

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет геосистем и технологий»
(СГУГиТ)

ИНТЕРЭКСПО ГЕО-СИБИРЬ

XXI Международный научный конгресс

Сборник материалов в 8 т.

Т. 7

Научно-технологическая конференция
молодых ученых

«МОЛОДЕЖЬ. ИННОВАЦИИ. ТЕХНОЛОГИИ»

№ 3

Новосибирск
СГУГиТ
2025

Ответственные за выпуск:

Кандидат технических наук, доцент, зав. кафедрой прикладной информатики
и информационных систем СГУГиТ, Новосибирск

Т. Ю. Бугакова

Кандидат технических наук, доцент, зав. кафедрой фотоники
и приборостроения СГУГиТ, Новосибирск

Д. М. Никулин

Кандидат технических наук, доцент кафедры кадастра
территориального планирования, СГУГиТ, Новосибирск

А. В. Ершов

С26 Интерэкспо ГЕО-Сибирь. XXI Международный научный конгресс,
21–22 мая 2025 г., Новосибирск : сборник материалов в 8 т. Т. 7: Научно-
технологическая конференция молодых ученых «Молодежь. Инновации.
Технологии». – Новосибирск : СГУГиТ, 2025. № 3. – 261 с. – ISSN 2618-
981X. – Текст : непосредственный.

В сборнике опубликованы материалы XXI Международного научного конгресса
«Интерэкспо ГЕО-Сибирь», представленные на Научно-технологической конференции
«Молодежь. Инновации. Технологии».

Печатается по решению редакционно-издательского совета СГУГиТ

Материалы публикуются в авторской редакции

Издание может содержать сведения об иностранных агентах

В. Ю. Сапегин¹✉

Метод обнаружения маскировки сетевого трафика

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: gvlad224@gmail.com

Аннотация. В работе исследуются современные методы и принципы, используемые для сокрытия сетевого трафика в корпоративных вычислительных сетях, функционирующих на основе стека протоколов TCP/IP версий 4 и 6, а также техники их идентификации в реальном времени. В рамках исследования разработан новый подход к детектированию зашифрованных и замаскированных VPN-каналов, основанный на комбинации анализа независимых компонент (ICA) и ансамблевого машинного обучения, включающего алгоритмы градиентного бустинга и случайного леса. В ходе исследования был разработан экспериментальный стенд, развернутый с использованием системы автоматизированного управления конфигурацией Ansible, что обеспечило высокую воспроизводимость тестовых испытаний. На базе созданного стенда сформирован специализированный датасет, включающий как валидный сетевой трафик, так и трафик виртуальных защищенных каналов в условиях их маскировки, что позволило провести комплексную валидацию предложенного метода обнаружения. Проведенные тесты подтвердили высокую результативность предложенного решения, показав его преимущества в точности и скорости обнаружения скрытых соединений, что способствует оперативному реагированию на угрозы в корпоративных сетях. Ключевым фактором повышения эффективности стало применение метода ICA и отбор признаков объектов классификации, обеспечивающей более надежное выявление аномалий в реальных условиях. Полученные результаты могут быть использованы при создании и оптимизации систем защиты данных, а также при разработке механизмов фильтрации и мониторинга сетевой активности.

Ключевые слова: технологии маскировки, виртуальные защищенные каналы, VPN, стек протоколов TCP/IP, классификация информационных потоков, методы обнаружения VPN

V. Yu. Sapegin¹✉

Method for detecting network traffic obfuscation

¹National Research Nuclear University «MEPhI» (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: gvlad224@gmail.com

Abstract. This study examines modern methods and principles used to conceal network traffic in corporate computer networks operating on TCP/IP protocol stacks (versions 4 and 6), as well as techniques for their real-time identification. As part of the research, a novel approach for detecting encrypted and obfuscated VPN channels was developed, based on a combination of independent component analysis (ICA) and ensemble machine learning, including gradient boosting and random forest algorithms. An experimental testbed was designed and deployed using the Ansible automated configuration management system, ensuring high reproducibility of test trials. A specialized dataset was compiled using this testbed, containing both legitimate network traffic and traffic from obfuscated secure virtual channels, enabling comprehensive validation of the proposed detection method. The conducted tests confirmed the high efficacy of the proposed solution, demonstrating its advantages in accuracy and speed of detecting covert connections, thereby facilitating prompt threat response in

corporate networks. A key factor in improving detection efficiency was the application of ICA and feature selection for classification objects, ensuring more reliable anomaly detection in real-world conditions. The obtained results can be utilized in the development and optimization of data protection systems, as well as in designing network activity filtering and monitoring mechanisms.

Keywords: obfuscation techniques, virtual secure channels, VPN, TCP/IP protocol stack, traffic flow classification, VPN detection methods

Введение

В эпоху цифровой трансформации вопросы обеспечения информационной безопасности корпоративных сетей выходят на первый план. Парадоксальным образом, технологии сокрытия сетевой активности, изначально разработанные для защиты конфиденциальности, одновременно создают существенные риски для информационной инфраструктуры. Их способность эффективно маскировать передаваемые данные делает их одинаково востребованными как в легитимных целях защиты информации, так и для организации скрытых каналов передачи данных в кибератаках.

Данное противоречие особенно актуально в свете современных тенденций к усилению защиты персональных данных и одновременного ужесточения требований к мониторингу сетевой активности. Представленное исследование направлено на комплексный анализ современных механизмов маскировки трафика в IPv4/IPv6-сетях с разработкой инновационного подхода к идентификации скрытых Virtual Private Network (VPN) соединений в корпоративных сетевых инфраструктурах. Так, согласно данным исследования F.A.C.C.T. [1], в 2023 году наблюдалась устойчивая тенденция к использованию VPN-технологий при организации целевых атак на корпоративные сети Российской Федерации. Данный факт объясняется фундаментальной способностью виртуальных частных сетей к имитации легитимного сетевого трафика, что существенно осложняет процесс своевременного обнаружения вредоносной активности. Таким образом особое внимание уделяется методам, позволяющим эффективно дифференцировать легитимное использование технологий защиты трафика от их злонамеренного применения.

Современные научные группы предлагают различные подходы к решению указанной проблемы. В работах Wu Н. и соавторов [2, 3] рассматриваются перспективные методы нейросетевой классификации трафика, демонстрирующие высокую эффективность при детекции сложных протоколов, включая V2Ray и Shadowsocks. Однако практическая реализация данных методов сталкивается с существенными вычислительными затратами, что ограничивает их применение в реальных корпоративных сетях.

В исследованиях Канатьева К. Н. и соавторов [4, 5] проводится системный анализ современных методов обнаружения виртуальных защищенных каналов связи. Авторы акцентируют внимание на принципиальных ограничениях существующих методов детекции, обусловленных постоянным совершенствованием технологий маскировки трафика. В своих работах они обосновывают необходимость разработки новых аналитических подходов, способных адаптироваться к

эволюции методов обхода защиты. Особое внимание уделяется перспективам создания комплексных систем мониторинга, сочетающих различные методы анализа сетевой активности.

Особое место в исследованиях занимают работы научной школы «Сетевая информационная безопасность» под руководством Басыни Е. А. [6–8], посвященные анализу оверлейных сетей типа Tor и I2P. В работах детально исследуются механизмы обхода фильтрации, применяемые в рассматриваемых протоколах, а также разрабатываются методы их детекции на основе анализа параметров и характеристик сетевого трафика. Эти исследования имеют особую ценность в контексте постоянного совершенствования технологий анонимизации и соответствующих методов противодействия.

Эволюция технологий сокрытия сетевой активности оказывает существенное влияние на формирование правового поля в сфере информационной безопасности. Ярким примером такого регулирования является изданный Роскомнадзором Приказ № 168 от 08.11.2023 Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций «О внесении изменений в Критерии оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 февраля 2023 г. N 25» от 08.11.2023 № 168, который предписывает создание Единого реестра VPN- и прокси-сервисов. Данная мера обусловлена способностью этих технологий обходить установленные ограничения доступа к ресурсам с запрещенным контентом. Принятие подобных нормативных актов подчеркивает острую необходимость в разработке эффективных методов обнаружения маскированного трафика и предотвращения его использования для обхода систем фильтрации. Особую значимость приобретают решения, позволяющие осуществлять мониторинг VPN-соединений в корпоративных сетях без нарушения требований к защите персональных данных. Реализация таких мер требует комплексного подхода, сочетающего технические решения с учетом постоянно меняющегося законодательного ландшафта в области информационной безопасности.

Постановка задачи

Целью настоящей работы является разработка нового метода выявления замаскированных сетевых потоков виртуальных защищенных каналов связи в

корпоративной вычислительной сети, функционирующей на базе стека протоколов TCP/IP версии 4 и версии 6.

Результаты работы

В рамках исследования создана комплексная тестовая инфраструктура (рис. 1) для анализа методов обнаружения виртуальных защищенных каналов связи. Архитектура стенда включает: клиентские устройства на платформах iOS (FoXray), Android (V2RayNG), Windows и Linux (Xray-core [9]); VPN-серверы в Японии и Польше для моделирования реальных сетевых задержек; а также коммутационное оборудование и межсетевой экран для захвата трафика. В качестве тестового окружения использовалось решение Xray с поддержкой протоколов VLESS-reality, VLESS-vision и VLESS-mkcp, обеспечивающих продвинутую маскировку трафика под стандартные TLS/DTLS-соединения.

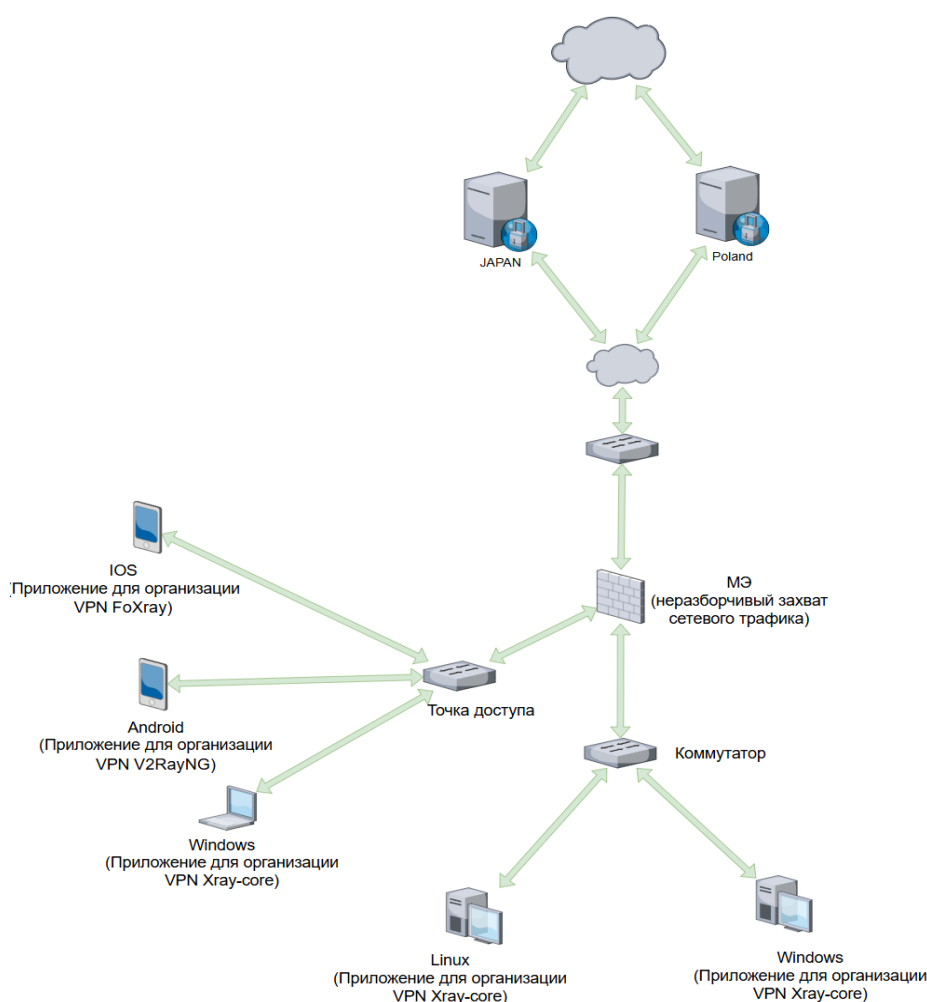


Рис. 1. Топология сети виртуального лабораторного стенда

Стенд обеспечивает генерацию зашифрованного трафика с различных платформ, его маршрутизацию через коммутатор и захват пакетов межсетевым экраном для последующего анализа. Автоматизированное развертывание стенда, при

помощи системы управления конфигурацией Ansible, гарантирует воспроизводимость результатов. Конфигурация оборудования позволяет оценивать эффективность методов обнаружения ВЗКС в условиях, приближенных к реальным, включая анализ устойчивости к современным технологиям маскировки трафика и влияние сетевых задержек на качество детектирования.

В ходе работы был разработан метод обнаружения (рис. 2). Предложенный метод реализует трехуровневый конвейер обработки данных, начиная со сбора сетевого трафика (DataCollectionTask). Первый этап (DataProcessing) включает параллельное выполнение двух ключевых операций: фильтрацию данных (DataFilteringTask) для устранения шума и нормализации, и извлечение признаков (FeatureExtractionTask) таких как временные метки и размеры пакетов.

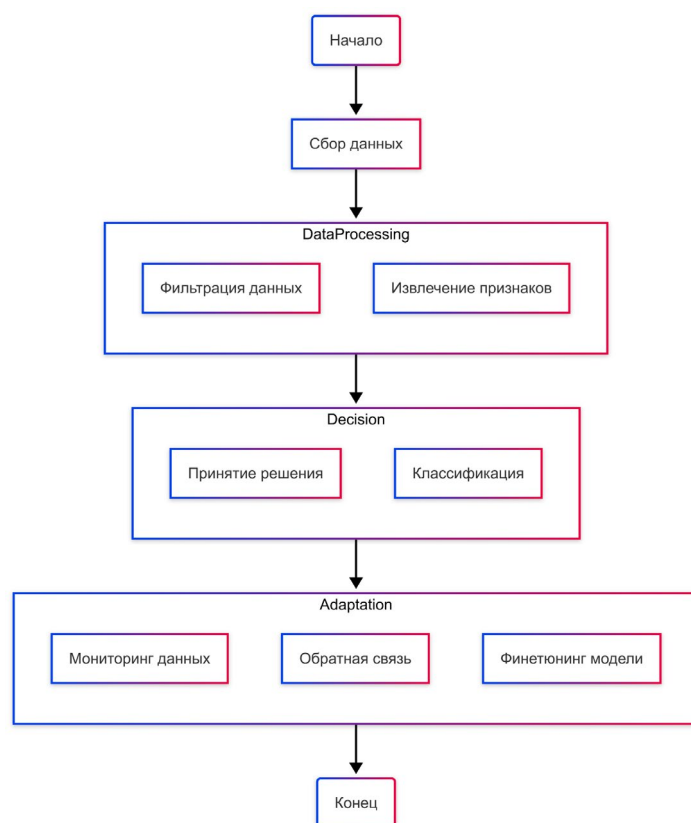


Рис. 2. Высокоуровневый метод обнаружения виртуальных защищенных каналов связи в условиях маскировки

Обработанные данные поступают на этап принятия решений (Decision), где сначала выполняется классификация трафика (ClassifierTask) с использованием современных ML-алгоритмов, а затем формируется итоговое решение (Decision-MakingTask) о характере сетевой активности. Финальный адаптационный этап (Adaptation) обеспечивает непрерывное совершенствование системы через мониторинг данных (DataMonitoringTask), анализ ошибок (FeedbackLoopTask) и тонкую настройку модели (ModelFinetuningTask), создавая замкнутый цикл самообучения системы.

На основе разработанного метода и экспериментального стенда был произведен сбор репрезентативного набора данных, включающего как обычный легитимный сетевой трафик, так и замаскированные VPN-соединения. Полученная выборка охватывает широкий спектр сценариев передачи данных, что создает надежную основу для валидации алгоритмов детектирования.

Для анализа сетевых потоков были выделены ключевые временные и пространственные характеристики сетевого трафика:

- `interpacket_interval` – временные интервалы между последовательными пакетами;
- `packet_length` - размеры отдельных пакетов в порядке их передачи;
- `packet_number_per_<time>` – количество пакетов в заданных временных интервалах (характеризуют плотность сетевых потоков);
- `<aggregate_func>interpacket_interval_per<time>` – агрегированные значения временных интервалов (среднее, медиана и др.);
- `<aggregate_func>packet_length_per<time>` – статистические показатели размеров пакетов в временных окнах.

Метод извлечения признаков реализует принцип скользящего анализа, аналогичный алгоритму скользящего среднего. Такой подход обеспечивает:

- эффективное подавление сетевого шума;
- точное описание мультиплексированных соединений;
- выявление паттернов маскировки в зашифрованных потоках.

Методология извлечения признаков позволяет детектировать даже сложные случаи обфускации трафика, сохраняя высокую чувствительность к аномальным сетевым активностям.

В процессе разработки модели был выполнен комплексный feature engineering, позволивший идентифицировать наиболее информативные признаки для классификации сетевых потоков (рис. 3).

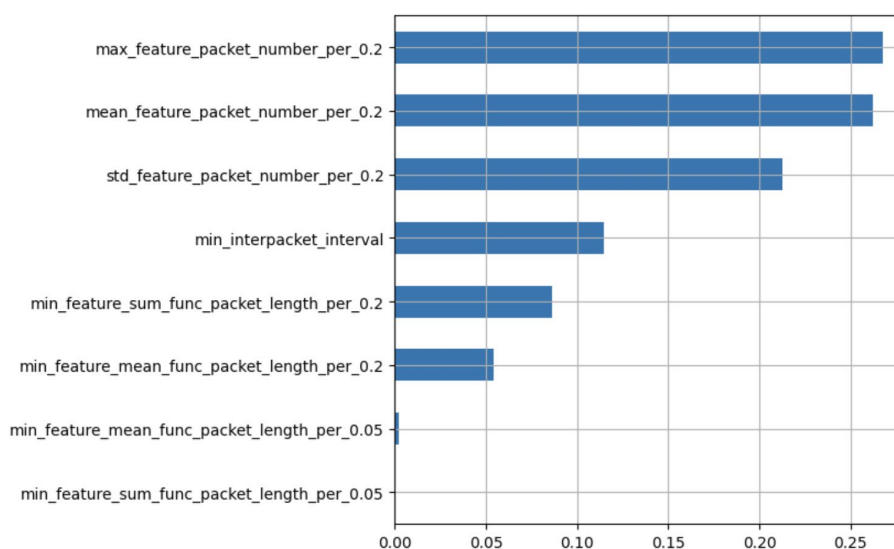


Рис. 3. Сравнительная диаграмма значимости сетевых признаков для задачи классификации VPN и Non-VPN сетевых потоков

Анализ значимости признаков выявил, что ключевую роль в детекции играют агрегированные статистические характеристики, в частности `<aggregate_func>packet_length_per<time>` и `packet_number_per_<time>`.

Эти признаки демонстрируют наибольшую дискриминативную способность, что объясняется их устойчивостью к шуму и способностью отражать фундаментальные различия в паттернах легитимного и замаскированного трафика. Их высокая значимость подтверждает гипотезу о том, что временные и размерные характеристики потока содержат наиболее релевантную информацию для задач идентификации VPN-туннелей.

Отбор этих признаков позволил оптимизировать модели классификации сетевых потоков, при этом сохранив высокую точность классификации при сокращении размерности feature space.

Выявленные высокосignимые признаки были использованы в комбинации с методом анализа независимых компонент (ICA), что позволило существенно улучшить качество классификации (рис. 4). ICA продемонстрировал исключительную эффективность в выделении статистически независимых компонент, которые максимально разделяют VPN и Non-VPN трафик в признаковом пространстве. Это связано со способностью ICA:

- 1) выделять скрытые факторы, лежащие в основе наблюдаемых параметров трафика;
- 2) устранять корреляции между признаками;
- 3) усиливать различия в фундаментальных характеристиках потоков.

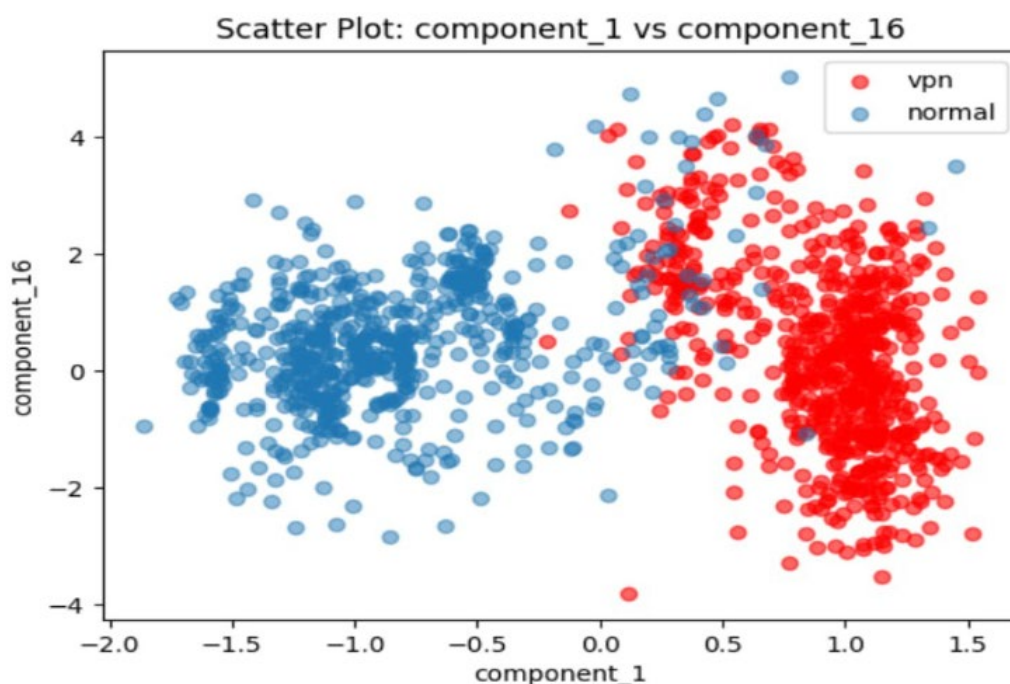


Рис. 4. Диаграмма рассеивания сетевых потоков относительно двух выделенных

Полученные независимые компоненты были использованы в качестве входных данных для ансамблевых алгоритмов (XGBoost и Random Forest), что привело к значительному улучшению показателей классификации (рис. 5).

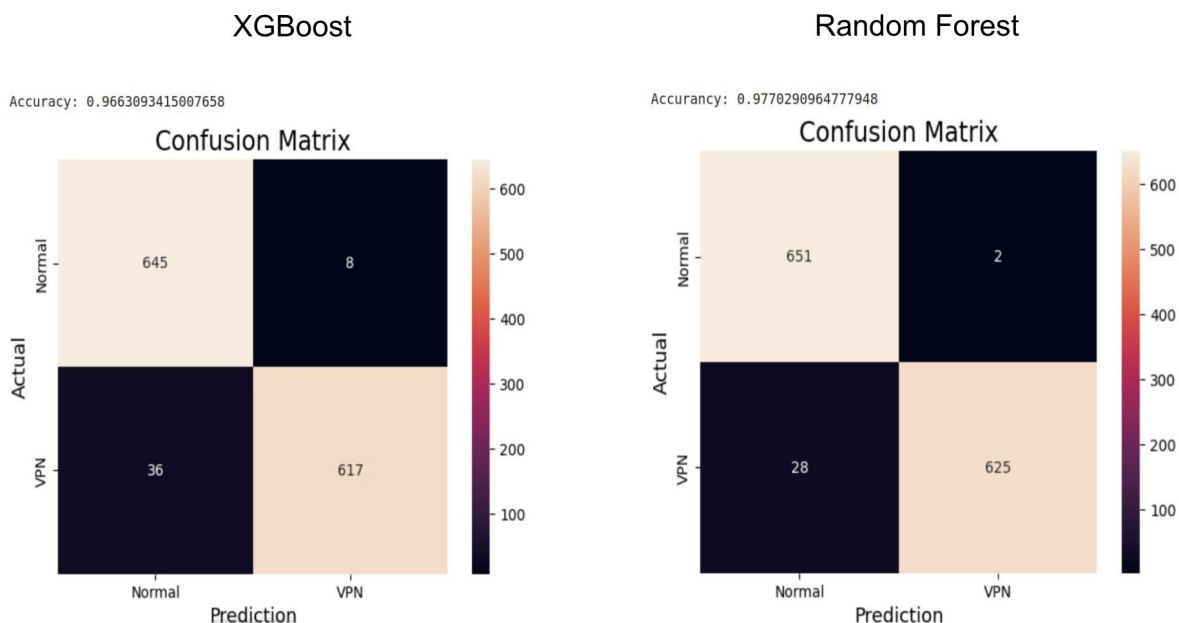


Рис. 5. Матрица ошибок классификации XGBoost и RandomForest в связке с методом ICA

Результаты подтверждают, что комбинация ICA с современными методами машинного обучения образует мощный инструмент для анализа сетевого трафика, особенно эффективный против современных технологий обфускации.

