме того, значимым фактором является предыстория участка: если ранее здесь располагались искусственные насаждения, то, как правило, снижается неопределённость, связанная с проходимость территории и возможностью применения стандартной техники; в случае же естественного леса возрастает необходимость адаптации технологических решений к сложному рельефу и почвенным условиям.

В связи с этим возникает задача систематизации многообразия природно-климатических, антропогенных и биотических факторов, влияющих на выбор технологических схем и машинно-тракторного парка [2, 3]. Ранее разработанные алгоритмы формирования технологических операций послужили основой для дальнейших исследований. Проведённые изыскания охватили широкий круг аспектов: оценку природно-климатических условий [4], анализ пригодности семенного материала [5, 6, 7], изучение характеристик доступной техники [8] и др.

Была разработана реляционная модель базы данных (рисунок 1) и сама база данных [9], которая содержит сведения о технологических операциях, машинах и механизмах, используемых в процессе восстановления лесных ландшафтов. Также была предложена модель и разработана база данных, объединяющая сведения о типах почв и лесорастительных условиях. На основе предложенных баз данных и алгоритма выбора технологических операций было создано программное обеспечение (ПО) [10], позволяющее осуществлять обоснованный подбор машинно-тракторного парка и комплекса лесных орудий с учётом указанных ограничений.

ПО работает следующим образом: на основе задаваемых пользователем параметров (природно-климатические показатели, рельеф и другие характеристики участка, которые имеют численное выражение) и данных из встроенных справочников (почвенные характеристики, технологические операции, модели машин и механизмов) система генерирует перечень рекомендуемых операций и подбирает соответствующий состав машинно-тракторного парка и комплекса лесных орудий.



Рисунок 1 – Реляционная модель базы данных

Преимущество предложенного подхода заключается в возможности интеграции широкого спектра факторов, а также в вариативном анализе сочетаний различных агрегатов. Вместе с тем дальнейшее развитие инструментария предполагает включение расчётов производительности (применение сетевых технологий позволит рассчитать оптимальный технологический процесс с учетом производительности машинно-тракторного парка и лесных орудий на каждом этапе проекта лесовосстановления [11, 12]), постоянный мониторинг новых технологических решений и интеграцию блока выбора посадочного материала для достижения максимальной эффективности лесовосстановительных мероприятий.

Список литературы

1. Асадов, Х. Г. Моделирование температурного поля при лесных пожарах / Х. Г. Асадов, Г. З. Байрамов // Моделирование систем и процессов. – 2024. – Т. 17, № 4. – С. 7-15. – DOI 10.12737/2219-0767-2024-17-4-7-15. – EDN ECSUWP.
2. Новикова, Т. П. Исследование набора технологических операций подготовки семенного материала хвойных пород для лесовосстановления / Т. П. Новикова // Лесотехнический журнал. – 2021. – Т. 11, № 4(44). – С. 150-160. – DOI 10.34220/issn.2222-7962/2021.4/13. – EDN DORNDT.
3. Подход к глубокому изучению для выявления фузариозной гнили в семенах пшеницы с использованием недорогой технологии визуализации / Р. С. Бернардес, А. Де Медейрос, Л. Да Силва [и др.] // Agriculture. – 2022. – Том 12, № 11. – С. 1801. – DOI 10.3390/agriculture12111801. – EDN HKVPRE.
4. Новикова, Т. П. Влияние климатического индекса градусо-дней на виталитет 3-летних сеянцев сосны обыкновенной из сортированных по спектрометрическим свойствам семян / Т. П. Новикова, В. И. Малышева, Е. П. Петрищев // Лесотехнический журнал. – 2022. – Т. 12, № 1(45). – С. 110-118. – DOI 10.34220/issn.2222-7962/2022.1/9. – EDN JZWCHI.
5. Рост диаметра корневой шейки выявляет тесную взаимосвязь с ростом высоты молодых деревьев сосны обыкновенной из семян, дифференцированных по спектрометрическому признаку / Т. П. Новикова, П. Тайлек, К. Б. Мастранджело [и др.] // Forests. – 2023. – Том 14, № 6. – С. 1164. – DOI 10.3390/f14061164. – EDN ONMQTP.
6. Экспресс-анализ семян в лесохозяйственном производстве: теоретические и технологические аспекты / А. И. Новиков, М. В. Драпалюк, С. В. Соколов, Т. П. Новикова. – Воронеж: Воронежский государственный лесотехнический университет им. Г.Ф. Морозова, 2022. – 176 с. – ISBN 978-5-7994-0976-0. – EDN HMRFVD.
7. Новиков, А. И. Влияние сортирования семян сосны обыкновенной по цвету и размерам на их грунтовую всхожесть в контейнерах / А. И. Новиков // Хвойные бореальной зоны. – 2019. – Т. 37, № 5. – С. 313-319. – EDN VSKFOD.
8. Как технические параметры ИК-сканера могут повлиять на эффективность сортировки семян? / Т. П. Новикова, С. Б. Мастранджело, П. Тайлек [и др.] // Agriculture. – 2022. – Том 12, № 12. – С. 2125. – DOI 10.3390/agriculture12122125. – EDN ESQXMV.

9. Свидетельство о государственной регистрации базы данных № 2025620063 Российская Федерация. Технологические операции, машины и механизмы, используемые в процессе восстановления лесных ландшафтов: заявл. 08.12.2024: опубл. 09.01.2025 / Т. П. Новикова, Е. П. Петрищев, С. А. Евдокимова, А. И. Новиков; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Воронежский государственный лесотехнический университет имени Г.Ф. Морозова".

10. Свидетельство о государственной регистрации программы для ЭВМ № 2025610716 Российская Федерация. Справочная информационная система FLR-Library для поддержки принятия управленческих решений при реализации проектов адаптивного восстановления лесных ландшафтов: заявл. 07.12.2024: опубл. 14.01.2025 / Т. П. Новикова, С. А. Евдокимова, А. И. Новиков; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Воронежский государственный лесотехнический университет имени Г.Ф. Морозова".

11. Новикова, Т. П. Разработка и исследование базовой модели PERT для планирования работ по проекту / Т. П. Новикова, С. А. Евдокимова, А. И. Новиков // Моделирование систем и процессов. – 2021. – Т. 14, № 4. – С. 75-81. – DOI 10.12737/2219-0767-2021-14-4-75-81. – EDN XTKUFJ.

12. Сумин, В. И. Разработка сетевой модели целевых установок сложных организационных систем специального назначения / В. И. Сумин, А. С. Кравченко, С. В. Родин // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 79-87. – DOI 10.12737/2219-0767-2024-17-3-79-85. – EDN QIRWOK.

References

1. Asadov, Kh. G. Modeling of the Temperature Field in Forest Fires / Kh. G. Asadov, G. Z. Bayramov // Modeling of Systems and Processes. – 2024. – Vol. 17, No. 4. – Pp. 7-15. – DOI 10.12737/2219-0767-2024-17-4-7-15. – EDN ECSUWP.

2. Novikova, T. P. Research of a set of technological operations for preparing coniferous seed material for reforestation / T. P. Novikova // Lesotekhnicheskyy Zhurnal. – 2021. – Vol. 11, No. 4(44). – Pp. 150-160. – DOI 10.34220/issn.2222-7962/2021.4/13. – EDN DORNDT.

3. Deep-learning approach for fusarium head blight detection in wheat seeds using low-cost imaging technology / R. C. Bernardes, A. De Medeiros, L. Da Silva [et al.] // Agriculture. – 2022. – Vol. 12, No. 11. – P. 1801. – DOI 10.3390/agriculture12111801. – EDN HKVPRE.

4. Novikova, T. P. Influence of the climatic index of degree-days on the vitality of 3-year-old Scots pine seedlings from seeds sorted by their spectrometric properties / T. P. Novikova, V. I. Malysheva, and E. P. Petrishchev // *Lesotekhnichesky Zhurnal*. – 2022. – Vol. 12, No. 1(45). – Pp. 110-118. – DOI 10.34220/issn.2222-7962/2022.1/9. – EDN JZWCHJ.

5. The Root Collar Diameter Growth Reveals a Strong Relationship with the Height Growth of Juvenile Scots Pine Trees from Seeds Differentiated by Spectrometric Feature / T. P. Novikova, P. Tylek, C. B. Mastrangelo [et al.] // *Forests*. – 2023. – Vol. 14, No. 6. – P. 1164. – DOI 10.3390/f14061164. – EDN ONMQTP.

6. Express analysis of seeds in forestry production: theoretical and technological aspects / A. I. Novikov, M. V. Drapalyuk, S. V. Sokolov, and T. P. Novikova. – Voronezh: Voronezh State Forestry University named after G. F. Morozov, 2022. – 176 p. – ISBN 978-5-7994-0976-0. – EDN HMRFVD.

7. Novikov, A. I. Influence of sorting of Scots pine seeds by color and size on their soil germination in containers / A. I. Novikov // *Conifers of the Boreal Zone*. – 2019. – Vol. 37, No. 5. – Pp. 313-319. – EDN VSKFOD.

8. How Can the Engineering Parameters of the NIR Grader Affect the Efficiency of Seed Grading? / T. P. Novikova, C. B. Mastrangelo, P. Tylek [et al.] // *Agriculture*. – 2022. – Vol. 12, No. 12. – P. 2125. – DOI 10.3390/agriculture12122125. – EDN ESQXMV.

9. Certificate of State Registration of the Database No. 2025620063, Russian Federation. Technological operations, machines, and mechanisms used in the process of restoring forest landscapes: application No. 08.12.2024: published on 09.01.2025 / T. P. Novikova, E. P. Petrishchev, S. A. Evdokimova, and A. I. Novikov; applicant: Federal State Budgetary Educational Institution of Higher Education "Voronezh State Forestry University named after G. F. Morozov".

10. Certificate of State Registration of the Computer Program No. 2025610716, Russian Federation. FLR-Library reference information system for supporting management decision-making in the implementation of adaptive restoration projects for forest landscapes: application No. 07.12.2024: published on 14.01.2025 / T. P. Novikova, S. A. Evdokimova, A. I. Novikov; applicant: Federal State Budgetary Educational Institution of Higher Education "Voronezh State Forestry University named after G. F. Morozov".

11. Novikova, T. P. Development and Research of the Basic PERT Model for Project Work Planning / T. P. Novikova, S. A. Evdokimova, and A. I. Novikov // Modeling of Systems and Processes. – 2021. – Vol. 14, No. 4. – Pp. 75-81. – DOI 10.12737/2219-0767-2021-14-4-75-81. – EDN XTKUFJ.

12. Sumin, V. I. Development of a Network Model of Target Settings for Complex Special-Purpose Organizational Systems / V. I. Sumin, A. S. Kravchenko, and S. V. Rodin // Modeling of Systems and Processes. – 2024. – Vol. 17, No. 3. – Pp. 79-87. – DOI 10.12737/2219-0767-2024-77-85. – EDN QIRWOK.

АЛГОРИТМЫ СКРЫТОЙ И НАДЁЖНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ НА ОСНОВЕ КОРРЕЛЯЦИОННОГО АНАЛИЗА И МАСКИРОВКИ ВО ВРЕМЕННОЙ ОБЛАСТИ

К.М. Поляков¹, А.И. Заревич¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье исследуются методы повышения надёжности и скрытности передачи информации в беспроводных сетях связи на основе корреляционного анализа временных паттернов сигналов. Предложен алгоритм адаптивного выбора паттерна из базы данных на основе анализа его востребованности в текущий момент времени. Разработана методика маскировки полезного сигнала под выбранный эталонный паттерн с сохранением его автокорреляционных свойств. Проведено моделирование предложенных алгоритмов в каналах с замираниями. Результаты показывают возможность достижения коэффициента ошибок по битам не выше 10^{-4} при отношении сигнал/шум от 3 дБ и обеспечении скрытности передачи.

Ключевые слова: скрытая передача информации, беспроводные сети, корреляционный анализ, временные паттерны, маскировка сигналов, когнитивное радио, надёжность связи.

ALGORITHMS FOR COVERT AND RELIABLE DATA TRANSMISSION IN WIRELESS NETWORKS BASED ON CORRELATION ANALYSIS AND TIME-DOMAIN MASKING

K.M. Polyakov¹, A.I. Zarevich¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article examines methods for increasing the reliability and secrecy of information transmission in wireless communication networks based on correlation analysis of time patterns of signals. An algorithm for adaptive selection of a pattern from a database based on an analysis of its relevance at the current time is proposed. A technique has been developed to mask a useful signal for a selected reference pattern while preserving its autocorrelation properties. The proposed algorithms are modeled in channels with fading. The results show the possibility of achieving a bit error rate of no more than 10^{-4} with a signal-to-noise ratio of 3 dB and ensuring transmission secrecy.

Keywords: cover information transmission, wireless networks, correlation analysis, time patterns, signal masking, cognitive radio, communication reliability.

Введение

Обеспечение конфиденциальности передачи данных в беспроводных сетях традиционно решается методами криптографии на сетевом уровне. Однако шифрование не скрывает сам факт наличия радиопередачи, что делает канал уязвимым для целевого перехвата, пеленгации и последующего криптоанализа [1, 2]. В условиях плотного радиоэфира актуальной становится задача реализации концепции Low Probability of Intercept (LPI) – снижения вероятности обнаружения сигнала средствами радиоразведки.

Методы физического уровня, основанные на маскировке полезного сигнала под легитимный трафик или шумовую помеху, позволяют решить эту проблему. В отличие от широкополосных систем (DSSS, FHSS), которые обладают признаками широкополосности и легко детектируются энергетическими приемниками, стеганографические методы внедрения информации в структуру существующих сигналов обеспечивают статистическую неотличимость от фона [3].

В данной работе предлагается алгоритм адаптивной маскировки во временной области. Ключевое отличие подхода заключается в динамическом выборе эталонного паттерна из базы данных известных сигналов (преамбулы Wi-Fi, Bluetooth, радарные импульсы) на основе анализа текущей радиообстановки. Система может либо сливаться с доминирующим трафиком (стратегия «фона»), либо использовать редкие, маловероятные паттерны для работы в «слепых зонах» мониторинга. Цель исследования – оценка компромисса между скрытностью такой передачи и её помехоустойчивостью в каналах с замираниями.

1. Математическая модель и предложенные алгоритмы

Предлагаемый нами подход в своей основе опирается на принципы когнитивного радио или когнитивной маскировки. Здесь огибающей своего сигнала под характеристики окружающих излучателей. Важной etapом здесь является формирование базы эталонных сигналов, которые могут выступать в роли маски. Также эти маски мы будем называть далее временными паттернами.

Формально, под временным паттерном мы понимаем детерминированную или статистически устойчивую огибающую сигнала $p_i(t)$ длительностью T , которая присутствующая в контролируемом спектре.

База данных таких временных паттернов $P = \{p_1(t), p_2(t), \dots, p_n(t)\}$ формируется из сигналов, типичных для данной местности в исследуемые интервалы времени. Примерами таких паттернов могут являться многие виды сигналов.

Например:

- преамбулы стандартов протоколов связи IEEE 802.11/802.15.4, Wi-Fi, Bluetooth, ZigBee;
- импульсы первичных радиолокаторов;
- маяковые сигналы IoT-устройств.

Критерием пригодности паттерна для его сохранения в базу данных (стеганографии) является вид его автокорреляционной функции (АКФ). Для надежного извлечения информации на приеме АКФ должна иметь четко выраженный главный лепесток при низком уровне боковых. Это будет явно соответствовать высокой повторяемости этого сигнала. Автокорреляционная функция паттерна $p_i(t)$ определяется как:

$$R_{p_i}(\tau) = \int_0^T p_i(t)p_i(t - \tau)dt$$

Наличие острого пика корреляции позволяет использовать согласованную фильтрацию на приеме, что максимизирует отношение сигнал/шум (ОСШ) даже при малых амплитудах внедряемого сигнала.

Выбор оптимального паттерна для маскировки осуществляется на основе метрики его востребованности M_i в текущем окне наблюдения T_{obs} . Метрика рассчитывается как степень корреляции принятого суммарного сигнала эфира $r(t)$ с эталоном $p_i(t)$:

$$M_i = \frac{1}{T_{obs}} \int_0^{T_{obs}} \left| \int r(t)p_i(t - \tau)dt \right|^2 d$$

Система реализует две стратегии поведения:

1. Стратегия А (Мимикрия). Выбирается паттерн с максимальной метрикой M_{max} . Сигнал маскируется под самый частый тип трафика, растворяясь в общем фоне.
2. Стратегия В (Аномальность). Выбирается паттерн с минимальной ненулевой метрикой M_{min} . Передача ведется в тех типах сигналов, которые присутствуют в эфире редко, что снижает вероятность их целенаправленного анализа системами РЭБ.

Далее, после выбора временного паттерна нам необходимо внедрить в него, или замаскировать им, необходимую для передачи информацию. Саму информацию, в рамках данной статьи, мы представляем в дискретном виде как последовательность битов $b = \{b_1, b_2, \dots, b_k\}$, гдн $b_j \in \{-1, +1\}$. Внедрение битовой последовательности осуществляется методом амплитудной стего-модуляции. При этом передаваемый сигнал $s(t)$ формируется как произведение временного представления битовой последовательности на временное описание паттерна:

$$s(t) = p_{sel}(t) \cdot \left(1 + \sum_{j=1}^k b_j \cdot \delta A_j(t) \right)$$

где $\delta A_j(t)$ – малые возмущения амплитуды ($|\delta A_j| \ll 1$).

Коэффициент модуляции выбирается таким образом, чтобы изменение энергии сигнала оставалось в пределах естественных флуктуаций легитимного трафика (например, из-за замираний или изменений мощности передатчика источника). По сути, для внешнего наблюдателя исходный временной паттерн остаётся практически неизменным. Он только слегка флуктуационно искажается. Это вполне соответствует естественным искажениям сигналов, вызванных внешними факторами и помехами. Малые амплитудные возмущения обеспечивают сохранение статистических свойств АКФ исходного паттерна.

На приемной стороне, обладающей априорной информацией о выбранном паттерне $p_{sel}(t)$, применяется согласованный фильтр. Выходной сигнал фильтра $y(t)$ в момент времени t_0 , соответствующий максимуму корреляции, используется для принятия решения:

$$\hat{b}_j = \text{sgn}(y(t_0))$$

Такой подход обеспечивает оптимальный прием в гауссовском шуме. Устойчивость к межсимвольной интерференции достигается за счет ортогональности или слабой корреляции соседних битовых интервалов внутри паттерна.

2. Результаты моделирования

Эффективность алгоритмов оценивалась путем имитационного моделирования в среде MATLAB. Моделировался канал связи с рэлеевскими замираниями (доплеровский сдвиг $f_d = 10$ Гц) и аддитивным белым гауссовским шумом (АБГШ). Длительность паттерна составляла $T = 10$ мкс.

В качестве эталонов использовались последовательности Баркера (Barker-13), М-последовательности длиной 31 и 63 бита, а также гауссовы импульсы. Их параметры приведены в Таблице 1.

Таблица 1. Параметры эталонных паттернов

Тип паттерна	Длительность, бит	Уровень боковых лепестков АКФ, дБ	Устойчивость к замираниям
Barker-13	13	-22.3	Средняя
M-seq-31	31	-14.9	Высокая
M-seq-63	63	-18.0	Высокая
Gauss-impulse	16	-25.1	Низкая

Заметим, что Гауссовы импульсы имеют хорошую локализацию во времени, но худшие корреляционные свойства по сравнению с псевдослучайными последовательностями, что снижает помехоустойчивость.

На Рисунке 1 представлены зависимости коэффициента ошибок по битам (BER) от отношения сигнал/шум (SNR).

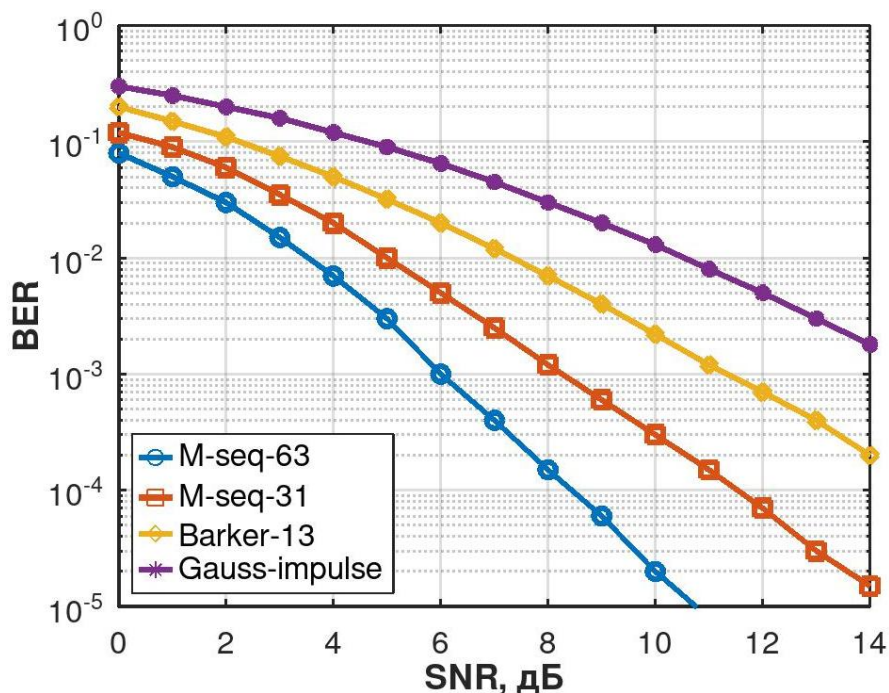


Рисунок 1 – Зависимость BER от SNR для различных паттернов в канале с рэлеевскими замираниями

Анализ показывает, что длинные М-последовательности (M-seq-63) обеспечивают наилучшую помехоустойчивость. Значение BER 10^{-4} достигается при SNR около 6 дБ. Коды Баркера уступают из-за меньшей длины кодового слова, что снижает выигрыш от обработки сигналом. Гауссовы импульсы демонстрируют наихудшие результаты из-за отсутствия внутреннего кодирования и высокой чувствительности к глубоким замираниям.

Оценка скрытности проводилась путем моделирования идеального детектора, использующего энергетический порог и корреляционный анализ. Результаты моделирования приведены в Таблице 2 и на Рисунке 2.

Таблица 2. Показатели скрытности для различных стратегий выбора паттерна

Стратегия	Вероятность обнаружения, P_d	Ложная тревога, P_{fa}	Коэффициент скрытности, ξ
Без маскировки	0.92	0.05	0.08
Стратегия А (фон)	0.23	0.08	0.77
Стратегия В (редкий)	0.11	0.12	0.89

Здесь коэффициент скрытности $\xi = 1 - P_d$ характеризует вероятность необнаружения передачи.

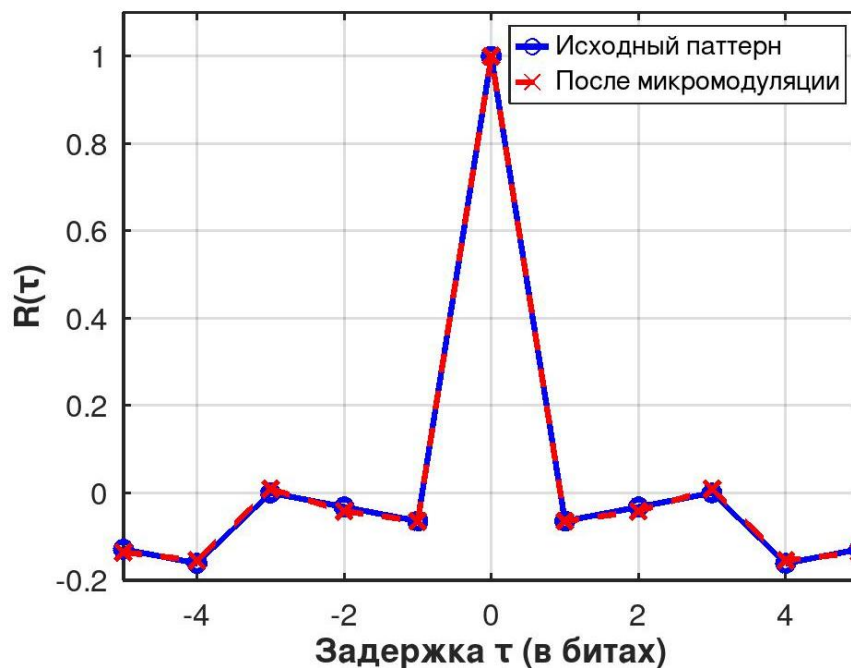


Рисунок 2 – Автокорреляционные функции паттернов до и после маскировки

Как видно из Рисунка 2, применение амплитудной стего-модуляции незначительно искажает АКФ. Отклонение пика спектра от исходного значения не превышает 2%. Это подтверждает, исходное предположение о том, что для внешнего наблюдателя сигнал остается статистически идентичным выбранному паттерну. То есть, модуляция паттерна информационной последовательностью крайне незначительно исказило сам исходный паттерн. По сути – это обеспечило скрытность передачи информации.