Заключение

В данной работе представлен комплексный анализ современных технологий сокрытия сетевой активности в инфраструктурах IPv4 и IPv6. Исследование включает детальное изучение принципов работы различных методов маскировки трафика, их классификацию по степени эффективности и способам противодействия системам обнаружения. Для экспериментальной проверки был развернут виртуальный лабораторный стенд, позволяющий моделировать реальные условия работы корпоративных сетей.

В ходе работы сформирован уникальный датасет, содержащий как легитимный, так и замаскированный сетевой трафик. Применение методов feature engineering позволило выделить наиболее значимые характеристики потоков данных, среди которых особую информативность показали временные и объемные параметры передачи пакетов. Использование анализа независимых компонент (ICA) продемонстрировало высокую эффективность в разделении VPN и Non-VPN трафика, что подтверждается результатами классификации с точностью 0,966 при использовании ансамблевых методов машинного обучения.

Полученные результаты имеют существенное значение для развития систем информационной безопасности. Разработанный метод может служить основой для создания эффективных решений по обнаружению и блокировке скрытых каналов передачи данных в корпоративных сетях. Особую ценность представляет адаптивность предложенного подхода, позволяющая противодействовать постоянно эволюционирующим технологиям маскировки трафика в современных сетевых инфраструктурах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Universal Encryptor: The number of cyberattacks in Russia increased by 140% in 2023 // F.A.C.C.T. URL: <https://www.facct.ru/media-center/press-releases/cyberattacks-2023/> (accessed: 21.04.2024).
2. Wu H. et al. Real-time identification of VPN traffic based on counting Bloom filter and chained hash table from sampled data in high-speed networks // ICC 2022-IEEE International Conference on Communications. – IEEE, 2022. – P. 5070-5075.
3. Wu H. et al. RT-CBCH: Real-time VPN Traffic Service Identification based on Sampled Data in High-speed Networks // IEEE Transactions on Network and Service Management. – 2023.
4. Обзор методов обнаружения VPN и DNS-анализ для классификации на примере Hotspot Shield Free / К. Н. Канатъев, С. Р. Шишкин, И. И. Басыров [и др.] // Инновации и инвестиции. – 2023. – № 10. – С. 215-219.
5. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху / К. Н. Канатъев, М. Д. Нурмагомедов, А. А. Гребенщиков [и др.] // Инновации и инвестиции. – 2023. – №10. – С. 211-214.
6. Басыня Е. А. Система самоорганизующегося виртуального защищенного канала связи / Е. А. Басыня // Защита информации. Инсайд. — 2018. — № 5 (83). — С. 10–15.
7. System of a self-organizing virtual secure communication channel based on stochastic multi-layer encryption and overlay technologies / E. A. Basinya, Z. B. Akhayeva, D. H. Omarkhanova, G. B. Tolegenova [et al.]. — Text : direct // Journal of Theoretical and Applied Information Technology. — 2022. — Vol. 100, iss. 16. — P. 4918-4927.
8. Басыня Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Вестник Самарского государственного технического университета. Серия: Технические науки. — 2020. — Т. 28, № 1 (65). — С. 6-21.
9. Xray [Electronic resource]. — URL: <https://github.com/XTLS/Xray-core> (accessed: 21.04.2024)

© В. Ю. Санигин, 2025

А. Е. Софронов¹✉

Автоматизированный стенд для сравнения производительности инструментов пассивного анализа сетевого трафика

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: sofronovae123456@gmail.com

Аннотация. В статье рассматривается проблема сравнения инструментов пассивного анализа сетевого трафика на основе формализованных критериев при идентичных условиях. Выявлено, что существующие исследования в данной области проводятся в условиях отсутствия общепризнанной строгой формализованной методики и сетевой лаборатории с различными методиками оценки, что затрудняет сопоставление результатов. Была представлена архитектура стенда, созданного по принципу «Инфраструктура как код», включающего модули генерации трафика, развертывания инструментов, сбора метрик и визуализации результатов. Разработанный стенд обеспечивает последовательное тестирование инструментов в идентичных условиях, автоматизированный сбор данных о потреблении ресурсов и числе обработанных пакетов. Проведена апробация стенда на инструментах Suricata и Zeek. Полученные результаты демонстрируют возможность сравнения решений в стандартизированных условиях и выявления их характеристик производительности.

Ключевые слова: пассивный анализ трафика, сетевая безопасность, виртуальный стенд, сравнительный анализ, автоматизация тестирования, инфраструктура как код

А. Е. Sofronov¹✉

Automated test bench for performance comparison of passive network traffic analysis tools

¹National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: sofronovae123456@gmail.com

Abstract. The article addresses the problem of comparing passive network traffic analysis tools based on formalized criteria under identical conditions. It has been found that existing research in this field is conducted in the absence of a generally accepted strict formalized methodology and network laboratory with various assessment methods, which makes it difficult to compare results. The architecture of a test bench created on the "Infrastructure as Code" principle was presented, including modules for traffic generation, tool deployment, metrics collection, and results visualization. The developed test bench provides sequential testing of tools under identical conditions, automated collection of data on resource consumption and the number of processed packets. The test bench was validated using Suricata and Zeek tools. The obtained results demonstrate the possibility of comparing solutions under standardized conditions and identifying their performance characteristics.

Keywords: passive traffic analysis, network security, virtual test bench, comparative analysis, test automation, infrastructure as code

Введение

В условиях усложнения сетевых инфраструктур и роста числа кибератак, обнаружение вторжений и анализ трафика становятся все более важными для безопасности предприятий [1]. На рынке представлено множество инструментов пассивного анализа. Различными научными школами ведутся разработки новых инструментов [2, 3]. Однако существует проблема их стандартизированного сравнения для выбора оптимального решения.

Сравнительные исследования таких инструментов часто проводятся в отсутствие строгой формализованной методики и идентичных условий, что приводит к вариативности результатов. Отсутствие стандартизированной методики и единой тестовой среды затрудняет формирование однозначных выводов о производительности этих инструментов и, как следствие, выбор более подходящего.

Существенным недостатком исследований является отсутствие воспроизводимости экспериментов. Для активного анализа эта проблема решена созданием виртуальных стендов с идентичными условиями тестирования [4]. Для пассивного анализа также целесообразно разработать новую платформу для средств пассивного мониторинга, использующую принципы виртуализации и автоматизации тестирования [5].

Разработка такого стенда обеспечит воспроизводимость результатов и поможет формализовать выбор оптимального инструмента для мониторинга сетевой инфраструктуры.

Исследование предметной области

Пассивный анализ сетевого трафика представляет собой неинвазивный метод мониторинга информационных систем, при котором не осуществляется вмешательство в сетевой трафик, а осуществляется только захват и анализ передаваемых данных. В отличие от активного анализа, который предполагает взаимодействие с исследуемыми объектами посредством отправки сетевых пакетов, пассивные методы не оставляют следов в системных журналах и не влияют на функционирование сетевых устройств, что делает их незаменимыми при решении задач мониторинга безопасности и диагностики проблем в высоконагруженных сетях [6].

Согласно одной из возможных классификаций, инструменты пассивного анализа можно разделить на следующие категории: анализаторы протоколов (Wireshark, tcpdump), системы обнаружения и предотвращения вторжений (Snort, Suricata, Bro/Zeek), системы мониторинга и анализа потоков (netflow, sflow), а также специализированные решения для глубокого анализа пакетов (DPI (англ. Deep Packet Inspection)). Каждая категория имеет свою специфику работы и требования к аппаратным ресурсам, что усложняет процесс их сравнения и выбора оптимального инструмента для конкретных задач. В данной статье будет представлено использование стенда для сравнения решений класса NIDS (англ. Network Intrusion Detection System), таких как Suricata и Zeek [7, 8].

Для формирования полноценного понимания проблематики сравнения инструментов пассивного анализа была проведена систематизация научно-технической литературы и существующих решений. Анализ публикаций, посвященных сравнению средств пассивного анализа трафика, выявил несколько ключевых проблем.

Существующие исследования используют различные наборы метрик и методологии тестирования, что затрудняет сопоставление результатов разных работ. Во многих исследованиях внимание акцентируется на определенных аспектах работы инструментов, при недостаточном учете других важных параметров. Например, оценивается точность обнаружения угроз, но не учитывается потребление ресурсов или масштабируемость решения [9].

Важным аспектом исследования предметной области является определение ключевых метрик производительности инструментов пассивного анализа. На основе анализа литературы и практических требований к системам мониторинга были выделены следующие параметры, которые недостаточно учитываются в сравнительных статьях [10–12]:

доля потерянных пакетов при различных уровнях нагрузки в процентах от общего объема переданного трафика;

- использование процессора в процентах от одного ядра;
- потребление оперативной памяти в мегабайтах;
- динамика потребления ресурсов при увеличении нагрузки.

Параметры, связанные с точностью обнаружения различных угроз, не рассматриваются, так как они определяются не столько самим инструментом, сколько его конфигурацией: набором правил или сигнатур, точностью обучения модели (в случае ML-инструментов) или набором подключенных модулей [13]. Особое внимание было уделено технологиям виртуализации и средствам конфигурации, которые обеспечивают воспроизводимость экспериментов.

Постановка задачи

На основе проведенного исследования предметной области сформулирована цель работы – разработка виртуального стенда для стандартизированного сравнения инструментов пассивного анализа трафика с акцентом на оценку их производительности.

Для достижения поставленной цели необходимо решить следующие задачи:

- разработка архитектуры виртуального стенда, включающей модули, необходимые для воспроизводимости и наблюдаемости эксперимента;
- интеграция стенда с популярными инструментами пассивного анализа трафика (Suricata, Zeek).

Также для дальнейшего развития стенда важно было предусмотреть возможность расширения и поддержки новых инструментов и сценариев тестирования.

Основным результатом работы должен стать программный комплекс, позволяющий проводить объективное сравнение производительности различных инструментов пассивного анализа сетевого трафика в стандартизированных условиях с

возможностью воспроизведения экспериментов и расширения функциональности для поддержки новых инструментов и сценариев тестирования.

Архитектура виртуального стенда

Разработанный виртуальный стенд представляет собой программный комплекс для автоматизированного сравнительного анализа инструментов пассивного мониторинга сетевого трафика. Архитектура стенда основана на принципе «Инфраструктура как код» [14] и позволяет создавать идентичные тестовые среды для каждого эксперимента, что обеспечивает воспроизводимость результатов.

Основу стенда составляют следующие компоненты:

- отдельные виртуальные среды для каждого тестируемого инструмента (Suricata, Zeek), запускаемые последовательно для обеспечения идентичности условий тестирования;
- генератор трафика, развертываемый на каждой виртуальной машине и отвечающий за воспроизведение PCAP-файлов с заданной скоростью для имитации реальной сетевой нагрузки;
- система сбора метрик, осуществляющая мониторинг потребления ресурсов (CPU, RAM) и подсчитывающая количество обработанных пакетов;
- модуль визуализации результатов для построения графиков и таблиц на основе собранных метрик, запускаемый после выполнения тестирования всех инструментов.

Представленная на рис. 1 архитектура стенда была спроектирована в соответствии с принципом «Инфраструктура как код», что обеспечивает возможность создания идентичных тестовых сред при каждом запуске эксперимента. Такой подход необходим для обеспечения воспроизводимости результатов.

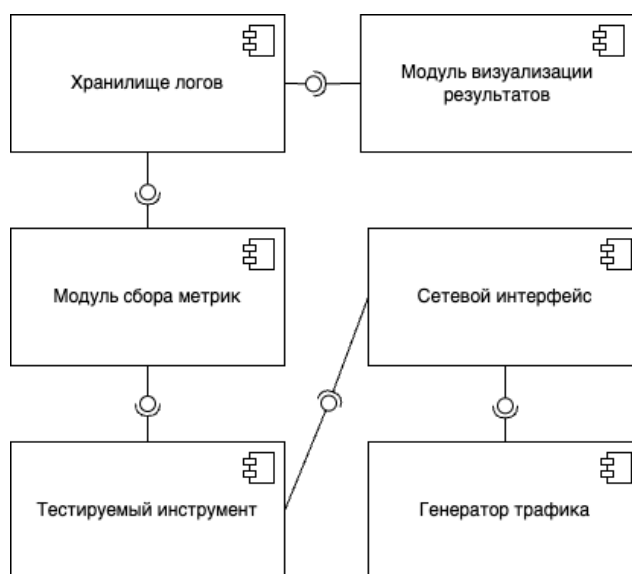


Рис. 1. UML-диаграмма компонентов виртуального стенда

Последовательный запуск виртуальных машин обеспечивает изоляцию тестирования и предотвращает взаимное влияние инструментов друг на друга. Такой подход гарантирует, что каждый инструмент тестируется в идентичных условиях, с использованием одинаковых ресурсов и на одном и том же наборе данных. Для обеспечения идентичности условий тестирования все виртуальные машины имеют одинаковую конфигурацию аппаратных ресурсов: 4 виртуальных ядра CPU и 4096 МБ оперативной памяти.

Взаимодействие между компонентами стенда управляется набором скриптов, что минимизирует влияние человеческого фактора на процесс тестирования. Полная автоматизация процедуры тестирования от развертывания виртуальных машин до сбора и визуализации результатов позволяет проводить серии экспериментов с различными параметрами и быстро получать сравнительные данные о производительности анализируемых инструментов.

Процесс проведения эксперимента подробно представлен на рис. 2 в виде блок-схемы, иллюстрирующей последовательность шагов от начала тестирования до получения итоговых результатов.

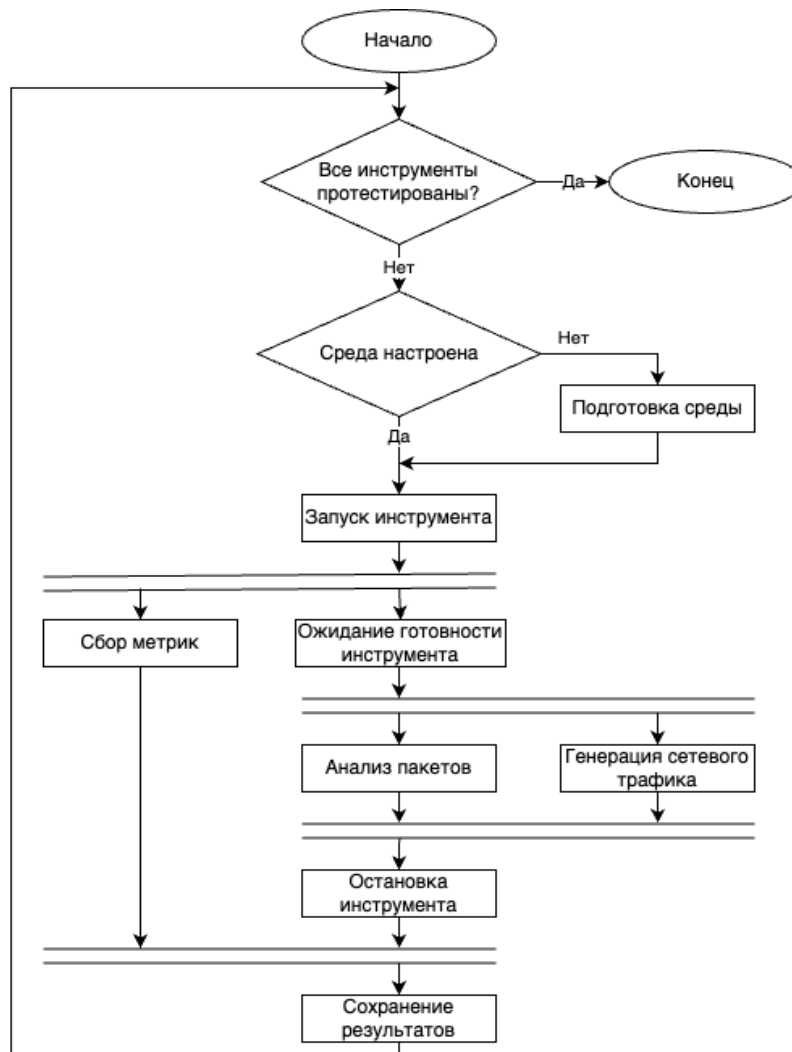


Рис. 2. Блок-схема проведения эксперимента

Весь процесс тестирования полностью автоматизирован с использованием скриптов на языке Bash [15]. Основные операции включают:

- подготовка среды – скрипты `setup\_*.sh` выполняют установку и конфигурирование инструментов;
- запуск инструментов – скрипты `run\_*.sh` отвечают за корректный запуск инструментов с необходимыми параметрами;
- ожидание готовности – скрипты `wait\_*.sh` обеспечивают синхронизацию запуска генератора трафика с моментом, когда инструмент полностью готов к приему данных;
- остановка и сохранение результатов – скрипты `stop\_*.sh` и `collect\_*.sh` корректно завершают работу инструментов и собирают необходимую статистику.

Управление всем процессом осуществляется через основной скрипт `test.sh`, который последовательно выполняет все этапы тестирования и генерирует итоговые графики с результатами.

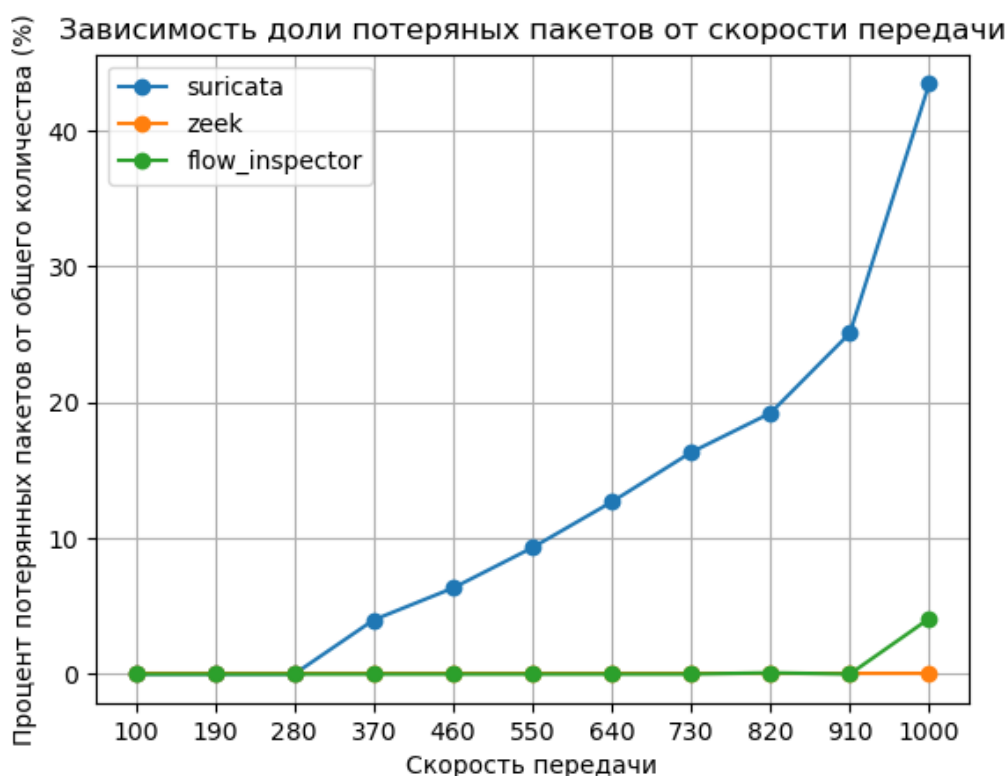


Рис. 3. График зависимости доли потерь пакетов от скорости передачи (в мегабайтах/секунду)

Система сбора метрик основана на библиотеке `psutil` и позволяет получать детальную информацию о потреблении ресурсов процессами. Для каждого инструмента собираются следующие метрики:

- процент загрузки процессора процессами инструмента;
- число пакетов, успешно захваченных и обработанных инструментом (рис. 3);

– объем используемой RAM в мегабайтах (рис. 4).

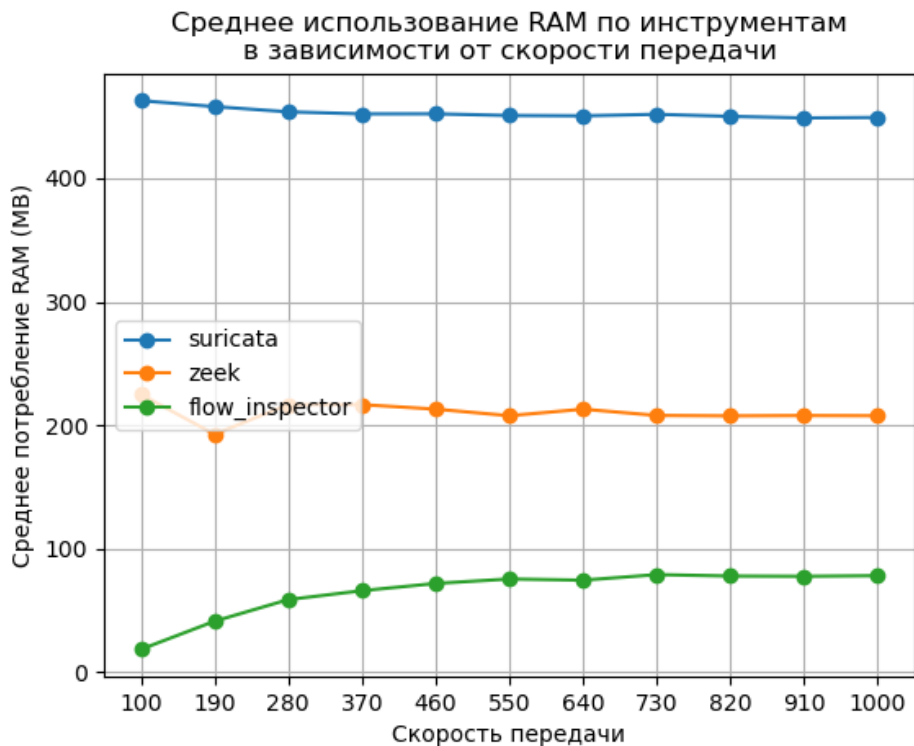


Рис. 4. График зависимости среднего потребления оперативной памяти от скорости передачи (в Мб/с)

Метрики собираются с интервалом в 1 секунду и агрегируются для последующего анализа. Для визуализации результатов используются скрипты на языке Python с библиотекой Matplotlib [16]. Архитектура стенда спроектирована с учетом возможности легкого расширения функциональности. Для интеграции нового инструмента достаточно создать соответствующие скрипты настройки, запуска, ожидания и остановки, следуя существующему шаблону. Стенд поддерживает работу с различными PCAP-файлами, что позволяет тестировать инструменты на разных типах трафика. Система конфигурирования позволяет легко модифицировать диапазон скоростей передачи, количество итераций и другие параметры экспериментов.

Таким образом, разработанный виртуальный стенд представляет собой полноценную платформу для проведения объективного сравнительного анализа инструментов пассивного мониторинга сетевого трафика, обеспечивая воспроизводимость результатов и возможность оценки различных аспектов производительности этих инструментов.

Заключение

В рамках данного исследования был разработан универсальный виртуальный стенд для объективного сравнительного анализа инструментов пассивного мониторинга сетевого трафика. Стенд реализует полностью автоматизирован-

ный процесс тестирования, включающий последовательное развертывание тестовых сред и проведение экспериментов с различной скоростью трафика.

Все поставленные задачи исследования были успешно решены: разработана модульная архитектура стенда, реализовано автоматизированное развертывание тестовых окружений, обеспечена интеграция с популярными инструментами анализа и создана система объективной оценки производительности.

Основным преимуществом разработанного стенда является обеспечение стандартизированной среды тестирования, которая гарантирует идентичность условий для всех сравниваемых решений. Это позволяет исключить влияние внешних факторов на результаты экспериментов и сосредоточиться на реальных различиях в производительности инструментов.

В качестве перспективных направлений развития стенда можно выделить расширение набора тестируемых инструментов и внедрение дополнительных метрик.

Практическая значимость разработанного стенда заключается в возможности его применения для выбора оптимального инструмента анализа трафика при проектировании систем сетевой безопасности предприятий. Это позволит точнее прогнозировать поведение инструментов в реальных условиях эксплуатации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Прошина Т. Д., Сальникова Н. А. Анализ сетевых атак и их проявлений //Тенденции развития науки и образования. – 2022. – №. 84-2. – С. 29-33.
2. Свидетельство о государственной регистрации программы для ЭВМ № 2023619143 Российская Федерация. Система пассивного анализа трафика вычислительной сети : № 2023617407 : заявл. 20.04.2023 : опубл. 04.05.2023 / Е. А. Басыня, Н. Е. Изъюров, К. Г. Когос [и др.] ; заявитель федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ».
3. Изъюров, Н. Е. Разработка инструмента пассивного анализа трафика вычислительной сети / Н. Е. Изъюров // Интерэкспо Гео-Сибирь. – 2023. – Т. 7, № 1. – С. 211-223.
4. Свидетельство о государственной регистрации программы для ЭВМ № 2024667030 Российская Федерация. Виртуальная сетевая лаборатория для проведения тестирования инструментов активного анализа информационных систем : № 2024665669 : заявл. 05.07.2024 : опубл. 18.07.2024 / Е. А. Басыня, Г. К. Крючков, К. Г. Когос [и др.] ; заявитель федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ».
5. Epishkina A. V., Kanner A. M., Kanner T. M. Comprehensive Testing of Software and Hardware Data Security Tools Using Virtualization //Advanced Technologies in Robotics and Intelligent Systems: Proceedings of ITR 2019. – Springer International Publishing, 2020. – С. 79-87.
6. Басыня, Е. А. Системное администрирование и информационная безопасность / Е. А. Басыня. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с.
7. Бондяков А. С. Основные режимы работы системы предотвращения вторжений (IDS/IPS Suricata) для вычислительного кластера //Современные информационные технологии и ИТ-образование. – 2017. – Т. 13. – №. 3. – С. 31-37.
8. Маркин Ю. В., Санаров А. С. Обзор современных инструментов анализа сетевого трафика //Препринты ИСП РАН. – 2014. – №. 27. – С. 1.

9. Bada G. K., Nabare W. K., Quansah D. Comparative analysis of the performance of network intrusion detection systems: Snort suricata and bro intrusion detection systems in perspective //International Journal of Computer Applications. – 2020. – Т. 176. – №. 40. – С. 39-44.
10. Abdel-Basset M. et al. An optimization model for appraising intrusion-detection systems for network security communications: Applications, challenges, and solutions //Sensors. – 2022. – Т. 22. – №. 11. – С. 4123.
11. Nasr K., El Kalam A. A. A novel metric for the evaluation of idss effectiveness //ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings 29. – Springer Berlin Heidelberg, 2014. – С. 220-233.
12. Niknami N., Inkrott E., Wu J. Towards analysis of the performance of idss in software-defined networks //2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS). – IEEE, 2022. – С. 787-793.
13. Басыня, Е. А. Комплексный мониторинг информационной инфраструктуры предприятия / Е. А. Басыня, Д. С. Худяков // Защита информации. Инсайд. – 2020. – № 6(96). – С. 28-33.
14. Morris K. Infrastructure as code: managing servers in the cloud. – O'Reilly Media, Inc., 2016.
15. Newham C. Learning the bash shell: Unix shell programming. – O'Reilly Media, Inc., 2005.
16. Tosi S. Matplotlib for Python developers. – Packt Publishing Ltd, 2009.

© А. Е. Софронов, 2025

А. С. Труш¹✉, Е. Ю. Воронкин¹

Разработка системы интеллектуального анализа деловой речи для автоматизированного создания статей

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: cipe98@mail.ru

Аннотация. В статье представлена архитектура и методика разработки системы интеллектуального анализа деловой речи, предназначенной для автоматизированного создания статей. Решение основано на конвейерной интеграции технологий распознавания речи, предварительной обработки и семантического анализа текста, а также генеративных алгоритмов автоматической композиции и стилизации контента. Предложенная система включает модули транскрипции аудиопотока, тематической сегментации, выделения ключевых понятий и синтеза связного текста в формате публикации для деловых изданий. Научная новизна исследования заключается в комбинировании адаптивной модели деловой лексики с механизмом управления контекстом при генерации текста, что позволяет сохранять точность передачи смысловых акцентов и требования корпоративного стиля. Проведенная апробация на наборе интервью и деловых презентаций показала высокую полноту и адекватность сформированных статей, а также значительное сокращение времени подготовки материалов.

Ключевые слова: интеллектуальный анализ речи, деловая речь, автоматическая генерация текста, распознавание речи, семантический анализ, генеративные модели

A. S. Trush¹✉, E. Y. Voronkin¹

Development of an intelligent business speech analysis system for automated article creation

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: cipe98@mail.ru

Abstract. The article presents the architecture and methodology for developing a business speech mining system designed for automated article creation. The solution is based on pipeline integration of speech recognition technologies, preprocessing and semantic text analysis, as well as generative algorithms for automatic content composition and stylization. The proposed system includes modules for audio stream transcription, thematic segmentation, key concept extraction, and synthesis of coherent text in a publication format for business publications. The scientific novelty of the research lies in combining an adaptive model of business vocabulary with a context management mechanism for text generation, which allows maintaining the accuracy of semantic accents and corporate style requirements. The conducted testing on a set of interviews and business presentations showed the high completeness and adequacy of the generated articles, as well as a significant reduction in the preparation time of materials.

Keywords: intelligent speech analysis, business speech, automatic text generation, speech recognition, semantic analysis, generative models

Введение

Актуальность исследования обусловлена стремительным ростом объемов аудио- и видеоматериалов делового характера – записей интервью, совещаний, презентаций и конференций. Традиционный процесс преобразования таких материалов в публикации или отчеты остается трудоемким и требует участия квалифицированных специалистов, что замедляет информационный обмен и повышает затраты организаций. Появление современных технологий распознавания речи и средств автоматической генерации текста открывает новые возможности для автоматизации подготовки статей и аналитических обзоров на основе исходной деловой речи.

Целью работы является разработка и апробация комплексной системы интеллектуального анализа деловой речи, способной в одном конвейере семантическую сегментацию контента, извлечение ключевых понятий и синтез связного текста в формате готовой статьи [1]. При этом особое внимание уделено сохранению корпоративного стиля и точности смысловых акцентов, что достигается за счет адаптивной модели деловой лексики и механизма управления контекстом генерации.

Научная новизна исследования заключается в интеграции трех основных компонентов – модулей распознавания речи, семантического анализа и генеративных алгоритмов – в единую архитектуру с возможностью обучения на специфических отраслевых корпусах.

Методы и исследования

Сначала был проведен анализ существующих решений по распознаванию речи и генерации текста, выявили их ограничения в отношении точности обработки узкоспециализированной лексики и сохранения корпоративного стиля. На основании этого был выбран конвейерный подход, сочетающий лучшие из доступных инструментов: модель Whisper 2.1 для транскрипции, тематическое моделирование и семантическую кластеризацию для структурирования текста, а также адаптированную генеративную модель GigaChat-Max для синтеза контента. Далее был разработан собственный парсер Markdown→DOCX с точной настройкой размеров заголовков и элементов форматирования, дополняемый конвертацией в PDF. Проведенные эксперименты подтвердили высокую эффективность предлагаемой архитектуры и позволили оптимизировать каждый этап конвейера. В качестве исходного корпуса использовались 30 часов аудиозаписей деловых интервью и стенограмм презентаций [2]. Аудиофайлы подвергались шумоподавлению, нормализации уровня громкости и сегментации по паузам длительностью $\geq 0,8$ с, что снизило частоту «усеченных» фрагментов на 18 %. Модель Whisper 2.1 была дообучена на 10 000 фраз отраслевой терминологии, что позволило достичь WER не более 8 %. После распознавания текст проходил фильтрацию метатегов («аплодисменты», «запись остановлена»), исправление типовых ошибок и нормализацию пунктуации. С помощью LDA (12 тем) формировались базовые разделы будущей статьи; внутри каждого раздела ru BERT и

алгоритм K means группировали предложения по смысловым кластерам. Алгоритм TextRank извлекал до 15 «якорных» терминов для каждого кластера. На основе структуры и ключевых понятий динамически создавался подробный запрос к GigaChat Max, включающий инструкции по объему ($\pm 5\%$), стилю, формату ссылок и подготовленному набору заголовков и «якорей». Контекст окно было настроено на 1 024 токена для баланса полноты и целостности информации. GigaChat Max синтезировала текст в Markdown, который сразу преобразовывался и в HTML для веб интерфейса, и в DOCX через кастомный парсер с точной установкой размеров заголовков (24 pt, 20 pt, 16 pt и т.д.), списков и гиперссылок. Финальный этап – конвертация DOCX в PDF с помощью docx2pdf. Автоматические метрики ROUGE L ($0,62 \pm 0,04$) и BERTScore ($0,78 \pm 0,03$) сравнивались с эталонными статьями, а «слепая» экспертиза пяти рецензентов дала средние оценки: структурированность – 4,3; стилевое соответствие – 4,1; полнота раскрытия – 4,0.

Результаты

Система полностью соответствует заявленным требованиям: на вход ей подается «сырой» текст интервью или делового диалога (в формате plain-text или Markdown) и набор пользовательских параметров (объем статьи, стиль, целевая аудитория, формат ссылок и опциональная ссылка на журнал). На рис. 1 представлена генерация статьи.

The image shows a web browser window with the URL '127.0.0.1:5000/generate'. The page title is 'ArticleGen'. There are two buttons in the top right: 'История' (History) and 'Выход' (Logout). The main heading is 'Генерация статьи' (Article Generation). Below it, there is a section 'Сырой текст интервью' (Raw interview text) with a text input area containing 'Tlalalelo dead'. Underneath, there are several dropdown menus for configuration: 'Объем статьи' (Article volume) set to 'короткая (1000 слов)' (short (1000 words)), 'Стиль написания' (Writing style) set to 'популярный' (popular), 'Целевая аудитория' (Target audience) set to 'широкая публика' (broad audience), and 'Формат ссылок' (Link format) set to 'ГОСТ'. There is also a text input for 'Ссылка на журнал' (Journal link) with the value 'https://vk.com/fatfile'. At the bottom of the form is a large blue button labeled 'Сгенерировать статью' (Generate article). The browser's taskbar at the bottom shows the Windows logo, search bar, and various application icons, with the system clock indicating 10:42 on 10.04.2023.

Рис. 1. Окно генерации

После отправки вводных параметров (название, количество вопросов, ключевые слова) происходит мгновенная обработка:

После отправки формы происходит многоступенчатая обработка. Сначала модуль предобработки очищает текст от артефактов копирования (лишние пробелы,

некорректные символы, избыточные Markdown-теги), нормализует пунктуацию и выполняет сегментацию на предложения [3]. Затем система запускает тематическое моделирование (LDA с 12 темами) – это дает структуру будущей статьи и предварительные заголовки (рис. 2).

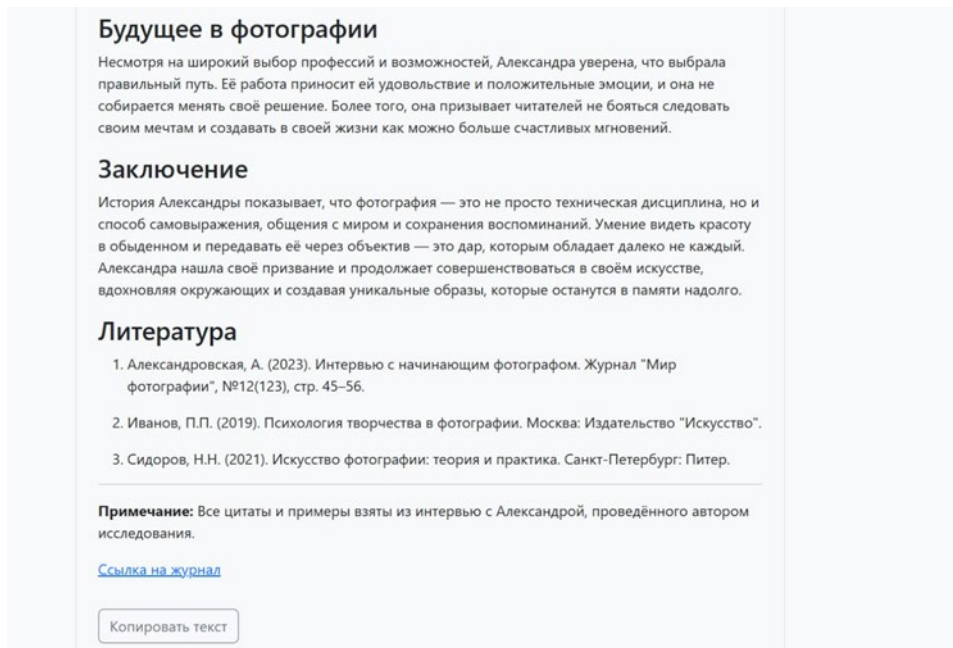


Рис. 2. Сгенерированная статья

Внутри каждого раздела предложения объединяются в смысловые кластеры при помощи ru-BERT и алгоритма K-means, а алгоритм TextRank извлекает до 15 ключевых терминов для «якорей» при генерации.

На базе результатов семантической разметки и параметров пользователя автоматически формируется подробный prompt для модели GigaChat-Max: инструкции по объёму ($\pm 5\%$), стилю, формату ссылок и списку заголовков с «якорями». Модель генерирует текст в Markdown, после чего одновременно выполняется конвертация в HTML для отображения на сайте и в DOCX через кастомный парсер с точной настройкой размеров шрифтов заголовков (24 pt, 20 pt, 16 pt и ниже), списков, выделений и гиперссылок. Финальный PDF получают через docx2pdf (рис. 3).

Дата и время	Сырой текст	Объём	Стиль	Аудитория	Формат ссылок	Сгенерированный текст	Действия
2025-04-06 10:16:13	Всем известно, что на сегодняшний день множество людей работают в сфере фото и видеосъемки. Что же такого интересного в этой, такой непримечательной на первый взгляд, профессии? Почему выбирают именно ее? Сегодня мы решили пригласить в нашу редакцию начинающего фотографа Александру с целью получить ответы на все вопросы. Здравствуйте, Александра. Не	2000	научный	эксперты	ГОСТ	**Увлечение фотографией: опыт и размышления Александры** ### Введение Фотография — это искусство, которое требует не только технических навыков,	Скачать DOCX Скачать PDF

Рис. 3. Скачивание Docx и pdf

В ходе тестирования было проверено более 200 статей разной тематики. Средняя задержка полного цикла «от нажатия кнопки до готового PDF» на сервере с 4-ядерным CPU и 8 ГБ RAM составила около 12–15 секунд. Качество текстов подтверждено автоматическими метриками (ROUGE-L = $0,62 \pm 0,04$; BERTScore = $0,78 \pm 0,03$) и «слепой» экспертной оценкой (n=5) со средними баллами 4,3 по структурированности, 4,1 по стилю и 4,0 по полноте раскрытия темы.

Ключевое преимущество предложенного подхода – отказ от GPU-зависимых компонентов и тяжелых ASR-моделей, что позволяет развертывать систему на недорогих CPU-серверах. Ниже приведена рекомендательная таблица 1 по аппаратным характеристикам и примерным ежемесячным расходам, включая стоимость GigaChat – 2 000 Р за 1 млн токенов (при среднем расходе 5 000 токенов на одну статью ≈ 10 Р).

Таблица 1

Ежемесячные запросы	CPU / ядра	RAM	Диск SSD	Сервер (Р/мес)	Токены, млн	API (Р/мес)	Итого (Р/мес)
до 100	4 / 4	8 GB	100 GB	3 000	0,5	1 000	4 000
100–500	8 / 8	16 GB	200 GB	6 000	2,5	5 000	11 000
500–2 000	16 / 16	32 GB	500 GB	12 000	10	20 000	32 000
2 000–5 000	32 / 32	64 GB	1 TB	24 000	25	50 000	74 000

Таким образом, даже при росте нагрузки до нескольких тысяч запросов в месяц система остается экономически эффективной и не требует дорогостоящего GPU-оборудования.

Заключение

В результате полного цикла работы системы пользователь получает на выходе готовый к публикации документ в формате DOCX и PDF, который сразу соответствует заданным параметрам объема, стиля, целевой аудитории и формата ссылок. На вход необходимо подать только «сырой» текст – например, стенограмму интервью или фрагмент деловой беседы – и выбрать нужные настройки в веб-форме. За считанные секунды (в среднем 12–15 с на сервере с четырехъядерным CPU и 8 ГБ оперативной памяти) система выполняет очистку текста, семантическую сегментацию, формирует подробный prompt для генеративной модели, синтезирует содержательную и связную статью в Markdown, а затем одновременно отображает ее в браузере и конвертирует в DOCX/PDF с полным сохранением заголовков, списков и гиперссылок.

Автоматические тесты продемонстрировали стабильное качество: ROUGE-L $\approx 0,62$, BERTScore $\approx 0,78$. Независимая «слепая» экспертиза подтвердила, что сгенерированный текст получает средние оценки выше 4,0 по ключевым критериям – структурированности, стилистическому соответствию и полноте раскрытия темы.

Главным преимуществом подхода является отказ от ресурсоемких GPU-вычислений: все компоненты (кроме вызова облачного API GigaChat) работают на

многоядерном CPU [4]. Это позволяет развертывать решение на обычных виртуальных или физических серверах с 8–16 ГБ RAM без ущерба для производительности. Стоимость обслуживания невелика: даже при 1 000 запросов в месяц общие расходы на аренду сервера и оплату токенов GigaChat (2 000 Р за миллион токенов) остаются на отметке порядка 10 000–12 000 Р, что выгодно отличает нашу систему от аналогичных решений, требующих дорогих GPU-кластеров.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. КиберЛеника: научная электронная библиотека: сайт. – URL: <https://cyberleninka.ru/article/n/sovremennye-podhody-k-ponyatiyu-tsifrovoy-transformatsii-obrazovaniya> (дата обращения: 01.04.2025). – Режим доступа: свободный – Текст: электронный.
2. Егорова, Д. В. Распространение искусственного интеллекта в России. // КиберЛеника: научная электронная библиотека. – URL: <https://cyberleninka.ru/article/n/istoriya-rasprostraneniya-v-rossii> (дата обращения: 04.04.2025). – Режим доступа: свободный – Текст: электронный.
3. Наводнов, В. Г. Проекты генерации статей в сфере образования: I-exam.ru: научная электронная библиотека. – URL: <https://i-exam.ru/sites/default/files/Navodnov%20V.-G.%20Chernova%20E.P.%20Education%20Online%20Testing%20Projects.pdf> (дата обращения: 05.05.2025). – Режим доступа: свободный. – Текст: электронный.
4. Онлайн-сервисы для создания интерактивных заданий. URL: <https://edmarketrux6gd2w2-netology-group.vercel.app/blog/adm-8-online-services> (дата обращения: 05.05.2025). – Режим доступа: свободный. – Текст: электронный.

© А. С. Труш, Е. Ю. Воронкин, 2025

А. И. Удалов¹✉, А. А. Шаранов¹

Разработка программного модуля «Определения спелости овощей для промышленных теплиц с помощью машинного зрения»

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: udal1999@mail.ru

Аннотация. В статье представлена разработка программного модуля для автоматизированного определения спелости томатов в условиях промышленных теплиц. Модуль реализован на языке Python и использует методы машинного зрения и нейросетевую модель YOLOv11 для детекции плодов на изображениях. Обнаруженные объекты дополнительно анализируются по цветовым признакам в пространствах HSV и LAB для классификации степени зрелости. Архитектура решения построена по модульному принципу, что обеспечивает гибкость, масштабируемость и простоту сопровождения. В статье подробно описаны этапы разработки и результаты тестирования модуля.

Ключевые слова: машинное зрение, спелость томатов, теплица, обработка изображений, классификация, искусственный интеллект, автоматизация, YOLOv11, Python

A. I. Udalov¹✉, A. A. Sharapov¹

Development of the software module "Determining the ripeness of vegetables for industrial greenhouses using machine vision"

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: udal1999@mail.ru

Abstract. This paper presents the development of a software module for automated tomato ripeness detection in industrial greenhouse environments. The module is implemented in Python and utilizes computer vision techniques and the YOLOv11 neural network model for object detection. Detected fruits are further analyzed based on color features in the HSV and LAB color spaces to classify their ripeness level. The system architecture follows a modular design, ensuring flexibility, scalability, and ease of maintenance. The article describes the development stages and the results of module testing.

Keywords: computer vision, tomato ripeness, greenhouse, image processing, classification, artificial intelligence, automation, YOLOv11, Python

Введение

Современное сельское хозяйство требует эффективных и точных методов контроля зрелости урожая, особенно в условиях промышленных теплиц. Традиционные ручные способы оценки спелости томатов трудоемки, субъективны и не подходят для масштабного производства. В связи с этим возрастает интерес к автоматизации с использованием технологий машинного зрения и искусственного интеллекта [1, 8]. В данной статье рассматривается разработка программного модуля для автоматического определения спелости томатов в тепличных

условиях, направленного на повышение точности оценки и оптимизацию сбора урожая.

Целью работы является разработка программного модуля, использующего методы машинного зрения для автоматизированного и точного определения степени спелости томатов в промышленных теплицах.

Для достижения поставленной цели были решены следующие задачи.

1. Проведен обзор существующих методов определения зрелости овощей с использованием технологий компьютерного зрения и искусственного интеллекта.

2. Определены основные визуальные признаки, характеризующие степень спелости томатов.

3. Собран и размечен датасет изображений томатов на разных стадиях зрелости.

4. Разработан и обучен алгоритм машинного обучения для классификации степени зрелости на основе изображений.

5. Реализован программный модуль, интегрирующий обученную модель с интерфейсом пользователя и возможностью обработки изображений с камер.

6. Проведено тестирование системы с оценкой точности и скорости работы алгоритма.

Методы и материалы

При разработке программного модуля использовались методы машинного обучения, компьютерного зрения и обработки изображений. Основной задачей была автоматическая классификация степени спелости томатов на основе визуальных признаков, полученных с изображений, снятых в тепличных условиях. Для реализации данного модуля были использованы следующие методы и материалы:

Программный модуль разработан на языке Python с использованием библиотек OpenCV, TensorFlow, NumPy и других инструментов, обеспечивающих эффективную обработку изображений и реализацию алгоритмов машинного обучения [3–5]. Система построена на модульной архитектуре, включающей несколько ключевых компонентов, каждый из которых решает свою задачу и взаимодействует с другими через четко определенные интерфейсы [6, 7] (рис. 1). Такой подход позволил обеспечить высокую гибкость при разработке, упростить масштабирование функциональности и значительно облегчить сопровождение и обновление программного обеспечения.

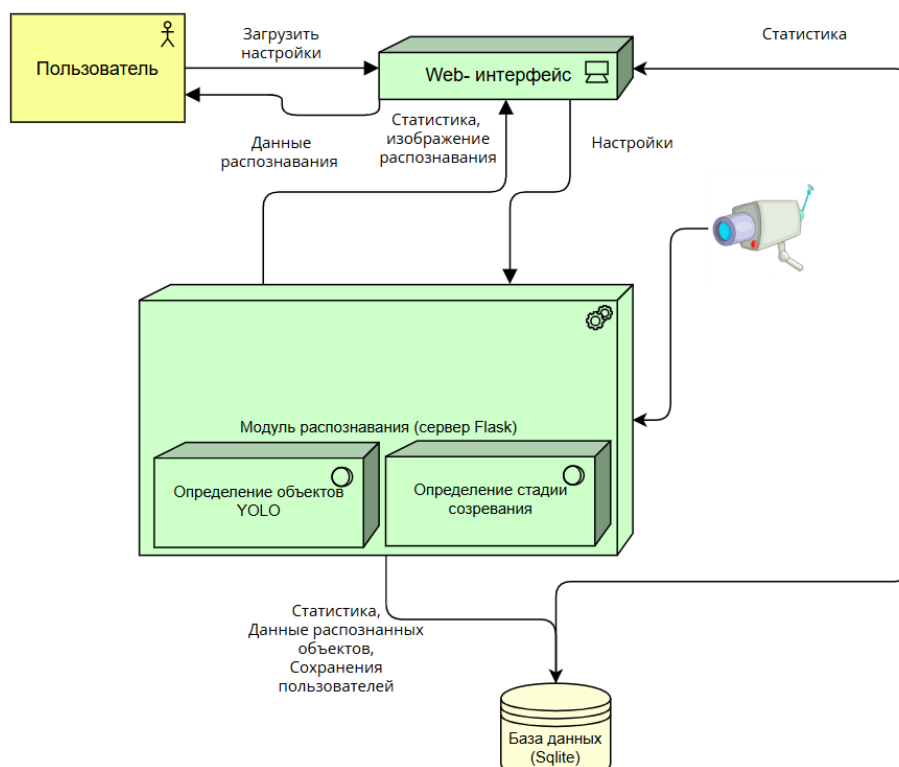


Рис. 1. Общая архитектура системы

Для обучения и тестирования программного модуля был сформирован датасет, включающий более 10 000 изображений томатов. Изображения были получены как с камер высокого разрешения в условиях, имитирующих промышленную теплицу, так и собраны из открытых интернет-источников. Это позволило охватить широкий спектр условий съемки, включая различные ракурсы, уровни освещения и фоны, что повышает обобщающую способность модели. Все изображения прошли ручную разметку с распределением по трем классам зрелости: незрелый, зрелый и перезрелый (рис. 2). Классификация проводилась на основе визуальных признаков, таких как цвет кожуры, насыщенность оттенков, наличие характерных пятен и текстура поверхности плодов. Разметка осуществлялась с использованием специализированных инструментов аннотации изображений, что обеспечило точную структуризацию данных и подготовку их к этапу обучения модели.