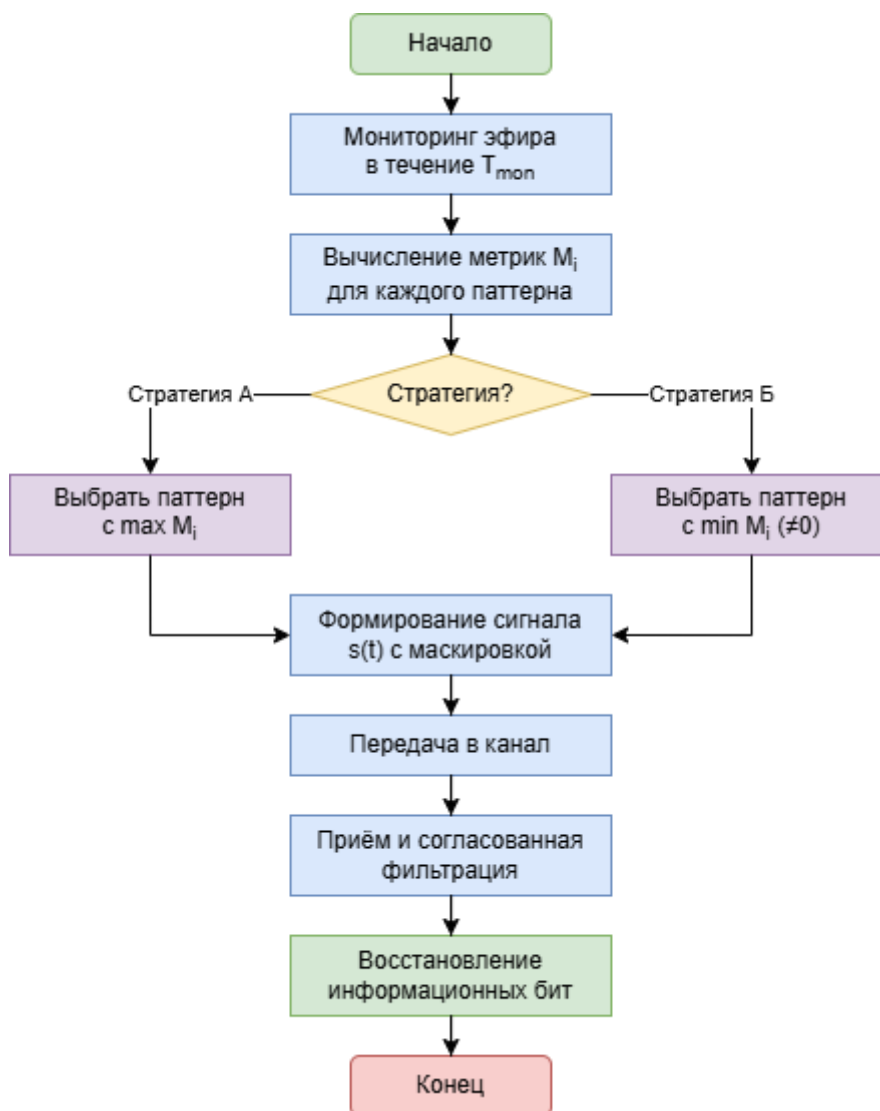


Рисунок 3 – Временная диаграмма работы алгоритма выбора паттерна

Анализируя полученные результаты компьютерного моделирования, нами сделаны предположения применимости предложенных стратегий. Так, стратегия А (Мимикрия) предпочтительна в перегруженных диапазонах, где любой «редкий» сигнал сразу привлечет внимание анализаторов спектра. И наоборот,

стратегия В (Аномальность) демонстрирует наибольшую эффективность в условиях разреженного эфира, снижая вероятность обнаружения до 11%.

Полученные данные указывают на существование компромисса между длиной паттерна, помехоустойчивостью и скрытностью. Использование М-последовательностей длиной 63 бита дает выигрыш в ОСШ до 4 дБ по сравнению с короткими кодами, однако требует более сложной синхронизации на приеме.

Стратегия выбора паттерна позволяет адаптироваться к условиям среды: в городской застройке с плотным Wi-Fi трафиком эффективнее маскироваться под него (Стратегия А), тогда как в промышленных зонах или сельской местности целесообразно использовать редкие сигналы (Стратегия В). Главным ограничением метода является необходимость точной синхронизации по времени между передатчиком и приемником, так как рассинхронизация приводит к резкому падению корреляционного пика.

Заключение

В рамках данной работы было выполнено комплексное исследование алгоритмов скрытой и надёжной передачи информации в беспроводных сетях на основе анализа временных паттернов, предложен комплекс алгоритмов для скрытой и надёжной передачи информации во временной области.

Основные результаты работы:

1. Разработана методика формирования базы временных паттернов с оценкой их автокорреляционных свойств.
2. Предложен алгоритм адаптивного выбора паттерна на основе анализа текущей востребованности в эфире.
3. Метод микромодуляции амплитуды позволяет внедрять полезную информацию без существенного искажения автокорреляционной функции паттерна, что обеспечивает надёжное извлечение данных.

Перспективным направлением исследований является расширение подхода на частотную область и разработка гибридных алгоритмов, адаптирующихся как во времени, так и по частоте.

Список литературы

1. Джанвеккьо С. Модельные скрытые временные каналы: автоматическое моделирование и уклонение / С. Джанвеккьо, Х. Ван, Д. Виджесекера, С. Яджодия // Lecture Notes in Computer Science. – 2008. – Т. 5230. – С. 211–230. – DOI: 10.1007/978-3-540-87403-4_12.

2. Головачев В. Ю. Практические оценки стойкости некоторых стеганографических систем / В. Ю. Головачев, Р. М. Ковалев, И. Н. Оков // Конфидент. – 2002. – № 6 (48).

3. Бонати Л. SteaL-TE: предоставление частной сотовой связи 5G как услуги с полностековой беспроводной стеганографией / Л. Бонати, С. Д'Оро, Ф. Рестуккья, С. Базаньи, Т. Мелодия // IEEE INFOCOM 2021 – IEEE Conference on Computer Communications. – 2021. – С. 1–10. – DOI: 10.1109/INFOCOM42981.2021.9488755.

4. Проскуряков В. Когнитивные радиосистемы в сетях тактического назначения / В. Проскуряков // Электронные компоненты. – 2014. – № 3. – С. 36–38.

5. Дусматов Д. Х. Когнитивное радио - новая беспроводная технология в недалеком будущем / Д. Х. Дусматов, Ж. К. Назирханов // АК ТТЕ. – 2009. – № 2 (9).

6. Разработка технологических и конструкторских платформ при топологических нормах менее 90 нм / Е. Грошева, А. Заревич, А. Денискина, К. Фатуллаева // BIO Web of Conferences. – 2024. – Т. 145. – С. 03018. – DOI 10.1051/bioconf/202414503018.

7. Компьютерное моделирование работы транзисторов и полупроводниковых приборов на его основе / А. В. Полуэктов, Ф. В. Макаренко, Р. Ю. Медведев // Моделирование систем и процессов. – 2023. – Т. 16, № 1. – С. 77–84. – DOI 10.12737/2219-0767-2023-16-1-77-84. – EDN LOLZMT.

8. Исследование способов защиты информации от утечки по акустическому и виброакустическому каналам / В. К. Зольников, С. А. Сазонова, А. И. Заревич, С. С. Башун // Моделирование систем и процессов. – 2025. – Т. 18, № 2. – С. 27–40.

9. Локальная устойчивость колебаний магнетрона со связанными резонаторами / А. И. Заревич, С. С. Новиков // Вестник науки Сибири. – 2013. – № 4 (10). – С. 109–114.

10. Моделирование колебательных процессов в пакете MVStadium / А. В. Полуэктов, К. В. Зольников, В. И. Анциферова // Моделирование систем и процессов. – 2021. – Т. 14, № 4. – С. 139–148. – DOI 10.12737/2219-0767-2021-14-4-139-148. – EDN PPOUDI.

11. Исследование эффективности защиты от гамма-излучения с использованием многослойного полусферического экрана / А. В. Полуэктов, А. И. Заревич, Ф. В. Макаренко, М. В. Солодилов // Моделирование систем и процессов. – 2025. – Т. 18, № 4. – С. 71–83.

12. Анализ количества потребления SF_6 и CF_4 для заправки коммутационной аппаратуры высокого напряжения / Н. Ю. Заленская, Ф. В. Макаренко, А. И. Заревич, А. В. Полуэктов // Известия высших учебных заведений. Проблемы энергетики. – 2024. – Т. 26, № 4. – С. 3–16. – DOI 10.30724/1998-9903-2024-26-4-3-16. – EDN HOOMCR.

References

1. Gianvecchio S. Model-based covert timing channels: automated modeling and evasion / S. Gianvecchio, H. Wang, D. Wijesekera, S. Jajodia // Lecture Notes in Computer Science. – 2008. – Vol. 5230. – P. 211-230. – DOI: 10.1007/978-3-540-87403-4_12.

2. Golovachev V. Yu. Practical estimates of the durability of some steganographic systems / V. Y. Golovachev, R. M. Kovalev, I. N. Okov // Confi-dent. – 2002. – № 6 (48).

3. Bonati L. SteaL-TE: Private 5G Cellular Connectivity as a Service with Full-stack Wireless Steganography / L. Bonati, S. D'Oro, F. Restuccia, S. Basagni, T. Melodia // IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. – 2021. – P. 1-10. – DOI: 10.1109/INFOCOM42981.2021.9488755.

4. Proskuryakov V. Cognitive radio systems in tactical networks / V. Proskuryakov // Electronic components. 2014. No. 3. pp. 36-38.

5. Dusmatov D. H. Cognitive radio – a new wireless technology in the near future / D. H. Dusmatov, J. K. Nazirkhanov // AK TTE. – 2009. – № 2 (9).

6. Development of technology and design platforms at topological norms less than 90 nm / E. Grosseva, A. Zarevich, A. Deniskina, K. Fatullaeva // BIO Web of Conferences. – 2024. – Vol. 145. – P. 03018. – DOI 10.1051/bioconf/202414503018.

7. Computer simulation of transistor operation and semiconductor devices based on it / A.V. Poluektov, F. V. Makarenko, R. Y. Medvedev // Modeling of systems and processes. – 2023. – Vol. 16, No. 1. – pp. 77-84. – DOI 10.12737/2219-0767-2023-16-1-77-84. – EDN LOLZMT.

8. V. K. Zolnikov, S. A. Sazonova, A. I. Zarevich, S. S. Bashun, Research of ways to protect information from leakage through acoustic and vibroacoustic channels // Modeling of systems and processes. 2025. Vol. 18, No. 2. pp. 27-40.

9. Local stability of magnetron oscillations with coupled resonators / A. I. Zarevich, S. S. Novikov // Bulletin of Siberian Science. – 2013. – № 4 (10). – Pp. 109-114.

10. Modeling of oscillatory processes in the MVStudium package / A.V. Poluektov, K. V. Zolnikov, V. I. Antsiferova // Modeling of systems and processes. – 2021.

– Vol. 14, No. 4. – pp. 139-148. – DOI 10.12737/2219-0767-2021-14-4-139-148. – EDN PPOUDI.

11. Poluektov A.V., Zarevich A. I., Makarenko F. V., Solodilov M. V. Investigation of the effectiveness of protection against gamma radiation using a multilayer hemispherical screen // Modeling of systems and processes. - 2025. – Vol. 18, No. 4. – pp. 71-83.

12. Analysis of the amount of SF₆ and cf₄ consumption for refueling high-voltage switching equipment / N. Y. Zalenskaya, F. V. Makarenko, A. I. Zarevich, A.V. Poluektov // Izvestiya vysshikh uchebnykh zavedeniy. Energy problems. – 2024. – Vol. 26, No. 4. – pp. 3-16. – DOI 10.30724/1998-9903-2024-26-4-3-16. – EDN HOOMCR.

КИБЕРБЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

М. Хуссейн¹, Е.А. Аникеев¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация. В статье рассматриваются ключевые аспекты обеспечения кибербезопасности в условиях цифровой трансформации экономики и социальной сферы. Проведён анализ современных киберугроз, включая практический случай атаки программой-вымогателем, описаны архитектурные и технологические подходы к защите информационных систем, а также рассмотрена роль нормативно-правовой базы и человеческого фактора в построении комплексной системы информационной безопасности организации.

Ключевые слова: кибербезопасность, цифровая трансформация, программы-вымогатели, архитектура нулевого доверия, защита данных, искусственный интеллект, информационная безопасность.

CYBERSECURITY IN THE AGE OF DIGITAL TRANSFORMATION

M. Hussain¹, E.A. Anikeev¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article examines the key aspects of ensuring cybersecurity in the context of the digital transformation of the economy and social sphere. An analysis of modern cyber threats is carried out, including a practical case of a ransomware attack, architectural and technological approaches to protecting information systems are described, and the role of the regulatory framework and the human factor in building a comprehensive information security system of an organization are considered.

Keywords: cybersecurity, digital transformation, ransomware, zero trust architecture, data protection, artificial intelligence, information security.

The transition to digital economy and smart government services where many processes are migrated to cloud computing and Internet of Things become prevalent have significantly altered the cybersecurity threat landscape. Previously, information

security was considered an issue of technologies that resided only in the IT department. Nowadays, cybersecurity has transformed into one of the crucial elements of running business, and the global cost of cybercrime is expected to reach more than \$9.5 trillion in 2024 according to Cybersecurity Ventures [1].

Thus, the digital transformation involves the reconsideration of business models, operations in supply chain management, and collaboration among humans and technologies. Every newly introduced technology, cloud-based application, or connected thing increases the risk of successful attack. Hence, there is a need to abandon purely perimeter-based solutions in favour of comprehensive cyber security strategies.

Cybersecurity has a history that is very similar to the history of digital technologies. The first computer viruses came out in the 1980s. In the 2000s, organized cybercriminal groups took their place. In the 2010s, state-sponsored advanced persistent threat (APT) actors joined them. There are a few main vectors that make up the threat landscape today.

Ransomware is now one of the most damaging types of attacks for businesses. The double-extortion model, which involves encrypting data and threatening to publish it at the same time, has given attackers a lot more power. The 2021 attack on the Colonial Pipeline, which stopped fuel supplies across the eastern United States, and the 2024 attack on the Change Healthcare payment processor, which stopped the processing of prescriptions at thousands of pharmacies, show that ransomware is now a systemic threat to critical infrastructure [2].

Ransomware attacks don't just happen to big companies and important infrastructure; they also work just as well on individual users. The author of this article wrote about the following case, which shows how a modern ransomware attack on a personal computer usually works and how it uses social engineering.

The attack started when someone downloaded a program from a third-party website that was not authorized. When the malicious program ran, it silently installed ransomware that changed all the files on the device, including documents, images, and other personal data, into shortcut files. The attacker had to use their decryption tool to get to these files. There was no warning during or right after the infection; the data just seemed to disappear and be replaced by shortcut icons that looked the same. After the encryption phase, the victim was told to pay 800 US dollars to get a proprietary recovery software that the attackers said would bring back all the affected files.

In this case, there is a known ransomware propagation technique that involves distributing malware-infected software using third-party websites for downloads. This particular ransomware attack demonstrates several features that are consistent with

what researchers have observed in previous studies on cybersecurity. For example, the use of shortcuts to hide files instead of deleting them is a planned social engineering strategy intended to induce confusion in the victim's mind and increase the chances of payment. Moreover, a ransom value of 800 USD falls into the category of ransomware attacks that target individual users or small enterprises. In other words, it is sufficiently large to generate a profit while remaining affordable for some individuals or small business owners. Finally, the claim that the “recovery software” will enable the user to recover their files appeals to the victim's instinct to restore their system, although ransomware distributors cannot be certain that decryption software will work.

This case highlights a significant and often undervalued risk factor: the utilization of software from unverified sources. Legitimate application distribution channels, such as official vendor websites, verified software repositories, and platform-managed stores, offer significant, albeit not infallible, protection against this attack vector. The incident further confirms that individual cybersecurity awareness is just as important as organizational and technical controls. This is because end-user behavior is still the most common way that ransomware gets into systems [3].

Even now, phishing and social engineering remain the most widespread methods to penetrate enterprise networks. The role of human element remains significant despite advancements in email scanning solutions and endpoint security tools. FBI statistics reveal that in 2023 BEC schemes cost more than \$2.9 billion in financial losses to the United States economy. BEC schemes exploit sophisticated spoofing techniques that result in leaking user passwords and unauthorized transfer of money. With the development of generative AI technologies, cybercriminals can generate fake yet convincing content even more easily [1, 3].

Supply chain attacks are particularly risky since they leverage the trust established between companies and software and hardware providers. A vivid example was provided by the Solar Winds incident back in 2020 when malicious code inserted into an official IT monitoring and management software package penetrated hundreds of organizations and even some US government agencies. Nowadays software supply chains grow increasingly complex due to reliance on open-source and third-party software packages. Thus, it is easier to deliver malware through them [4].

The fact that traditional perimeter-based security models don't work well with cloud computing, remote work, and mobile devices has sped up the move to Zero Trust Architecture (ZTA). The Zero Trust model, which is explained in NIST Special Publication 800-207, is based on the idea of “never trust, always verify”. This means that no

user, device, or network segment is automatically trusted, and every access request must be explicitly verified, authorized, and continuously validated [3].

There are a few important technologies and practices that make Zero Trust work in real life. Multi-factor authentication (MFA) greatly lowers the chance that someone will get access to your account by stealing your password. An attacker needs the extra factor to get in. Micro-segmentation breaks the network into small, separate areas, making it harder for an attacker who has already broken through the perimeter to move around. The principle of least privilege says that users and systems should only be given the permissions they need to do their jobs. This lowers the risk of damage from a hacked account.

Misconfigurations are among the leading causes of cloud data breaches, and CSPM tools provide an automatic scan and resolution of the problem, a significant advantage for companies working in the cloud environment. The 2024 IBM Cost of a Data Breach report estimates that the average cost of a breach due to cloud misconfiguration is \$4.14 million, highlighting the importance of configuration validation in multi-cloud environments. [5]

In contrast to the conventional security strategy, DevSecOps regards cybersecurity as an integral component of the software development process and not an add-on. Integrating security practices such as SAST, DAST, and SCA into CI/CD workflows enables the identification and resolution of security vulnerabilities at the earliest, most economical stage possible [2, 3].

In fact, AI is changing the face of cybersecurity not only for hackers but also for organizations. In terms of machine learning, cybersecurity solutions become capable of analyzing huge amounts of telemetry information and discovering any deviations that could be overlooked by basic security rules. AI-powered SIEM and XDR systems detect even the most complex and multi-staged cyber-attacks by connecting all the dots between endpoints, networks, and cloud services.

UEBA creates unique behavior patterns for every user or device and detects any deviations, such as atypical hours of logging into the system or unusual access to certain data resources. At the same time, natural language processing technologies allow cybersecurity experts to automatically analyze various threat intelligence feeds, vulnerability databases, and dark web resources to obtain valuable insights into the latest threats.

At the same time, enemies are using AI more and more to make their attacks bigger, faster, and more effective. Generative AI tools are used to make phishing emails

that are very specific to each person, find software flaws automatically, and make polymorphic malware that can't be found by signature-based detection. The arms race between AI-powered attacks and AI-powered defenses is one of the most important things about modern cybersecurity. Researchers at top Russian universities are also working on systems that use neural network models to find strange patterns in network traffic. These systems are being added to national cyber security platforms [6].

As the recognition of the relationship between cybersecurity and national security and economic stability increases, laws and regulations take an expansionist path across Russia and the globe. In Russia, Federal Law No. 187-FZ “On the Security of Critical Information Infrastructure” introduces mandatory requirements for protecting information systems in key industries, such as healthcare, financial institutions, transport systems, and the energy sector. The requirements include categorization of critical infrastructure according to its security level, protection methods, and notification of every cyber-attack to the National Coordination Center for Computer Incidents (NCCCI) referred to as (NKTsKI) [2].

The latest update of the NIST Cybersecurity Framework (CSF 2.0) introduced in 2024 continues to be the go-to solution to design cybersecurity efforts based on six fundamental pillars: govern, identify, protect, detect, respond, and recover. In Europe, the implementation of the NIS2 Directive became effective from January 2023, extending the scope of responsibilities to ensure cybersecurity to providers of essential services and digital service providers.

There have been numerous changes made in relation to cybersecurity governance within corporate organizations. CISOs have transitioned from taking care of technological tasks to playing a more strategic role, reporting directly to the board. Boards of directors are now expected to play an active role in managing cybersecurity risk for companies operating in diverse geographical locations. This shows that cybersecurity risk is basically a business risk which needs to be tackled by top management. [1, 3].

At a time of rapid digital transformation, modern cybersecurity requires a comprehensive, flexible approach based on state-of-the-art technology, effective governance, and continuous skill-building of people. The ransomware case highlighted in the current article proves that the scope of cybersecurity threats extends beyond single individuals to include important national infrastructure. It also proves that the number one entry point for a cyber-threat is a human being whose actions have caused a vulnerability. The involvement of non-sanctioned distribution channels of software, data concealment practices associated with social engineering tactics and, finally, a rational economics of ransom demand are all factors making human involvement crucial.

Transitioning to Zero Trust Architecture, using machine learning and artificial intelligence to detect and mitigate cyber threats, integrating security into software development, and engaging proactively with the changing regulatory landscape constitute some key aspects of achieving cyber resilience. Cybersecurity as a strategic priority for both individuals and organizations puts them in the best possible position in the context of reaping benefits and mitigating risks of digital transformation.

Список литературы

1. Хидаятуллах Д.Е.Р., Кунти Р., Харвахю Р. Проектирование и анализ управления рисками информационной безопасности на основе ISO 27005: пример внедрения в системе управления аудитом (AMS) отдела внутреннего аудита XYZ // Международный журнал электротехники, компьютерных и биомедицинских наук. – 2024. – № 3, том 2. – DOI: 10.62146/ijecbe.v2i3.81.
2. ФСТЭК России. Методические рекомендации по обеспечению информационной безопасности критической информационной инфраструктуры // ФСТЭК России. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2456> (дата обращения: 10.03.2025).
3. Сумин, В. И. Использование ситуационного моделирования в разработке систем принятия решений для сложных организационных систем / В. И. Сумин, А. С. Кравченко, А. В. Толкачев // Моделирование систем и процессов. — 2024. — Т. 17, № 3. — С. 71–79. — DOI 10.12737/2219-0767-2024-69-77. — EDN FBBHJO.
4. Тираканок С., Уэхара Т., Инохата А. Миграция к архитектуре нулевого доверия: обзоры и проблемы // Security and Communication Networks. – 2021. – № 1, том 2021. – С. 9947347. DOI: 10.1155/2021/9947347.
5. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. — М.: ДМК Пресс, 2021. — 592 с.
6. Хрящев В.В., Ненашев А.В. Эффективность внедрения одноранговой распределенной системы хранения и обработки защищаемой информации (TheOOL Project) // Моделирование систем и процессов. – 2021. – № 3, том 14. – С. 82–89. DOI: 10.12737/2219-0767-2021-14-3-82-89.

References

1. Hidayatullah D.E.R., Kunthi R., Harwahyu R. Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department // International Journal of Electrical, Computer, and Biomedical Engineering. – 2024. – No. 3, Vol. 2. – DOI: 10.62146/ijecbe.v2i3.81.
2. FSTEC of Russia. Methodological Recommendations for Ensuring Information Security of Critical Information Infrastructure // FSTEC of Russia. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2456> (date of reference: 10.03.2025).
3. Sumin V.I., Kravchenko A.S., Tolkachev A.V. The use of situational modeling in the development of decision-making systems for complex organizational systems. Modeling of systems and processes. 2024. Vol. 17, No. 3. pp. 71–79. DOI 10.12737/2219-0767-2024-69-77. EDN FBBHJO.
4. Teerakanok S., Uehara T., Inomata A. Migrating to Zero Trust Architecture: Reviews and Challenges // Security and Communication Networks. – 2021. – No. 1, Vol. 2021. – P. 9947347. DOI: 10.1155/2021/9947347.
5. Shangin V.F. Information protection in computer systems and networks. Moscow: DMK Press, 2021. 592 p.
6. Khryashchev V.V., Nenashev A.V. Efficiency of Implementing a Peer-to-Peer Distributed Storage and Processing System for Protected Information (TheOOL Project) // Modeling of Systems and Processes. – 2021. – No. 3, Vol. 14. – P. 82–89. DOI: 10.12737/2219-0767-2021-14-3-82-89.