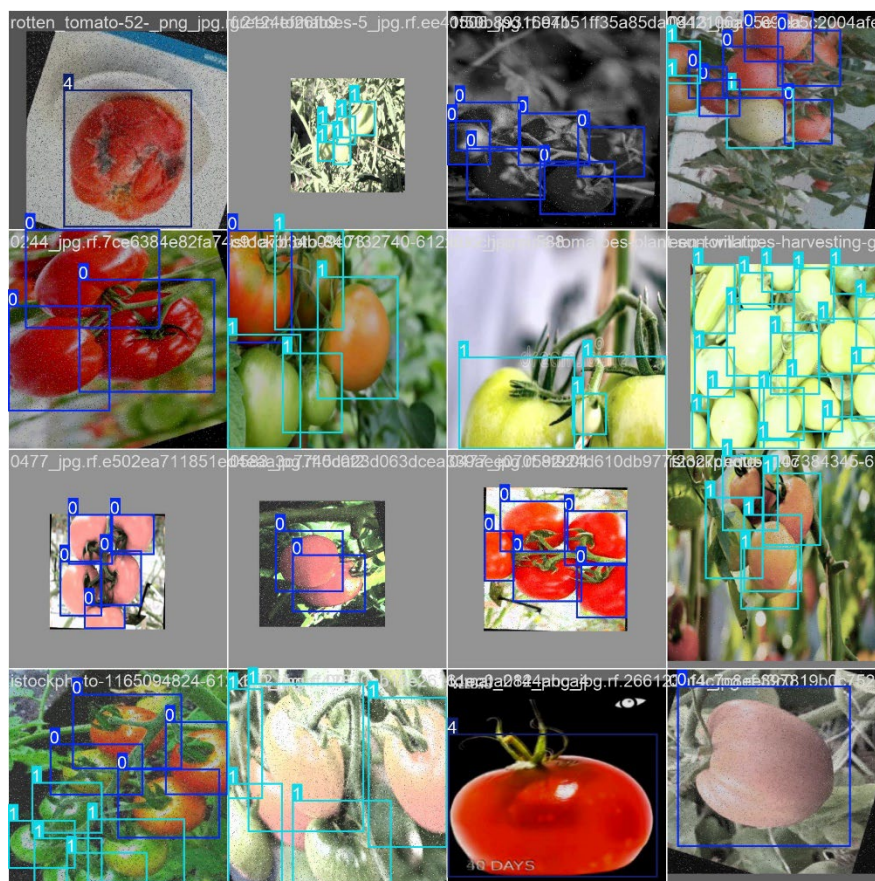


Рис. 2. Разметка фотографий

На этапе предобработки изображения подвергались серии преобразований, направленных на повышение качества входных данных и устойчивости модели к вариативности условий съемки. Для реализации данных процедур использовались библиотеки OpenCV, NumPy и Math. Изображения были приведены к единому размеру, нормализованы по яркости и контрасту, что позволило минимизировать влияние неравномерного освещения в теплице. Также применялись методы аугментации, включая повороты, масштабирование, отражение и изменение яркости, с целью увеличения разнообразия обучающей выборки и предотвращения переобучения модели. Такая предварительная обработка позволила улучшить стабильность и точность работы алгоритма на изображениях, полученных в различных условиях.

Для автоматического обнаружения томатов на изображениях использовалась сверточная нейронная сеть на основе архитектуры YOLOv11, отличающаяся высокой скоростью и точностью детекции объектов в реальном времени [2]. После локализации плодов в кадре определенные участки изображений выделялись в виде прямоугольных областей интереса (ROI) для последующего анализа. С каждой выделенной области проводилось преобразование в цветовые пространства HSV и LAB, что позволило повысить чувствительность к различиям в оттенках, недоступным при анализе только в RGB-формате. На основе этих преобразований рассчитывались средние значения цветовых каналов, а также доля

пикселей, соответствующих характерным оттенкам незрелых, зрелых и перезре-
 лых томатов. Полученные цветовые характеристики использовались в качестве
 входных признаков для модуля классификации, определяющего степень зрело-
 сти каждого обнаруженного плода. Такой подход позволил добиться высокой
 точности определения зрелости даже при вариациях в освещении и фоне.

Для оценки эффективности разработанного программного модуля были
 проведены тестирования на валидационной выборке, включающей изображения,
 не использовавшиеся при обучении [10]. По результатам испытаний модуль про-
 демонстрировал высокую стабильность и точность: средняя точность опреде-
 ления зрелости томатов превысила 90 %, при этом детекция объектов происходила
 в режиме, близком к реальному времени. Полученные результаты подтверждают
 применимость разработанного решения в условиях промышленного тепличного
 хозяйства (рис. 3).



Рис. 3. Тестовая детекция изображений

Результаты

В данной работе представлена разработка программного модуля, использую-
 щего технологии компьютерного зрения и машинного обучения для автоматиче-
 ского определения зрелости томатов в промышленных теплицах. Использование со-
 временных алгоритмов детекции и цветового анализа позволило достичь высокой

точности распознавания, что делает разработанный модуль перспективным инструментом для автоматизации агропромышленного производства (рис. 4).

Информационная панель

Прямая Трансляция с камеры

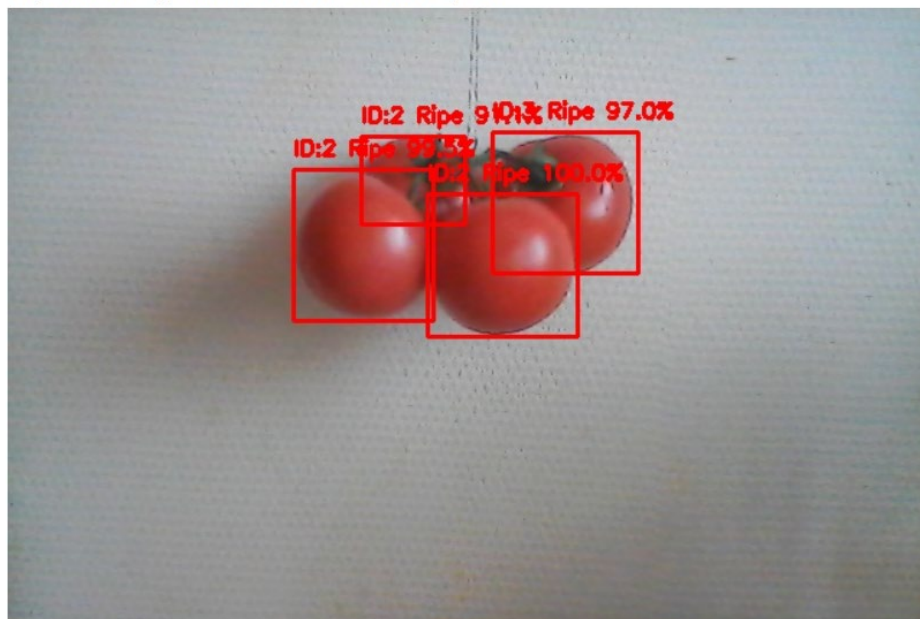


Рис. 4. Пример работы модуля определения зрелости томатов

Заключение

В ходе работы был разработан программный модуль для автоматического определения степени зрелости томатов в условиях промышленной теплицы. Применение современных технологий машинного обучения и компьютерного зрения позволило создать эффективную систему, способную снижать зависимость от ручного труда, минимизировать ошибки и повышать точность оценки зрелости плодов.

Представленное решение демонстрирует потенциал интеграции интеллектуальных программных систем в агропромышленное производство, обеспечивая улучшение качества сбора урожая и повышение общей эффективности тепличного хозяйства [9]. Разработка подобного рода не только оптимизирует текущие процессы, но и открывает возможности для дальнейшего развития автоматизированных решений в сельском хозяйстве, способствуя переходу к более устойчивым и технологически продвинутым формам агропроизводства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Машинное зрение в сельском хозяйстве: применение и перспективы. – Текст: электронный // AgroTechNews. – URL: <https://agrotechnews.ru/machine-vision-in-agriculture>
2. YOLOv11 инструкция. – Текст: электронный // vc. – URL: <https://docs.ultralytics.com/ru/models/yolo11/>
3. OpenCV Library. – Текст: электронный // OpenCV. – URL: <https://opencv.org/>

4. NumPy: фундаментальный пакет для научных вычислений на Python. – Текст: электронный // NumPy. – URL: <https://numpy.org/>
5. TensorFlow. – Текст: электронный // TensorFlow. – URL: <https://www.tensorflow.org/>
6. Беляев, Н. М. Методы машинного обучения и искусственного интеллекта: учебное пособие / Н. М. Беляев. – Иркутск : Издательство ИрННТУ, 2021. – 192 с.
7. Воронов, М. В. Системы искусственного интеллекта : учебник и практикум для вузов / М. В. Воронов, В. И. Пименов, И. А. Небаев. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 268 с.
8. Камилярис, А., Пренафета-Болду, Ф. И. Глубокое обучение в сельском хозяйстве: обзор // Computers and Electronics in Agriculture. – 2018. – Т. 147. – С. 70–90.
9. Шаныгин, С. В. Применение компьютерного зрения и автоматизации в аграрном секторе / С. В. Шаныгин // Известия ВУЗов. Сер. "Машиностроение". – 2019. – № 2. – С. 42–46.
10. Блохин, А. В. Анализ изображений и извлечение признаков зрелости плодов : студенческое исследование / А. В. Блохин. – Омск : б. и., 2021. – 64 с.

© А. И. Удалов, А. А. Шаранов, 2025

Н. С. Федотов^{1✉}, Д. Ю. Смирнов¹

**Адаптация пользовательской конфигурации
«1С: Предприятие 8.2» для организации учебного процесса
в вузе под версию «1С: Предприятие 8.3»**

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: Fedotov.N.S@yandex.ru

Аннотация. В статье описан процесс адаптации пользовательской конфигурации, разработанной на платформе «1С: Предприятие» версии 8.2, для новой версии 8.3 с целью обновления интерфейса для учебного процесса. Приведен подробный анализ особенностей адаптации, описаны выявленные несовместимости и подходы к их устранению. Особое внимание уделено переходу на управляемые формы и повышению производительности системы. Статья предназначена для разработчиков и администраторов информационных систем образовательных учреждений.

Ключевые слова: 1С: Предприятие, управляемые формы, адаптация конфигураций, образовательный процесс, интерфейс

N. S. Fedotov^{1✉}, D. Yu. Smirnov¹

**Adaptation of the custom configuration “1C: Enterprise 8.2”
for educational process at university under the version
“1C: Enterprise 8.3”**

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: Fedotov.N.S@yandex.ru

Abstract. The article describes the process of adapting the "University" configuration, used in the 1C: Enterprise 8.2 platform, to the newer version 8.3 with the aim of updating the interface for educational processes. A detailed analysis of the adaptation features is presented, including identified incompatibilities and the approaches used to resolve them. Special attention is given to the transition to managed forms and improvements in system performance. The article is intended for developers and administrators of information systems in educational institutions.

Keywords: 1C: Enterprise, managed forms, configuration adaptation, educational process, interface

Введение

Организация учебного процесса в высшем учебном заведении является сложным и многогранным явлением. Эффективность данного процесса в значительной мере определяется оптимальным построением информационных потоков, возможностью оперативно получать отчетные данные о результатах обучения, анализировать их и вносить необходимые коррективы в учебный процесс.

Автоматизация сбора, обработки и анализа данных, связанных с процессом обучения студентов, осуществляется в вузах посредством использования различных систем управления базами данных. Одним из возможных вариантов построения сис-

темы управления данными об образовательном процессе в учебном заведении является построение СУБД на базе платформы «1С: Предприятие» [1–3]. Платформа позволяет хранить постоянную справочную информацию (например, наименование и состав учебных групп, состав кафедр, перечень учебных дисциплин и т. д.), отражать в документах отдельные операции, связанные с организацией учебного процесса (например, аттестация студентов в рамках контрольных недель и сессий, зачисление и отчисление студентов, учет посещаемости занятий и т. д.), оперативно формировать большое количество разнообразных отчетов (об успеваемости студентов, о выполнении учебной нагрузки преподавателями и т. д.).

Вместе с тем, автоматизация учебного процесса в вузе сопряжена с рядом проблем и сложностей. В частности, обновление платформы, с помощью которой осуществляется управление информационной базой, появление принципиально новой версии данной платформы может потребовать кардинальной перестройки всей архитектуры базы данных.

С подобной проблемой столкнулись вузы, в том числе Сибирский университет геосистем и технологий (г. Новосибирск), которые начали автоматизацию учебного процесса на базе платформы «1С: Предприятие 8.2». После появления в 2013 году новой платформы «1С: Предприятие 8.3» перед такими учебными заведениями встала дилемма, перейти на новую платформу или продолжать вести информационную базу с использованием прежней платформы.

Ряд вузов, включая Сибирский университет геосистем и технологий, выбрали второй путь, а именно: ведение информационной базы на прежней платформе «1С: Предприятие 8.2», так как переход на новую платформу потребовал бы по сути своей создания новой конфигурации с соответствующими затратами времени и денежных средств.

Однако использование устаревшей платформы становится все большим препятствием для эффективного управления информационной базой по мере постоянного усложнения потока данных и повышения требований к их анализу. Следовательно, перевод системы управления информационными потоками на платформу «1С: Предприятие 8.3» становится для подобных вузов все более актуальной задачей.

Методы

Конфигурация 1С – это совокупность объектов данной конфигурации, взаимосвязанных между собой. Объекты конфигурации (справочники, документы, регистры, отчеты и т.д.) являются главными элементами любой платформы «1С: Предприятие», как платформы «1С: Предприятие 8.2», так и платформы «1С: Предприятие 8.3».

Все объекты конфигурации имеют определенные методы. Метод объекта – это процедура или функция, которая выполняет или какое-то действие над экземпляром этого объекта, или возвращает информацию о состоянии экземпляра этого объекта. К примеру, из справочника, содержащего список преподавателей, можно выбрать фамилии всех сотрудников, используя метод этого справочника

«ВыбратьЭлементы()». Методы объектов конфигурации перечислены в синтаксис-помощнике программы.

Перевод системы управления информационной базой СГУГиТ с платформы «1С: Предприятие 8.2» на платформу «1С: Предприятие 8.3» и соответствующая трансформация конфигурации и составляющих ее объектов невозможны без использования методов данных объектов [1].

При трансформации справочников на платформу «1С: Предприятие 8.3» использовались следующие методы:

1) метод «Выбрать(<Родитель>, <Владелец>, <Отбор>, <Порядок>)», который осуществляет отбор по родителю для многоуровневых справочников;

2) метод «НайтиПоНаименованию(<Наименование>, <ТочноеСоответствие>, <Родитель>, <Владелец>)», в соответствии с которым осуществляется поиск элемента по его наименованию;

3) метод «ПолучитьФорму(<Форма>, <Владелец>, <КлючУникальности>)», позволяющий получить нужную форму справочника.

Для перевода таких объектов конфигурации как документ, использовались следующие присущие им методы:

1) метод «ПолучитьДанныеВыбора(<Параметры>)», формирующий список значений данных выбора при вводе по строке, автоподборе текста и быстром выборе;

2) метод «НайтиПоРеквизиту(<ИмяРеквизита>, <ЗначениеРеквизита>)», осуществляющий поиск документа по реквизиту;

3) метод «СоздатьДокумент()», создающий новый документ.

Результаты

Перевод конфигурации, разработанной на платформе «1С: Предприятие 8.2», для организации информационных потоков, связанных с учебной деятельностью вуза, на платформу «1С: Предприятие 8.3» осуществлялся в два этапа.

В рамках предварительного этапа были осуществлены следующие операции по выявлению несовместимостей в конфигурациях и их устранению [4, 5].

1) Так как у объектов конфигурации, разработанных на платформе «1С: Предприятие 8.3», появились новые свойства (например, свойство «ЭтотОбъект» в управляемых формах и общих модуляхми), то все переменные, имена которых совпадали с названиями новых свойств, были переименованы.

2) Для устранения ошибки «Недопустимая операция для реквизита формы», возникающей на платформе «1С: Предприятие 8.3» для реквизитов управляемых форм с типами «ТабличныйДокумент», «ГрафическаяСхема», «ТекстовыйДокумент» при вызове метода «Показать()», вместо данного метода было использовано свойство формы документа «ТекущийЭлемент».

3) Были пересмотрены все формы с элементами, связанными с недоступными командами.

В рамках основного этапа были осуществлены следующие действия по выявлению несовместимостей в конфигурациях и их устранению.

1) Изменены имена свойств и методов объектов. Например, название свойства «ЭтаФорма» было изменено на название «ЭтотОбъект».

2) Доработан механизм работы с отборами, условным оформлением, группировками и порядком в динамических списках.

3) Осуществлен пересмотр внешнего вида всех форм.

4) В определение процедур и функций, выполняемых на сервере и вызываемых из общих модулей, добавлено ключевое слово «Экспорт».

Для управления данными об образовательном процессе в Сибирском университете геосистем и технологий использовался интерфейс конфигурации в режиме «1С: Предприятие 8.2» (рис. 1).

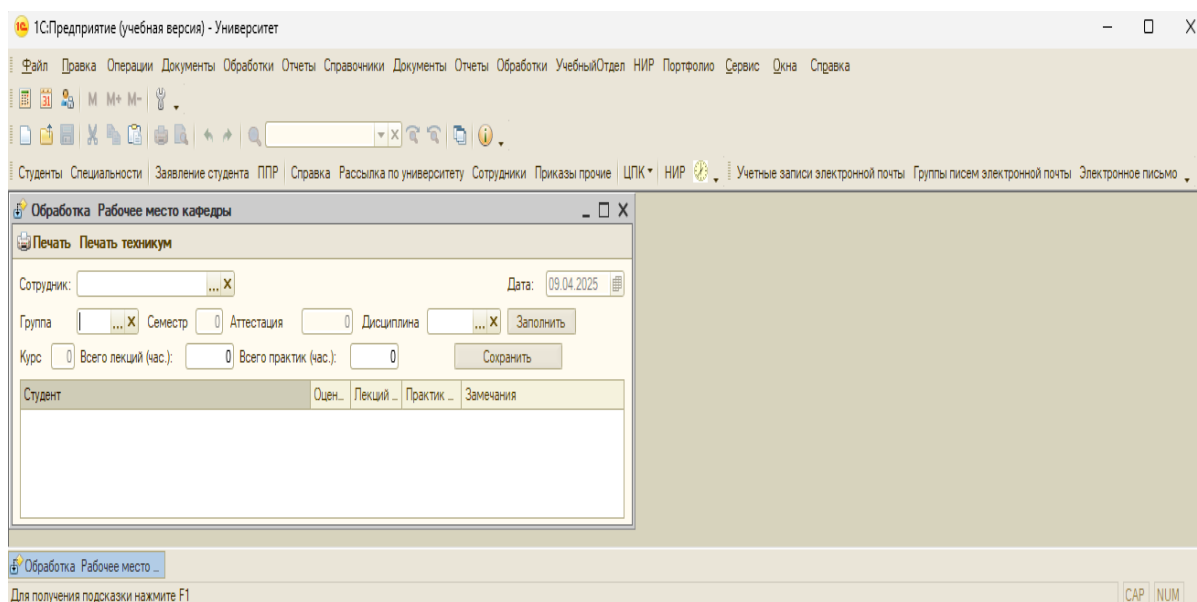


Рис. 1. Интерфейс конфигурации в режиме «1С: Предприятие 8.2»

После перевода конфигурации с платформы «1С: Предприятие 8.2» на платформу «1С: Предприятие 8.3» соответствующим образом изменился пользовательский интерфейс для ввода и редактирования данных об учебном процессе (рис. 2).

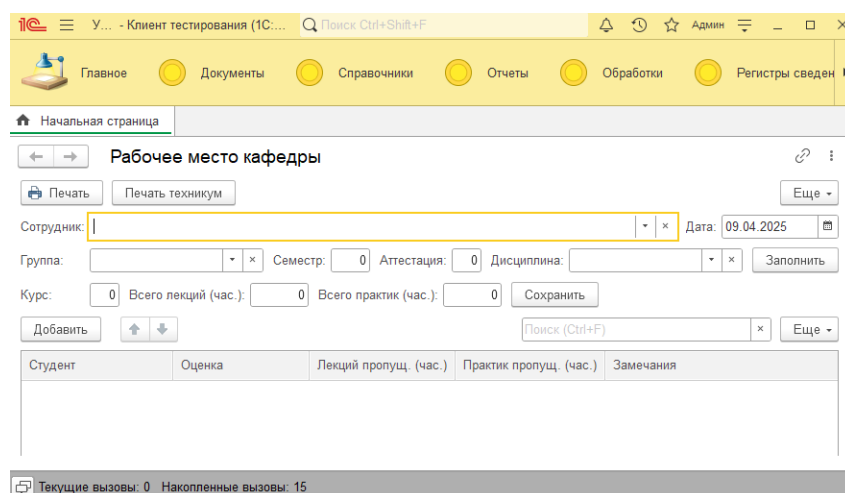


Рис. 2. Интерфейс конфигурации в режиме «1С: Предприятие 8.3»

Обсуждение результатов

Платформа «1С: Предприятие 8.3» позволяет обеспечить полноценную работу программы по сервисной модели с удаленных объектов [6]. Перевод конфигурации, разработанной в СГУГиТ для управления образовательной деятельностью, на платформу «1С: Предприятие 8.3» предоставляет возможности работать с системой для веб-клиентов с помощью облачных технологий: преподаватели и сотрудники университета теперь могут входить в систему через Интернет и использовать мобильные гаджеты.

Также конфигурация на платформе «1С: Предприятие 8.3» имеет более удобный, интуитивно понятный сотрудникам вуза интерфейс, который они могут подстраивать под свои предпочтения в процессе работы.

Так как каждым годом «облачные» сервисы все более активно используются для хранения данных, работы с электронной почтой и офисными приложениями, то переход на новую платформу открывает широкие возможности для дальнейшего развития конфигурации, используемой в СГУГиТ для организации учебного процесса: интеграция с другими образовательными системами, разработка мобильных приложений и т. д.

Заключение

Перевод конфигурации, разработанной на платформе «1С: Предприятие 8.2», на платформу «1С: Предприятие 8.3» позволил в СГУГиТ оптимизировать информационные потоки, повысил оперативность получения отчетных данных о текущем состоянии учебного процесса, улучшил качество анализа полученных данных. Как результат, вносимые в учебный процесс коррективы положительно сказались на эффективности образовательной деятельности университета.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Голубицкий Р.А., Булавский А.В., Фролов Ю.В. Оценка персонала образовательной организации на базе платформы «1С: Предприятие 8.3» // Новые информационные технологии

в образовании: XXV Международная научно-практическая конференция. – Москва: Изд-во ООО «1С-Паблишинг», 2025. – С. 114-117.

2. Елисеева Д.Ю., Воробьева А.И., Селютин Д.Ю., Каторгин М.К., Нагина К.С. Технология обработки стипендиальных заявок на платформе «1С: Предприятие» // Современные информационные технологии в образовании, науке и промышленности: XX Международная конференция, XVIII Международный конкурс научных и научно-методических работ, Международный конкурс «Нейросетевой рисунок». – Москва: Изд-во ООО «Издательство «Экон-Информ», 2021. – С. 23-25.

3. Лысковцев И.В., Бендик Н.В. Внедрение модуля аспирантуры системы "1С: Предприятие" для оптимизации работы отдела подготовки кадров высшей квалификации Иркутского ГАУ // Аграрная наука в инновационном развитии агропромышленного комплекса Иркутской области: Материалы очно-заочной научно-практической конференции посвященной 90-летию Иркутского ГАУ и Дню Российской науки. – Иркутск: Издательство: Иркутский государственный аграрный университет им. А.А. Ежевского, 2024. – С. 267-268.

4. Перевод конфигураций на платформе "1С: Предприятие 8.2" на платформу "1С:Предприятие 8.3" без режима совместимости с версией 8.2.URL: <https://its.1c.ru/db/metod8dev/content/5293/hdoc> . Текст: электронный.

5. Интерфейс "Такси". Концепция и назначение. URL:<https://its.1c.ru/db/metod8dev#content:5471:hdoc>. Текст: электронный.

6. Соколова Ю.И, Землякова А.А., Кудрявцева И.И. Развитие программы "1С: Предприятие" Эволюция платформы // Молодые ученые - развитию национальной технологической инициативы (Поиск). – 2022. – №1. – С. 1093-1095

© Н. С. Федотов, Д. Ю. Смирнов, 2025

А. Д. Филькова^{1✉}, А. А. Шаранов¹

Разработка системы автономного управления дроном с использованием компьютерного зрения для непрерывного слежения за объектом

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: anastasiyadeniisovna@mail.ru

Аннотация. В статье представлена разработка системы автономного управления дроном, обеспечивающей непрерывное слежение за объектом на основе технологий компьютерного зрения. Актуальность работы обусловлена возрастающим спросом на автономные системы мониторинга в таких областях, как безопасность, поисково-спасательные операции и видеосъемка. Система реализована на языке Python с использованием библиотек OpenCV и Pioneer SDK, что обеспечивает высокую производительность и гибкость. Основные компоненты системы включают модуль компьютерного зрения для обнаружения и отслеживания объектов, модуль управления дроном и пользовательский интерфейс. Тестирование системы показало среднюю точность обнаружения объектов на уровне 85 % при скорости обработки 15 кадров в секунду. Разработанное решение демонстрирует устойчивость к изменениям освещения и ракурса, а также возможность адаптации для различных типов объектов.

Ключевые слова: автономные системы, компьютерное зрение, OpenCV, Pioneer SDK, Python, обнаружение объектов, управление дроном

A. D. Filkova^{1✉}, A. A. Sharapov¹

Development of an autonomous drone control system using computer vision for continuous object tracking

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: anastasiyadeniisovna@mail.ru

Abstract. The article presents the development of an autonomous drone control system for continuous object tracking based on computer vision technologies. The relevance of the work is due to the growing demand for autonomous monitoring systems in areas such as security, search and rescue operations, and videography. The system is implemented in Python using OpenCV and Pioneer SDK libraries, ensuring high performance and flexibility. The main components of the system include a computer vision module for object detection and tracking, a drone control module, and a user interface. System testing showed an average object detection accuracy of 85% at a processing speed of 15 FPS. The developed solution demonstrates resilience to changes in lighting and perspective, as well as adaptability to various object types.

Keywords: autonomous systems, computer vision, OpenCV, Pioneer SDK, Python, object detection, drone control

Введение

Современные беспилотные летательные аппараты (БПЛА) активно применяются в различных сферах, включая безопасность, мониторинг и видеосъемку.

Однако большинство коммерческих решений для автоматического отслеживания объектов обладают ограниченными возможностями настройки и адаптации к специфическим задачам. Это обуславливает необходимость разработки специализированных систем, способных эффективно работать в изменяющихся условиях.

Целью данной работы является создание системы автономного управления дроном для непрерывного слежения за объектом с использованием технологий компьютерного зрения. Для достижения этой цели были поставлены следующие задачи:

- анализ существующих решений и технологий;
- проектирование модульной архитектуры системы;
- реализация алгоритмов обнаружения и отслеживания объектов;
- разработка пользовательского интерфейса;
- тестирование и оптимизация производительности системы.

Обзор и выбор технологий для разработки

Для обнаружения и отслеживания объектов в режиме реального времени проводился сравнительный анализ ключевых технологий компьютерного зрения. Каскадные классификаторы Хаара демонстрируют высокую скорость работы при низких вычислительных затратах, однако их существенным ограничением является чувствительность к изменениям освещения и ракурса наблюдения. Альтернативные алгоритмы на основе HOG и SVM обеспечивают повышенную точность детекции, но предъявляют значительно более высокие требования к вычислительным ресурсам. Наиболее передовые методы глубокого обучения, такие как YOLO и SSD, показывают превосходную точность распознавания, однако их практическое применение в бортовых системах дронов ограничено из-за экстремальных требований к производительности оборудования.

На основании комплексного анализа была выбрана гибридная архитектура, сочетающая каскадные классификаторы Хаара для первичного обнаружения объектов и алгоритм KCF (Kernelized Correlation Filter) для их последующего отслеживания. Данное решение обеспечивает оптимальный баланс между точностью детекции и производительностью, что является критически важным для работы в условиях ограниченных вычислительных ресурсов бортовых систем дронов.

Управление дроном реализовано через Pioneer SDK, предоставляющий программный интерфейс для отправки управляющих команд и получения телеметрических данных. Технологический стек реализации включает язык Python и библиотеку OpenCV для обработки видеопотока в реальном времени, что обеспечило кроссплатформенность и эффективную интеграцию компонентов системы.

Разработка программного обеспечения

Система построена по модульному принципу, что обеспечивает гибкость и расширяемость. Основные модули включают модуль компьютерного зрения, который обрабатывает видеопоток, обнаруживает и отслеживает объекты; модуль управления

дроном, формирующий команды для его перемещения на основе данных от модуля компьютерного зрения; и пользовательский интерфейс, предоставляющий инструменты для управления системой и визуализации процесса отслеживания.

Для обнаружения объектов используется каскадный классификатор Хаара. После обнаружения объект отслеживается с помощью алгоритма KCF, который устойчив к небольшим изменениям внешнего вида объекта. Для повышения точности реализован механизм адаптивного отслеживания, учитывающий динамику изменения положения и размера объекта.

При потере объекта система автоматически переключается в режим поиска, последовательно проверяя заданные высоты (150 см, 165 см, 180 см). Это повышает вероятность повторного обнаружения объекта.

Интерфейс разработан на основе библиотеки PyQt5 и включает:

- область отображения видеопотока;
- панель управления для запуска/остановки отслеживания;
- панель статуса с информацией о текущем состоянии системы.

Пример кода для обработки видеопотока:

```
def detect_face(self, frame):
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    faces = self.face_cascade.detectMultiScale(gray, scaleFactor=1.1, minNeighbors=5)
    if len(faces) > 0:
        return max(faces, key=lambda rect: rect[2] * rect[3])
    return None
```

Разработка программного обеспечения

Система проходила комплексное тестирование в различных условиях для оценки ее надежности, точности и производительности.

Были проведены тестовые запуски с объектами (при разных условиях освещения (дневной свет, сумерки, искусственное освещение)). Средняя точность обнаружения составила 85 %, что подтверждает эффективность выбранного сочетания каскадных классификаторов Хаара и алгоритма KCF [1]. Наибольшая точность (92 %) достигнута при хорошем освещении, наименьшая (78 %) – в условиях недостаточной освещенности.

Система демонстрировала стабильную работу со скоростью 15 кадров в секунду на оборудовании с процессором Intel Core i5 и 8 ГБ оперативной памяти. Задержка между получением кадра и формированием управляющей команды не превышала 100 мс, что соответствует требованиям реального времени [2]. При этом нагрузка на ЦПУ не превышала 65 %, что свидетельствует о хорошей оптимизации алгоритмов.

В ходе тестирования специально создавались сложные условия:

- частичное перекрытие объекта (точность снижалась на 15–20 %);
- резкие изменения освещения (система адаптировалась за 2–3 секунды);

– быстрое движение объекта (потеря трекинга происходила только при скорости свыше 8 м/с).

При тестировании механизма поиска на разных высотах эффективность повторного обнаружения объекта после потери составила:

- на высоте 150 см – 82 %;
- на высоте 165 см – 88 %;
- на высоте 180 см – 76 %.

Среднее время повторного обнаружения – 4,7 секунды [3].

Таблица 1

Параметр	Условия тестирования	Результат
Точность обнаружения	Хорошее освещение	92 %
	Плохое освещение	78 %
Скорость обработки	Стандартные условия	15–18 FPS
Задержка управления	Максимальная нагрузка	98 мс
Устойчивость к помехам	Частичное перекрытие	15 % к точности

Заключение

Разработанная система автономного управления дроном для непрерывного слежения за объектом успешно прошла все этапы тестирования и показала следующие ключевые преимущества.

Система демонстрирует стабильную работу в различных условиях с точностью обнаружения объектов до 92 % [1]. Реализованный механизм адаптивного трекинга позволяет компенсировать изменения освещения и ракурса, а модульная архитектура обеспечивает гибкость при модернизации отдельных компонентов.

Достигнутая скорость обработки 15 FPS при задержке менее 100 мс полностью удовлетворяет требованиям систем реального времени [2]. Оптимизация алгоритмов позволила снизить вычислительную нагрузку, что особенно важно для бортовых систем дронов.

Система может быть использована в различных областях:

- системы видеонаблюдения и безопасности;
- поисково-спасательные операции;
- профессиональная видеосъемка;
- промышленный мониторинг [4].

Для дальнейшего совершенствования системы предлагается:

- интеграция алгоритмов глубокого обучения (YOLO, SSD) для повышения точности обнаружения [5];
- разработка механизма обхода препятствий;
- реализация распознавания жестов для управления;
- оптимизация для работы на одноплатных компьютерах.

Проведенные испытания подтвердили, что система соответствует всем заявленным требованиям и готова к практическому применению. Особенно перспективным направлением представляется ее использование в комбинации с другими технологиями компьютерного зрения для создания комплексных решений в области автономных систем мониторинга [3].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кузнецов А.В., Иванов С.М. Современные методы обнаружения объектов в видеопотоке // Вестник компьютерных и информационных технологий. - 2021. - №5. - С. 34-42.
2. Соколов И.А., Николаев Д.П. Алгоритмы компьютерного зрения для БПЛА // Информационные технологии. - 2022. - №2. - С. 78-89.
3. Zhang K. et al. Joint face detection and alignment using multitask cascaded convolutional networks // IEEE Signal Processing Letters. - 2020. - Vol. 27. - P. 1499-1503.
4. Laganière R. OpenCV Computer Vision Application Programming Cookbook // Packt Publishing. - 2020. - 420 с.
5. Mordvintsev A. Advanced OpenCV-Python Tutorials // OpenCV. - 2023. URL: <https://opencv-python-tutorials.readthedocs.io/> (дата обращения: 10.05.2025).

© А. Д. Филькова, А. А. Шаранов, 2025

А. А. Цыганков¹

Виртуальный стенд для проведения экспериментального сравнительного исследования методов активного анализа информационных систем

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: aatsygankov@mephi.ru

Аннотация. Сбор информации об атакуемой сетевой инфраструктуре и активное сканирование являются техниками атак на корпоративную инфраструктуру. Некорректная конфигурация сетевого и серверного оборудования может стать точкой входа атакующих в информационную систему. Для оценки защищенности системы используются сетевые сканеры. В работе рассматривается виртуальный стенд для проведения экспериментального сравнительного исследования методов активного анализа информационных систем. Целью исследования является разработка платформы для анализа поведения сетевых сканеров. В рамках исследования проанализированы сценарии использования и приведены рекомендации по автоматизации установки и конфигурирования виртуального стенда. На обзор вынесена архитектура платформы, а также изложен подход к ее разработке. Результаты исследования могут использоваться для построения ряда виртуальных стендов, исследующих поведение методов активного анализа информационных систем. Область применимости включает инфраструктуру, функционирующую на базе стека протоколов TCP/IP.

Ключевые слова: виртуальный стенд, сетевая безопасность, сетевые сканеры, TCP/IP

A. A. Tsygankov¹

Virtual stand for experimental comparative study of active analysis methods for information systems

¹National Research Nuclear University MEPHI (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: aatsygankov@mephi.ru

Abstract. Gathering information about the targeted network infrastructure and active scanning are common attack techniques against corporate systems. Misconfigured network and server equipment can serve as an entry point for attackers into an information system. Network scanners are widely used to assess system security. This study presents a virtual testbed for conducting experimental comparative research on active analysis methods for information systems. The research aims to develop a platform for analyzing the behavior of network scanners. The study examines usage scenarios and provides recommendations for automating the deployment and configuration of the virtual testbed. The paper reviews the platform's architecture and outlines the development approach. The findings can be applied to construct a range of virtual testbeds for studying the behavior of active analysis methods in information systems. The proposed solution is applicable to infrastructures operating on the TCP/IP protocol stack.

Keywords: virtual stand, network security, network scanners, TCP/IP

Введение

Активное развитие информационных технологий способствует расширению собственной информационной инфраструктуры государственных учреждений и частных компаний, что не только расширяет поверхность потенциальной атаки, но и увеличивает влияние человеческого фактора на безопасность сетевого и серверного оборудования. Согласно исследованиям Лаборатории Касперского, одного из ведущих вендоров в области информационной безопасности в Российской Федерации, 12 % срабатываний антивирусного оборудования в день приходится на сканирование UDP (англ. User Datagram Protocol) портов, 13 % – на атаки, использующие уязвимости TCP (англ. Transmission Control Protocol, Internet Protocol). Однако методы активного анализа информационных систем используются не только злоумышленниками, но и специалистами информационной безопасности для поддержания актуальных данных о состоянии корпоративной инфраструктуры, инвентаризации активов и проверки соответствия узлов сети требованиям безопасности [1–3].

На стандартизацию обеспечения сетевой информационной безопасности также направлены ряд нормативно-правовых актов, в частности Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и Приказом Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств». Актуальность исследования также подтверждается Концепцией государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий, утвержденной Правительством Российской Федерации.

Исследованиями в области методов активного анализа занимается ряд научных школ, в частности Zakir Durumeric, Eric Wustrow и J. Alex Halderman (университет Мичигана). В своих работах научная группа выносит на обзор сетевой сканер Zmap, а также производит сравнительный анализ собственного решения с актуальными аналогами [4]. Поиск оптимального решения позволяет минимизировать не только риски ложноположительных срабатываний систем мониторинга состояния корпоративной инфраструктуры, но и затраченное на исследование время и ресурсы. Приведенные данные свидетельствуют об актуальности темы исследования и указывают на растущую потребность в разработке решений для анализа сканеров сети.

Моделирование предметной области

Методы активного анализа, используемые для исследования информационной системы, функционируют идентичным образом и эксплуатируют уязвимости стека протоколов TCP/IP. Для разработки виртуального стенда для проведения сравнительного анализа сетевых сканеров была разработана UML-диаграмма (англ. Unified

Modeling Language) последовательности взаимодействия (рис. 1), демонстрирующий процесс взаимодействия модулей виртуального стенда на примере исследования порта на доступность [5].

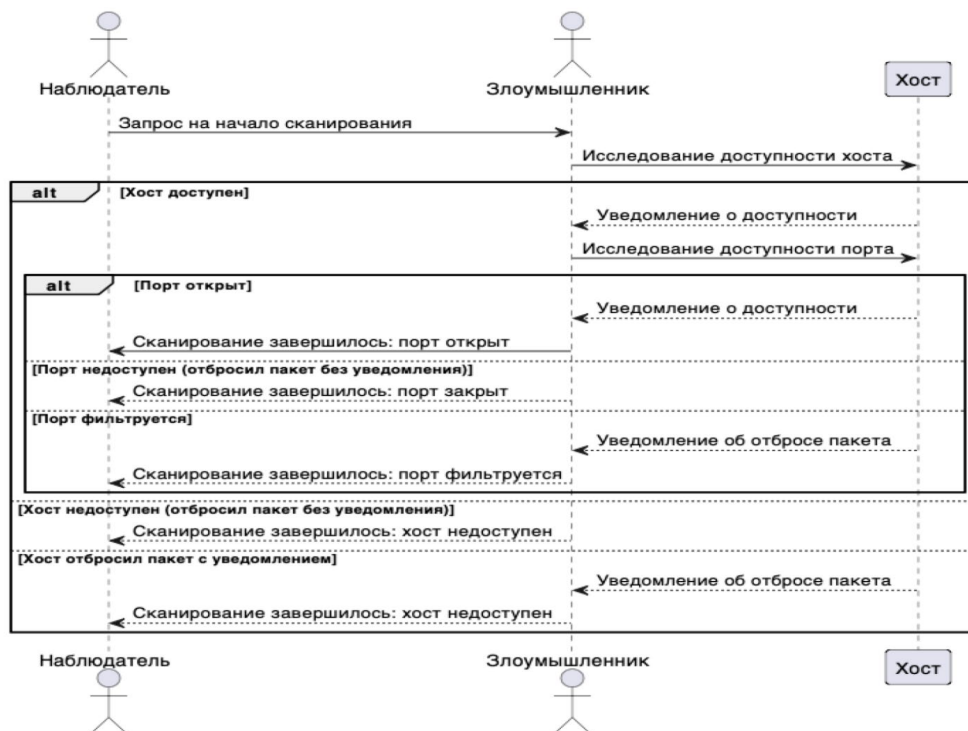


Рис. 1. UML-диаграмма последовательности взаимодействия с виртуальным лабораторным стендом

Предусматривается три участника сетевого взаимодействия: наблюдатель, инициирующий процесс сканирования; злоумышленник, выполняющий непосредственное взаимодействие с хостом для получения информации; хост, объект сканирования.

Постановка задачи

Целью исследования является разработка платформы для сравнительного анализа поведения сетевых сканеров. В рамках декомпозиции цели выделены следующие задачи:

- 1) определение требований к системе;
- 2) моделирование топологии сети виртуального стенда;
- 3) выбор стека технологий.

Результатом работы является описание функциональности, архитектуры и стека технологий выносимого на обзор виртуального стенда для проведения экспериментального сравнительного исследования методов активного анализа информационных систем. Топология сети и сама платформа удовлетворяют установленным в рамках исследования критериям с целью имитации корпоративной инфраструктуры предприятия.

Требования к виртуальному стенду

Топология сети виртуального стенда для имитации корпоративной инфраструктуры должна удовлетворять требованиям [6]:

- 1) должна содержать демилитаризованную зону с помещенными в нее виртуальными машинами, имитирующими вычислительные мощности;
- 2) должна удовлетворять трехуровневой иерархической модели построения сети и содержать объекты на всех трех уровнях: доступа, распределения и ядра;
- 3) в топологии сети должны быть созданы оптимальные условия для скоростного обмена информацией между хостами (в том числе с использованием технологии связующего дерева);
- 4) наборы хостов сети виртуального стенда должны быть логически разделены;
- 5) топология сети не должна содержать единой точки отказа;
- 6) любое взаимодействие объектов локальной сети с глобальной сетью должно происходить через межсетевой экран.

Выполнение требований к топологии сети виртуального стенда обеспечивает корректные выходные данные сравнительного анализа сетевых сканеров, сопоставимые с реальной корпоративной инфраструктурой предприятия [7].

Виртуальный лабораторный стенд также должен удовлетворять ряду требований [8, 9]:

- 1) установка и конфигурирование каждого модуля стенда должна происходить автоматически;
- 2) в составе стенда должен быть определен механизм поддержания декларируемого состояния модулей;
- 3) в составе стенда должен быть определен механизм централизованного сбора и хранения системных журналов модулей.

Важным аспектом также является возможность установки виртуального стенда на различные платформы, операционные системы и гипервизоры.

Топология сети виртуального стенда

Учитывая требования, описанные в предыдущей главе, была разработана топология сети виртуального стенда (рис. 2).

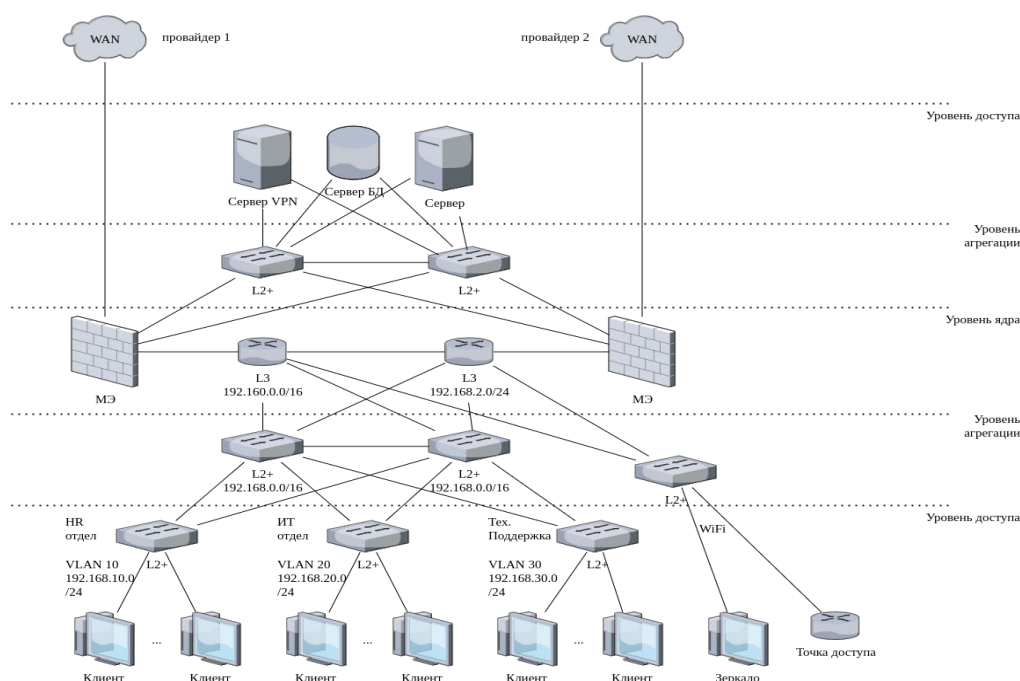


Рис. 2. Топология сети виртуального стенда

На рис. 2 представлена топология сети, построенная с учетом трехуровневой иерархической модели построения сети. На уровне доступа располагаются виртуальные машины, имитирующие хосты сотрудников. Стоит отметить, что предложенная топология содержит логическое разделение конечных хостов на группы с использованием технологии виртуальных локальных сетей VLAN (англ. Virtual Local Area Network). Также на уровне доступа располагаются виртуальные машины, имитирующие сервера (в рамках примера сервер VPN (англ. Virtual Private Network), баз данных) [10–12].

На уровне агрегации находятся виртуальные коммутаторы. Отказоустойчивость оборудования на этом уровне обеспечивается использованием технологии связующего древа.

На уровне ядра расположены два межсетевых экрана, ограничивающие трафик между локальной сетью предприятия, глобальной сетью и демилитаризованной зоной.

Предложенная в рамках исследования топология полностью удовлетворяет поставленным целям построения виртуального стенда и определенным требованиям.

Стек технологий

Важными аспектами при выборе технологий виртуального лабораторного стенда является воспроизводимость, масштабируемость и точность конечных измерений. Стек технологий, основываясь на предложенных требованиях, содержит:

- 1) систему управления конфигурациями;
- 2) систему мониторинга;

3) систему агрегации журналов событий.

Основу управления конфигурациями составляет Ansible, выбранный в силу его агент-независимой архитектуры, поддержки декларативного подхода через YAML-сценарии (англ. YAML Ain't Markup Language) и кроссплатформенной совместимости. Важным преимуществом решения является минимизация вмешательства в тестовую среду в связи с архитектурой системы. Для обеспечения идемпотентности конфигураций применяются модули Terraform, позволяющие программно определять топологию сети и виртуальные машины в гипервизорах [13].

Мониторинг сетевой активности предлагается выстраивать на базе Prometheus – системы сбора временных рядов, обладающей высокой производительностью при обработке потоковых данных. Prometheus интегрирован с экспортерами для сбора метрик сетевых интерфейсов, состояния сервисов и трафика межсетевых экранов. Визуализация данных осуществляется через Grafana, предоставляющую гибкие инструменты построения дашбордов на основе запросов к PromQL [14].

Для централизованного сбора и анализа журналов событий предлагается платформа Loki, отличающаяся от традиционных решений низкими накладными расходами на хранение и возможностью использования меток для индексации логов [15].

Виртуальный лабораторный стенд, предложенный в рамках настоящего исследования, возможно реализовать в рамках программных эмуляторов, симуляторов, гипервизоров 1-го и 2-го типа.

Заключение и обсуждение

В ходе научно-практических изысканий была предложена топология сети и стек технологий виртуального стенда для проведения экспериментального сравнительного исследования методов активного анализа информационных систем. Архитектура стенда основана на трехуровневой модели сети, включающей зоны доступа, агрегации и ядра, что обеспечивает соответствие реальным корпоративным инфраструктурам. Применение технологий автоматизации развертывания, мониторинга и агрегации журналов позволяет создать воспроизводимую среду, пригодную для многократного тестирования сетевых сканеров. Область применения полученного решения включает информационные системы, функционирующие на базе стека протоколов TCP/IP.

Практическая значимость исследования заключается в возможности использования разработанного стенда для валидации сетевых сканеров, обучения специалистов по информационной безопасности и тестирования систем обнаружения вторжений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия //Безопасность информационных технологий. – 2018. – Т. 25. – №. 4. – С. 42-51.

2. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия //Защита информации. Инсайд. – 2021. – №. 5. – С. 101.
3. Басыня Е. А., Малышев Е. А. Обеспечение достоверности результатов научно-практических изысканий с применением программной инженерии //Защита информации. Инсайд. – 2023. – Т. 112. – №. 4. – С. 14.
4. Durumeric Z., Wustrow E., Halderman J. A. {ZMap}: Fast internet-wide scanning and its security applications //22nd USENIX Security Symposium (USENIX Security 13). – 2013. – С. 605-620.
5. Wang Y. et al. A Unified Modeling Framework for Automated Penetration Testing //arXiv preprint arXiv:2502.11588. – 2025.
6. Bringhenti D. et al. Automation for network security configuration: State of the art and research trends //ACM Computing Surveys. – 2023. – Т. 56. – №. 3. – С. 1-37.
7. Медведев Ю. С., Терехов В. В. Особенности построения распределенной корпоративной сети предприятия для обеспечения информационными и вычислительными ресурсами //Научные чтения имени профессора НЕ Жуковского. – 2022. – С. 258-260.
8. Врублевский Д. Н. Разработка лабораторных работ для изучения средств защиты компьютерных сетей //Молодость. Интеллект. Инициатива. – 2016. – С. 10-10.
9. Кукушкина Н. В., Новохрестов А. К. Разработка лабораторного стенда для изучения систем обнаружения вторжений //Безопасность цифровых технологий. – 2021. – №. 4 (103). – С. 37.
10. Lavrov E. A. et al. Analysis of information security issues in corporate computer networks //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2021. – Т. 1047. – №. 1. – С. 012117.
11. Varadharajan V. et al. A policy-based security architecture for software-defined networks //IEEE Transactions on Information Forensics and Security. – 2018. – Т. 14. – №. 4. – С. 897-912.
12. Добрышин М. М. Иерархическая модель изменения уровня информационной безопасности в условиях компьютерных атак на корпоративную сеть связи //Экономика и качество систем связи. – 2024. – №. 3 (33). – С. 108-119.
13. Opdebeeck R., Zerouali A., De Roover C. Smelly variables in ansible infrastructure code: Detection, prevalence, and lifetime //Proceedings of the 19th international conference on mining software repositories. – 2022. – С. 61-72.
14. An S. Y. et al. A pre-study on the open source prometheus monitoring system //Smart Media Journal. – 2021. – Т. 10. – №. 2. – С. 110-118.
15. Pai K., Srinivas B. K. Enhanced Visibility for Real-time Monitoring and Alerting in Kubernetes by Integrating Prometheus, Grafana, Loki, and Alerta //International Journal of Scientific Research in Engineering and Management. – 2024.

© А. А. Цыганков, 2025

*А. В. Челнокова*¹✉

Система автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: chelalex1511@gmail.com

Аннотация. На обзор выносятся проблема обеспечения подотчетности и неотказуемости объектов инфраструктуры предприятия, функционирующей на базе стека протоколов TCP/IP версии 4, посредством их автоматизированного развертывания и технологического сопровождения на каждом этапе жизненного цикла. С целью решения данной проблемы разработана система автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия. Утверждается, что представленная система позволяет предприятию реализовать автоматизацию настройки виртуальных машин, исключив при этом ошибки ручного конфигурирования. В качестве стека технологий выбрана система управления конфигурациями Ansible и инструмент управления внешними ресурсами Terraform. Тестовый стенд развертываемой инфраструктуры представлен на базе системы оркестрации Kubernetes. Областью применения представленной работы являются корпоративные вычислительные сети, функционирующие на основе стека протоколов TCP/IP.

Ключевые слова: инфраструктура как код, контейнеризация, оркестрация Kubernetes, мониторинг инфраструктуры, Ansible, Terraform

*A. V. Chelnokova*¹✉

System of automated deployment and technological support of enterprise infrastructure

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: chelalex1511@gmail.com

Abstract. The problem of ensuring accountability and fault tolerance of enterprise infrastructure objects operating on the basis of TCP/IP version 4 protocol stack by means of their automated deployment and technological support at each stage of the life cycle is brought up for review. In order to solve this problem, a system of automated deployment and technological support of enterprise infrastructure is developed. It is argued that the presented system allows the enterprise to implement automation of virtual machine configuration, while eliminating manual configuration errors. Ansible configuration management system and Terraform external resource management tool are selected as the technology stack. A testbed of the deployed infrastructure is presented based on the Kubernetes orchestration system. The application area of the presented work is corporate computing networks operating on the basis of TCP/IP protocol stack.

Keywords: infrastructure as code, containerization, Kubernetes orchestration, infrastructure monitoring, Ansible, Terraform

Введение

Современные информационные технологии играют ключевую роль в функционировании предприятий, обеспечивая эффективность их работы и развитие. Однако

с ростом сложности и масштабов инфраструктуры увеличиваются и риски, связанные с безопасностью, производительностью и управлением. На фоне глобальных изменений, связанных с внедрением облачных технологий, контейнеризации и виртуализации, предприятия сталкиваются с необходимостью внедрения эффективных механизмов автоматизации развертывания и технологического сопровождения инфраструктуры. Эксперты организации Cloud Native Computing Foundation утверждают, что 41 % из всех организаций внедрили систему оркестрации Kubernetes, а в ближайшие 5 лет это число удвоится [1]. Проблематикой комплексной методологии интеллектуально-адаптивного управления информационной инфраструктурой предприятия занимается научная школа Басыни Е. А. [2, 3].

Эти механизмы должны обеспечивать стабильную работу всех компонентов инфраструктуры, соответствовать требованиям безопасности и быть устойчивыми к различным внешним и внутренним угрозам. Так в работах, представленных группой ученых Ammar Zeini, Ruth G. Lennon, Patrick Lennon, Abbas Medhi, Ranjan Walia, Syed Imran Abbas и Ankit Garg, исследуются проблемы безопасности подхода «Инфраструктура как код» (IaC) [4–6]. Несмотря на то, что данный подход предлагает значительные преимущества в развертывании и управлении инфраструктурой, он также создает серьезные проблемы безопасности, требующие тщательного анализа.

Развитие технологий контейнеризации и виртуализации оказало влияние на законодательный аспект данной области. Согласно требованиям ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», необходимо учитывать аспекты безопасности на всех этапах жизненного цикла программного обеспечения, включая проектирование, разработку, тестирование и эксплуатацию [7]. В связи с этим возникает необходимость не только в проектировании и разработке системы автоматизированного развертывания, но и в ее интеграции с существующими механизмами безопасности, что включает в себя обеспечение подотчетности всех действий, выполняемых в системе, а также неотказуемости, исключающей возможность отрицания выполненных операций. Эти аспекты играют ключевую роль в повышении надежности, отказоустойчивости и защищенности инфраструктуры.

В связи с существующей проблематикой становится актуальным решения класса задач по автоматизации развертывания и технологического сопровождения инфраструктуры предприятия.

Исследование предметной области

Несколько групп ученых занимаются исследованиями, посвященными вопросам обеспечения безопасности автоматизированных систем, включая подотчетность и неотказуемость операций. Так, в работе ученых Daniele Brighenti, Guido Marchetto, Riccardo Sisto, Fulvio Valenza исследуется новый подход к конфигурированию и развертыванию графа функций безопасности, который позволил бы выбирать лучшие виртуальные функции безопасности среди большого пула, что делает принятие решений вручную невыполнимым [8]. Достоинства предложенного подхода заключаются в его способности оптимизировать процесс выбора и разверты-

вания виртуальных функций безопасности в условиях масштабных виртуальных сетей. Однако у предложенного решения имеются и недостатки. Во-первых, определение функциональной абстракции требует дальнейших исследований для выбора оптимального уровня детализации, что может усложнить процесс ее стандартизации и внедрения. Во-вторых, текущая реализация основывается на решении задач типа MaxSMT, что может оказаться недостаточно производительным для некоторых сценариев. Это указывает на необходимость разработки и внедрения альтернативных или дополнительных методов, таких как эвристики, для повышения общей производительности системы.

В исследовании, опубликованном учеными Ruiqi Zeng, Yiru Niu, Lanfei Qiao, предлагается новая технология построения автоматического развертывания и обновления многоэкземплярной системы микросервиса, позволяющая упростить развертывание и дальнейшее технологическое сопровождение инфраструктуры [9]. Достоинства предложенного подхода заключаются в его комплексности и автоматизации всех этапов работы с контейнеризованными микросервисными системами. Решение охватывает процесс разработки, сборки, развертывания и обновления, обеспечивая бесперебойную работу приложений даже в процессе их модернизации. Несмотря на вышеупомянутые достоинства, у работы имеются и недостатки. Во-первых, в исследовании уделено недостаточно внимания вопросам информационной безопасности, что особенно важно в условиях эксплуатации распределенных микросервисных систем. Во-вторых, тестирование предложенного решения проводится на ограниченном наборе сценариев, что может не полностью отражать все возможные сложности, возникающие при развертывании и обновлении в более масштабных и гетерогенных системах. Также работа недостаточно подробно рассматривает взаимодействие между компонентами платформы, что может вызывать вопросы относительно ее масштабируемости и интеграции с уже существующими инструментами разработки и управления.

В работе, опубликованной учеными Mohamed Oulaaffart, Remi Badonnel, Olivier Festor, исследуется подход автоматизации повышения безопасности облачных сервисов [10]. Достоинства работы заключаются в предложении системного подхода к автоматизации повышения безопасности облачных композитных сервисов в процессе миграции их ресурсов. Основное внимание уделено решению проблем, связанных с уязвимостями, возникающими при изменении конфигурации сервисов. Разработка алгоритмов для выбора адекватных механизмов безопасности на этапах до, во время и после миграции ресурсов подчеркивает глубокую проработку исследуемой темы. Недостатки работы связаны с отсутствием реализованного прототипа предложенного подхода, что ограничивает возможность оценки его производительности в реальных условиях. Использование иллюстративных примеров вместо тестирования на реальных сценариях снижает прикладную ценность результатов исследования.

Таким образом, в исследуемой области можно выделить несколько значимых проблем, а именно:

- 1) недостаточная подотчетность;

- 2) ошибки ручного конфигурирования;
- 3) отсутствие гарантий неотказуемости.

Постановка задачи

Целью настоящей работы является обеспечение подотчетности и неотказуемости объектов инфраструктуры предприятия, функционирующей на базе стека протоколов TCP/IP версии 4, посредством их автоматизированного развертывания и технологического сопровождения на каждом этапе жизненного цикла.

В ходе работы проведена ее декомпозиция на следующие задачи:

- 1) исследование предметной области;
- 2) проектирование системы автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия;
- 3) программная реализация спроектированной системы.

Предлагаемое решение

Системы автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия представляют собой комплексные информационно-технологические платформы, объединяющие инструменты автоматизации, методы оркестрации ресурсов, механизмы мониторинга и архитектурные решения для обеспечения эффективного управления жизненным циклом инфраструктуры. Эти системы играют ключевую роль в современных условиях, где требования к скорости развертывания, неотказуемости и подотчетности инфраструктуры становятся критически важными для успешного функционирования предприятий.

Метод автоматизированного развертывания инфраструктуры предприятия представляет собой последовательность взаимосвязанных этапов, направленных на обеспечение корректного создания и настройки инфраструктуры, а также последующего развертывания. На рис. 1 представлена блок-схема метода автоматизированного развертывания инфраструктуры предприятия.

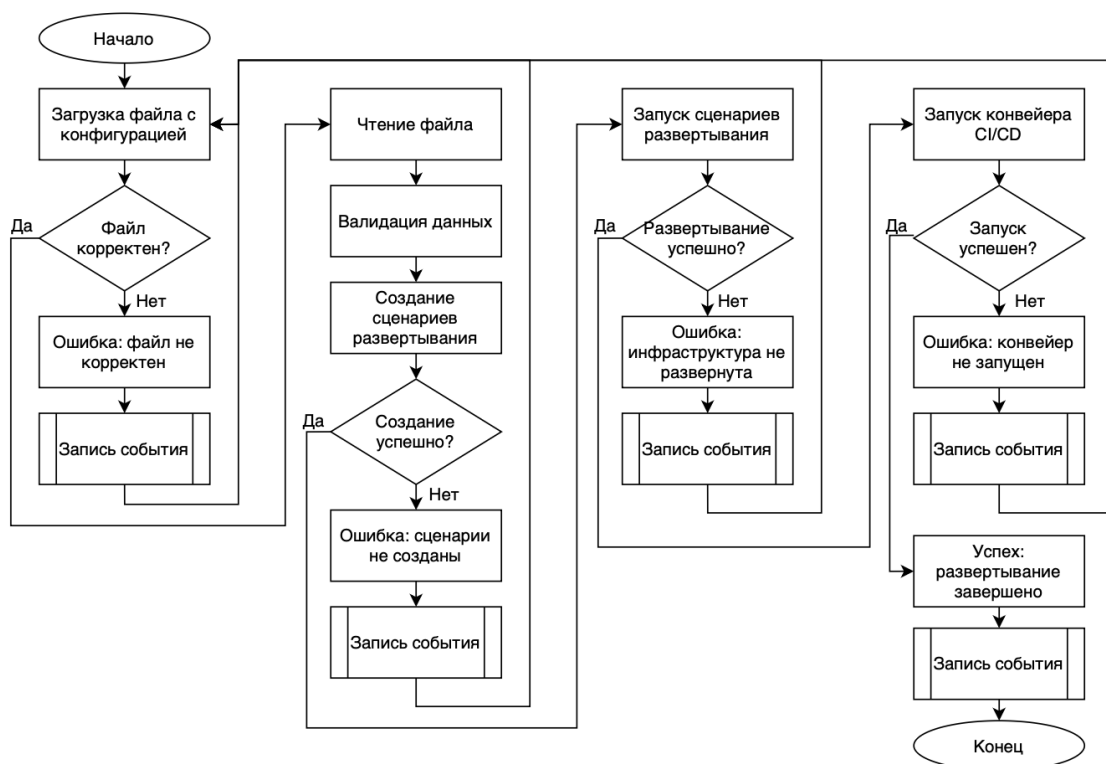


Рис. 1. Блок-схема метода автоматизированного развертывания инфраструктуры предприятия

На начальном этапе пользователь загружает файл конфигурации, содержащий описание инфраструктуры. Система проверяет корректность файла, включая его структуру и соответствие заданным требованиям. В случае обнаружения ошибок пользователь уведомляется и получает возможность загрузить исправленный файл.

После успешной проверки файла конфигурации система создает сценарии для развертывания. Если создание сценариев завершается неудачно, система предоставляет пользователю возможность исправить входные данные и повторить процесс.

Созданные сценарии последовательно выполняются для создания и настройки инфраструктуры. В случае возникновения ошибок на данном этапе система фиксирует их в событиях, уведомляет пользователя и предоставляет возможность повторного запуска сценариев после исправления параметров.

После успешного развертывания инфраструктуры система запускает конвейер CI/CD для развертывания сервисов. Если данный этап завершается с ошибкой, система регистрирует событие, уведомляет пользователя и предоставляет возможность повторного запуска после устранения неполадок.

В случае успешного завершения всех этапов система фиксирует результаты в событиях и уведомляет пользователя об успешном завершении процесса. Все

события регистрируются с помощью подпрограммы «Запись события». Ее блок-схема представлена на рис. 2.

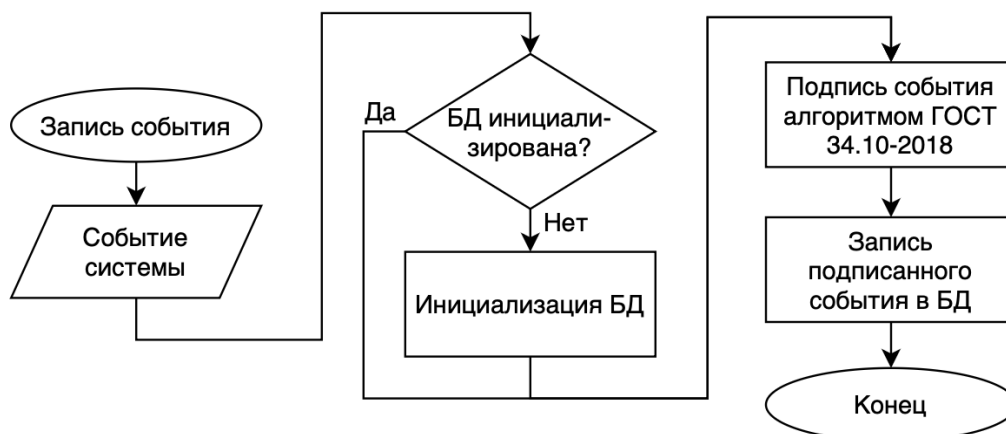


Рис. 2. Блок-схема подпрограммы «Запись события»

Формализованная подпрограмма представляет собой последовательность действий, направленных на обеспечение подотчетности и неотказуемости всех операций в системе. Подотчетность подразумевает возможность однозначно идентифицировать субъекта, ответственного за выполнение действия, а неотказуемость гарантирует, что субъект не сможет отрицать факт выполнения действия.

На начальном этапе система проверяет доступность и корректность базы данных. Если событие фиксируется впервые, то подпрограмма запускает процесс инициализации БД.

Подпрограмма принимает на вход событие системы, который содержит информацию о произошедшем действии, например, успешное развертывание инфраструктуры или ошибка в конвейере CI/CD. Запись включает в себя информацию о пользователе, время события и его описание.

Событие подписывается с использованием криптографического алгоритма ГОСТ 34.10-2018. Подпись связывает лог с конкретным пользователем, что обеспечивает неотказуемость: пользователь не сможет отрицать выполнение действия, так как подпись подтверждает его участие.

Подписанное событие сохраняется в базу данных. Это позволяет в дальнейшем использовать его для анализа, аудита и подтверждения факта выполнения действия. Проверка подписи событий осуществляется в соответствии с методом, представленным на рис. 3.

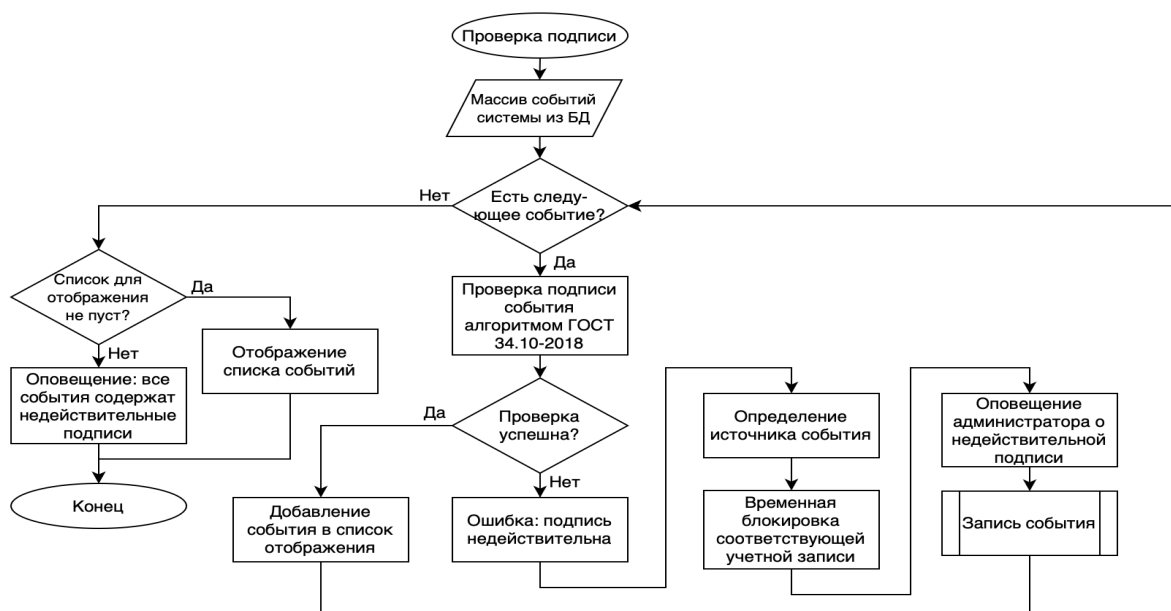


Рис. 3. Блок-схема метода проверки подписи события

На начальном этапе на вход подается массив событий из базы данных, которые содержат описание действия, метаданные (время, идентификатор пользователя и т. д.) и криптографическую подпись. Подпись была создана с использованием закрытого ключа пользователя, соответствующего открытому ключу, хранящемуся в системе (см. подпрограмму «Запись события»). В случае успешной проверки подпись признается валидной, что подтверждает неизменность данных с момента их подписания и участие пользователя в выполнении действия.

Если подпись успешно проверена, событие отображается в пользовательском интерфейсе, и процесс завершается успешно. Однако в случае обнаружения невалидной подписи подпрограмма переходит к обработке ошибки. На этом этапе система идентифицирует учетную запись пользователя, связанную с событием, и временно блокирует ее для предотвращения потенциально вредоносных действий. Одновременно с этим администраторы системы уведомляются о недействительной подписи, что позволяет оперативно реагировать на возможные угрозы. Само событие уведомления администраторов и блокировки пользователя фиксируется с помощью подпрограммы «Запись события» для последующего анализа и расследования.

В завершение метод отображает список действительных записей событий или в противном случае оповещает пользователя о том, что все события оказались с недействительными подписями.

На рис. 4 представлен снимок экрана, демонстрирующий работоспособность данной системы. На экране отображен результат анализа конфигурационного файла, а также выведено сообщение «Конфигурация успешно принята!»,

что свидетельствует о корректной работе системы автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия.

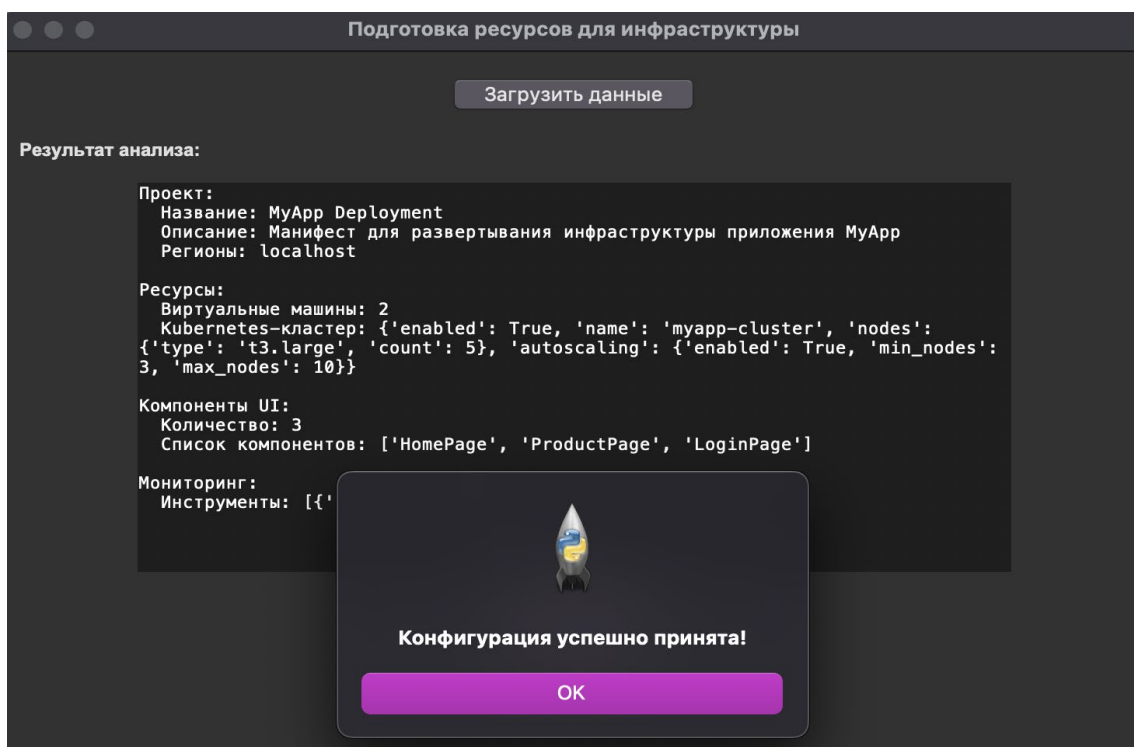


Рис. 4. Демонстрация работоспособности системы

Система демонстрирует модульность и гибкость, предоставляя возможность расширения функциональности, например, интеграции с инструментами Terraform и Ansible для автоматизации развертывания и настройки инфраструктуры. Таким образом, программная реализация сочетает в себе удобство взаимодействия с пользователем, эффективность обработки данных и потенциал для дальнейшего развития, что делает ее надежным решением для управления инфраструктурой предприятия.

Заключение

В рамках данной работы была предложена система, автоматизирующая развертывание инфраструктуры предприятия с дальнейшим технологическим сопровождением, которая была программно реализована и успешно продемонстрировала свою работоспособность.

Практическая значимость работы состоит в повышении безопасности инфраструктуры предприятия и в устранении ошибок ее ручного конфигурирования.