СЕКЦИЯ 2

СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ

DOI: 10.58168/IntInfSys2026_51-58

УДК 004.85

КОНВЕЙЕР РАЗВЁРТЫВАНИЯ И МОНИТОРИНГА МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ С КОНТРОЛЕМ ДРЕЙФА ДАННЫХ

В.Э. Буздин¹, Е.А. Аникеев¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. Рассмотрен конвейер вывода моделей машинного обучения в эксплуатацию, объединяющий автоматическое развёртывание, мониторинг качества и контроль дрейфа входных данных. Предложена схема с обратной связью, в которой переобучение запускается по индексу дрейфа. На учебном примере показано, что контроль дрейфа сокращает время обнаружения деградации модели и простой на устаревшей версии без постоянного переобучения по расписанию.

Ключевые слова: машинное обучение, развёртывание моделей, дрейф данных, мониторинг качества, переобучение, конвейер, обработка информации, обратная связь, интеллектуальные системы.

A PIPELINE FOR DEPLOYING AND MONITORING MACHINE LEARNING MODELS WITH DATA DRIFT CONTROL

V.E. Buzdin¹, E.A. Anikeev¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. A pipeline for putting machine learning models into operation is considered, combining automatic deployment, quality monitoring, and control of input data drift. A feedback scheme is proposed in which retraining is triggered by a drift index. Using an educational example, it is shown that drift control reduces the time to detect model degradation and the downtime on an outdated version without constant scheduled retraining.

Keywords: machine learning, model deployment, data drift, quality monitoring, retraining, pipeline, information processing, feedback, intelligent systems.

Интеллектуальные информационные системы всё чаще включают модели машинного обучения: классификаторы, прогнозы спроса, обнаружение мошенничества, рекомендации. В отличие от обычного программного модуля, обученная модель имеет особенность – её качество со временем падает, даже если код не менялся. Причина в том, что меняются сами данные: пользователи ведут себя иначе, появляются новые категории, смещаются распределения признаков. Это явление называют дрейфом данных, и из-за него модель, точная на момент обучения, постепенно начинает ошибаться.

Поэтому вывод модели в эксплуатацию нельзя сводить к разовому развёртыванию. Нужен повторяемый процесс, который не только доставляет модель в работающую систему, но и следит за её качеством и за изменением входных данных, а при необходимости запускает переобучение. Такой процесс по аналогии с практиками автоматизации поставки программного обеспечения [1] выстраивают как конвейер с обратной связью.

На практике встречаются две крайности. В первой модель обучают один раз и забывают – тогда деградация обнаруживается поздно, по жалобам пользователей. Во второй модель переобучают по расписанию (например, еженедельно) независимо от того, изменились данные или нет, это расходует ресурсы и иногда даже вредит, если свежих размеченных данных мало. Разумная середина – переобучать тогда, когда это действительно нужно, то есть по факту дрейфа.

Цель работы – описать конвейер развёртывания и мониторинга модели машинного обучения, в котором переобучение запускается по измеримому признаку дрейфа входных данных, и оценить, что это даёт по сравнению с переобучением по расписанию и с отсутствием мониторинга.

Рассмотрим типовую задачу: модель-классификатор используется в информационной системе и обрабатывает поток заявок. У модели есть два рода показателей. Первый – качество предсказаний (например, доля верных решений или площадь под ROC-кривой, ROC-AUC); его можно посчитать только тогда, когда становится известен истинный ответ, а это бывает с задержкой. Второй – характеристики входных данных (распределения признаков); их видно сразу, ещё до того, как известен правильный ответ. Идея мониторинга дрейфа в том,

чтобы по второму, доступному немедленно, показателю заранее предупреждать о вероятном падении первого.

Контроль качества модели перед вводом в эксплуатацию и в ходе работы по смыслу близок к тестированию и контролю качества программного обеспечения [2]: прежде чем заменить рабочую версию, новая модель должна пройти проверку на отложенной выборке и не уступить текущей. Сам процесс удобно описывать как систему с обратной связью, где наблюдаемое состояние модели влияет на решение о её обновлении [3].

Предлагаемый конвейер показан на рисунке 1. Он состоит из пяти стадий: подготовка данных и признаков, обучение модели, валидация качества, развёртывание модели как сервиса (serving) и мониторинг качества и дрейфа. Принципиальным элементом является обратная связь: стадия мониторинга при обнаружении значимого дрейфа запускает переобучение, и цикл повторяется уже на свежих данных.

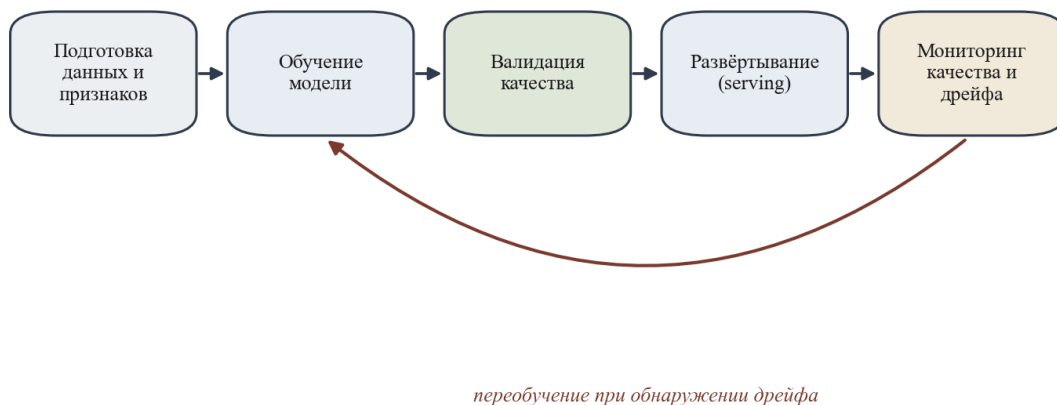


Рисунок 1 – Конвейер вывода модели в эксплуатацию с переобучением по обратной связи

Стадия валидации играет роль защитного барьера: новая модель выводится в эксплуатацию только если на отложенной выборке она не хуже текущей. Развёрнутая модель работает как сервис, к которому обращается остальная система; при росте потока запросов сервис масштабируется горизонтально, а распределение запросов между его экземплярами решается средствами балансировки нагрузки [4]. Стадия мониторинга собирает два потока сведений – отложенные

оценки качества и характеристики входных данных – и сравнивает их с эталонными значениями, полученными при обучении.

Такое построение делает поведение системы предсказуемым и объяснимым: каждое переобучение имеет причину (зафиксированный дрейф), а каждая замена модели проходит через валидацию. По духу это близко к интеллектуальным системам управления качеством, где решение принимается не вручную, а по измеренным показателям процесса [5].

Для числовой оценки дрейфа применялся индекс стабильности популяции (population stability index, PSI). Область значений каждого признака разбивается на интервалы; для эталонной (обучающей) выборки и для текущего потока считаются доли наблюдений, попавших в каждый интервал, после чего вычисляется суммарное расхождение этих долей:

$$PSI = \sum_i (q_i - p_i) \cdot \ln(q_i / p_i) \quad (1)$$

где p_i – доля наблюдений в i -м интервале для эталонной выборки;

q_i – доля для текущего потока.

Чем сильнее текущее распределение отличается от эталонного, тем больше значение по формуле (1). Приняты привычные границы интерпретации: PSI до 0,1 – дрейфа практически нет; от 0,1 до 0,2 – умеренный дрейф, требующий внимания; свыше 0,2 – значимый дрейф, при котором назначается переобучение. Индекс рассчитывается отдельно по каждому значимому признаку, а в качестве сигнала берётся наибольшее из значений.

Достоинство такого показателя в том, что он не требует знания истинных ответов и доступен сразу. Это и позволяет предупреждать деградацию заранее: рост PSI обычно опережает падение качества, давая время подготовить и проверить новую модель до того, как ошибки станут заметны пользователям.

Конвейер проверялся на учебной задаче классификации заявок с потоком данных за 24 недели. Эталонные распределения признаков и исходное качество модели зафиксированы на момент обучения (ROC-AUC около 0,92). Затем по неделям отслеживались качество модели и индекс дрейфа PSI. Результаты показаны на рисунке 2.

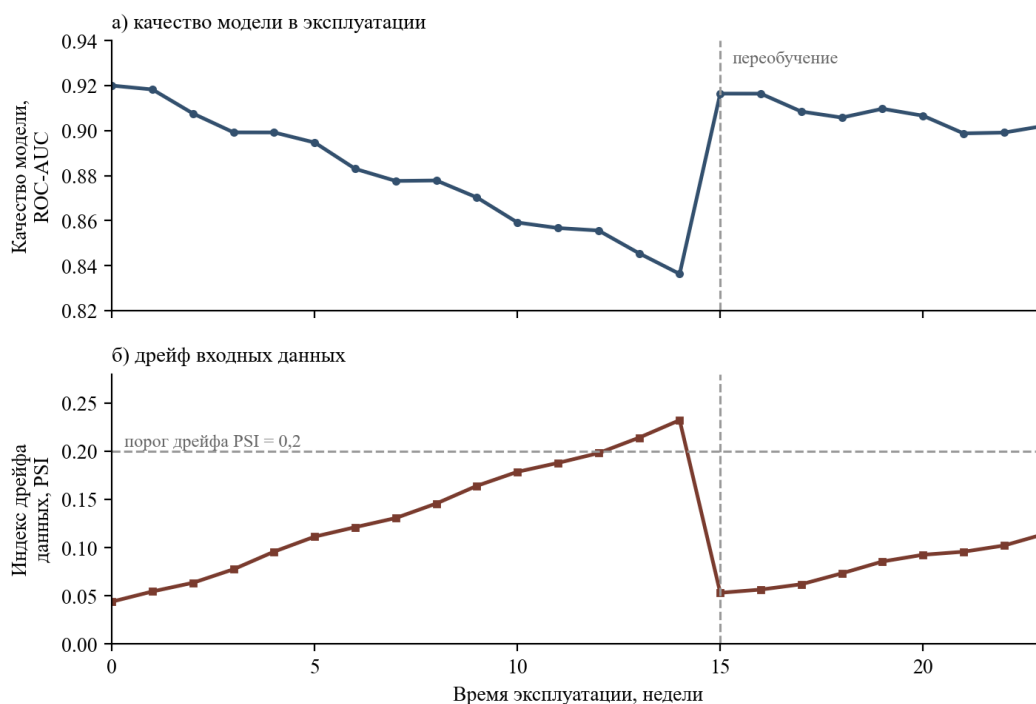


Рисунок 2 – Качество модели (а) и индекс дрейфа входных данных (б) в ходе эксплуатации

Видно, что по мере накопления изменений во входных данных индекс PSI рос и к 13–14-й неделе превысил порог 0,2, а качество модели к этому времени снизилось с 0,92 до примерно 0,84. Превышение порога запустило переобучение на свежих данных; после замены модели на 15-й неделе качество вернулось к уровню около 0,91, а индекс дрейфа сбросился, поскольку эталонные распределения были пересчитаны. Важно, что сигнал о дрейфе появился раньше, чем падение качества стало критичным, – это и есть практическая польза опережающего мониторинга.

Конвейер сопоставлялся с двумя базовыми стратегиями на том же потоке данных: без мониторинга (модель не обновляется) и с переобучением строго по расписанию (раз в 4 недели). Сравнение приведено в таблице 1.

Таблица 1 – Сравнение стратегий сопровождения модели

Стратегия	Мин. ROC-AUC	Переобучений	Простой на плохой модели, нед.
Без мониторинга	0,84	0	10
По расписанию (4 нед.)	0,88	6	3
По дрейфу (PSI)	0,89	2	1

Стратегия без мониторинга показала наибольшее и самое долгое падение качества. Переобучение по расписанию держало качество выше, но потребовало шести переобучений, часть из которых пришлась на периоды без заметного дрейфа и не дала выигрыша. Управление по дрейфу удержало качество на сопоставимом уровне всего двумя переобучениями и с наименьшим простоем на устаревшей модели – ресурсы тратились тогда, когда это было оправдано.

Перевод сопровождения модели в измеримые величины делает решения обоснованными: модель обновляется не «на всякий случай» и не по жалобам, а по зафиксированному признаку дрейфа. Такой подход согласуется с идеей информационно-интеллектуальной поддержки принятия решений, когда выбор момента действия опирается на наблюдаемые показатели, а не на интуицию. Дополнительное преимущество – прослеживаемость: для каждой версии модели известно, на каких данных она обучена и почему была заменена.

Ограничения подхода связаны с тем, что дрейф входных данных не всегда совпадает с падением качества. Возможен дрейф без потери качества (изменение, к которому модель устойчива) и, наоборот, падение качества без заметного дрейфа признаков – например, при изменении самой зависимости между признаками и ответом. Поэтому контроль дрейфа разумно дополнять отложенной оценкой качества, а пороги PSI подбирать под конкретную задачу. Тем не менее даже простой контроль дрейфа заметно улучшает сопровождение модели и не требует сложной инфраструктуры.

Описан конвейер развёртывания и мониторинга модели машинного обучения с обратной связью, в котором переобучение запускается по индексу дрейфа входных данных PSI. На учебном потоке данных за 24 недели показано, что рост дрейфа опережает падение качества и служит ранним сигналом для переобучения. По сравнению с отсутствием мониторинга и переобучением по расписанию управление по дрейфу удержало качество модели меньшим числом переобучений и с наименьшим простоем на устаревшей версии. Предложенный конвейер даёт практичный и объяснимый способ сопровождения моделей в интеллектуальных информационных системах.

Список литературы

1. Баланов, А. Н. DevOps: интеграция и автоматизация: учебное пособие для СПО / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 68 с. — ISBN 978-5-507-54085-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/505387> (дата обращения: 14.06.2026). — Режим доступа: для авториз. пользователей.

2. Турнецкая, Е. Л. Программная инженерия. Тестирование и контроль качества программного обеспечения: учебное пособие для вузов / Е. Л. Турнецкая, А. В. Аграновский. — Санкт-Петербург: Лань, 2025. — 172 с. — ISBN 978-5-507-51677-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/455672> (дата обращения: 14.06.2026). — Режим доступа: для авториз. пользователей.

3. Моделирование систем и процессов. Практический курс: учебник для вузов / под редакцией В. Н. Волковой. — Москва: Издательство Юрайт, 2025. — 295 с. — (Высшее образование). — ISBN 978-5-534-01442-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561270> (дата обращения: 14.06.2026).

4. Мочалов, В. П. Алгоритм динамического распределения и балансировки нагрузки в распределенных облачных вычислениях / В. П. Мочалов, Н. Ю. Братченко, Д. В. Гостева // Моделирование систем и процессов. — 2024. — Т. 17, № 1. — С. 92-102. — DOI 10.12737/2219-0767-2024-17-1-92-102. — EDN EWMPYM.

5. Бантюков, С. М. Создание интеллектуальной системы управления качеством предприятия «Эталон» в авиационной промышленности / С. М. Бантюков // Моделирование систем и процессов. — 2024. — Т. 17, № 2. — С. 15-23. — DOI 10.12737/2219-0767-2024-17-2-15-23. — EDN YHXUPY.

References

1. Balanov, A. N. DevOps: integration and automation: a textbook for vocational education / A. N. Balanov. — 2nd ed., ster. — Saint Petersburg: Lan, 2025. — 68 p. — ISBN 978-5-507-54085-3. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/505387> (date of access: 14.06.2026). — Access mode: for authorized users.

2. Turnetskaya, E. L. Software engineering. Software testing and quality control: a textbook for universities / E. L. Turnetskaya, A. V. Agranovsky. — Saint Petersburg:

Lan, 2025. — 172 p. — ISBN 978-5-507-51677-3. — Text: electronic // Lan: electronic library system. — URL: <https://e.lanbook.com/book/455672> (date of access: 14.06.2026). — Access mode: for authorized users.

3. Modeling of systems and processes. Practical course: a textbook for universities / edited by V. N. Volkova. — Moscow: Yurait Publishing House, 2025. — 295 p. — (Higher education). — ISBN 978-5-534-01442-6. — Text: electronic // Yurait educational platform [website]. — URL: <https://urait.ru/bcode/561270> (date of access: 14.06.2026).

4. Mochalov, V. P. An algorithm for dynamic distribution and load balancing in distributed cloud computing / V. P. Mochalov, N. Yu. Bratchenko, D. V. Gosteva // Modeling of systems and processes. — 2024. — Vol. 17, No. 1. — pp. 92-102. — DOI 10.12737/2219-0767-2024-17-1-92-102. — EDN EWMPYM.

5. Bantyukov, S. M. Creation of an intelligent quality management system of the Etalon enterprise in the aviation industry / S. M. Bantyukov // Modeling of systems and processes. — 2024. — Vol. 17, No. 2. — pp. 15-23. — DOI 10.12737/2219-0767-2024-17-2-15-23. — EDN YHXUPY.

АНАЛИЗ МЕТОДОВ АВТОМАТИЗАЦИИ МОНИТОРИНГА КОРМЛЕНИЯ НА ЖИВОТНОВОДЧЕСКИХ ПРЕДПРИЯТИЯХ

М.Е. Завьялова¹, С.Н. Волкова¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье проведён сравнительный анализ существующих методов и программных решений для автоматизации мониторинга кормления животных на животноводческих предприятиях. Рассмотрены традиционные подходы, SCADA-системы, зарубежные и отечественные ERP-платформы, а также специализированные IoT-решения. Выявлены ключевые недостатки существующих систем, построена радарная диаграмма сравнения и сформулированы требования к перспективной платформе для контроля кормления.

Ключевые слова: мониторинг кормления, IoT, животноводство, автоматизация, SCADA, ERP, платформа управления.

ANALYSIS OF METHODS FOR AUTOMATING FEEDING MONITOR-ING ON LIVESTOCK ENTERPRISES

M.E. Zavyalova¹, S.N. Volkova¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. The article provides a comparative analysis of existing methods and software solutions for automating feeding monitoring at livestock enterprises. Traditional approaches, SCADA systems, foreign and domestic ERP platforms, and specialized IoT solutions are considered. Key limitations of existing systems are identified, a radar comparison diagram is constructed, and requirements for a prospective feeding control platform are formulated.

Keywords: feeding monitoring, IoT, livestock, automation, SCADA, ERP, management platform.

Эффективное управление кормлением является одним из ключевых факторов продуктивности животноводческих предприятий. Развитие современного

животноводства опирается на цифровизацию и освоение систем автоматизации технологических процессов, среди которых доминируют технологии интернета вещей, робототехника и цифровые платформы [1]. При этом ручной контроль рационов и расписаний кормления остаётся широко распространённой практикой, особенно в малых и средних хозяйствах, что ведёт к систематическим ошибкам нормирования, перерасходу кормов и снижению продуктивности поголовья.

Цифровизация агропромышленного комплекса создаёт предпосылки для перехода к автоматизированному мониторингу кормления на основе технологий Интернета вещей (IoT), облачных вычислений и интеллектуальной аналитики. Однако существующие решения либо ориентированы на крупные агропромышленные комплексы с высоким бюджетом внедрения, либо предлагают ограниченный функционал без полноценной IoT-интеграции.

Цель настоящей работы – систематизировать и сравнить существующие методы автоматизации мониторинга кормления, выявить их ограничения и обосновать направления разработки специализированной платформы для контроля кормления.

Обзор существующих подходов

Традиционный подход (ручной учёт) предполагает ведение бумажных или электронных журналов кормления операторами. Оператор фиксирует время кормления, вид и количество корма, а зоотехник периодически проверяет соответствие фактических данных нормативам. Несмотря на низкую стоимость, данный метод характеризуется высоким уровнем ошибок – по различным оценкам, до 15–20% записей содержат неточности [2] – зависимостью от человеческого фактора и отсутствием оперативного контроля отклонений.

Системы диспетчерского управления и сбора данных (SCADA) широко применяются в промышленности, в том числе в крупных агрокомплексах. Они обеспечивают сбор данных с датчиков, визуализацию технологических процессов и формирование отчётности. Вместе с тем адаптация SCADA к задачам животноводства требует значительных затрат на кастомизацию, а сами системы ориентированы преимущественно на управление оборудованием, а не на биологические параметры животных [3].

Среди зарубежных корпоративных платформ наиболее распространены SAP S/4HANA Agri и Oracle Agri Business. Обе системы предоставляют широкие возможности планирования кормовых рационов, управления поголовьем и финансового учёта, а также поддерживают интеграцию с внешними системами че-

рез стандартизованные API. Однако IoT-интеграция реализуется преимущественно через сторонние middleware-решения, стоимость лицензирования является одной из наиболее высоких на рынке, а после 2022 года доступность этих платформ для российских предприятий существенно сократилась [4].

Среди отечественных корпоративных платформ для агропромышленного комплекса широко используется «1С:Агропромышленный комплекс». Система включает модули планирования кормления и управления поголовьем, обеспечивает интеграцию с бухгалтерским и складским учётом, соответствует требованиям российского законодательства. Вместе с тем возможности подключения IoT-устройств ограничены и требуют разработки дополнительных коннекторов. Высокая стоимость внедрения и длительные сроки настройки делают платформу труднодоступной для хозяйств среднего масштаба [5].

На рынке также представлены специализированные IoT-решения для мониторинга животных: SCR by Allflex (мониторинг здоровья и активности КРС), Nedap Livestock Management (управление кормлением и RFID-идентификация), Afimilk (молочное животноводство). Эти системы обеспечивают глубокую IoT-интеграцию, однако ориентированы на узкие ниши, слабо масштабируются между видами животных и требуют приобретения проприетарного оборудования производителя [6].

На основании проведённого обзора составлена сравнительная таблица существующих подходов и предлагаемой платформы по четырём ключевым критериям: наличие IoT-интеграции, аналитические возможности, масштабируемость и стоимость внедрения (таблица 1).

Для наглядной визуализации многокритериального сравнения построена радарная диаграмма (рисунок 1), в которой каждый критерий оценивается по пятибалльной шкале. Диаграмма показывает, что зарубежные ERP-решения превосходят остальных по аналитике, но уязвимы по доступности и IoT-интеграции; отечественные ERP сопоставимы по функциональности, однако разрыв с IoT-платформами по интеграции с датчиками остаётся значительным. Предлагаемая платформа для контроля кормления нацелена на устранение этого дисбаланса.

Таблица 1 – Сравнительный анализ методов автоматизации мониторинга кормления

Метод / Система	IoT-интеграция	Аналитика	Масштабируемость	Стоимость внедрения
Ручной учёт (журналы)	Нет	Минимальная	Низкая	Низкая
SCADA-системы	Частичная	Средняя	Средняя	Высокая
Зарубежные ERP (SAP, Oracle)	Ограниченная	Высокая	Высокая	Очень высокая
Отечественные ERP (1C Agro)	Ограниченная	Высокая	Высокая	Высокая
Специализир. IoT (SCR, Nedap)	Полная	Средняя	Средняя	Высокая
Платформа для контроля кормления	Полная	Высокая	Высокая	Средняя

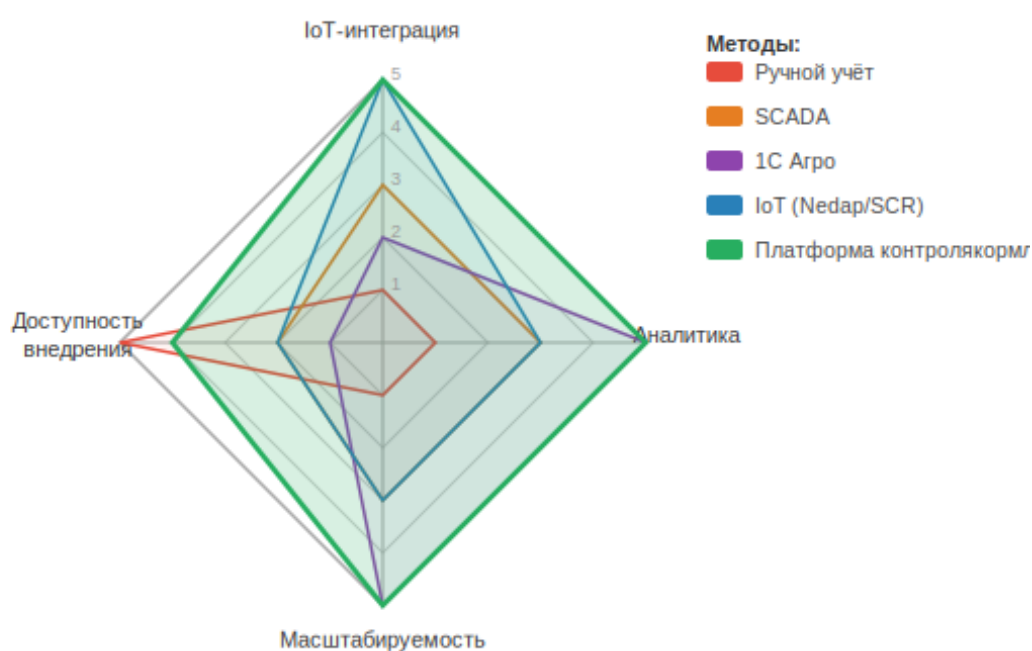


Рисунок 1 – Радарная диаграмма сравнения методов автоматизации мониторинга кормления (шкала 1–5)

На основе выявленных ограничений существующих решений сформулированы следующие ключевые требования к разрабатываемой платформе для контроля кормления:

- интеграция с гетерогенными IoT-устройствами (датчики веса, RFID-сканеры, датчики температуры и влажности) по открытым протоколам (MQTT, REST API);

- автоматическое формирование и корректировка расписаний кормления с учётом нормативов на голову и фактических показаний датчиков;
- обнаружение аномалий в режиме реального времени и генерация тревожных уведомлений операторам и зоотехникам;
- поддержка многоуровневой ролевой модели (оператор, зоотехник, администратор) с разграничением прав доступа;
- масштабируемая микросервисная архитектура, допускающая развёртывание как в облаке, так и на локальной инфраструктуре хозяйства.