Новизна данной работы состоит в предложении новых методов автоматизированного развертывания инфраструктуры и ее дальнейшего сопровождения, повышающего подотчетности и неотказуемости объектов инфраструктуры предприятия на каждом этапе жизненного цикла.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. The voice of Kubernetes experts report 2024: the data trends driving the future of the enterprise // Cloud Native Computing Foundation URL: <https://www.cncf.io/blog/2024/06/06/the-voice-of-kubernetes-experts-report-2024-the-data-trends-driving-the-future-of-the-enterprise/> (дата обращения: 28.03.2025).
2. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия – Comprehensive Methodology of Intelligently Adaptive Management of an Enterprise Information Infrastructure / Е. А. Басыня. - Текст : непосредственный // Защита информации. Инсайд – Zasita informacii. Inside. - 2021. - № 5 (101). - С. 16-25.
3. Basinya E. A. Enterprise information infrastructure management [Electronic resource] / E. A. Basinya, D. S. Khudiakov // International multi-conference on industrial engineering and modern technologies (FarEastCon) : [proc.], Vladivostok, 6–9 Oct. 2020. – Vladivostok : IEEE, 2020. – 6 p. - Mode of access: <https://ieeexplore.ieee.org/document/9271463/authors#authors>. - Title from screen - DOI: 10.1109/FarEastCon50210.2020.9271463.
4. Zeini A., Lennon R. G., Lennon P. Securing Infrastructure as Code (IaC) through DevSecOps: A Comprehensive Risk Management Framework //2023 Cyber Research Conference-Ireland (Cyber-RCI). – IEEE, 2023. – С. 1-11.
5. Mehdi A., Walia R. Terraform: Streamlining Infrastructure Deployment and Management Through Infrastructure as Code // 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). – IEEE, 2023. – С. 851-856.
6. Abbas S. I., Garg A. Integrating Emerging Technologies with Infrastructure as Code in Distributed Environments // 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC). – IEEE, 2024. – С. 1138-1144.
7. ГОСТ Р 56939–2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования = Information protection. Secure software development. General requirements : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. № 1504-ст : введен взамен ГОСТ Р 56939-2016 : дата введения 2024-12-20. – Москва : Стандартинформ, 2024. – 36 с. ; 29 см. – Текст : непосредственный.
8. Bringhenti D. et al. A novel approach for security function graph configuration and deployment // 2021 IEEE 7th International Conference on Network Softwarization (NetSoft). – IEEE, 2021. – С. 457-463.
9. Zeng R., Niu Y., Qiao L. A Novel Construction Technology of Microservice Multi-Instance System Automatic Deployment and Upgrade // 2023 International Conference on Networking and Network Applications (NaNA). – IEEE, 2023. – С. 674-679.
10. Oulaaffart M., Badonnel R., Festor O. Towards Automating Security Enhancement for Cloud Services // 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). – IEEE, 2021. – С. 692-696.

© А. В. Челнокова, 2025

А. С. Чулкова^{1✉}, Я. А. Карташов¹, А. А. Шаронов¹

Разработка системы мониторинга состояния дорожного покрытия для анализа и принятия решения о дальнейшей эксплуатации

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: a.chulkova03@mail.ru

Аннотация. В данной статье рассматривается процесс разработки системы мониторинга состояния дорожного покрытия для анализа и принятия решения о дальнейшей эксплуатации. Описывается сравнительный анализ современных разработок в сфере мониторинга состояния дорожного покрытия, выявляются основные плюсы и минусы для определения функциональных возможностей. Анализирование фреймворков, для оптимального написания кода. Проектирование архитектуры системы, подбор компонентов аппаратной части, и моделирование интерфейса веб-сервиса. Разработка программно-аппаратного комплекса и функционала веб-сервиса сбора данных мониторинга о состоянии дорожного покрытия, тестирование и доработка.

Ключевые слова: программно-аппаратный комплекс, веб-сервис, сбор данных, обработка данных, передача данных, распознавание данных, мониторинг состояния покрытия, состояние дорожного покрытия, анализ, проектирование

A. S. Chulkova^{1✉}, Y. A. Kartashov¹, A. A. Sharapov¹

Development of a road surface condition monitoring system for analysis and decision-making on further operation

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: a.chulkova03@mail.ru

Abstract. This article discusses the process of developing a road surface condition monitoring system for analysis and decision-making on further operation. It describes a comparative analysis of modern developments in the field of road surface condition monitoring, identifies the main advantages and disadvantages for determining functional capabilities. Analysis of frameworks for optimal code writing. Design of system architecture, selection of hardware components, and modeling of web service interface. Development of software and hardware complex and functionality of web service for collecting monitoring data on road surface condition, testing and refinement.

Keywords: hardware and software complex, web service, data collection, data processing, data transmission, data recognition, monitoring of road surface conditions, road surface conditions, analysis, design

Введение

В современных условиях эксплуатации дорожной инфраструктуры остро стоит проблема эффективного мониторинга состояния покрытия и оперативного принятия решений о его ремонте или замене. Традиционные методы оценки, основанные на визуальном осмотре и ручном сборе данных, не позволяют получать актуальную и объективную информацию в масштабах всей дорожной сети. Это приводит к запаздыванию реагирования, нерациональному распределению ресурсов и, как следствие,

ухудшению качества дорог. Целью является разработка системы мониторинга состояния дорожного покрытия для анализа и принятия решения о дальнейшей эксплуатации. Для этого необходимо решить следующие задачи:

- выполнить проектирование аппаратно-программного комплекса;
- выполнить проектирование структуры и интерфейса веб-сервиса;
- разработать программного-аппаратный комплекс;
- реализовать функционал веб-сервиса сбора данных мониторинга о состоянии дорожного покрытия.

Разработка системы мониторинга состояния дорожного покрытия позволит автоматизировать выявление дефектов (ям, трещин и других неровностей) и улучшить эффективность и постоянность ремонтных работ, за счет визуального представления. Это сократит затраты, путем своевременного устранения проблем и улучшит безопасность дорожного движения.

Обзор современных разработок

Существует множество различных современных разработок предназначенных для сбора данных мониторинга о состоянии покрытия и анализа повреждений. Наиболее распространенные из них:

DRIVECONTROL – это коммерческая система мониторинга состояния дорожной инфраструктуры, разработанная российской компанией «Интеллектуальные дорожные технологии». Система устанавливается на транспортные средства и использует видеокамеры, GPS/ГЛОНАСС-модули, а также алгоритмы компьютерного зрения и машинного обучения для распознавания дефектов дорожного полотна. Также поддерживается анализ дорожной разметки, бордюров и дорожных знаков [1].

АЛЬФАДОРПРОЕКТ – разработка в рамках национального проекта «Безопасные качественные дороги». Внедряется Росавтодором совместно с научными организациями. Представляет собой комплекс, включающий в себя автомобильные лаборатории с видеосъемкой и ИИ-обработкой [2].

RoadAR Analytics – это инновационная система видеомониторинга, позволяющая распознавать различные события. Благодаря искусственному интеллекту, RoadAR Analytics значительно расширяет возможности видеонаблюдения и сбора данных. Система выполняет основную работу: распознает, классифицирует и анализирует события в автоматическом режиме, предупреждая о значимых ситуациях. Оператору остается только принять решение [3].

Каждая из этих разработок имеет свои преимущества и недостатки. Сделав данный анализ, стало понятно какие требуемые функциональные возможности необходимы для веб-сервиса сбора данных мониторинга о состоянии дорожного покрытия.

Проектирование программно-аппаратного комплекса

Первым этапом в разработке стало создание общей технологической схемы (рис. 1).

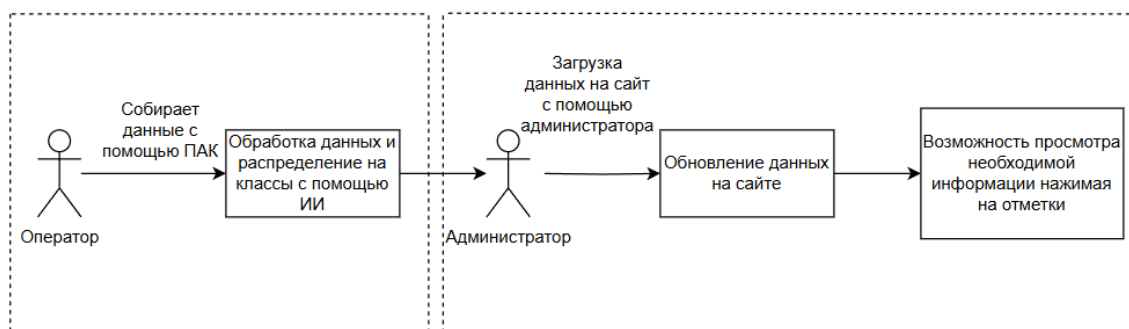


Рис. 1. Общая технологическая схема

При проектировании аппаратно-программного комплекса (АПК) особое внимание уделялось выбору компонентов, обеспечивающих устойчивую работу в различных условиях и отсутствия постоянного интернет-соединения. Предпочтение отдавалось недорогим, но надежным компонентам, которые совместимы с ОС Linux и экосистемой Python.

Для этого первоначально была спроектирована общая схема работы АПК (рис. 2).

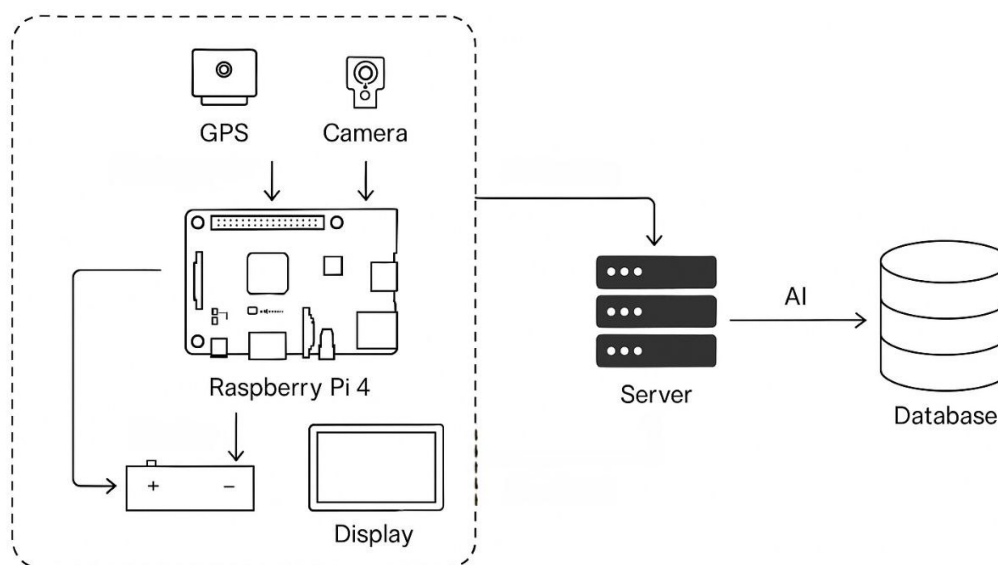


Рис. 2. Схема работы АПК

На этой схеме хорошо видно, как работает аппаратно-программный комплекс.

Сам комплекс представляет из себя компактное, мобильное устройство на базе Raspberry Pi 4, к которой подключена встроенная Pi Camera через специальный соединительный шлейф, GPS модуль для считывания координат, дисплей с возможностью сенсорного управления, на котором будет отображен сам веб-интерфейс и сам аккумулятор, с помощью него аппаратно-программный комплекс сможет работать автономно.

Ниже представлена тестовая модель АПК, которая была собрана по предыдущей схеме (рис. 3).



Рис. 3. Тестовая модель АПК

Далее был спроектирован веб-интерфейс для управления аппаратно-программным комплексом.

Веб-интерфейс является ключевым инструментом взаимодействия оператора с аппаратно-программным комплексом. Он обеспечивает простое и интуитивно понятное управление процессом сбора данных: запуск и остановку съемки, отслеживание текущего статуса, перезагрузки либо выключение системы, а также передачу собранной информации на удаленный сервер или внешний носитель.

Поэтому для функциональных возможностей был спроектирован веб-интерфейс «Главного экрана», на котором отображены кнопки управления комплексом (рис. 4).

Также был продуман статус системы, с помощью которого оператор может наблюдать в реальном времени процесс работы аппаратно-программного комплекса.

Когда камера подключена, под надписью «статус системы» высвечивается статус камеры, и информация с каким промежутком времени комплекс делает фотографии. После того как оператор останавливает систему высвечивается количество фотографий, которые были сделаны во время съемки. При выгрузке данных на сервер отображается количество отправленной информации, а также в самой системе сохраняются лог-файл с возможными ошибками в системе.

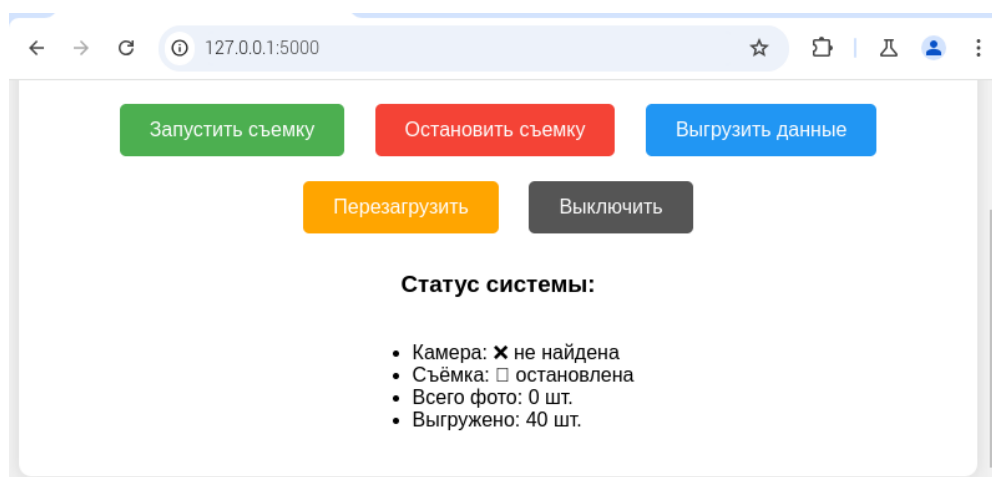


Рис. 4. Интерфейс главного экрана

Веб-интерфейс был написан на фреймворке Flask, выбран он был из-за того, что он очень гибкий, что позволяет не нагружать плату RPi 4 и работать только с нужными компонентами.

В рамках реализации аппаратно-программного комплекса (АПК) особое внимание уделяется этапу автоматической обработки изображений с целью выявления и классификации дефектов дорожного покрытия. Для решения этой задачи была выбрана модель нейронной сети YOLO.

В качестве вычислительной платформы использовался ноутбук с видеокартой NVIDIA RTX 3070, поддерживающей аппаратное ускорение на базе CUDA версии 12.5. Также система была оснащена процессором Intel Core i7-12700H, 32 гигабайтами оперативной памяти и двумя твердотельными накопителями объемом 1 и 2 ТБ, что обеспечивало высокую скорость обработки данных и стабильность работы при длительном обучении модели.

Проектирование структуры и интерфейса веб-сервиса

Были спроектированы схемы структуры работы роли «Пользователь» и работы роли «Администратор» (рис. 5, 6)

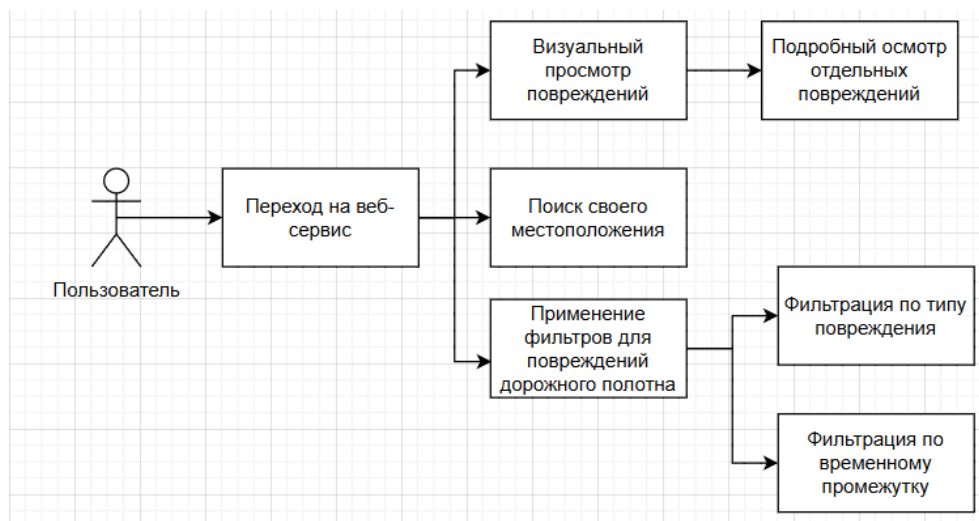


Рис. 5. Структура работы роли «Пользователь»

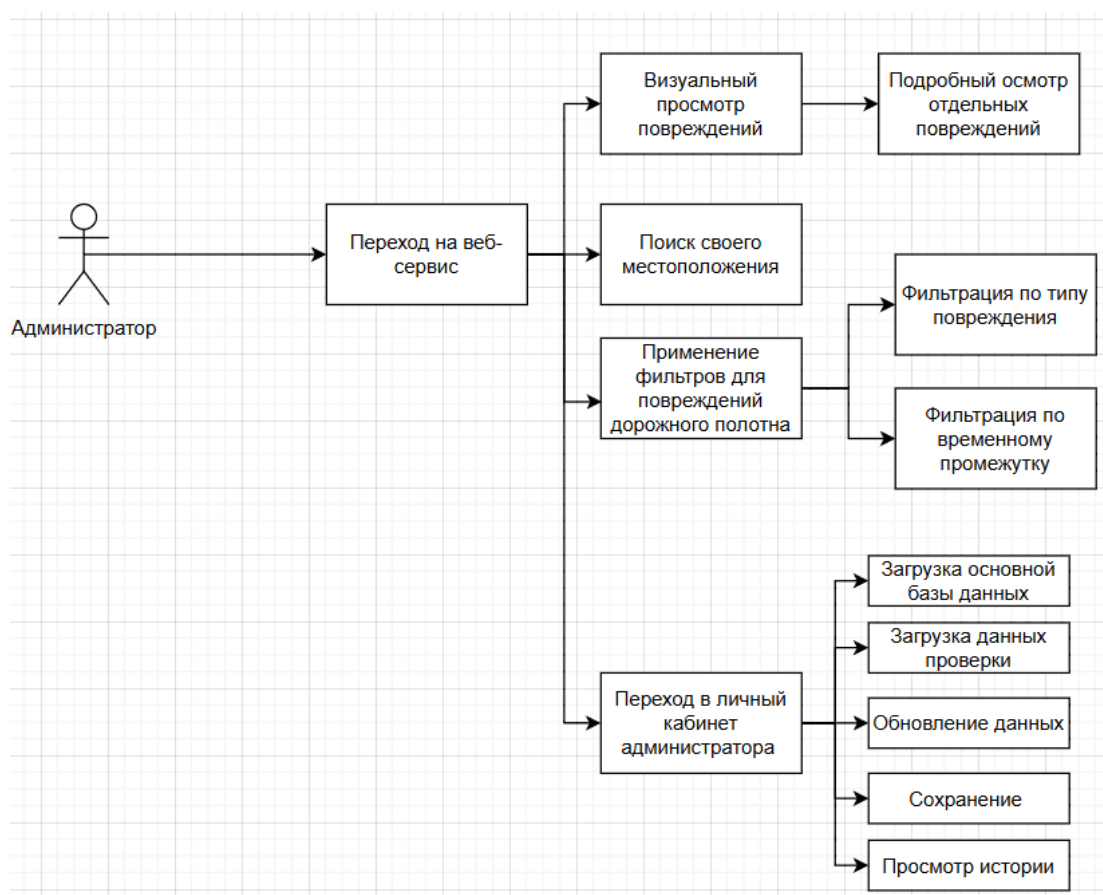


Рис. 6. Структура работы роли «Администратор»

После структуры функционирования был спроектирован интерфейс веб-сервиса на платформе Figma (рис. 7, 8). За основу была взята карта компании 2ГИС, для наглядного представления. В последующей разработке будет отображаться карта OpenStreetMap.

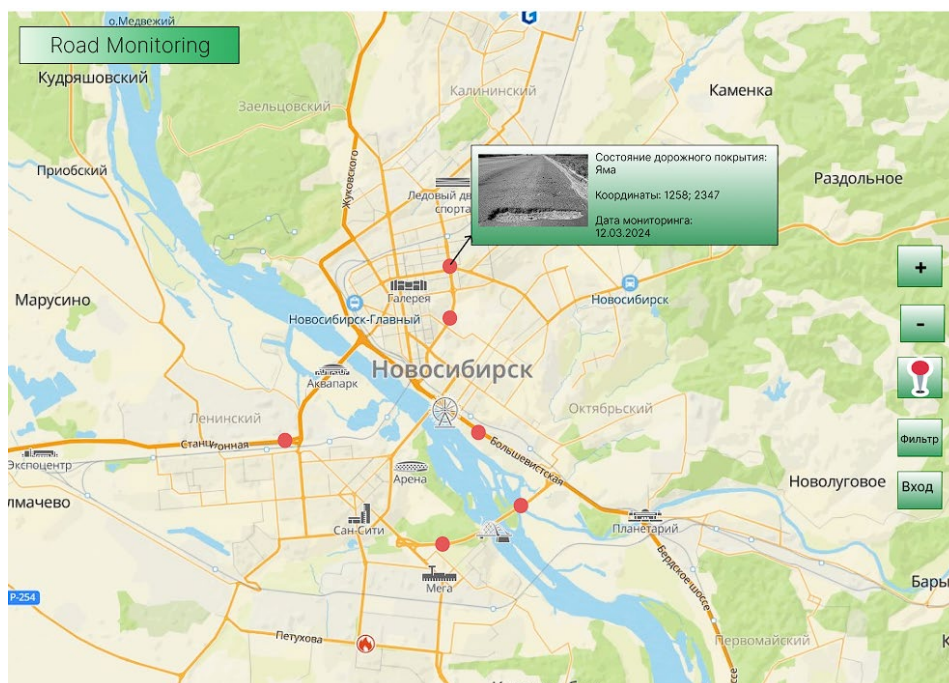


Рис. 7. Дизайн-макет интерфейса главной страницы

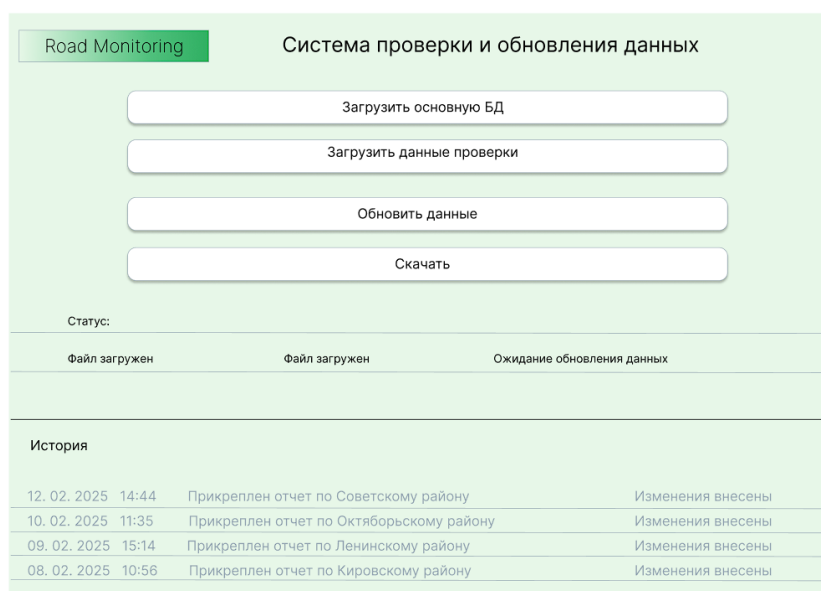


Рис. 8. Дизайн-макет интерфейса системы проверки и обновления данных

Также был проведен сравнительный анализ фреймворков, которые понадобятся для написания кода и по результатам анализа был выбран фреймворк FastAPI, по причине того, что он отвечает самым важным критериям для создания веб-сервиса, а именно: поддержка OpenStreetMap и большая скорость. Таким образом был определен следующий стек технологий для написания веб-сервиса:

- язык программирования для frontend HTML, JavaScript;
- язык программирования для backend Python;

- Framework FastAPI;
- база данных SQLite.

Результат разработки

В результате работ, описанных в данном разделе, была завершена полноценная реализация аппаратно-программного комплекса (АПК) мониторинга состояния дорожного покрытия с применением методов искусственного интеллекта. На этапе разработки была выполнена интеграция аппаратных компонентов, обеспечивающих сбор изображений и GPS-координат, а также реализован веб-интерфейс для управления комплексом с планшета.

Сформированы и протестированы алгоритмы автоматического сбора данных, выгрузки изображений по сетевым протоколам SSH и SCP, а также дальнейшей передачи на удаленный сервер для обработки. Особое внимание было уделено построению устойчивой архитектуры взаимодействия между модулями комплекса.