Ключевым функциональным блоком платформы для контроля кормления является подсистема обработки информации, поступающей с IoT-датчиков в режиме реального времени. Поток данных от датчиков веса, RFID-сканеров и сенсоров микроклимата непрерывно сопоставляется с нормативными значениями, хранящимися в базе данных расписаний кормления. На рисунке 2 представлен обобщённый алгоритм обнаружения аномалий и выработки управляющих воздействий.

Алгоритм функционирует следующим образом. На первом этапе производится сбор показаний датчиков и их первичная фильтрация для устранения выбросов, вызванных помехами канала связи. На втором этапе фактические значения сравниваются с плановыми нормативами. При обнаружении отклонения, превышающего допустимый порог, система классифицирует аномалию по типу: недокорм, перекорм или пропуск кормления. На третьем этапе в зависимости от типа и критичности аномалии формируется управляющее воздействие: push-уведомление оператору, автоматическая корректировка расписания или эскалация тревоги зоотехнику. Все события фиксируются в журнале для последующего аналитического отчёта.

Подобный подход относится к классу систем управления на основе пороговых правил с обратной связью и соответствует принципам системного анализа технологических процессов. Применение многоуровневой классификации аномалий позволяет снизить количество ложных срабатываний и сосредоточить внимание персонала на действительно критичных отклонениях.

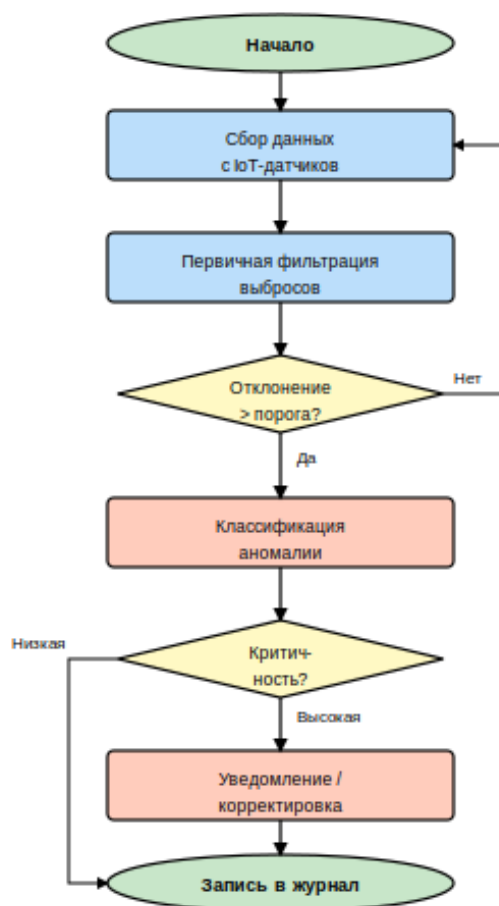


Рисунок 2 – Алгоритм обнаружения аномалий и принятия решений в платформе для контроля кормления

Проведённый анализ показал, что существующие методы автоматизации мониторинга кормления не в полной мере удовлетворяют современным требованиям. Традиционный учёт страдает от человеческого фактора; SCADA-системы не адаптированы к биологической специфике животноводства; зарубежные ERP-платформы обладают высокой функциональностью, но недоступны для большинства российских хозяйств по стоимости и геополитическим причинам; отечественные ERP ограничены по IoT-интеграции; специализированные IoT-решения привязаны к проприетарному оборудованию и узким нишам.

Построенная радарная диаграмма наглядно подтверждает отсутствие на рынке комплексного решения, одновременно обеспечивающего высокую IoT-интеграцию, развитую аналитику, масштабируемость и доступную стоимость. Совокупность выявленных ограничений обосновывает целесообразность разработки специализированной платформы для контроля кормления. Дальнейшие исследования направлены на проектирование архитектуры платформы, выбор технологического стека и реализацию прототипа.

Список литературы

1. Буклагин, Д. С. Цифровые технологии и системы управления в животноводстве / Д. С. Буклагин // Аграрная наука. – 2021. – № 3. – С. 45-49.
2. Кирсанов, В. В. Сравнительный анализ и подбор систем мониторинга здоровья КРС / В. В. Кирсанов, Ф. Е. Владимиров, Д. Ю. Павкин // Вестник высшей школы. – 2022. – № 5. – С. 78–85.
3. Валлоне, Л. Системы SCADA в сельском хозяйстве: современные приложения и перспективы на будущее / Л. Валлоне [и др.] // Computers and Electronics in Agriculture. – 2021. – Том 185. – С. 106–119.
4. Маргоева, М. В. Технологии искусственного интеллекта на молочных фермах / М. В. Маргоева, О. В. Чепуштанова // Молочное и мясное скотоводство. – 2022. – № 4. – С. 29–33.
5. Федоров, А. Д. О перспективах цифровизации животноводства / А. Д. Федоров, О. В. Кондратьева, О. В. Слинько // Вестник Всероссийского научно-исследовательского института механизации животноводства. – 2019. – № 1 (33). – С. 127–131.
6. Арапов, Д. В. Математическое обеспечение информационно-управляющей системы для хранения продукции с ограниченным сроком хранения / Д. В. Арапов, Н. Ю. Юдина, В. А. Курицын, Л. А. Коробова // Моделирование систем и процессов. – 2024. – Т. 17, № 1. – С. 7–18. – DOI 10.12737/2219-0767-2024-17-1-7-18.
7. Юрчишина, М. В. Алгоритмическая модель СППР «Оптимальный учебный план» / М. В. Юрчишина, К. И. Бушмелева // Моделирование систем и процессов. – 2024. – Т. 17, № 4. – С. 84–95. – DOI 10.12737/2219-0767-2024-17-4-84-95.
8. Сумин, В. И. Использование ситуационного моделирования в разработке систем принятия решений для сложных организационных систем / В. И. Сумин, А. С. Кравченко, А. В. Толкачев // Моделирование систем и процессов. – 2024. – Т. 17, № 3. – С. 71–79. – DOI 10.12737/2219-0767-2024-69-77.

References

1. Buklagin, D. S. Digital technologies and management systems in animal husbandry / D. S. Buklagin // *Agrarnaya nauka [Agricultural Science]*. 2021. No. 3. P. 45–49.
2. Kirsanov, V. V. Comparative analysis and selection of cattle health monitoring systems / V. V. Kirsanov, F. E. Vladimirov, D. Yu. Pavkin // *Vestnik vysshey shkoly [Bulletin of Higher School]*. 2022. No. 5. P. 78–85.
3. Vallone, L. SCADA Systems in Agriculture: Current Applications and Future Perspectives / L. Vallone [et al.] // *Computers and Electronics in Agriculture*. 2021. Vol. 185. P. 106–119.
4. Margoeva, M. V. Artificial intelligence technologies on dairy farms / M. V. Margoeva, O. V. Chepushtanova // *Molochnoe i myasnoe skotovodstvo [Dairy and Beef Cattle Breeding]*. 2022. No. 4. P. 29–33.
5. Fedorov, A. D. On the prospects of digitalization of animal husbandry / A. D. Fedorov, O. V. Kondratyeva, O. V. Slinko // *Vestnik Vserossiyskogo nauchno-issledovatel'skogo instituta mekhanizatsii zhivotnovodstva [Bulletin of VNIIMZH]*. 2019. No. 1 (33). P. 127–131.
6. Arapov, D. V. Mathematical support of an information and control system for storing products with a limited shelf life / D. V. Arapov, N. Yu. Yudina, V. A. Kuritsyn, L. A. Korobova // *Modelirovanie sistem i protsessov [Modeling of systems and processes]*. 2024. Vol. 17, no. 1. P. 7–18. DOI 10.12737/2219-0767-2024-17-1-7-18.
7. Yurchishina, M. V. Algorithmic model of the DSS 'Optimal curriculum' / M. V. Yurchishina, K. I. Bushmeleva // *Modelirovanie sistem i protsessov [Modeling of systems and processes]*. 2024. Vol. 17, no. 4. P. 84–95. DOI 10.12737/2219-0767-2024-17-4-84-95.
8. Sumin, V. I. Use of situational modeling in the development of decision-making systems for complex organizational systems / V. I. Sumin, A. S. Kravchenko, A. V. Tolkachev // *Modelirovanie sistem i protsessov [Modeling of systems and processes]*. 2024. Vol. 17, no. 3. P. 71–79. DOI 10.12737/2219-0767-2024-69-77.

ИНТЕГРАЦИЯ ГЕНЕРАТИВНОГО ДИЗАЙНА И ПАРАМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ В САПР ДЛЯ ОПТИМИЗАЦИИ КОНСТРУКЦИЙ АЭРОКОСМИЧЕСКИХ КОМПОНЕНТОВ

И.Н. Занин¹, Е.А. Аникеев¹, П.А. Мельникова¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье рассматриваются современные подходы к проектированию силовых конструкций аэрокосмической техники с использованием методов топологической оптимизации и генеративного дизайна. Обоснована необходимость интеграции параметрического моделирования для обеспечения технологичности сложных геометрических форм. Показано, что применение аддитивных технологий в сочетании с генеративным дизайном позволяет снизить массу компонентов на 40–50% при сохранении прочностных характеристик.

Ключевые слова: топологическая оптимизация, генеративный дизайн, аддитивные технологии, параметрическое моделирование, массовое совершенство, селективное лазерное сплавление, САПР.

INTEGRATION OF GENERATIVE DESIGN AND PARAMETRIC MODELING IN CAD FOR OPTIMIZATION OF AEROSPACE COMPONENT STRUCTURES

I.N. Zanin¹, E.A. Anikeev¹, P.A. Melnikova¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This paper discusses modern approaches to the design of load-bearing structures for aerospace equipment using topology optimization and generative design methods. The need to integrate parametric modeling to ensure the manufacturability of complex geometric shapes is substantiated. It is shown that the application of additive technologies in combination with generative design allows reducing the weight of components by 40–50% while maintaining their strength characteristics.

Keywords: topology optimization, generative design, additive technologies, parametric modeling, mass perfection, selective laser melting, CAD.

В современной аэрокосмической отрасли ключевым критерием эффективности летательных аппаратов является их массовое совершенство. Снижение массы силовых конструкций при сохранении или повышении их прочности и жесткости позволяет значительно увеличить массу полезной нагрузки или запас топлива, что напрямую влияет на экономическую эффективность миссий. Традиционные методы проектирования уже давно исчерпали свой потенциал, им на смену приходят новые методы вычислительного проектирования, такие как топологическая оптимизация и генеративный дизайн [1].

Актуальность данной работы заключается в важности систематизации подходов к интеграции генеративного дизайна в реальное производство. Важнейшим аспектом является выбор технологии изготовления на ранних этапах проектирования, так как она диктует набор технологических ограничений, которые должны быть учтены в математической модели оптимизации. В статье проводится сравнительный анализ двух стратегий: использования аддитивных технологий, снимающих большинство геометрических ограничений, и применения традиционных методов с наложением строгих технологических ограничений на процесс оптимизации.

Топологическая оптимизация (ТО) является численным методом распределения материала в заданной проектной области таким образом, чтобы минимизировать целевую функцию при соблюдении системы ограничений. Наиболее распространенным методом ТО является метод пенализации для твердого изотропного тела.

Математически задача формулируется следующим образом: найти вектор проектных переменных $\mathbf{x}$ (относительная плотность конечных элементов), который минимизирует целевую функцию $f(\mathbf{x})$, например, податливость конструкции:

$$\min_{\mathbf{x}} f(\mathbf{x}) = \mathbf{U}^T \mathbf{K}(\mathbf{x}) \mathbf{U}$$

при ограничениях:

$$V(\mathbf{x}) \leq V_0, 0 < x_{\min} \leq x_i \leq 1, i=1, \dots, N$$

где: $\mathbf{U}$ – вектор перемещений;

$\mathbf{K}$ – глобальная матрица жесткости;

$V(\mathbf{x})$ – текущий объем материала;

V_0 – начальный объем;

f_v – заданная доля объема;

N – количество конечных элементов [2].

Для связи модуля упругости E_i i -го элемента с его относительной плотностью x_i используется степенной закон с параметром штрафа p :

$$E_i(x_i) = E_0 \cdot x_i^p$$

где E_0 – модуль упругости исходного материала.

При этом важно понимать, что исключительно математическая оптимизация без учета производственных ограничений часто приводит к появлению структур дефектами, что в свою очередь мешает переводить результаты в CAD-модели, используемые на производстве.

Было установлено, что при проектировании переходного отсека космического аппарата (ПО КА) для изготовления традиционными методами использование ограничений типа EХТ – экструзия, позволяет получить предсказуемую геометрию, состоящую из набора ребер и оболочек. Однако такая конструкция оказывается значительно тяжелее аналога, полученного без ограничений. В приведенном примере масса ПО КА, изготовленного традиционным методом, составила 16 кг, тогда как допустимое напряжение и запасы устойчивости были обеспечены с большим избытком, что свидетельствует о недоиспользовании материала [3].

Аддитивные технологии позволяют изготавливать детали практически любой геометрической сложности методом послойного синтеза из металлического порошка.

Генеративный дизайн даёт нам свободу геометрии, минимизирует количество отходов, также мы получаем возможность объединения нескольких деталей в одну монолитную и как следствие более прочную конструкцию.

При этом несмотря на все преимущества алгоритмов генеративного дизайна, их прямой вывод в производство часто невозможен без этапа параметризации и доработки, так как результаты ТО обычно представлены в виде полигональной сетки, что делает их непригодными для инженерных расчетов и использовании в управляющих программ для ЧПУ.

Поэтому процесс интеграции должен состоять из интерпретации топологии, с дальнейшим параметрическим реконструированием и итоговой оптимизацией формы и размеров [3].

Таким образом мы можем сформулировать следующие рекомендации для инженеров-конструкторов:

1. На ранних этапах проектирования целесообразно проводить топологическую оптимизацию без технологических ограничений.
2. При выборе технологии изготовления необходимо проводить технико-экономическое обоснование.
3. Для серийного производства необходимо использовать ТО с наложением строгих технологических ограничений, это позволит получить конструкцию близкую к оптимальной [4].
4. Интеграция генеративного дизайна в САПР должна сопровождаться развитием навыков параметрического моделирования у конструкторов, так как автоматическая конвертация результатов ТО в твердотельные модели все еще требует ручного вмешательства и инженерной экспертизы.

Интеграция генеративного дизайна и параметрического моделирования открывает новые горизонты в проектировании аэрокосмических компонентов. Переход от интуитивного конструирования к алгоритмическому синтезу форм позволяет существенно улучшить массовое совершенство изделий. Однако успех внедрения этих технологий критически зависит от правильного выбора производственного базиса.

Аддитивные технологии являются естественным продолжением генеративного дизайна, позволяя реализовывать сложные бионические структуры, недоступные для традиционных методов. В то же время, для широкого промышленного применения необходимо развитие гибридных подходов, сочетающих свободу топологической оптимизации с жесткими требованиями технологичности традиционных процессов. Дальнейшие исследования должны быть направлены на автоматизацию процесса реконструкции параметрических моделей по результатам ТО и учет физики аддитивных процессов непосредственно в цикле генеративного проектирования.[5]

Список литературы

1. Roper S.W.K., Lee H., Huh M., Kim Il.Y. Simultaneous isotropic and anisotropic multi-material topology optimization for conceptual-level design of aerospace components // Structural and multidisciplinary optimization. - 2021. - №1, том 64. - С. 441-456, DOI: 10.1007/s00158-021-02893-4.
2. Зольников К.В., Ачкасов Д.А. Моделирование и оптимизация конструкции полосового фильтра на основе коаксиального резонатора // Моделирование систем и процессов. - 2024. - №2, том 17. - С. 43-50, DOI: 10.12737/2219-0767-2024-17-2-43-50.
3. Полуэктов А.В., Зольников К.В., Ачкасов А.В., Чевычелов Ю.А. Повышение формализации задач верификации топологии и электрической схемы для систем автоматизированного проектирования // Моделирование систем и процессов. - 2024. - №1, том 17. - С. 102-111, DOI: 10.12737/2219-0767-2024-17-1-102-111.
4. Скворцова Т.В., Зольников К.В., Плотников А.М., Скоркин И.В. Формализация верификации топологии и электрической схемы для систем автоматизированного проектирования // Моделирование систем и процессов. - 2024. - №3, том 17. - С. 61-70, DOI: 10.12737/2219-0767-2024-59-68.
5. Юров А.Н., Анциферова В.И., Пачевский Д.Е. Визуализация процессов металлообработки в разработке имитационных программ для оборудования с ЧПУ // Моделирование систем и процессов. – 2021. №1, том 14. – с. 85-92, DOI: 10.12737/2219-0767-2021-14-1-85-92

References

1. Roper S.W.K., Lee H., Huh M., Kim Il.Y. Simultaneous isotropic and anisotropic multi-material topology optimization for conceptual-level design of aerospace components // Structural and Multidisciplinary Optimization. – 2021. – No. 1, Vol. 64. – P. 441–456, DOI: 10.1007/s00158-021-02893-4.
2. Zolnikov K.V., Achkasov D.A. Modeling and optimization of the design of a bandpass filter based on a coaxial resonator // Modeling of Systems and Processes. – 2024. – No. 2, Vol. 17. – P. 43–50, DOI: 10.12737/2219-0767-2024-17-2-43-50.
3. Poluektov A.V., Zolnikov K.V., Achkasov A.V., Chevychelov Yu.A. Enhancing the formalization of topology and electrical circuit verification tasks for computer-aided design systems // Modeling of Systems and Processes. – 2024. – No. 1, Vol. 17. – P. 102–111, DOI: 10.12737/2219-0767-2024-17-1-102-111.

4. Skvortsova T.V., Zolnikov K.V., Plotnikov A.M., Skorkin I.V. Formalization of topology and electrical circuit verification for computer-aided design systems // Modeling of Systems and Processes. – 2024. – No. 3, Vol. 17. – P. 61–70, DOI: 10.12737/2219-0767-2024-59-68.

5. Yurov A.N., Antsiferova V.I., Pachevsky D.E. Visualization of metal-working processes in the development of simulation programs for CNC equipment // Modeling of Systems and Processes. – 2021. – No. 1, Vol. 14. – P. 85–92, DOI: 10.12737/2219-0767-2021-14-1-85-92.

СЕКЦИЯ 3
СОВРЕМЕННАЯ ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА

DOI: 10.58168/IntInfSys2026_73-79

УДК 681.5:004.85

**ПРИМЕНЕНИЕ ГЛУБОКОГО ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ
ДЛЯ УПРАВЛЕНИЯ МАНИПУЛЯТОРАМИ СЕРВИСНЫХ РОБОТОВ
В НЕСТРУКТУРИРОВАННЫХ СРЕДАХ**

И.Н. Занин¹, Е.А. Аникеев¹, Ю.О. Авилов¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье рассмотрено управление манипуляторами в неструктурированных средах методами глубокого обучения с подкреплением. Обоснованы ограничения классических подходов и предложена гибридная архитектура, сочетающая DRL и импедансное управление для безопасного контакта. Проанализированы проблемы переноса политик из симуляции в реальный мир и даны рекомендации по выбору алгоритмов с учетом вычислительных ресурсов бортовых систем.

Ключевые слова: глубокое обучение с подкреплением, роботизированный манипулятор, неструктурированная среда, импедансное управление, функция вознаграждения, сервисная робототехника.

**APPLICATION OF DEEP REINFORCEMENT LEARNING FOR CONTROL
OF SERVICE ROBOT MANIPULATORS IN UNSTRUCTURED
ENVIRONMENTS**

I.N. Zanin¹, E.A. Anikeev¹, Yu.O. Avilov¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This paper examines the control of robotic manipulators in unstructured environments using deep reinforcement learning. The limitations of classical approaches are substantiated, and a hybrid architecture combining DRL and impedance control for safe contact is proposed. The

challenges of sim-to-real policy transfer are analyzed, and recommendations for algorithm selection are provided, taking into account the computational resources of onboard systems.

Keywords: deep reinforcement learning, robotic manipulator, unstructured environment, impedance control, reward function, service robotics.

Быстрое развитие сервисной робототехники привело к тому, что роботы-манипуляторы все чаще покидают ограничения структурированных промышленных цехов и выходят в офисы, больницы, склады и домашние хозяйства. В отличие от заводских линий, где положение объектов строго фиксировано, а окружающая среда предсказуема, сервисные роботы сталкиваются с неструктурированными средами. Здесь объекты могут иметь произвольную форму, массу и коэффициент трения, а их расположение меняется случайным образом. Кроме того, часто требуется физическое взаимодействие с людьми или хрупкими предметами, что накладывает жесткие ограничения на силы и моменты, возникающие в контакте [1].

Традиционные методы управления, такие как ПИД-регуляторы или алгоритмы планирования траекторий, требуют наличия точной кинематической и динамической модели робота и среды.

В этом контексте глубокое обучение позволяет агенту самостоятельно обучаться оптимальной стратегии поведения через взаимодействие со средой, такой подход не требует программирования каждого движения, однако применение DRL в реальной робототехнике сопряжено с рядом трудностей.

Целью данной работы является обзор существующих методов применения DRL для управления манипуляторами, анализ ключевых алгоритмов и архитектур, а также рассмотрение путей преодоления барьера между симуляцией и реальностью.

Задача управления манипулятором в рамках DRL формализуется как процесс принятия решений Маркова, описываемый кортежем (S, A, P, R, γ) , где S – пространство состояний, A – пространство действий, P – функция перехода вероятностей, R – функция вознаграждения, γ – коэффициент дисконтирования будущих наград [2].

Для манипулятора состояние $s_t \in S$ обычно включает углы в суставах, угловые скорости, данные с датчиков усилия/момента и визуальную информацию. Действие $a_t \in A$ представляет собой приращения углов или целевые положения

суставов. Функция вознаграждения $R(s_t, a_t)$ конструируется инженером таким образом, чтобы поощрять успешное выполнение задачи и штрафовать за нежелательные события.

Одной из главных сложностей является проектирование функции вознаграждения. Слишком простые функции приводят к тому, что робот находит «лазейки» в правилах, выполняя задачу некорректным способом. Слишком сложные функции трудно настраивать, и они могут приводить к нестабильности обучения. [3]

Обучение непосредственно на физическом роботе занимает недели или месяцы и несет риск поломки дорогостоящего оборудования. Поэтому большинство современных подходов предполагают предварительное обучение в симуляторе. Однако перенос политики, обученной в идеализированной симуляции, в реальный мир часто терпит неудачу из-за «разрыва реальности». Различия в трении, массе звеньев, люфтах редукторов и задержках сенсоров приводят к тому, что действия, оптимальные в симуляции, становятся неэффективными или опасными в реальности [4].

Для преодоления этой проблемы применяются методы доменной рандомизации. Во время обучения в симуляции параметры среды случайным образом изменяются в широких пределах. Это заставляет агента учиться инвариантным признакам и стратегиям, которые работают в широком спектре условий, повышая его робастность при переносе на реального робота.

В неструктурированной среде робот должен исследовать новые действия, чтобы найти оптимальную стратегию. Однако случайные движения манипулятора могут привести к столкновению с человеком или повреждению объекта. Для обеспечения безопасности используются методы ограниченного исследования, такие как добавление штрафных вознаграждений за близость к препятствиям или использование барьерных сертификатов, которые математически гарантируют, что система не войдет в небезопасное состояние [5].

Также перспективным направлением является использование экспертных демонстраций. Предварительное обучение сети на наборе данных, собранных оператором-человеком, позволяет задать начальную точку для политики DRL, сокращая время обучения и снижая количество опасных действий на ранних этапах [6].

Чистое позиционное управление, часто выдаваемое политиками DRL, плохо подходит для задач, требующих силового взаимодействия. В таких случаях целесообразно использовать гибридные архитектуры.

Объединяя DRL с интеллектуальным импедансным управлением. В этой схеме нейросеть не выдает напрямую положения суставов, а адаптирует параметры импеданса в реальном времени в зависимости от состояния среды. Это позволяет роботу быть «мягким» при контакте с непредвиденными препятствиями и «жестким» при выполнении точных движений. Такой подход значительно повышает безопасность и естественность поведения сервиса робота при взаимодействии с людьми. [7]

Аналогичным образом, агент DRL учится сначала менять конфигурацию объектов в куче путем толкания, чтобы сделать их доступными для захвата. Это демонстрирует способность DRL решать многоэтапные задачи манипуляции, которые трудно запрограммировать вручную. [8]

В таблице 1 приведено сравнение различных стратегий управления манипуляторами в неструктурированных средах.

Таблица 1 – Сравнительная характеристика методов управления

Метод	Требование к модели среды	Адаптивность к изменениям	Безопасность контакта	Сложность настройки
Классическое позиционное (PID)	Высокая	Низкая	Низкая	Средняя
Планирование траекторий (RRT*)	Высокая	Средняя	Средняя	Высокая
Чистое DRL (End-to-End)	Низкая	Высокая	Низкая (требует штрафов)	Очень высокая
Гибридное (DRL + Impedance)	Низкая	Высокая	Высокая	Высокая
Обучение с демонстрациями (LfD)	Низкая	Средняя	Средняя	Средняя

Как видно из таблицы, гибридные подходы предлагают наилучший баланс между адаптивностью и безопасностью.

Применение глубокого обучения с подкреплением открывает новые возможности для создания автономных сервисных роботов, способных действовать в сложных, неструктурированных средах. Отказ от жестких математических моделей в пользу самообучающихся политик позволяет роботам адаптироваться к разнообразию объектов и условий, с которыми они сталкиваются в реальной жизни.

Ключевыми направлениями дальнейших исследований являются:

1. Повышение эффективности переноса навыков из симуляции в реальность через улучшение методов доменной рандомизации и мета-обучения.
2. Разработка безопасных алгоритмов исследования, гарантирующих отсутствие повреждений при обучении на физических системах.
3. Создание стандартизированных бенчмарков и сред для оценки прогресса в области манипуляции, что ускорит обмен знаниями между исследовательскими группами.
4. Интеграция больших языковых моделей (LLM) с DRL для высокоуровневого планирования задач, где LLM разбивает абстрактную команду на последовательность примитивов, выполняемых политикой DRL.

Гибридные архитектуры, сочетающие гибкость нейросетей с надежностью классических методов контроля, представляют собой наиболее перспективный путь к созданию роботов, способных безопасно и эффективно помогать человеку в повседневной жизни.

Список литературы

1. Хан Д., Муляна Б., Станкович В., Ченг С. Обзор алгоритмов глубокого обучения с подкреплением для роботизированных манипуляций // СЕНСОРЫ. – 2023. – № 7, Том 23. – С. 3762. – DOI: 10.3390/s23073762.
2. Высоцкая, И. А. Обоснование информационно-интеллектуальной поддержки принципов действия технических систем / И. А. Высоцкая // Моделирование систем и процессов. – 2024 – Т. 17, № 1. – С. 19-26. – DOI 10.12737/2219-0767-2024-17-1-19-26. – EDN DCEATL.
3. Высоцкая, И. А. Обоснование методов поиска принципов действия сложных технических систем и объектов / И. А. Высоцкая // Моделирование систем и процессов. – 2024 – Т. 17, № 1. – С. 27-34. – DOI 10.12737/2219-0767-2024-17-1-27-34. – EDN GASZOW.
4. Чен У., Вонг К.К.Л., Лонг С., Сун Чжоу. Относительная энтропия корректных алгоритмов оптимизации проксимальной политики с модифицированным штрафным коэффициентом в сложной среде // Entropy. – 2022. – № 4, Том 24. – С. 440. – DOI: 10.3390/e24040440.
5. Феррейра Х.С., Барбоза Р. Глубокое обучение с подкреплением для адаптивного роботизированного захвата и манипулирования после захвата в моделируемых динамических средах // Интернет будущего. – 2025. – № 10, том 17. – С. 437. – DOI: 10.3390/fi17100437.

6. Лю Дж., Яп Х. Дж., Хайруддин А.С. Планирование траектории движения робота-манипулятора в динамических средах на основе метода глубокого обучения с подкреплением // Журнал интеллектуальных и робототехнических систем. – 2024. – № 1, Том 111. – С. 3. – DOI: 10.1007/s10846-024-02205-0.

7. Шао Х., Ху У., Ян Ли., Ван У., Сузуки С., Гао Ж. Интеллектуальная импедансная стратегия для силового управления роботизированными манипуляторами в неизвестных условиях с помощью глубокого обучения с подкреплением под руководством эксперта // Процессы. – 2025. – № 8, Том 13. – С. 2526. – DOI: 10.3390/pr13082526.

8. Шиферау Б.А., Агидью Т.Ф., Альзахрани А.С., Шринивасаган Р. Синергетическое подталкивание и хватание для улучшения манипуляций роботами с использованием глубокого обучения с подкреплением // Приводы. – 2024. – № 8, Том 13. – С. 316. – DOI: 10.3390/act13080316.

References

1. Han D., Mulyana B., Stankovic V., Cheng S. A Survey on deep reinforcement learning algorithms for robotic manipulation // SENSORS. - 2023. - № 7, Vol. 23. - P. 3762. – DOI: 10.3390/s23073762.

2. Vysotskaya, I. A. Justification of Information and Intellectual Support for the Principles of Technical Systems Operation / I. A. Vysotskaya // Modeling of Systems and Processes. – 2024. – Vol. 17, No. 1. – Pp. 19-26. – DOI 10.12737/2219-0767-2024-17-1-19-26. – EDN DCEATL.

3. Vysotskaya, I. A. Justification of Methods for Finding the Principles of Operation of Complex Technical Systems and Objects / I. A. Vysotskaya // Modeling of Systems and Processes. – 2024. – Vol. 17, No. 1. – Pp. 27-34. – DOI 10.12737/2219-0767-2024-17-1-27-34. – EDN GASZOW.

4. Chen W., Wong K.K.L., Long S., Sun Zh. Relative entropy of correct proximal policy optimization algorithms with modified penalty factor in complex environment // Entropy. - 2022. - № 4, Vol. 24. - P. 440. – DOI: 10.3390/e24040440.

5. Ferreira H.C., Barbosa R.S Deep reinforcement learning for adaptive robotic grasping and post-grasp manipulation in simulated dynamic environments // Future internet. - 2025. - №10, Vol. 17. - P. 437. – DOI: 10.3390/fi17100437.

6. Liu J., Yap H.J., Khairuddin A.S.M. Path planning for the robotic manipulator in dynamic environments based on a deep reinforcement learning method // Journal of intelligent and robotic systems. - 2024. - №1, Vol. 111. - P. 3. – DOI: 10.1007/s10846-024-02205-0.

7. Shao H., Hu W., Yang Li., Wang W., Suzuki S., Gao Zh. Intelligent impedance strategy for force–motion control of robotic manipulators in unknown environments via expert-guided deep reinforcement learning // Processes. - 2025. - № 8, Vol. 13. - P. 2526. – DOI: 10.3390/pr13082526.

8. Shiferaw B.A., Agidew T.F., Alzahrani A.S., Srinivasagan R. Synergistic pushing and grasping for enhanced robotic manipulation using deep reinforcement learning // Actuators. - 2024. - № 8, Vol. 13. - P. 316. – DOI: 10.3390/act13080316.

ИСКУССТВЕННЫЕ РАЗУМЫ В ЧЕЛОВЕЧЕСКОМ ОБЛИКЕ: ЭВОЛЮЦИЯ ГУМАНОИДНЫХ РОБОТОВ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

М. Хуссейн¹, А.В. Акименко¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В этой статье прослеживается развитие человекоподобных роботов с системами искусственного интеллекта, способных взаимодействовать с людьми в реальном мире. Анализируются технологические компоненты. Особое внимание уделяется таким современным платформам, как Tesla Optimus, Figure 01, Unitree H1 и Boston Dynamics Atlas. В статье исследуются потенциальные области применения человекоподобных, а также этические и социальные проблемы, возникающие при использовании таких систем.

Ключевые слова: гуманоидные роботы, искусственный интеллект, машинное обучение, нейронные сети, робототехника, цифровизация, автономные системы, взаимодействие человека и машины.

ARTIFICIAL MINDS IN HUMAN FORMS: THE EVOLUTION OF AI-POWERED HUMANOID ROBOTS

M. Hussain¹, A.V. Akimenko¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This article traces the development of humanoid robots with artificial intelligence systems capable of interacting with humans in the real world. The technological components are analyzed. Special attention is paid to such modern platforms as Tesla Optimus, Figure 01, Unitree H1 and Boston Dynamics Atlas. The article explores potential applications of humanoid robots, as well as the ethical and social issues arising from the use of such systems.

Keywords: humanoid robots, artificial intelligence, machine learning, neural networks, robotics, digitalization, autonomous systems, human-machine interaction.

There's something very human about the desire to make a machine that looks like us, moves like us. Before the first transistor was ever soldered onto a circuit board

people were drawing mechanical men in notebooks and making clockwork figures to perform in royal courts. But today, what used to be the province of imagination is in engineering labs, on factory floors and in hospital corridors. The humanoid robot a two-legged walking machine with articulated arms, cameras and sensors to perceive its surroundings and ever more natural language conversation is no longer science fiction. This is an engineering problem that is being solved in real time and AI is the engine that is driving that progress.

The combination of deep learning, large language models, advanced materials, and high-torque actuators has created a moment unlike any previous era in robotics. Systems that once needed painstaking hand-coding of every movement can now learn to walk by falling down thousands of times in simulation, and then transfer that learned skill to physical hardware within hours. In the past five years, the difference between a robot's potential in a laboratory and its potential in an unstructured kitchen or hospital ward has narrowed faster than it did in the previous three decades [1].

This acceleration raises questions that go far beyond engineering. What is the impact on the organization of economies when a machine can perform physical and cognitive labor of a human worker? Where does the line between tool and companion fall, if it can talk, sense emotions and react with apparent empathy? The paper traces the evolution of technology from early automata to today's platforms, analyzes the AI architectures that enable today's humanoid robots, surveys the most important current systems, and takes a candid look at both the opportunities and the challenges.

Humanoid robotics has been an academic field for several decades, but its nature has changed dramatically with the advent of machine learning. Early efforts, such as Honda's P-series and Sony's QRIO project, focused on mastering bipedal locomotion through carefully engineered control systems. These robots were great displays of mechanical engineering but their behavior was essentially scripted, each movement pre-planned and any deviation from the expected environment could lead to failure [1].

The addition of reinforcement learning to locomotion research was a real game-changer. Schulman et al. showed that control policies can be trained directly from high-dimensional sensory inputs using policy gradient methods, without the need for hand-crafted dynamics models [2]. This approach was improved upon with the development of proximal policy optimization and later a combination of model-free and model-based methods that allowed policies trained in simulation to transfer to real hardware with a tolerable degradation of performance.

In parallel, advances in computer vision, driven by the introduction of convolutional neural networks and, later, vision transformers, allowed robots to interpret camera feeds with a reliability that previous systems could not provide [2]. Object detection, depth estimation, and semantic segmentation tasks that used to require dedicated hardware and carefully controlled lighting became tractable on mobile computer platforms. It allowed a robot that wandered around a room to interpret its visual input and plan its actions accordingly.

The advent of large language models added yet another layer of capability. SayCan, a work done by Ahn et al. showed that language models can be applied to decompose high-level natural language instructions into a sequence of low-level robot actions, thus endowing a physical robot with the ability to reason about tasks in human terms [2]. More recent architectures have combined vision, language and action in unified multimodal frameworks, allowing robots to perceive their environment, understand instructions given in everyday language and produce suitable physical responses, all within a single learned model [3].

Recent reviews of the field have pointed to three broad challenges that remain only partially solved: generalization across novel environments, safe and predictable behavior under distribution shift, and energy efficiency for untethered operation over meaningful time horizons [3]. Each of these is making rapid progress, but none are yet fully resolved, and all three have implications for real world deployment

The present work is a systematic review and comparative evaluation of published research, technical documentation, and publicly available performance data of AI-powered humanoid robot systems released or significantly updated between 2019 and 2025. Sources were obtained through a search of IEEE Xplore, ACM Digital Library, arXiv and the proceedings of the major robotics conferences (ICRA, IROS, CoRL). Furthermore, the official technical reports were reviewed and the demonstration material of the main robotics developers was looked at.

An Analytical Framework. We compared each platform across five axes: 1) mechanical architecture (degrees of freedom, actuator type, payload capacity and energy autonomy), 2) perception stack (sensor modalities, processing hardware and sensing range), 3) AI and control architecture (learning algorithms, training methodology and inference approach), 4) task capability (demonstrated behaviors and breadth of environments in which they have been validated), 5) deployment context (industrial, healthcare, domestic or research).

Where quantitative performance data were available from peer-reviewed sources or documented manufacturer testing, these are reported directly. For the dimensions

for which only qualitative descriptions exist, the analysis is based on a structured comparison across the stated dimensions. The review does not seek to arbitrate between competing performances claims by manufacturers without independent verification.

The analysis identified a clear stratification among existing humanoid platforms in terms of both technical maturity and the AI architectures that underpin their capabilities. Four systems Boston Dynamics Atlas (Generation 2), Tesla Optimus Gen 2, Figure 01 and Unitree H1 were identified to meet all the three selection criteria and are discussed in detail below.

Atlas by Boston Dynamics. Atlas is the longest-running continuous development path in general-purpose humanoid robotics, with roots in DARPA-funded research that began in 2013. The electric version, introduced in 2024, replaced earlier hydraulic versions with brushless electric actuators, which have a higher energy efficiency and significantly lower maintenance requirements. Atlas moves around with parkour-like movements, uses tools and can work together with a human partner to manipulate objects. Its control architecture combines model predictive control of whole body dynamics and learned perception modules to understand the environment. Importantly, Atlas can dynamically adjust its gait on uneven terrain in real-time without pre-mapping the surface [4].

Tesla Optimus Gen 2. Optimus breaks away from the research-first tradition of most humanoid development. Tesla has pitched the platform explicitly as a future product rather than a demonstration, with stated ambitions of volume manufacturing and deployment in its own factories as an initial application. The second generation version greatly improved the dexterity of the hand with the addition of tactile sensing in the fingertips and a new tendon driven finger mechanism. The system is based on Tesla's existing investments in vision-based neural networks developed for the Autopilot program, adapted to the embodied context. Task learning relies heavily on imitation from human demonstrations collected by motion capture at scale [5].

Figure 01 and the integration of OpenAI Figure 01 attracted a lot of attention in early 2025 when the company released a video showing the robot holding a natural-language conversation with a human operator, while also making a cup of coffee. In this demo we showed how a large multimodal language model can be integrated into the real-time control loop of a robot in the real world. The robot is able to explain its actions, receive spoken corrections and change its behavior mid-task based on verbal feedback. The architecture decouples high-frequency motion control, running at ~200 Hz, from the language model inference loop that runs at a much lower frequency and provides goal-level guidance [5].

Unitree H1 and Accessibility Shift. The Unitree H1 isn't so much about raw performance as it is about price point. H1 delivered a research-grade bipedal humanoid at a fraction of the cost of comparable platforms, making it accessible to university labs and smaller businesses that previously couldn't afford to experiment at this scale. The platform runs open source locomotion controllers trained with reinforcement learning and has been widely used by the research community to test new control algorithms, sensor fusion approaches and manipulation policies. This democratization of hardware access has accelerated the rate of published research in embodied AI [5].

A common theme emerges across all four platforms: the most capable behaviors combine a learned high-level planning component, typically language-conditioned, with a robust low-level motion controller trained via reinforcement learning in simulation. Neither component alone yields the full range of capabilities. It is the combination of reasoning about goals and reliable physical execution that makes these systems useful in real-world environments.

The industrial application domain has been shown to be the most tractable initial deployment target, partly for technical reasons, partly for economic reasons. Factory environments are variable but much more structured than domestic spaces: objects are located in predictable locations, lighting is controlled, and the range of tasks that need to be performed is bounded. Tesla has deployed Optimus in its Fremont factory to sort battery cells and Agility Robotics has used its Digit platform to handle totes in an Amazon warehouse, demonstrating the technology is mature enough to do repetitive, structured tasks in supervised settings. The economic calculus is compelling for physically demanding, repetitive and hard to automate tasks with fixed-purpose machinery [6].

Healthcare applications are at an earlier stage but are probably the field where the stakes are the biggest. In experimental settings, researchers have shown humanoid systems to assist with medication dispensing, to support patient transfer under human supervision, and to provide companionship and monitoring for elderly patients in care facilities. The regulatory pathway to physically interacting with patients autonomously is long and rightly demanding, but the demographic pressure of aging populations in high-income countries provides strong motivation to push these applications forward [6].

The most technically challenging applications are the domestic ones. The diversity of objects, surfaces, lighting conditions, the unstructured setting of homes, and the unpredictability of other residents including children and animals, stretch current systems to their limits. Most of the demonstrations of the domestic tasks performed by

humanoid robots have been achieved either through extensive pre-mapping of the specific environment or through carefully designing the demonstration scenario. Generalization to arbitrary home environments is still an open problem, but the pace of progress on vision-language-action models suggests that the gap is closing.

We should seriously consider ethical issues of humanoid robots. Three topics often addressed in the literature and in public discourse are labor displacement, safety, and the psychology of human-robot interaction. Evidence from industrial deployments on labor displacement suggests the near-term effect is more likely to be task displacement than job elimination, with robots performing specific physically demanding or repetitive subtasks while human workers move into supervisory, maintenance, and judgment-intensive roles. But the long term trend as capabilities increase is really uncertain and policy frameworks have not kept pace with technological development [6].

Safety is a technical and governance challenge. If a robot operating in a home or hospital misidentifies a fragile object, fails to detect a person in its path, or executes a learned behavior in a context outside its training distribution, it can cause serious harm. The present systems have hardware torque limits, proximity sensing and conservative planning margins but no system has reached the reliability standard to warrant fully autonomous unsupervised operation in close proximity to vulnerable people. Regulatory frameworks in most jurisdictions are poorly suited to autonomous physical agents. Developing suitable standards is an active area of work for standards bodies and regulators.

The human-robot interaction with humanoid systems is psychologically hard to explain and somewhat counterintuitive. Research consistently finds that people are more likely to form stronger functional relationships with robots that have a humanoid form, are more willing to follow instructions from them, and are more distressed when humanoid robots are treated harshly effects that do not seem to the same degree with non-humanoid machines. This has implications for the design of therapeutic and assistive applications and the prevention of inappropriate Anthropomorphization which may lead users to over-trust systems with real limitations [6].

The humanoid robot has crossed a threshold that was not so apparent even five years ago. AI systems that can learn complex physical behaviors from experience, understand natural language instructions, and adapt to novel environments have changed the technical possibilities for a machine that moves through and inhabits the physical world designed for human bodies. The platforms we survey here are not science-fiction props, they are operational systems, installed in real facilities doing real work.

That's not to say all the challenges are behind us. Genuine open problems are the generalization to unstructured environments, the energy autonomy for long-term operation, the safe and certified behavior around vulnerable people and the development of suitable governance frameworks. The pace of progress in the underlying AI technologies (e.g., large multimodal models, simulation-to-real transfer for reinforcement learning) provides reasonable grounds for optimism that these problems will yield to sustained research effort.

What may be most striking about the present moment is that the development of humanoid robots is no longer confined to a few well-funded government laboratories. The combination of readily available simulation environments, open-source control frameworks, lower-cost hardware platforms, and the general-purpose capabilities of large pretrained models has created conditions in which a graduate research team can make meaningful contributions to the frontier. This broadening of participation will almost certainly further accelerate progress.

The deeper question of what it means for human society to share its physical spaces with machines that look like people, move like people, and communicate like people with ever-increasing frequency does not have a technical answer. This requires continued engagement of ethicists, policy makers, social scientists and the general public, and of the engineers and computer scientists who develop these systems. Getting the conversation right matters at least as much as getting the technology right.

Список литературы

1. Трипати С., Гаур С. Четырёхногий робот для пересечённой местности — BigDog // Материалы сегодня: Труды. — 2023. — № 1, том 81. — С. 481–485. DOI: 10.1016/j.matpr.2021.03.638
2. Ито Т. Робототехника и тенденции её развития // Труды Международной конференции по искусственной жизни и робототехнике. — 2022. — № 1, том 27. — С. 378–382. DOI: 10.5954/icarob.2022.ps3.
3. Тоан Н.К., Туан Ле Д., Лонг Ле Б., Тинь Н.Т. Разработка головы гуманоидного робота на основе FACS // Международный журнал машиностроения и робототехники. — 2022. — № Online First. — С. 365–372. DOI: 10.18178/ijmerr.11.5.365-372.
4. Чэнь В., Вонг К.К.Л., Лонг С., Сунь Чж. Относительная энтропия корректных алгоритмов проксимальной оптимизации политики с модифицированным штрафным коэффициентом в сложной среде // Энтропия. — 2022. — № 4, том 24. — С. 440. DOI: 10.3390/e24040440.

5. Заревич А.И., Макаренко Ф.В., Ягодкин А.С., Зольников К.В. Моделирование поведения мобильных роботов с использованием генетических алгоритмов // Моделирование систем и процессов. – 2022. – № 3, том 15. – С. 7–16. DOI: 10.12737/2219-0767-2022-15-3-7-16.

6. Мещерякова А.А. Разработка автоматизированной системы управления мобильным роботом // Моделирование систем и процессов. – 2024. – № 1, том 17. – С. 73–84. DOI: 10.12737/2219-0767-2024-17-1-73-84.

References

1. Tripathy S., Gaur S. Rough Terrain Quadruped Robot — BigDog // Materials Today: Proceedings. — 2023. — No. 1, Vol. 81. — P. 481–485. DOI: 10.1016/j.matpr.2021.03.638

2. Ito T. Robot Technology, and Its Development Trend // Proceedings of International Conference on Artificial Life and Robotics. — 2022. — No. 1, Vol. 27. — P. 378–382. DOI: 10.5954/icarob.2022.ps3.

3. Toan N.K., Thuan Le D., Long Le B., Thinh N.T. Development of Humanoid Robot Head Based on FACS // International Journal of Mechanical Engineering and Robotics Research. — 2022. — No. Online First. — P. 365–372. DOI: 10.18178/ijmerr.11.5.365-372.

4. Chen W., Wong K.K.L., Long S., Sun Zh. Relative Entropy of Correct Proximal Policy Optimization Algorithms with Modified Penalty Factor in Complex Environment // Entropy. — 2022. — No. 4, Vol. 24. — P. 440. DOI: 10.3390/e24040440.

5. Zarevich A.I., Makarenko F.V., Yagodkin A.S., Zolnikov K.V. Modeling the Behavior of Mobile Robots Using Genetic Algorithms // Modeling of Systems and Processes. – 2022. – No. 3, Vol. 15. – P. 7–16. DOI: 10.12737/2219-0767-2022-15-3-7-16.

6. Meshcheryakova A.A. Development of an Automated Control System for a Mobile Robot // Modeling of Systems and Processes. – 2024. – No. 1, Vol. 17. – P. 73–84. DOI: 10.12737/2219-0767-2024-17-1-73-84.

ПОСТКВАНТОВАЯ БЛОКЧЕЙН-ПЛАТФОРМА ДЛЯ ПОДКЛЮЧЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Мд.Ш.И. Шхагор¹, Е.А. Аникеев¹, А.В. Акименко¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье представлен OmniGuard V2X – прототип системы безопасности для подключенных и автономных транспортных средств. Решение объединяет блокчейн-аудит, доказательства с нулевым разглашением, децентрализованную идентификацию, постквантовый обмен ключами, федеративное обучение и защищенный криминалистический журнал в единую архитектуру. Особое внимание уделено практической реализации и открытому описанию ограничений системы, включая отсутствие защиты от атак Сибиллы и большинства валидаторов.

Ключевые слова: V2X, блокчейн, доказательства с нулевым разглашением, постквантовая криптография, децентрализованная идентификация, федеративное обучение, безопасность транспортных средств.

A POST-QUANTUM BLOCKCHAIN FRAMEWORK FOR CONNECTED SMART VEHICLES

Md S.I. Shagor¹, E.A. Anikeev¹, A.V. Akimenko¹

¹Voronezh State University of Forestry and Technologies named
after G.F. Morozov

Abstract. This paper presents OmniGuard V2X, a security prototype for connected and autonomous vehicles. The system integrates blockchain auditing, zero-knowledge privacy, decentralized identity, post-quantum key establishment, federated learning, and an encrypted forensic black box into a unified architecture. Rather than making unrealistic performance claims, the study openly discusses its current limitations, including the lack of protection against Sybil attacks and majority-controlled validators.

Keywords: V2X, blockchain, zero-knowledge proofs, post-quantum cryptography, decentralized identity, federated learning, vehicle security.

Connected and autonomous vehicles depend on constant V2X communication to exchange telemetry, traffic, and safety data, and that dependence creates real problems for authentication, integrity, privacy, and secure transport of information. The long service life of a modern vehicle adds another constraint: any security architecture adopted today has to survive the transition to post-quantum cryptography and still produce forensic evidence that can be trusted after an incident [1].

This paper presents OmniGuard V2X, a prototype that combines blockchain-based audit logging [2], privacy-preserving data sharing, decentralized identity, hybrid post-quantum key establishment, federated learning for anomaly detection, and an encrypted forensic black box into one six-layer architecture. None of the cryptographic primitives are new; the contribution is in how established techniques are combined into a working, modular pipeline for connected vehicles. The paper reports a reproducible end-to-end latency of 5.34 ms and is deliberately open about what the system does not yet solve — Sybil resistance and majority-controlled validators chief among them — because a realistic account of the boundaries is more useful to other researchers than an inflated one.

Blockchain has repeatedly been shown to strengthen V2X security through trusted authentication, secure data sharing, and decentralized access control [3], but the literature is consistent on what is still missing: low-latency operation, lightweight security for constrained vehicle hardware, scalability, and real-world validation beyond simulation. Most published work isolates a single mechanism rather than evaluating a complete pipeline end to end.

OmniGuard V2X does not introduce new cryptography. It combines Pedersen commitments [4] with Schnorr-style zero-knowledge proofs for privacy, Lamport one-time signatures for identity, Merkle trees for compact verification, and SHA-3 with AES-GCM for integrity and storage, on top of a hybrid post-quantum key exchange [3] and a FedAvg-based federated learning model [5] with trimmed-mean aggregation for resilience against bad participants. What distinguishes this work from many conceptual security frameworks is that the prototype has actually been run, and its limitations — no defense against Sybil identities, majority-controlled validators, or large-scale Byzantine adversaries — are stated rather than glossed over.

Figure 1 shows the six-layer design. Sensor data is validated first, then passed through an authenticated key exchange, a privacy and identity layer, and an intermediate federated-learning stage where vehicles can collaborate on anomaly detection without sharing raw data. Verified events are written to a blockchain audit layer, and the top layer exposes APIs and a dashboard for monitoring. Two points about this layering matter for everything that follows. First, federated-learning updates are verified and logged exactly like any other event, rather than being treated as a special case. Second, the layers separate functions, not trust boundaries — a valid signature proves where data came from, not that the data is correct if the originating sensor was already compromised.

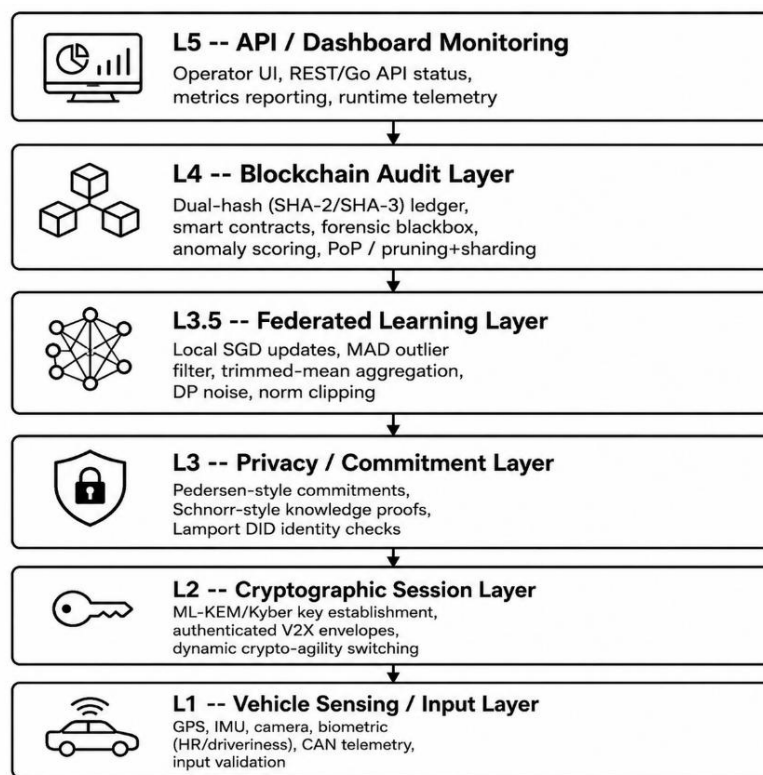


Figure 1– OmniGuard V2X six-layer prototype architecture (L1–L5, with the L3.5 federated-learning layer).

The proposed architecture combines various existing security techniques to create a unified framework for smart vehicles communication. Rather than trying to come up with a solution from scratch, the approach combines decentralized identities, private authentication, blockchain audit, quantum-resilient communications, federated learning, and forensic log encryption.

Every smart vehicle gets assigned a decentralized identity based on Lamport one-time signature scheme that only uses one-way hash functions and, therefore, is

believed to be adequate for post-quantum world. Each key pair can be used only once so a new one has to be created for every authentication attempt. The current implementation of the framework uses open registration and thus anybody can create an identity in the system. However, this doesn't prevent Sybil attack and thus a real-life implementation should include some external entity responsible for enrollment such as vehicle manufacturer or transportation authority.

To ensure privacy in the system the framework uses combination of Pedersen commitment and Schnorr-style zero-knowledge proof [4]. In particular, this enables vehicles to prove their compliance to certain rules, like remaining under certain speed limit, without disclosing their exact speed. Thus, it provides good privacy but relies on classical assumption of discrete logarithm problem and thus is not post-quantum yet.

Integrity of the blockchain is guaranteed through usage of dual-hash structure based on SHA-2-256 and SHA-3-256 hashes. Such structure makes detecting the modifications very easy. Proof-of-authority consensus guarantees proper validation of new blocks and thus provides robust auditing and traceability although still relying on trusted validators. Security of communications between vehicles starts from capability negotiation and then session key establishment based on ML-KEM (Kyber) [3]. Crypto-agility layer is implemented to select proper signing algorithm, while post-quantum security applies only to the key exchange.

Finally, the architecture uses federated learning for joint anomaly detection without exchanging raw vehicle data. Update of local models is secured with differential privacy, filtered to decrease influence of malicious contribution, and aggregated through trimmed mean strategy. First tests show good resistance to abnormal updates although larger scale test are necessary yet. Other features of the architecture include encryption of forensic logs, biometric safe-mode activation, proof of proximity verification, and AES-256-GCM encrypted blockchain storage.

The computational complexity of the proposed framework varies according to the function being executed. Most local operations, including telemetry validation, ML-KEM key establishment, and blockchain insertion, are performed in constant time, $O(1)$. As a result, the processing cost of an individual vehicle remains stable even as the number of connected vehicles increases. Communication-intensive operations behave differently. When every vehicle exchanges information with every other vehicle or when multiple validators participate in the same consensus round, the total communication cost grows to $O(n^2)$. Blockchain verification depends primarily on the number of stored blocks, whereas the cost of federated-learning aggregation increases with both the number of participating clients and the size of the learning model. These complexity

values describe expected theoretical behavior rather than measurements from large-scale deployment. Committee-based validation, hierarchical gossip, batching, and sharding are planned to improve scalability in future versions of the framework.

Performance was evaluated using the prototype implementation in a controlled local environment. The measured end-to-end latency of the complete processing pipeline was 5.34 ms, recorded after the system had reached a stable operating state with initialized cryptographic contexts and cached resources. This result is presented as a reproducible prototype measurement rather than as a benchmark for production-scale V2X networks. An earlier latency value of 3.57 ms was removed from the final evaluation because repeated experiments could not reproduce the same result with sufficient consistency.

Only results that could be reproduced reliably are included in this study; protocol overhead, large-scale adversarial detection accuracy, and comprehensive federated-learning robustness are therefore not reported as quantitative metrics. The current implementation demonstrates feasibility, while a more extensive evaluation involving larger vehicle fleets, diverse network conditions, and repeated trials remains necessary to validate performance under real-world operating conditions.

Four limitations recur often enough across the preceding sections to be worth restating together, summarized in Table 1. Identity and consensus share one root cause — open registration — since nothing under the current policy limits how many DIDs a single actor can create, so neither the majority-vote chain nor the proximity check is Sybil-resistant by itself; both assume an admission step that has not been built. Dual-hash integrity and majority-controlled validation answer different questions — whether a record was altered after the fact, versus whether enough validators agreed to accept it when it was written — and a quorum-controlling coalition can satisfy the second while still recording something false, which the hash chain will then faithfully preserve. Post-quantum coverage is real but partial: the ML-KEM handshake is genuinely protected against a future quantum adversary, while the Pedersen/Schnorr privacy layer is not, and describing the whole system as post-quantum without that qualification would be inaccurate. Finally, the federated-learning robustness result is the most provisional claim in the paper — a three-peer, single-trial sanity check demonstrates that one large, obvious outlier gets caught, not that the pipeline withstands an adversary operating near the detection boundary.

Table 1 – Documented limitations and what would close each one.

Mechanism	Documented limitation	What would close it
DID identity (4.1)	No Sybil resistance under open registration.	External admission: certificate, enrollment, or stake.
Majority-vote chain (4.2)	Quorum control can sign false but valid-looking blocks.	Bounded-committee BFT / certificate-gated validators.
PQC handshake (4.2)	Only the key-establishment path is post-quantum.	Lattice- or hash-based replacement for the privacy layer.
FL aggregation (4.3)	Validated on 3 peers, 1 trial, 24 samples only.	Larger peer counts, multi-trial, confidence intervals.
ZKP privacy (4.1)	Classical discrete-log security; commit-only mode.	PQC-safe proof system; secure-aggregation protocol.
Network layer (§5)	$O(n^2)$ volume under full mesh / naive gossip.	Committee selection, hierarchical gossip, batching.

The project's own label for these corrections — corrected but requiring new experiments — is, in the authors' view, the right level of confidence for a system at this stage: the architecture is coherent and each component is individually defensible, but Sybil resistance, Byzantine-robust learning, full post-quantum coverage, and large-scale performance all need experiments beyond what a single-developer prototype can currently provide.

The clearest next steps follow directly from the limitations above. Closing the Sybil gap means integrating an external admission mechanism, most plausibly a manufacturer certificate chain or transport-authority enrollment, ahead of DID issuance. Replacing simple-majority validation with a bounded-committee Byzantine-fault-tolerant protocol [6] would address majority control directly, provided committee size stays small enough to avoid reintroducing $O(n^2)$ communication cost. Extending post-quantum coverage past the key-establishment path means replacing the Pedersen/Schnorr construction with a lattice- or hash-based proof system, since post-quantum range proofs remain an active research problem rather than an off-the-shelf component. On the learning side, the immediate need is simply more evidence — a larger peer count, multiple trials, a published confidence interval — since the trimmed-mean technique already in use is adequate; what is missing is statistical power. Network-layer work includes committee-selection, hierarchical-gossip, and sharding mitigations to keep full-mesh and naive-gossip patterns from dominating at fleet scale, and the forensic black box would benefit from hardware secure-enclave key wrapping and a standardized chain-of-custody format.

This paper presented OmniGuard V2X, a prototype framework that integrates blockchain auditing, privacy-preserving mechanisms, decentralized identity, post-

quantum key establishment, federated learning, and secure forensic logging into a unified security architecture for connected smart vehicles, demonstrating how established security techniques can be combined into a practical, modular, and reproducible V2X security pipeline.

The prototype confirms that these components can operate together while maintaining a reproducible end-to-end latency and a clearly defined computational profile, and the study deliberately distinguishes validated results from future objectives by documenting current security boundaries and experimental limitations instead of making unsupported performance claims.

Although several challenges remain, including stronger identity admission, Byzantine-resilient consensus, broader post-quantum protection, and large-scale experimental validation, the proposed architecture provides a solid foundation for future research on secure intelligent transportation systems. The authors believe that openly presenting both the capabilities and the present limitations of the prototype makes OmniGuard V2X a useful reference platform for the continued development and evaluation of next-generation V2X security solutions.

Список литературы

1. Новикова, Т. П. Математическая модель интермодальных грузовых перевозок / Т. П. Новикова, С. А. Евдокимова, А. И. Новиков // Моделирование систем и процессов. – 2024. – Т. 17, № 2. – С. 62-70. – DOI: 10.12737/2219-0767 2024-17-2-62-70. – EDN ERRGGK.

2. Накамото, С. Биткойн: одноранговая электронная платежная система / С. Накамото. – 2008. – URL: <https://bitcoin.org/bitcoin.pdf> (дата обращения: 23.06.2026).

3. Стандарт механизма инкапсуляции ключей на основе модульной решетки: Федеральная публикация стандартов обработки информации FIPS 203 / Национальный институт стандартов и технологий. – Гайтерсберг, Мэриленд: Национальный институт стандартов и технологий, 2024. – DOI: 10.6028/NIST.FIPS.203 (дата обращения: 23.06.2026).

4. Педерсен, Т. П. Неинтерактивное и информационно-теоретически безопасное проверяемое разделение секрета / Т. П. Педерсен // Достижения в криптологии — CRYPTO'91. Лекционные заметки по информатике. – Берлин: Springer. – 1992. – Т. 576. – С. 129-140.

5. Макмахан, Х. Б., Мур, Э., Рамадж, Д., Хэмпсон, С., Аркас, Б. А. Коммуникационно-эффективное обучение глубоких сетей на основе децентрализованных данных // Труды 20-й Международной конференции по искусственному интеллекту и статистике (AISTATS). – PMLR. – 2017. – Т. 54. – С. 1273-1282.

6. Кастро, М. Практическая византийская отказоустойчивость / М. Кастро, Б. Лисков // Труды 3-го симпозиума USENIX по проектированию и реализации операционных систем (OSDI). – Новый Орлеан, Луизиана. – 1999. – С. 173-186.

References

1. Novikova, T. P. Mathematical Model of Intermodal Cargo Transportation / T. P. Novikova, S. A. Evdokimova, and A. I. Novikov // Modeling of Systems and Processes. – 2024. – Vol. 17, No. 2. – Pp. 62-70. – DOI: 10.12737/2219-0767 2024-17-2-62-70. – EDN ERRGGK.

2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System / S. Nakamoto. – 2008. – URL: <https://bitcoin.org/bitcoin.pdf> (date of access: 23.06.2026).

3. Module-Lattice-Based Key-Encapsulation Mechanism Standard: Federal Information Processing Standards Publication FIPS 203 / National Institute of Standards and Technology. – Gaithersburg, MD: National Institute of Standards and Technology, 2024. – DOI: 10.6028/NIST.FIPS.203 (date of access: 23.06.2026).

4. Pedersen, T. P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing / T. P. Pedersen // Advances in Cryptology — CRYPTO '91. Lecture Notes in Computer Science. – Berlin: Springer. – 1992. – Vol. 576. – P. 129-140.

5. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., Arcas, B. A. Communication-Efficient Learning of Deep Networks from Decentralized Data // Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS). – PMLR. – 2017. – Vol. 54. – P. 1273-1282.

6. Castro, M. Practical Byzantine Fault Tolerance / M. Castro, B. Liskov // Proceedings of the 3rd USENIX Symposium on Operating Systems Design and Implementation (OSDI). – New Orleans, LA. – 1999. – P. 173-186.

СЕКЦИЯ 4
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ
АППАРАТЫ И РОБОТИЗИРОВАННЫЕ СИСТЕМЫ

DOI: 10.58168/IntInfSys2026_96-102

УДК 004.8:656.13

КРИТЕРИАЛЬНАЯ СИСТЕМАТИЗАЦИЯ МЕТОДОВ МАШИННОГО
ОБУЧЕНИЯ ДЛЯ АДАПТИВНОГО СВЕТОФОРНОГО УПРАВЛЕНИЯ

Д.Н. Давиденко¹, А.В. Ачкасов¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация: Предложена критериальная схема сопоставления методов машинного обучения, применяемых в адаптивном управлении светофорными объектами. Подходы разделены по четырем уровням: представление транспортной ситуации, локальное принятие решения, координация сети и эксплуатационное развертывание. Показано, какие ограничения определяют выбор между DQN-, pressure-based, графовыми, attention- и offline-RL моделями.

Ключевые слова: критериальное сравнение, адаптивное управление, светофорный объект, обучение с подкреплением, транспортное давление, многоагентная координация, офлайн-обучение.

CRITERION-BASED SYSTEMATIZATION OF MACHINE LEARNING
METHODS FOR ADAPTIVE TRAFFIC SIGNAL CONTROL

D.N. Davidenko¹, A.V. Achkasov¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract: An engineering-oriented framework is proposed for comparing machine learning methods used in adaptive traffic signal control. The methods are examined at four levels: traffic-state representation, local decision making, network coordination, and operational deployment. The framework clarifies when DQN, pressure-based, graph, attention, and offline reinforcement learning models are appropriate and which limitations restrict their practical use.

Keywords: criterion-based comparison, adaptive control, signalized intersection, reinforcement learning, traffic pressure, multi-agent coordination, offline learning.

Светофорный контроллер распределяет ограниченное время между конфликтующими направлениями. Фиксированный план делает это по заранее рассчитанному сценарию и потому теряет эффективность, когда фактический спрос заметно отличается от расчетного. Адаптивная система должна реагировать на текущую очередь, загрузку выходных участков и последствия собственного решения для соседних перекрестков [1, 2].

Для машинного обучения ключевым является не только выбранный алгоритм. На итог влияют состав наблюдений, множество допустимых действий, транспортный смысл функции вознаграждения и способ сетевой координации. Поэтому сопоставление моделей только по названию нейросетевой архитектуры не позволяет оценить их применимость на реальном объекте [3].

Цель работы – систематизировать методы машинного обучения по четырем инженерным уровням: представлению транспортной ситуации, локальному выбору фазы, взаимодействию нескольких контроллеров и условиям безопасного развертывания. Прогнозирование трафика рассматривается как вспомогательная функция, а не как замена алгоритма управления.

Выполнен целевой тематический поиск в eLIBRARY.RU, IEEE Xplore, ACM Digital Library, arXiv и Google Scholar. В корпус включены 12 источников: обзоры [2, 3], исследования локальных и сетевых контроллеров [4-10], прогнозная модель STGCN [11], руководство FHWA [12] и обязательная для конференции публикация ВГЛУ [1]. Работа не претендует на метаанализ: источники отбирались для сравнения принципов построения систем.

Для каждого метода фиксировались измеряемое состояние, управляющее действие, функция вознаграждения, масштаб сети, происхождение обучающих данных и наличие ограничений безопасности. Проценты улучшения из разных публикаций не объединялись, поскольку они получены на несопоставимых топологиях, профилях спроса, симуляторах и базовых контроллерах.

В локальных DQN-моделях состояние перекрестка преобразуется в оценки полезности допустимых фаз [4]. Такой подход способен учитывать нелинейные зависимости, но обычно привязан к геометрии входа и чувствителен к способу задания награды. Pressure-based методы используют более компактный транспортный признак – дисбаланс между входными и выходными потоками. В

PressLight [5] он связывает обучение с принципом max-pressure, что облегчает интерпретацию решения.

FRAP [6] сравнивает конфликтующие фазы попарно и учитывает симметрии конфигурации. Вместе с PressLight этот подход вводит транспортную структуру непосредственно в контроллер и тем самым уменьшает зависимость от произвольного набора признаков. Ограничением остается требование надежно измерять очереди и корректно описывать допустимые фазы [5, 6].

Для сети перекрестков независимое обучение создает нестационарную среду: политика каждого агента меняет входной поток соседей. CoLight [7] представляет сеть графом и с помощью внимания выбирает значимые сообщения от связанных узлов. CityFlow [8] позволяет воспроизводимо проверять такие схемы на крупных сценариях. Сетевая координация повышает масштабируемость управления, но добавляет зависимость от каналов связи и качества топологии.

AttendLight [9] обрабатывает переменное число дорог, полос и фаз, поэтому одна архитектура может применяться к нескольким конфигурациям. Это не гарантирует работу за пределами обучающего распределения. D2TSC [10] переносит обучение в офлайн-режим: политика формируется по историческим данным, а сигнал награды восстанавливается с учетом транспортных закономерностей. Риск онлайн-эксперимента уменьшается, но качество ограничено покрытием исходного набора действий.

STGCN [11] прогнозирует транспортные показатели на графе дорожной сети и может заранее сообщать контроллеру о приближении перегрузки. Однако минимальная ошибка прогноза не равна минимальной задержке: окончательное решение обязано учитывать допустимые фазы, переходные интервалы и состояние выходных направлений. Поэтому прогнозный модуль следует оценивать совместно с управляющим алгоритмом.

Сопоставление показывает, что DQN удобен как базовый локальный контроллер; pressure-based методы дают более явную связь решения с транспортным состоянием; графовые модели нужны при сильном взаимодействии соседних объектов; attention-механизмы уменьшают жесткую привязку к конфигурации; offline-RL ограничивает риск обучения на дороге. Эти классы не взаимоисключающие и могут использоваться в одной многоуровневой системе.

Предлагаются семь критериев выбора: масштаб объекта, измеримость состояния, тип действия, транспортная интерпретация награды, механизм координации, переносимость и наличие независимого контура безопасности. Такой

набор отделяет свойства метода от условий конкретного эксперимента. Например, высокий результат в симуляторе не компенсирует использование признака, который невозможно получить от установленного детектора.

Проверка должна опираться на несколько эксплуатационных показателей. FHWA [12] рекомендует анализировать время поездки, надежность, задержку, скорость, число остановок, пропускную способность и очередь. Для сравнения светофорных политик минимально достаточны средняя задержка, очередь, число остановок и пропускная способность. Экологические показатели допустимы только при явно заданной модели расхода топлива или выбросов [1, 12].

Таблица 1 – Сопоставление рассматриваемых подходов

Подход и масштаб	Основной принцип	Ключевое ограничение
DQN [4], один перекресток	Оценка полезности фаз	Зависимость от награды
PressLight [5], локально или в сети	Максимизация транспортного давления	Нужны достоверные данные об очередях
FRAP [6], один перекресток	Конкуренция фаз с учетом симметрий	Нет сетевой координации
CoLight [7], сеть перекрестков	Графовое внимание к соседям	Сложность обучения и зависимость от связи
AttendLight [9], переносимый агент	Внимание к структуре дорог и фаз	Чувствительность к сдвигу распределения
D2TSC [10], офлайн-обучение	Архивные траектории и восстановленная награда	Неполное покрытие действий
STGCN [11], прогнозный модуль	Пространственно-временной граф	Не формирует безопасную фазу

Основной источник неопределенности – расхождение симуляции и реального объекта. Модель движения упрощает поведение водителей, пешеходные потоки, ошибки детекторов и редкие инциденты. Риск sim-to-real снижается при калибровке по полевым данным, варьировании параметров и проверке на нескольких профилях спроса, но не устраняется полностью [3, 10]. Состояние контроллера следует строить из реально доступных измерений и отдельно проверять деградацию при пропусках данных.

Безопасность должна обеспечиваться вне обучаемой политики. Агент может выбирать только из заранее разрешенного набора фаз, тогда как минимальное зеленое время, желтый и полностью красный интервалы, запрет конфликтующих направлений и время пешеходного перехода задаются детерминированной

логикой [2]. При недостоверных наблюдениях или сбое вычислений необходим автоматический переход к резервному плану.

Эксплуатационная ценность также зависит от объяснимости и совместимости с оборудованием. Pressure-based решение можно связать с измеренным дисбалансом потоков; сложная нейронная политика требует дополнительных средств диагностики. Интеллектуальная обработка транспортных данных применима и к экологическому мониторингу [1], однако сокращение задержки само по себе не доказывает уменьшение выбросов.

Систематизация показала, что применимость метода определяется всей архитектурой управления, а не только алгоритмом оптимизации. Для одиночного перекрестка разумной отправной точкой является политика управления, использующая очереди и транспортное давление: она имеет умеренную вычислительную сложность и допускает содержательное объяснение выбора фазы. Для сети потребуются графовая координация, а для переноса на реальный объект – проверка сдвига данных и внешний контур безопасности.

В дальнейшей экспериментальной части планируется в одной имитационной среде сопоставить фиксированный план, max-pressure и обучаемую pressure-based политику. Топология, профили спроса, интервалы управления и показатели эффективности будут зафиксированы заранее. До проведения такого эксперимента рассмотренным моделям не приписывается универсальное преимущество; статья определяет условия их корректного сравнения.

Список литературы

1. Мальцев В.В. Применение алгоритмов искусственного интеллекта для мониторинга загрязнения воздуха городским автотранспортом // Моделирование систем и процессов. – 2025. – Т. 18, № 2. – С. 86–96. – DOI: 10.12737/2219-0767-2025-18-2-86-96.
2. Вэй Х., Чжэн Г., Гайя В., Ли З. Обзор методов управления дорожным движением // arXiv preprint. – 2019. – arXiv:1904.08117.
3. Ван Х., Саннер С., Абдулхай Б. Критический обзор управления дорожным движением и новый объединённый взгляд на подходы с обучением с подкреплением и моделью прогнозирующего управления для адаптивного управления светофорами // arXiv preprint. – 2022. – arXiv:2211.14426.
4. Гао Дж., Шэнь Ю., Лю Дж., Ито М., Ширатори Н. Адаптивное управление светофорами: алгоритм глубокого обучения с подкреплением с повторным

воспроизведением опыта и целевой сетью // arXiv preprint. – 2017. – arXiv:1705.02755.

5. Вэй Х., Чэнь С., Чжэн Г. и др. PressLight: изучение управления максимальным давлением для координации светофоров на магистральной сети // Труды 25-й Международной конференции ACM SIGKDD по открытию знаний и интеллектуальному анализу данных. – 2019. – С. 1290–1298. – DOI: 10.1145/3292500.3330949.

6. Чжэн Г., Сюн Ю., Цзан Х. и др. Изучение конкуренции фаз для управления светофорами // arXiv preprint. – 2019. – arXiv:1905.04722.

7. Вэй Х., Сюй Н., Чжан Х. и др. CoLight: изучение сетевого взаимодействия для управления светофорами // arXiv preprint. – 2019. – arXiv:1905.05717.

8. Чжан Х., Фэн С., Лю С. и др. CityFlow: среда обучения с многоагентным подкреплением для крупномасштабных городских транспортных сценариев // arXiv preprint. – 2019. – arXiv:1905.05217.

9. Оруджлой А., Назари М., Хажинежад Д., Силва Дж. AttendLight: универсальная модель обучения с подкреплением на основе внимания для управления светофорами // arXiv preprint. – 2020. – arXiv:2010.05772.

10. Ли Дж., Линь С., Ши Т. и др. Полностью основанный на данных подход для реалистичного управления светофорами с использованием автономного обучения с подкреплением // arXiv preprint. – 2023. – arXiv:2311.15920.

11. Юй Б., Инь Х., Чжу З. Пространственно-временные свёрточные графовые сети: среда глубокого обучения для прогнозирования трафика // Труды Двадцать седьмой Международной совместной конференции по искусственному интеллекту. – 2018. – С. 3634–3640.

12. Федеральное управление автомобильных дорог. Показатели эффективности и руководство по валидации для адаптивных технологий управления светофорами. – Вашингтон, округ Колумбия, 2013. – Отчёт № FHWA-HOP-13-031.

References

1. Maltsev V.V. Application of artificial intelligence algorithms for monitoring air pollution caused by urban motor transport. Modeling of Systems and Processes. 2025;18(2):86-96. DOI: 10.12737/2219-0767-2025-18-2-86-96.

2. Wei H., Zheng G., Gayah V., Li Z. A Survey on Traffic Signal Control Methods. arXiv preprint, 2019, arXiv:1904.08117.

3. Wang X., Sanner S., Abdulhai B. A Critical Review of Traffic Signal Control and a Novel Unified View of Reinforcement Learning and Model Predictive Control Approaches for Adaptive Traffic Signal Control. arXiv preprint, 2022, arXiv:2211.14426.
4. Gao J., Shen Y., Liu J., Ito M., Shiratori N. Adaptive Traffic Signal Control: Deep Reinforcement Learning Algorithm with Experience Replay and Target Network. arXiv preprint, 2017, arXiv:1705.02755.
5. Wei H., Chen C., Zheng G., et al. PressLight: Learning Max Pressure Control to Coordinate Traffic Signals in Arterial Network. Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2019:1290–1298. DOI: 10.1145/3292500.3330949.
6. Zheng G., Xiong Y., Zang X., et al. Learning Phase Competition for Traffic Signal Control. arXiv preprint, 2019, arXiv:1905.04722.
7. Wei H., Xu N., Zhang H., et al. CoLight: Learning Network-Level Cooperation for Traffic Signal Control. arXiv preprint, 2019, arXiv:1905.05717.
8. Zhang H., Feng S., Liu C., et al. CityFlow: A Multi-Agent Reinforcement Learning Environment for Large Scale City Traffic Scenario. arXiv preprint, 2019, arXiv:1905.05217.
9. Oroojlooy A., Nazari M., Hajinezhad D., Silva J. AttendLight: Universal Attention-Based Reinforcement Learning Model for Traffic Signal Control. arXiv preprint, 2020, arXiv:2010.05772.
10. Li J., Lin S., Shi T., et al. A Fully Data-Driven Approach for Realistic Traffic Signal Control Using Offline Reinforcement Learning. arXiv preprint, 2023, arXiv:2311.15920.
11. Yu B., Yin H., Zhu Z. Spatio-Temporal Graph Convolutional Networks: A Deep Learning Framework for Traffic Forecasting. Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence, 2018, pp. 3634–3640.
12. Federal Highway Administration. Measures of Effectiveness and Validation Guidance for Adaptive Signal Control Technologies. Washington, DC, 2013. Report No. FHWA-HOP-13-031.

ТРЕХКОНТУРНАЯ МОДЕЛЬ ОБУЧАЕМОГО УПРАВЛЕНИЯ СВЕТОФОРНЫМ ОБЪЕКТОМ: РАНЖИРОВАНИЕ, СЕРВИСНЫЙ ДОЛГ И ФАЗОВЫЙ ДОПУСК

Д.Н. Давиденко¹, А.В. Ачкасов¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация: рассматривается обучаемый светофорный контроллер, в котором решение проходит три независимые проверки: транспортное ранжирование, учет накопленного сервисного долга и фазовый допуск. Для этой архитектуры заданы CMDP-модель, измеримый вектор наблюдений, правило маскирования команд и критерии проверки в SUMO. Разделение контуров исключает компенсацию опасного переключения улучшением средней задержки.

Ключевые слова: светофорное управление, CMDP, сервисный долг, фазовый граф, маскирование действий, транспортная очередь, безопасность.

A THREE-LOOP MODEL FOR LEARNING-BASED TRAFFIC SIGNAL CONTROL: RANKING, SERVICE DEBT, AND PHASE ADMISSIBILITY

D.N. Davidenko¹, A.V. Achkasov¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract: A learning-based traffic signal controller is represented by three independent loops: mobility ranking, accumulated service-debt control, and phase admissibility. The paper defines a CMDP model, a measurable observation vector, an action mask, and a SUMO verification protocol. The separation prevents an unsafe transition from being numerically compensated by lower average delay.

Keywords: traffic signal control, CMDP, service debt, phase graph, action masking, traffic queue, safety.

Средняя задержка удобна как итоговая статистика, однако она не задает полноценную логику контроллера. G. Zheng и соавторы отмечают, что существующие работы часто используют «an ad-hoc weighted linear combination of several traffic measures» [1]. Такая сумма допускает численную компенсацию: ухудшение одного направления может быть скрыто улучшением другого, а редкое опасное переключение – большим выигрышем по очереди. Поэтому в настоящей работе качество движения, своевременность обслуживания и физическая допустимость команды рассматриваются как разные типы требований [1, 2,].

Состав данных также нельзя выбирать только по удобству симулятора. Авторы D2TSC связывают слабую переносимость ряда решений с использованием «unrealistic fine-grained state observations and reward signals that are not directly obtainable from real-world sensors» [4]. Одновременно чисто автомобильное наблюдение неполно: B. Poudel и соавторы формулируют задачу как «jointly optimizing both pedestrian and vehicular efficiency» [4]. Следовательно, модель должна опираться на измеримые признаки и отдельно удерживать качество обслуживания каждой группы участников движения [4, 5].

Для разделения требований используется ограниченная марковская постановка. J. Achiam и соавторы считают более удобным «specify both a reward function and constraints, rather than trying to design behavior through the reward function» [3]. Но ограничение на ожидаемую стоимость само по себе не блокирует единичную запрещенную команду. Поэтому к CMDP добавляется фазовый супервизор: SafeLight предлагает «incorporate road safety standards as enforcement» [6], а A. Müller и M. Sabatelli используют «an action space that is safe by design» [7]. Цель статьи – связать эти идеи в единую трехконтурную архитектуру для одиночного перекрестка.

Архитектура содержит контур ранжирования, контур сервисного долга и контур фазового допуска. Первый сравнивает только те команды, которые уже признаны безопасными, и оценивает их по изменению транспортной нагрузки. Второй накапливает неудовлетворенный спрос отдельных направлений и пешеходных заявок; его состояние не обнуляется из-за кратковременного улучшения среднего показателя. Третий является детерминированным автоматом и не участвует в обучении: он удаляет конфликтные переходы, соблюдает минимальные длительности и вставляет обязательные промежуточные интервалы [2, 3, 6, 7].

$$M^* = \langle X, U, T, r, \gamma, c, b, H_\phi \rangle.$$

где: X – наблюдаемое состояние;

U – намерения политики;

T – динамика транспортной среды;

r – функция ранжирования;

γ – дисконтирование;

$c = \{c_1, \dots, c_m\}$ – сервисные стоимости;

$b = \{b_1, \dots, b_m\}$ – их бюджеты.

Компонент H_ϕ задает фазовый допуск и расширяет обычную CMDP-модель исполнительным контрактом.

Политика π формирует не электрические сигналы секций, а намерение выбрать одну из заранее проверенных транспортных фаз. Такая трактовка сохраняет смысл ограниченного процесса [2, 3], но переносит физическую безопасность из штрафа в структуру доступных действий [6, 7].

Вектор состояния строится от доступного измерительного канала к алгоритму, а не наоборот. Исследование G. Zheng и соавторов показывает, что более сложное представление может замедлять обучение без сопоставимого выигрыша [1]. D2TSC дополнительно требует, чтобы признаки и целевые сигналы могли быть восстановлены по реальным журналам и детекторам [4]. Поэтому в модель не включаются идеальные траектории всех автомобилей, точные будущие прибытия или другие величины, отсутствующие у реального контроллера.

Таблица 1 – Состав измерительного контракта

Элемент наблюдения	Источник измерения	Назначение в модели
$q_i, \Delta q_i$	Детектор или видео	Очередь и ее динамика [5, 9]
o_i	Датчик занятости	Режим плотности потока [5, 9]
p_t, τ_t	Журнал контроллера	Проверка фазовых таймеров [7, 11]
z_i	Детектор выхода	Исключение переполнения участка [4]
d_i^{ped}	Кнопка или видео	Учет пешеходного ожидания [8]
μ_i	Диагностика канала	Признак достоверности данных [9]

Очередь q_i и ее приращение Δq_i характеризуют не только размер накопления, но и направление изменения ситуации. Занятость o_i помогает различать свободный подход и плотный поток при одинаковом числе остановившихся машин [1, 4]. Пара p_t, τ_t берется из журнала контроллера и нужна супервизору. Резерв z_i

принимавшей полосы предотвращает передачу потока в уже заполненный участок и согласуется с логикой давления [8]. Пешеходный долг d_i^{ped} фиксирует продолжительность необслуженной заявки [5]. Коэффициент μ_i показывает доверие к измерению, чтобы отсутствие сообщения датчика не интерпретировалось как нулевой спрос [4].

Выход нейросетевой политики трактуется как запрос целевой фазы. Фактическая последовательность сигналов формируется отдельно. В работе А. Müller и М. Sabatelli пространство фаз содержит только неконфликтующие комбинации, а маска гарантирует, что «only appropriate phase transitions are carried out» [7]. SafeLight рассматривает безопасность как принудительно исполняемое требование, а не как пожелание, выраженное величиной штрафа [6]. На этой основе H_ϕ хранит вершины разрешенных фаз, допустимые ребра переходов и временные условия каждого ребра.

Алгоритм исполнения состоит из четырех операций. Сначала по графу E_ϕ удаляются недостижимые из текущей фазы намерения. Затем проверяются минимальное зеленое время и наличие места на выходном подходе. После выбора целевой вершины супервизор сам разворачивает переход в последовательность «зеленый – желтый – полностью красный – новая фаза». Наконец, если маска пуста, применяется заранее проверенное резервное действие, а не произвольный выход модели. Тем самым обучаемая часть не получает доступа к параметрам, нарушение которых запрещено проектом объекта и правилами применения светофоров [6, 7, 9].

Контур ранжирования оценивает краткосрочный транспортный эффект. В качестве базовой величины используется потенциал накопления Φ_i , зависящий от очередей на входах и доступного резерва выходов. Его уменьшение означает, что выбранная фаза высвобождает перегруженное движение, не создавая блокировку downstream-участка. Это сохраняет транспортную интерпретируемость *max-pressure* [8] и избегает набора несвязанных штрафов, критиковавшегося в [1].

Экологический член не объявляется измеренным результатом статьи: он задает место для модели выбросов или прокси-показателя по холостому ходу и разгонам. Возможность интеллектуальной обработки транспортных данных для мониторинга загрязнения рассмотрена В. В. Мальцевым [10], а SUMO предоставляет микроскопическую среду для последующего расчета движения и эмис-

сий [11]. Коэффициенты α являются параметрами сценария и должны исследоваться на устойчивость; ни одно их значение в данной работе не выдается за экспериментально оптимальное.

Таблица 2 – Разделение ответственности между контурами

Контур	Что вычисляется	Проверяемое требование
Ранжирование	r_t : изменение потенциала, выпуск, остановки, эмиссии	Выбор лучшего среди уже допустимых намерений [1, 4, 5]
Сервисный долг	d_i , c_i и бюджет b_i	Ограничение длительного ожидания автомобилей и пешеходов [2, 3, 8]
Фазовый допуск	N_ϕ и маска A_t	Нулевое число конфликтных и преждевременных переходов [6, 7, 11]

Сервисный контур нужен для требований, которые допускают краткое отклонение, но не должны систематически нарушаться. Вместо мгновенного штрафа вводится долг d_i : пока направление ожидает обслуживания, долг растет; во время эффективной зеленой фазы он уменьшается. Для пешеходов применяется отдельная переменная, поскольку их ожидание нельзя растворять в автомобильной средней [5]. Накопленные превышения формируют стоимости CMDP и сопоставляются с бюджетами b , что соответствует разделению вознаграждения и ограничений в [2, 3].

Проверка должна отделять эффективность архитектуры от эффекта конкретной нейросети. В SUMO [11] предлагается реализовать один и тот же перекресток и сравнить четыре контроллера: фиксированный план, max-pressure [8], RL с единой наградой и трехконтурную модель. Каждому варианту передаются одинаковые потоки и одинаковый набор измеримых признаков. Отдельно выполняется режим offline-обучения на журналах фиксированного управления, поскольку D2TSC показывает практическую ценность обучения по историческим данным без идеализированного онлайн-исследования [4].

Матрица сценариев включает равномерную нагрузку, устойчивую асимметрию, короткий пик, рост пешеходного спроса, заполнение выходной полосы и пропуски датчика. Результат считается подтвержденным только при одновременном выполнении трех групп критериев: транспортные показатели не хуже базовых методов [1, 8], долги и их квантили укладываются в заданные бюджеты [2, 3, 5], а журнал супервизора не содержит выполненных конфликтных переходов

[6, 7, 9]. Следует публиковать распределения по нескольким случайным реализациям, а не один лучший запуск. Численные результаты здесь отсутствуют намеренно: статья фиксирует проверяемую модель и условия ее опровержения.

Сформирована трехконтурная модель обучаемого управления одиночным светофорным объектом. Ее отличительный признак – разные вычислительные носители для разных требований. Транспортная награда ранжирует только разрешенные фазовые намерения; накопленный долг контролирует обслуживание автомобильных направлений и пешеходных заявок; фазовый автомат исключает конфликтные или преждевременные переходы до обращения к исполнительному устройству. Такая схема не позволяет обменять физическую безопасность на улучшение средней задержки. Заданы измерительный контракт, формулы награды и долга, а также воспроизводимая программа проверки без заявления несуществующих результатов.

Список литературы

1. Чжэн Г., Цзан Х., Сюй Н. и др. Диагностика обучения с подкреплением для управления светофорами. – 2019. – URL: <https://arxiv.org/abs/1905.04716> (дата обращения: 21.06.2026). – DOI 10.48550/arXiv.1905.04716.
2. Альтман Э. Ограниченные марковские процессы принятия решений. – Бока-Ратон: Chapman & Hall/CRC, 1999. – 256 с.
3. Ахиям Дж., Хелд Д., Тамар А., Аббил П. Оптимизация ограниченной политики // Труды 34-й Международной конференции по машинному обучению. – 2017. – Т. 70. – С. 22–31. – URL: <https://proceedings.mlr.press/v70/achiam17a.html> (дата обращения: 21.06.2026).
4. Ли Дж., Линь С., Ши Т. и др. Полностью основанный на данных подход для реалистичного управления светофорами с использованием автономного обучения с подкреплением. – 2023. – URL: <https://arxiv.org/abs/2311.15920> (дата обращения: 21.06.2026). – DOI 10.48550/arXiv.2311.15920.
5. Поудел Б., Ван Х., Ли В. и др. Совместная оптимизация движения пешеходов и транспортных средств в городских условиях с использованием обучения с подкреплением. – 2025. – URL: <https://arxiv.org/abs/2504.05018> (дата обращения: 21.06.2026). – DOI 10.48550/arXiv.2504.05018.
6. Ду В., Е Дж., Гу Дж. и др. SafeLight: метод обучения с подкреплением для безаварийного управления светофорами. – 2022. – URL: <https://arxiv.org/abs/2211.10871> (дата обращения: 21.06.2026). – DOI: 10.48550/arXiv.2211.10871.

7. Мюллер А., Сабателли М. Безопасное и психологически комфортное управление светофорами с помощью обучения с подкреплением с использованием маскировки действий // 25-я Международная конференция IEEE по интеллектуальным транспортным системам. – 2022. – С. 1696–1703. – URL: <https://arxiv.org/abs/2206.10122> (дата обращения: 21.06.2026). – DOI: 10.48550/arXiv.2206.10122.
8. Варайя П. Управление максимальным давлением в сети светофорных перекрёстков // Транспортные исследования. Часть С: Перспективные технологии. – 2013. – Т. 36. – С. 177–195. – DOI: 10.1016/j.trc.2013.08.014.
9. ГОСТ Р 52289-2019. Технические средства организации дорожного движения. Правила применения дорожных знаков, разметки, светофоров, дорожных ограждений и направляющих устройств. – Москва: Стандартинформ, 2020.
10. Мальцев В.В. Применение алгоритмов искусственного интеллекта для мониторинга загрязнения воздуха городским автотранспортом // Моделирование систем и процессов. – 2025. – Т. 18, № 2. – С. 86–96. – DOI: 10.12737/2219-0767-2025-18-2-86-96. – EDN EEZDKJ.
11. Альварес Лопес П., Бериш М., Бикер-Вальц Л. и др. Микроскопическое моделирование дорожного движения с использованием SUMO // 21-я Международная конференция по интеллектуальным транспортным системам. – 2018. – С. 2575–2582. – DOI: 10.1109/ITSC.2018.8569938.

References

1. Zheng G., Zang X., Xu N., et al. Diagnosing Reinforcement Learning for Traffic Signal Control. 2019. Available at: <https://arxiv.org/abs/1905.04716> (accessed 21 June 2026). DOI: 10.48550/arXiv.1905.04716.
2. Altman E. Constrained Markov Decision Processes. Boca Raton: Chapman & Hall/CRC; 1999. 256 p.
3. Achiam J., Held D., Tamar A., Abbeel P. Constrained Policy Optimization. Proceedings of the 34th International Conference on Machine Learning. 2017;70:22–31. Available at: <https://proceedings.mlr.press/v70/achiam17a.html> (accessed 21 June 2026).
4. Li J., Lin S., Shi T., et al. A Fully Data-Driven Approach for Realistic Traffic Signal Control Using Offline Reinforcement Learning. 2023. Available at: <https://arxiv.org/abs/2311.15920> (accessed 21 June 2026). DOI: 10.48550/arXiv.2311.15920.

5. Poudel B., Wang X., Li W., et al. Joint Pedestrian and Vehicle Traffic Optimization in Urban Environments using Reinforcement Learning. 2025. Available at: <https://arxiv.org/abs/2504.05018> (accessed 21 June 2026). DOI: 10.48550/arXiv.2504.05018.
6. Du W., Ye J., Gu J., et al. SafeLight: A Reinforcement Learning Method toward Collision-free Traffic Signal Control. 2022. Available at: <https://arxiv.org/abs/2211.10871> (accessed 21 June 2026). DOI: 10.48550/arXiv.2211.10871.
7. Müller A., Sabatelli M. Safe and Psychologically Pleasant Traffic Signal Control with Reinforcement Learning using Action Masking. 25th IEEE International Conference on Intelligent Transportation Systems. 2022:1696–1703. Available at: <https://arxiv.org/abs/2206.10122> (accessed 21 June 2026). DOI: 10.48550/arXiv.2206.10122.
8. Varaiya P. Max pressure control of a network of signalized intersections. *Transportation Research Part C: Emerging Technologies*. 2013;36:177–195. DOI: 10.1016/j.trc.2013.08.014.
9. GOST R 52289-2019. Traffic control devices. Rules for the application of road signs, markings, traffic lights, road barriers and guide devices. Moscow: Standartinform; 2020. (In Russ.).
10. Maltsev V. V. Artificial intelligence algorithms for monitoring urban transport air pollution. *Modeling of Systems and Processes*. 2025;18(2):86–96. DOI: 10.12737/2219-0767-2025-18-2-86-96. (In Russ.).
11. Alvarez Lopez P., Behrisch M., Bieker-Walz L., et al. Microscopic Traffic Simulation using SUMO. 21st International Conference on Intelligent Transportation Systems. 2018:2575–2582. DOI: 10.1109/ITSC.2018.8569938.

ГИБРИДНАЯ СИСТЕМА НАВИГАЦИИ БПЛА В УСЛОВИЯХ ОТКАЗА GNSS: КОМБИНАЦИЯ ВИЗУАЛЬНОЙ ОДОМЕТРИИ И ИНЕРЦИАЛЬНЫХ ИЗМЕРЕНИЙ

И.Н. Занин¹, Е.А. Аникеев¹, А.В. Акименко¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В статье рассматривается автономная навигация БПЛА в условиях отсутствия GNSS. Предложена гибридная визуально-инерциальная система на базе расширенного фильтра Калмана. Основной акцент сделан на коррекции масштабного дрейфа монокулярной камеры и повышении робастности алгоритмов. Подход обеспечивает точность, достаточную для городских миссий и поисково-спасательных операций.

Ключевые слова: беспилотный летательный аппарат, визуальная одометрия, инерциальная навигация, GNSS, расширенный фильтр Калмана, VIO, сенсорная фузия, масштабный фактор.

HYBRID UAV NAVIGATION SYSTEM IN GNSS-DENIED CONDITIONS: COMBINATION OF VISUAL ODOMETRY AND INERTIAL MEASUREMENTS

I.N. Zanin¹, E.A. Anikeev¹, A.V. Akimenko¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract. This paper addresses the autonomous navigation of unmanned aerial vehicles (UAVs) in GNSS-denied environments. A hybrid visual-inertial system based on an Extended Kalman Filter is proposed. The primary focus is on correcting the scale drift of a monocular camera and enhancing the robustness of the algorithms. The proposed approach ensures an accuracy level sufficient for urban missions and search-and-rescue operations.

Keywords: unmanned aerial vehicle, visual odometry, inertial navigation, GNSS, Extended Kalman Filter, VIO, sensor fusion, scale factor.

Широкое внедрение беспилотных летательных аппаратов в различные сферы деятельности, от мониторинга сельскохозяйственных угодий до поисково-спасательных операций в урбанизированных зонах, выявило критическую зависимость большинства коммерческих и промышленных дронов от сигналов глобальных навигационных спутниковых систем, таких как GPS, GLONASS или Galileo. Однако в ряде сценариев использование GNSS оказывается невозможным или неэффективным. К таким сценариям относятся полеты внутри помещений, в плотной городской застройке, вблизи высоковольтных линий электропередач, а также в условиях применения средств радиоэлектронной борьбы, приводящих к глушению или спуфингу навигационных сигналов [1].

В отсутствие внешнего позиционирования БПЛА вынужден полагаться на собственные бортовые сенсоры. Традиционно для решения этой задачи используются инерциальные навигационные системы, состоящие из акселерометров и гироскопов. Однако недорогие микроэлектромеханические системы, устанавливаемые на большинство легких БПЛА, характеризуются значительными шумами и смещениями нуля. Интегрирование зашумленного сигнала акселерометра для получения скорости и позиции приводит к квадратичному накоплению ошибки во времени, что делает чистую инерциальную навигацию непригодной для длительных миссий [2].

Альтернативным или дополняющим подходом является визуальная одометрия (VO), которая оценивает перемещение аппарата путем анализа последовательности изображений с бортовой камеры. VO не подвержена дрейфу в долгосрочной перспективе при наличии достаточного количества визуальных признаков, но страдает от проблем с оценкой абсолютного масштаба и чувствительна к изменениям освещенности, быстрому движению и отсутствию текстуры на поверхностях [3].

Целью данной работы является обзор и систематизация методов построения гибридных систем навигации, объединяющих преимущества визуальной одометрии и инерциальных измерений. В статье анализируются архитектуры тесного и слабого сопряжения сенсоров, рассматриваются методы решения проблемы масштаба и оценивается потенциальная точность таких систем в условиях отказа GNSS.

Инерциальная навигационная система определяет положение объекта путем двойного интегрирования измерений линейного ускорения. Уравнение движения в инерциальной системе координат может быть записано как:

$$p(t)=p_0+v_0t+\int_0^t\int_0^\tau(a(\xi)-b_a(\xi)-n_a(\xi))d\xi d\tau$$

где: $p(t)$ – вектор позиции;

v_0 – начальная скорость;

a – измеренное ускорение;

b_a – смещение нуля акселерометра;

n_a – шум измерения [4].

Даже небольшие постоянные смещения b_a приводят к ошибке позиции, растущей пропорционально t^2 . Для MEMS-датчиков типичное смещение может составлять десятки миллигравитаций, что приводит к ошибке в несколько метров уже через несколько секунд после потери внешнего сигнала корректировки. Гироскопы, измеряющие угловую скорость, также имеют дрейф, который приводит к ошибке в определении ориентации, что, в свою очередь, неправильно проецирует вектор ускорения в глобальную систему координат, усугубляя ошибку позиции.

Визуальная одометрия решает задачу оценки относительного перемещения камеры между кадрами. В случае использования монокулярной камеры система способна восстановить траекторию только с точностью до неизвестного масштабного коэффициента s . Это фундаментальное ограничение связано с тем, что одно и то же изменение размера объекта на изображении может быть вызвано как приближением камеры, так и использованием объектива с другим фокусным расстоянием, или же движением объекта меньшего размера на том же расстоянии [5].

Математически, если истинное перемещение равно ΔT , то визуальная одометрия оценивает его как $\Delta T_{est}=s\cdot\Delta T$. Без внешней информации определить s невозможно. Кроме того, VO требует наличия достаточного количества контрастных точек интереса на изображении для надежного отслеживания. В условиях однородных поверхностей или при быстром вращении БПЛА трекинг теряется, что приводит к накоплению ошибки или полному отказу системы [6].

Для компенсации недостатков каждого из методов применяется сенсорная фузия. Существует два основных подхода к интеграции данных: слабое сопряжение и тесное сопряжение.

При слабом сопряжении визуальная одометрия и инерциальная навигация работают как независимые модули. VO выдает оценку относительного переме-

щения, которая затем используется как измерение для фильтра Калмана, прогнозирующего состояние на основе данных IMU. Этот подход проще в реализации, но менее точен, так как не учитывает корреляцию ошибок между сенсорами на низком уровне [7].

Тесное сопряжение предполагает совместную обработку сырых данных с камеры и данных IMU в рамках единого оптимизационного процесса или фильтра. Наиболее распространенным математическим аппаратом для этого является Расширенный фильтр Калмана или оптимизация скользящего окна, используемая в таких системах, как OKVIS или VINS-Mono.

В архитектуре тесного сопряжения состояние системы x включает в себя не только позицию p , скорость v и ориентацию q , но и смещения датчиков IMU (b_a, b_g), а также, что критически важно, обратный масштабный фактор или глубину наблюдаемых точек.

$$x=[p,v,q,b_a,b_g,\lambda]$$

где λ – параметр, связанный с масштабом или глубиной точек.

Ключевым преимуществом интеграции IMU с монокулярной камерой является возможность восстановления абсолютного масштаба траектории. Акселерометр измеряет ускорение в физических единицах (m/s^2). Сравнивая величину ускорения с показаниями акселерометра, фильтр может оценить масштабный коэффициент s [8].

Процесс инициализации VIO-системы является критическим этапом, который требует от БПЛА выполнение определенных маневров. Данный фактор приводит к затруднению оценки масштабов [8].

Не менее важной проблемой является синхронизация сенсоров, поскольку камеры и IMU часто имеют разные частоты.

Реализация VIO на борту легкого БПЛА ограничена вычислительными ресурсами, так как использование полноценных алгоритмов SLAM, часто избыточно. Поэтому на практике чаще применяются алгоритмы визуальной одометрии без сохранения глобальной карты, либо с использованием локальных карт небольшого размера.

Для снижения нагрузки на процессор применяются методы оптимизации. Это позволяет сохранять точность оценки текущих параметров. Также перспективным направлением является использование нейросетевых подходов которые могут работать эффективнее традиционных геометрических методов, интегрированных в современные бортовые компьютеры.

Гибридные системы навигации, сочетающие визуальную одометрию и инерциальные измерения, представляют собой наиболее перспективное решение для обеспечения автономности БПЛА в условиях отказа GNSS.

Список литературы

1. Чан Ю., Чэн Ю., Манзур У., Мюррей Дж. Обзор автономной навигации БПЛА в условиях отсутствия GPS // Робототехника и автономные системы. – 2023. – №1, том 170. – С. 28–40, DOI: 10.1016/j.robot.2023.104533.
2. Хан М.К., Улла А. Влияние интернета вещей и его воздействие на библиотечные услуги: обзор // Инверж-журнал социальных наук. – 2024. – №2, том 3. – С. 63–72, DOI: 10.63544/ijss.v3i2.94.
3. Али Б., Садеков Р.Н., Цодокова В.В. алгоритмы навигации беспилотных летательных аппаратов с использованием систем технического зрения // Гироскопия и навигация. - 2022. - №4 (119), том 30. - С. 87-105, DOI: 10.17285/0869-7035.00105.
4. Ли Дж.Ч., Чэнь Ч.Ч., Шэнь Ч.Т., Лай Ю.Ч. Оценка масштаба на основе ориентиров и коррекция визуально-инерциальной одометрии для БПЛА вертикального взлёта и посадки в условиях отсутствия GPS // Сенсоры. – 2022. – №24, том 22. – С. 9654, DOI: 10.3390/s22249654.
5. Бывших Д.М., Зеленская С.Г., Перцев Ю.А. Оценка состояния научно-технического и технологического задела для создания комплексов радиоэлектронной борьбы // Моделирование систем и процессов. - 2025. - №3, том 18. - С. 28-40, DOI: 10.12737/2219-0767-2025-18-3-28-40.
6. Корсаков М.П., Гончарова Е.В., Курносов И.А., Замараев И.В. Обзор методов визуальной навигации и алгоритмов планирования пути для беспилотных летательных аппаратов // Главный механик. - 2024. - №6 (250), том 21. - С. 25-33.
7. Степанов Д. Н. Методики сопоставления особых точек в задаче визуальной навигации БПЛА // Вестник Южно-Уральского государственного университета. Серия «Вычислительная математика и информатика». 2015. Т. 4, № 4. С. 32–47.
8. Джарра И., Аль-Батати А., Кадри М.Б., Абделькадер М., Аммар А., Булила У., Кубаа А. Навигация беспилотных летательных аппаратов в условиях отсутствия GNSS: анализ вычислительной сложности, слияния сенсорных данных и методов локализации // Спутниковая навигация. – 2025. – №1, том 6. – С. 9, DOI: 10.1186/s43020-025-00162-z.

References

1. Chang Y., Cheng Y., Manzoor U., Murray J. A Review of UAV Autonomous Navigation in GPS-Denied Environments // *Robotics and Autonomous Systems*. – 2023. – No. 1, Vol. 170. – P. 28–40, DOI: 10.1016/j.robot.2023.104533.
2. Khan M.K., Ullah A. Implication of IoT and Its Impact on Library Services: An Overview // *Inverge Journal of Social Sciences*. – 2024. – No. 2, Vol. 3. – P. 63–72, DOI: 10.63544/ijss.v3i2.94.
3. Lee J.Ch., Chen Ch.Ch., Shen Ch.Te., Lai Y.Ch. Landmark-Based Scale Estimation and Correction of Visual Inertial Odometry for VTOL UAVs in a GPS-Denied Environment // *Sensors*. – 2022. – No. 24, Vol. 22. – P. 9654, DOI: 10.3390/s22249654.
4. Ali B., Sadekov R.N., Tsodokova V.V. Algorithms for Navigation of Unmanned Aerial Vehicles Using Computer Vision Systems // *Gyroscopy and Navigation*. – 2022. – No. 4 (119), Vol. 30. – P. 87–105, DOI: 10.17285/0869-7035.00105.
5. Byvykh D.M., Zelenskaya S.G., Pertsev Yu.A. Assessment of the Scientific, Technical and Technological Readiness Level for the Development of Electronic Warfare Systems // *Modeling of Systems and Processes*. – 2025. – No. 3, Vol. 18. – P. 28–40, DOI: 10.12737/2219-0767-2025-18-3-28-40.
6. Korsakov M.P., Goncharova E.V., Kurnosov I.A., Zamaraev I.V. Review of Visual Navigation Methods and Path Planning Algorithms for Unmanned Aerial Vehicles // *Chief Mechanic*. – 2024. – No. 6 (250), Vol. 21. – P. 25–33.
7. Stepanov D.N. Methods of Matching Key Points in the Problem of Visual Navigation of UAVs // *Bulletin of South Ural State University. Series "Computational Mathematics and Informatics"*. – 2015. – Vol. 4, No. 4. – P. 32–47.
8. Jarraya I., Al-batati A., Kadri M.B., Abdelkader M., Ammar A., Boulila W., Koubaa A. GNSS-Denied Unmanned Aerial Vehicle Navigation: Analyzing Computational Complexity, Sensor Fusion, and Localization Methodologies // *Satellite Navigation*. – 2025. – No. 1, Vol. 6. – P. 9, DOI: 10.1186/s43020-025-00162-z.

ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПОВСЕДНЕВНУЮ ЖИЗНЬ

Дж. Рахман¹, А.В. Акименко¹

¹ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»

Аннотация. В этой статье рассматривается, как искусственный интеллект (ИИ) в настоящее время влияет на повседневную жизнь обычных людей. В ней рассматриваются основные области, где ИИ используется здравоохранение, образование, транспорт, шопинг, дом и рабочее место. В статье рассматриваются как новые возможности, которые предоставляет ИИ, так и проблемы, которые он создает, такие как проблемы конфиденциальности, этические проблемы, угрозы рабочим местам и цифровой разрыв.

Ключевые слова: искусственный интеллект, машинное обучение, автоматизация, умный дом, здравоохранение, цифровое неравенство, конфиденциальность, будущее труда.

THE IMPACT OF AI ON EVERYDAY LIFE

J. Rahman¹, A.V. Akimenko¹

¹Voronezh State University of Forestry and Technologies named after G.F. Morozov

Abstract this article looks at how artificial intelligence (AI) now shapes the daily lives of ordinary people. It reviews the main areas where AI is used health care, education, transport, shopping, the home, and the workplace. The paper discusses both the new opportunities that AI provides and the problems that it creates, such as concerns about privacy, ethical issues, threats to jobs and the digital divide.

Keywords: Artificial intelligence, machine learning, automation, smart home, healthcare, digital inequality, privacy, future of work.

Artificial intelligence is no longer something you only meet in science fiction or inside a few elite research labs. In just a few decades it has moved out of computing theory and into the fabric of ordinary life. Most of us deal with AI dozens of times a

day without even noticing. The film a streaming service suggests, the voice assistant that sets a morning alarm, the program that approves or blocks a card payment, the map app that reroutes you around traffic all of these run on the same basic family of technologies.

The size of this change shows up in the economic numbers. The McKinsey Global Institute expects AI to add as much as \$13 trillion to the world economy by 2030, with the biggest gains in the areas that touch people most directly: health care, education, shopping, and transport [1]. Yet because AI is spreading so fast, it also creates problems that societies are only beginning to understand problems tied to privacy, jobs, fairness, and who actually gets to share in the benefits.

This article gives a broad picture of how AI is reshaping everyday life across several key areas. It examines the application of AI's power, the benefits of AI, the perils of AI, and the social consequences of its ongoing development. Understanding all of this matters not just for engineers and policymakers, but for everyone who has to find their way in a world increasingly run through.

Machine-learning programs that read medical images can already match, and sometimes beat, experienced doctors at certain tasks. Google DeepMind's system for spotting eye disease, for instance, was able to pick out more than 50 eye conditions from retinal scans about as accurately as the world's top specialists [2]. Similar progress has been made in finding skin cancers, lung nodules, and heart problems.

AI is also changing how patients handle long-term illness at home. Continuous glucose monitors paired with machine-learning models can warn diabetic patients about a coming low-blood-sugar episode before they feel any symptoms, so they can act early. Wearable ECG devices, now sold as ordinary consumer gadgets, use built-in AI to detect atrial fibrillation a major cause of stroke and tell the wearer to see a doctor. Tools like these bring clinical-grade monitoring into the home, ease the load on hospitals, and let patients take a more active part in their own care.

Research into new medicines is speeding up too. During the COVID-19 pandemic, machine-learning tools sorted through billions of molecules to find ones that might fight the virus work that would have taken decades by older methods. DeepMind's AlphaFold cracked the protein-folding problem that had blocked biologists for fifty years, opening new doors for drugs against everything from Alzheimer's to antibiotic-resistant infections [3]. Turning these findings into approved treatments still takes years, but the way AI shortens the research timeline marks a real change in how fast humanity can fight disease.

Fresh Challenges and Personalised Learning Another area where AI is starting to change daily life for millions of people is education.

The usual classroom teaches one lesson to many students at once, so by its very design it can't fully match the different speeds, styles, and needs of each learner. AI-powered adaptive learning platforms offer a partial fix for this old problem. Tools such as Khan Academy's AI tutor, or the commercial systems used in universities, keep checking how a student is doing and adjust the difficulty, pace, and format to fit that person [4].

Early results from controlled studies suggest that personal, AI-driven teaching really can improve learning, especially for students who are struggling or can't afford a private tutor. Where trained teachers are scarce which is true across much of the developing world AI learning tools could help close serious gaps in access to good teaching.

Transport is one of the most visible places where AI shows up in daily life. Navigation apps such as Google Maps and Yandex Navigator have already made it normal to get real-time, AI-optimized directions that take live traffic, accidents, and expected travel times into account. These apps crunch huge streams of data from millions of users at once to suggest routes that, together, cut congestion and travel times across whole cities [5].

The boldest use of AI in transport is the self-driving car. Companies like Waymo, Tesla, and many others have poured billions into building cars and trucks that can handle busy roads without a driver. Fully autonomous vehicles promise big safety gains human error is behind roughly 94% of serious road crashes in the United States along with smoother traffic and lower fuel use. By 2024, limited commercial robotaxi services were running in several cities, the first real-world rollout of Level 4 self-driving at a meaningful scale [6].

AI is reaching into city infrastructure as well. Smart traffic systems use computer vision and prediction to change signal timings on the fly, cutting idling and pollution. In public transport, AI predicts when equipment will need repair before it breaks down, which improves reliability and safety. In logistics, AI steers goods through incredibly complex networks, making possible the fast deliveries that online shoppers now expect.

In shopping and commerce, AI has quietly become the backbone of the consumer economy. Recommendation engines the algorithms that pick the next video, product, or song for you are among the most commercially important AI tools around. Amazon reckons that about 35% of its sales come from its recommendation system, which uses

collaborative filtering and deep learning to guess what each customer wants with striking accuracy [6]. Streaming services like Netflix and Spotify lean on the same kind of AI personalization to keep users watching and listening.

These systems matter beyond mere convenience. By choosing and pushing content that fits each person's taste, recommendation algorithms shape the information, entertainment, and ideas people run into. Critics warn that this can create «filter bubbles», where users are slowly cut off from views and content unlike their own something that could seriously affect public debate and how a society holds together. Designing recommendation systems that serve people's wellbeing instead of just maximizing screen time is one of the hardest problems in tech ethics today.

AI has crept into everyday life inside the home through smart speakers, connected appliances and home automation. Devices like Amazon Echo and Google Nest answer voice commands, control lights and heating, play music, set reminders, and order groceries.

The link between AI and jobs may be the most important and most argued-over part of the technology's effect on everyday life. Today's AI, driven mainly by large language models and advanced robotics, has widened automation well beyond the manual and routine office tasks that earlier waves touched. Systems that can draft legal papers, write software code, produce marketing text, analyze financial data, and handle customer service are now used at scale across many industries [6].

Research on what this means for jobs paints a mixed picture. A major McKinsey Global Institute study estimated that by 2030 somewhere between 75 and 375 million workers worldwide up to 14% of the global workforce may have to switch occupations because of automation. A 2023 Goldman Sachs study reckoned that generative AI alone could automate work equal to 300 million full-time jobs, while also creating new kinds of work. History suggests that lost jobs are usually replaced by new ones, but the speed of today's shift and the way it reaches into skilled, white-collar professions makes it different from past waves.

In practice, many people already treat AI as a day-to-day helper rather than a rival. AI tools boost the work of radiologists, lawyers, software engineers, and financial analysts, letting them work faster and handle more. The rise of “prompt engineering” the skill of writing good instructions for AI shows how new kinds of human expertise grow up alongside new technology. Reshaping education and job training so people can thrive in this human AI partnership is one of the defining policy challenges of our time.

As AI seeps into everyday life, it raises basic questions about privacy, freedom, and power. AI gets its abilities from data enormous amounts of it, taken from every digital action we make. Commercial AI continuously collects and processes personal data, creating an imbalance of information and power between tech companies and the people whose data they use. Laws like the EU's General Data Protection Regulation (GDPR) and the proposed EU AI Act try to address this imbalance by establishing rights and duties, but enforcement is challenging and the law continues to trail the technology.

Facial recognition shows the clash between AI's power and civil liberties especially sharply. Being able to identify people in public in real time, using cameras hooked to AI, has real value for policing and security. It also makes possible kinds of surveillance that clash with the expectation of anonymity in public that many ideas of freedom rest on. Several big cities, including San Francisco and Boston, have banned government use of facial recognition, showing how seriously democratic societies take these worries. In Russia, Federal Law No. 149-FZ on Information and its later amendments increasingly cover the use of biometric data, setting rules for consent and data security.

Artificial intelligence has gone from a narrow research topic to a constant presence in everyday life, changing how people get health care, learn, travel, shop, work, and live at home. Its benefits are real and large: earlier detection of disease, more personal education, safer travel, more efficient commerce, and stronger professional abilities. These are genuine improvements in human life and deserve credit alongside the challenges AI brings.

But at the same time, the embedding of AI into everyday life poses serious risks and ethical tangles that cannot be brushed aside or put off. Engineers, lawmakers, civil society and ordinary citizens all need to be actively mindful of privacy, algorithmic bias, job disruption and the digital divide. As history shows, the true impact of a powerful new technology is less a function of the technology itself than of the social, legal, and institutional rules that govern its use. So the job of this generation is not just to build AI faster, but to govern its use wisely.

That means strong rules, protecting basic rights while enabling useful innovation, investment in public education and job retraining, and a strong commitment to spreading the gains of AI fairly across society. AI is not a destiny we have to accept without question it is a set of tools whose impacts are shaped by the choices people, organisations and governments make about how they are built, used and limited.

As AI becomes more powerful and more embedded in the infrastructure of everyday life, the decisions we make today about how to govern it will determine whether AI becomes a driver of broadly shared human flourishing or a vehicle for power consolidation and deepening inequality. One of the defining tasks of the twenty-first century is to take this challenge seriously.

Список литературы

1. Ли Ч.С., Ли А.Ю. Клиническое применение машинного обучения с непрерывным обучением // The Lancet Digital Health. — 2020. — № 6, том 2. — С. e279–e281. DOI: 10.1016/s2589-7500(20)30102-3.
2. Баджорат Дж. Искусственный интеллект в междисциплинарных исследованиях в области наук о жизни и поиске новых лекарственных средств // Future Science OA. — 2022. — № 4, том 8. — DOI: 10.2144/fsoa-2022-0010.
3. Аникеев Е.А. Структура и применение автоматизированной системы мониторинга пассажиропотока // Моделирование систем и процессов. — 2021. — № 3, том 14. — С. 4–11. DOI: 10.12737/2219-0767-2021-14-3-4-11.
4. Победа С.А., Черных М.И., Макаренко Ф.В., Зольников К.В. Создание поведенческой модели LDMOS транзистора на основе искусственной MLP нейросети и ее описание на языке Verilog-A // Моделирование систем и процессов. — 2021. — № 2, том 14. — С. 28–34. DOI: 10.12737/2219-0767-2021-14-2-28-34.
5. Киреева К.А., Коробова Л.А., Арапов Д.В. Разработка искусственной нейронной сети для классификации ЭКГ // Моделирование систем и процессов. — 2023. — № 3, том 16. — С. 42–54. DOI: 10.12737/2219-0767-2023-16-3-42-54.
6. Мальцев В.В. Применение алгоритмов искусственного интеллекта для мониторинга загрязнения воздуха городским автотранспортом // Моделирование систем и процессов. — 2025. — № 2, том 18. — С. 86–96. DOI: 10.12737/2219-0767-2025-18-2-86-96.

References

1. Lee C.S., Lee A.Y. Clinical Applications of Continual Learning Machine Learning // *The Lancet Digital Health*. — 2020. — No. 6, Vol. 2. — P. e279–e281. DOI: 10.1016/s2589-7500(20)30102-3.
2. Bajorath J. Artificial Intelligence in Interdisciplinary Life Science and Drug Discovery Research // *Future Science OA*. — 2022. — No. 4, Vol. 8. — DOI: 10.2144/fsoa-2022-0010.
3. Anikeev E.A. Structure and Application of an Automated Passenger Flow Monitoring System // *Modeling of Systems and Processes*. — 2021. — No. 3, Vol. 14. — P. 4–11. DOI: 10.12737/2219-0767-2021-14-3-4-11.
4. Pobeda S.A., Chernykh M.I., Makarenko F.V., Zolnikov K.V. Creation of a Behavioral Model of an LDMOS Transistor Based on an Artificial MLP Neural Network and Its Description in Verilog-A Language // *Modeling of Systems and Processes*. — 2021. — No. 2, Vol. 14. — P. 28–34. DOI: 10.12737/2219-0767-2021-14-2-28-34.
5. Kireeva K.A., Korobova L.A., Arapov D.V. Development of an Artificial Neural Network for ECG Classification // *Modeling of Systems and Processes*. — 2023. — No. 3, Vol. 16. — P. 42–54. DOI: 10.12737/2219-0767-2023-16-3-42-54.
6. Maltsev V.V. Application of Artificial Intelligence Algorithms for Monitoring Air Pollution by Urban Vehicles // *Modeling of Systems and Processes*. — 2025. — No. 2, Vol. 18. — P. 86–96. DOI: 10.12737/2219-0767-2025-18-2-86-96.

Научное издание

ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ:
ОТ ТЕОРИИ К ПРАКТИКЕ – 2026

Материалы Международной научно-практической конференции

Воронеж, 02 июля 2026 г.

Ответственные редакторы В.К. Зольников, И.Н. Занин

Материалы издаются в авторской редакции

Подписано к изданию 05.10.2026. Объем данных 1,52 Мб
ФГБОУ ВО «Воронежский государственный лесотехнический университет
имени Г.Ф. Морозова»
394087, г. Воронеж, ул. Тимирязева, 8