Для решения задачи автоматического выявления дефектов дорожного покрытия была обучена модель на базе YOLO, адаптированная к специфике изображений с мобильных средств съемки. Модель продемонстрировала удовлетворительные результаты при тестировании на реальных дорогах, с корректной классификацией и локализацией объектов контроля.

Результаты работы АПК (рис. 9).



Рис. 9. Результат работы АПК

По итогам разработки веб-сервиса сбора данных мониторинга о состоянии дорожного покрытия для анализа и принятия решения о дальнейшей эксплуатации были осуществлены четыре основных процесса:

- настройка приложения;
- работа с базой данных;
- аутентификация;
- API для работы с данными;

– обработка данных.

Карта отображается с сервиса OpenStreetMap. Основные функции сервиса сделаны, а именно визуальный анализ оценки состояния дорожного покрытия, фильтрация данных, подробная информация про каждое повреждение. Также разработан личный кабинет администратора, где сотрудник может добавлять новые данные, обновлять карту, и скачивать базу данных. Из дополнительных функций осуществлено отслеживание состояния файлов и просмотр истории действий (рис. 10–12).

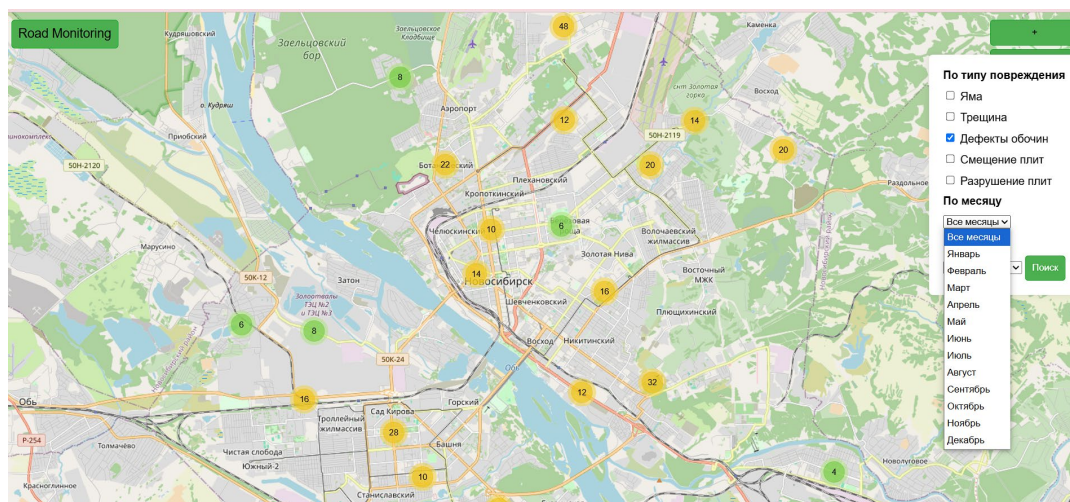


Рис. 10. Результат разработки веб-сервиса

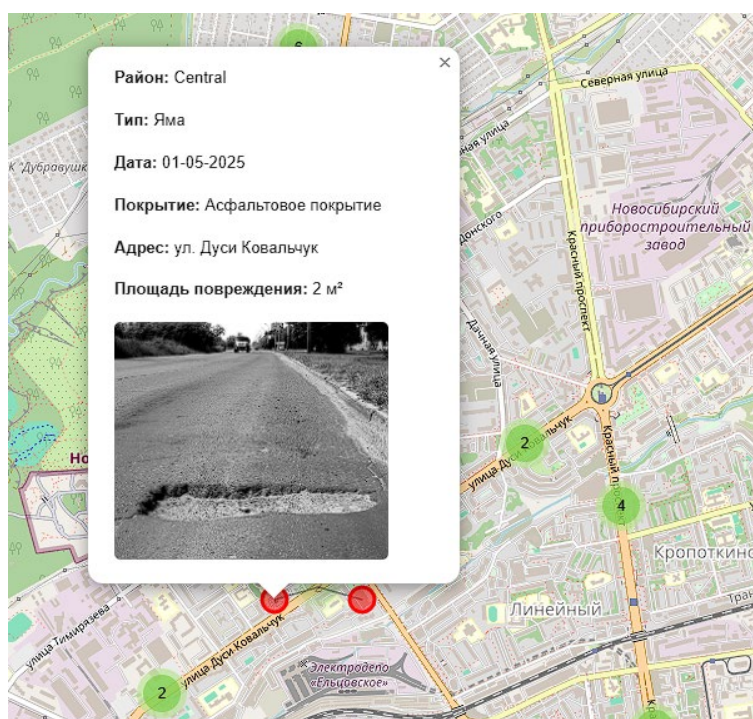


Рис. 11. Результат разработки веб-сервиса

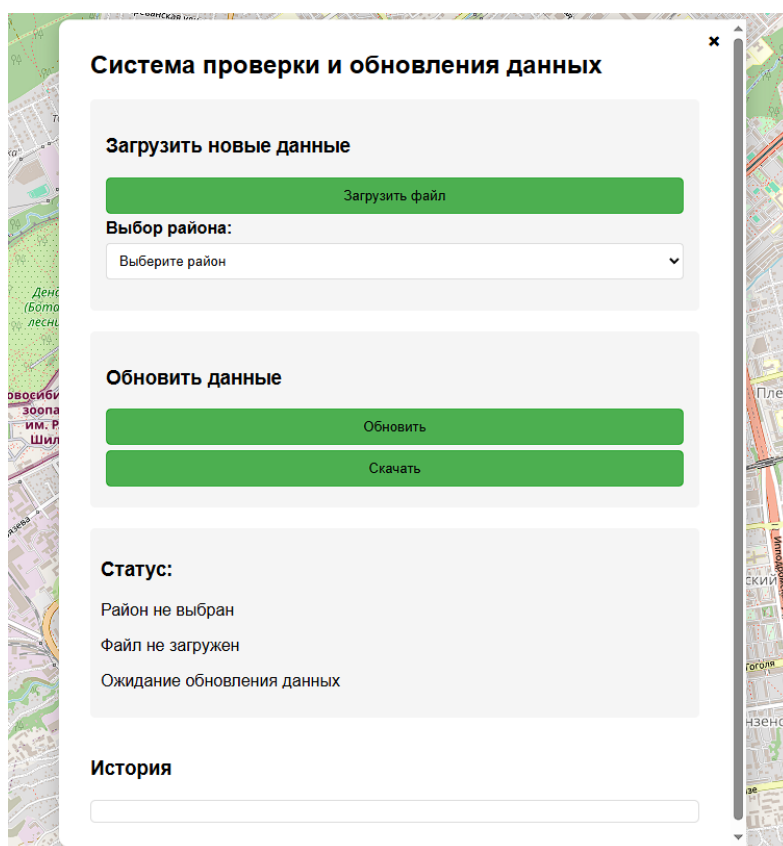


Рис. 12. Результат разработки веб-сервиса

Заключение

В результате выполнена работа на тему «Разработка системы мониторинга состояния дорожного покрытия для анализа и принятия решения о дальнейшей эксплуатации». Было выполнено проектирование аппаратно-программного комплекса, выполнено проектирование структуры и интерфейса веб-сервиса, разработан программно-аппаратный комплекс, реализовать функционал веб-сервиса сбора данных мониторинга о состоянии дорожного покрытия. Данный система сбора данных мониторинга о состоянии дорожного покрытия, позволит эффективно оценивать ситуацию и оперативно принимать решения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Drivecontrol. 2025. URL: <https://драйвконтроль.рф/> (дата обращения:21.04.2025).
2. Альфадорпроект. 2025. URL: <https://alfadorproekt2008.ru/> (дата обращения:21.04.2025).
3. Raodar 2013-2024. URL: <https://roadar.ru/> (дата обращения:21.04.2025).

© А. С. Чулкова, Я. А. Карташов, А. А. Шаранов, 2025

С. А. Чунарева¹✉, Н. С. Головачев¹

Разработка интерактивной информационно-справочной трехмерной модели номерного фонда базы отдыха средствами Unreal Engine

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: chusonya49@gmail.com

Аннотация. В данной статье рассматривается процесс разработки интерактивной информационно-справочной трехмерной модели номерного фонда базы отдыха с использованием современных цифровых инструментов – Blender и Unreal Engine. Объектом исследования является туристическая база, для которой требуется создание полноценной 3D-визуализации, сочетающей реалистичное отображение архитектурных элементов и доступ к справочной информации. Целью работы является создание цифровой модели, включающей детализированные трехмерные объекты зданий, интерьеров, элементов благоустройства и ландшафтного окружения, с возможностью свободного перемещения пользователя по территории, а также просмотра внутреннего и внешнего оформления различных сооружений. Модель также содержит встроенные справочные сведения о гостевых домах и инфраструктуре базы. В процессе разработки применялись методы трехмерного моделирования, визуального проектирования среды, а также создания интерактивных пользовательских сценариев. В качестве исходных материалов использовались техническое задание, графические референсы экстерьеров и интерьеров, а также кадастровый план участка. Полученная модель предназначена для презентации на тематических выставках и может быть использована в маркетинговых целях для продвижения туристических объектов и привлечения инвестиций. Работа демонстрирует потенциал использования игровых технологий в реальных сферах, выходящих за рамки развлечений.

Ключевые слова: Blender, Unreal Engine, интерактивная визуализация, трехмерное моделирование, информационно-справочная модель

S. A. Chunareva¹✉, N. S. Golovachev¹

Development of an interactive information and reference three-dimensional model of the number of rooms of the recreation center using Unreal Engine

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: chusonya49@gmail.com

Abstract. This article discusses the process of developing an interactive information and reference three-dimensional model of the number of rooms of a recreation center using modern digital tools - Blender and Unreal Engine. The object of research is a tourist base, which requires the creation of a full-fledged 3D visualization, combining realistic display of architectural elements and access to reference information. The aim of the work is to create a digital model that includes detailed three-dimensional objects of buildings, interiors, landscaping and landscape surroundings, with the ability to freely move the user around the territory, as well as view the internal and external design of various structures. The model also contains built-in reference information about guest houses and base infrastructure. During the development process, methods of three-dimensional modeling, visual design of the environment, as well as the creation of interactive user scenarios were used. The terms of

reference, graphic references of exteriors and interiors, as well as the cadastral plan of the site were used as initial materials. The resulting model is intended for presentation at thematic exhibitions and can be used for marketing purposes to promote tourist sites and attract investment. The work demonstrates the potential of using gaming technology in real-world areas beyond entertainment.

Keywords: Blender, Unreal Engine, interactive visualization, 3D modeling, reference model

Введение

В последние годы наблюдается устойчивый рост интереса к применению технологий трехмерной визуализации в различных отраслях, в том числе в туристической сфере, где возрастает потребность в средствах эффективной презентации объектов инфраструктуры. Одним из перспективных направлений является использование интерактивных информационно-справочных 3D-моделей, сочетающих визуальную реалистичность, пользовательскую навигацию и структурированное представление данных.

Актуальность настоящего исследования обусловлена необходимостью создания цифровых решений, обеспечивающих комплексное представление туристических объектов для целей рекламы, демонстрации и инвестиционного продвижения [1]. Общая тема исследования связана с разработкой интерактивной информационно-справочной трехмерной модели номерного фонда базы отдыха средствами современных программных инструментов.

Целью работы является построение цифровой модели, включающей архитектурно точные элементы застройки, ландшафтную составляющую и навигационные функции, дополненные справочными данными о размещении и инфраструктуре. В рамках исследования предполагается решить следующие задачи: анализ исходной проектной документации, создание трехмерных объектов в среде Blender, интеграция моделей в Unreal Engine, реализация интерфейса пользователя и элементов интерактивного взаимодействия.

Теоретическая значимость работы заключается в расширении методологических подходов к применению игровых технологий в прикладных задачах визуализации, а практическая – в создании инструмента, способного повысить эффективность продвижения туристических объектов на профильных мероприятиях и в инвестиционной деятельности.

Методы и материалы

Разработка интерактивной информационно-справочной трехмерной модели номерного фонда базы отдыха проводилась с использованием современных цифровых инструментов и методологических подходов в области архитектурной визуализации, геймдизайна и информационного моделирования. Работа включала в себя последовательные этапы, каждый из которых вносил вклад в формирование конечного программного продукта.

В качестве основных программных платформ применялись: Blender и Unreal Engine. Blender использовался для построения трехмерных моделей зданий, интерьеров и элементов ландшафта. Unreal Engine 5 необходим для разработки интера-

ктивной сцены, настройки визуальных эффектов, освещения, а также логики пользовательского взаимодействия и интеграции справочной информации [2].

Результаты

Весь объем работы можно разделить на этапы для упрощения процесса разработки, а также для более детального контроля над каждым из них. Это позволяет поэтапно решать задачи, обеспечивая качество и функциональность на каждом уровне. Ниже приведены основные этапы работы:

- анализ исходных данных;
- моделирование архитектурных объектов в Blender;
- сборка сцены в Unreal Engine;
- разработка пользовательского интерфейса и интерактивных элементов.

На начальном этапе было выполнено всестороннее изучение исходной документации, предоставленной заказчиком. В частности, анализу подвергались кадастровый план территории, определяющий границы и структуру застройки, а также графические референсы, иллюстрирующие стилистику архитектурных и интерьерных решений [3]. Этот этап позволил сформировать обоснованные проектные допущения, задать масштабы и геометрию будущей модели, а также определить функциональные зоны туристической базы (рис. 1).



Рис. 1. Кадастровый план территории базы отдыха

После анализа была осуществлена цифровая реконструкция архитектурных элементов и окружающей среды. Для этих целей применялась программа Blender, обеспечивающая создание высокополигональных моделей зданий с точной проработкой геометрии [4, 5]. В процессе моделирования особое внимание уделялось архитектурной достоверности – формам кровли, пропорциям оконных и дверных проемов, деталям фасадов [6]. Помимо зданий, моделировались элементы ландшафтной инфраструктуры, включая дорожки, ограждения, малые архитектурные формы, а также насаждения, такие как деревья и кустарники [7]. Это обеспечивало целостное пространственное восприятие объекта (рис. 2).

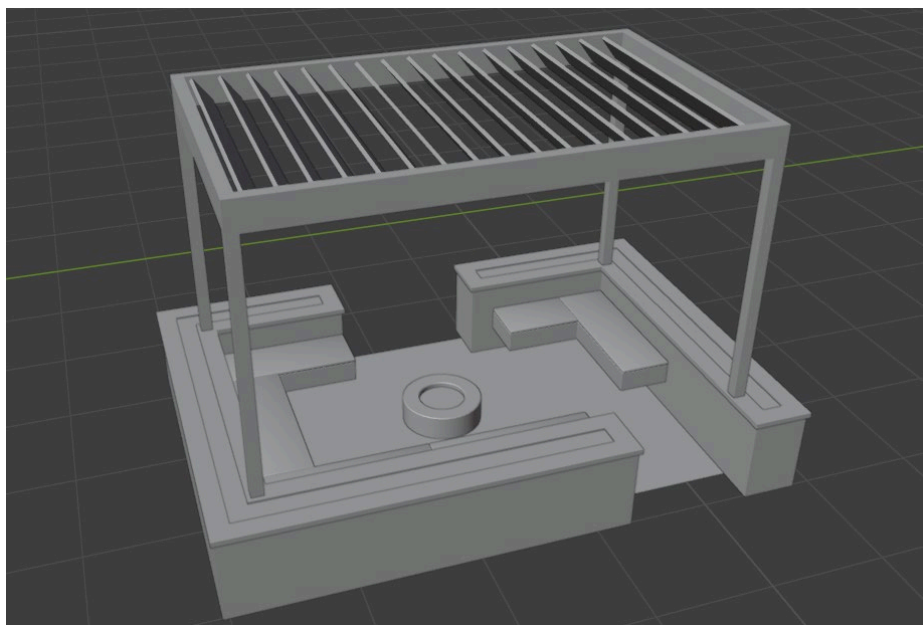


Рис. 2. Процесс моделирования каминной зоны в Blender

Следующим этапом стала проработка визуальных свойств моделей, включая создание и наложение текстур. Применялись материалы, соответствующие принципам физически корректного рендеринга (PBR), что позволило добиться реалистичного внешнего вида поверхностей [8, 9]. Использовались как готовые текстурные библиотеки, так и индивидуально разработанные материалы, включая карты нормалей, шероховатости и отражения. Объекты текстурировались с учетом освещенности, расположения в пространстве и материала отделки (рис. 3) [10].

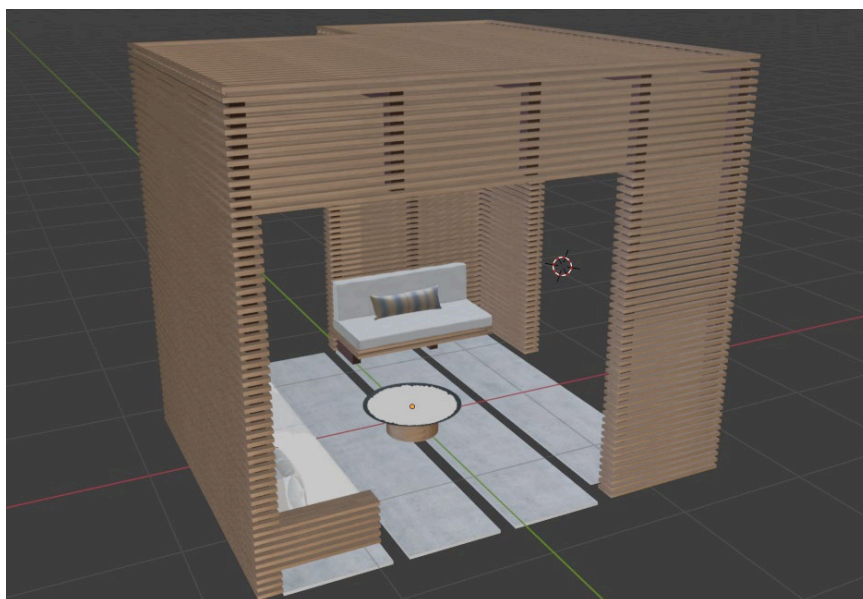


Рис. 3. Текстурирование моделей

После завершения моделирования и текстурирования все элементы были экспортированы в формат, поддерживаемый игровым движком Unreal Engine 5 [11]. На базе этого программного комплекса осуществлялась сборка интерактивной сцены. Сначала в виртуальном пространстве формировалась территория базы: задавался рельеф, воссоздавалась структура участка на основе кадастровых данных, размещались архитектурные модели (рис. 4) [12].



Рис. 4. Общая сцена в Unreal Engine

Далее производилась настройка освещения с учетом времени суток, тени, атмосферных эффектов и динамической экспозиции. Таким образом формировалась реалистичная среда восприятия (рис. 5).



Рис. 5. Вариант внутреннего интерьера гостевого дома в Unreal Engine

Пользователь мог свободно перемещаться в режиме от первого лица, приближаться к интересующим зданиям, а при нажатии на определенную клавишу – получать справочную информацию о каждом объекте (рис. 6) [13].

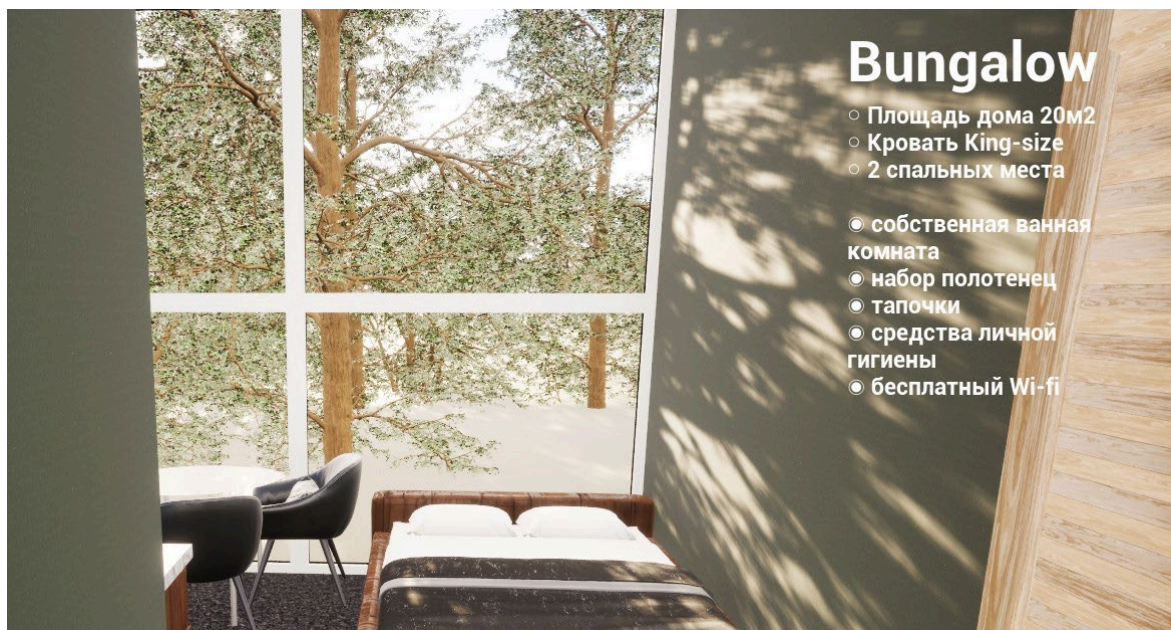


Рис. 6. Интерфейс отображения информации о гостевом доме

Для реализации этой логики использовалась визуальная система программирования Blueprint (рис. 7).

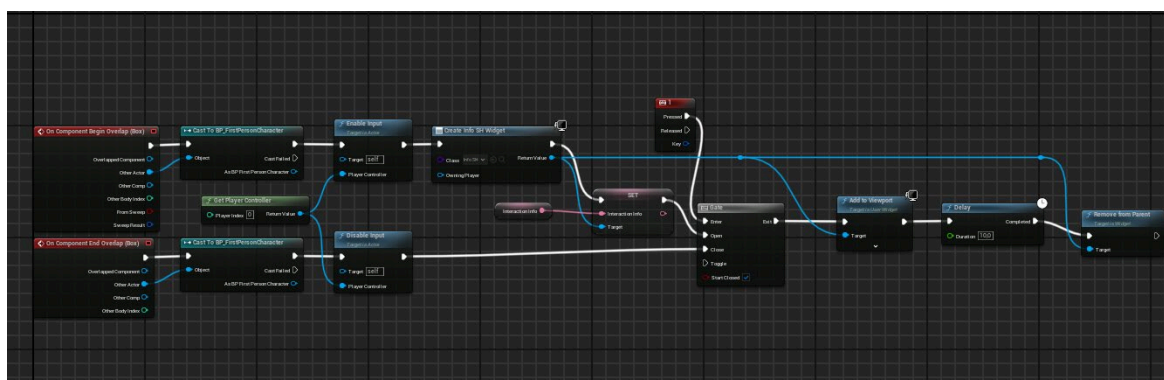


Рис. 7. Blueprint взаимодействия пользователя с гостевым домом

Заключение

Созданная программа тестировалась на персональном компьютере, с процессором Ryzen 5 7500F, оперативной памятью на 32 ГБ, с видеокартой GeForce RTX 4060. Разрешение экрана тестовой системы 1920*1080.

При указанных характеристиках интерактивная трехмерная модель не снижала уровень отображения кадров в секунду ниже 40, что является приемлемым показателем.

В результате работы была создана интерактивная информационно-справочная трехмерная модель номерного фонда базы отдыха, включающая архитектурные объекты, элементы ландшафта и справочную информацию. Проект продемонстрировал эффективность использования 3D-моделирования и игрового движка Unreal Engine для визуализации туристических объектов и их презентации.

Модель обладает высокой наглядностью и функциональностью, что делает ее полезной для выставок, рекламы и привлечения инвесторов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баланова А. Н. Информационные технологии в сфере туризма и гостеприимства. Учебное пособие для вузов. – СПб. : Лань, 2023. – 413 с.
2. Максименкова О. В., Веселко Н. И. Программирование в Unreal Engine 5 для начинающего игродела. Основы визуального языка Blueprint. – М. : Бомбора, 2023. – 321 с.
3. Отнюкова М. С. Инновации в туризме. – М. : Юрайт, 2022. – 256 с.
4. Прахов А. Blender: 3D-моделирование и анимация. Руководство для начинающих. – М. : ЛитРес, 2022. – 384 с.
5. Прахов А. А. Самоучитель Blender 2.7 – СПб.: БХВ-Петербург, 2017. – 400 с.
6. Миловская О. С. Визуализация архитектуры и интерьеров в 3ds Max 2008 – СПб. : БХВ-Петербург, 2008. – 240 с.
7. Серова М. Н. Учебник-самоучитель по трехмерной графике в Blender 3D. Моделирование, дизайн, анимация, спецэффекты. – М. : Солон-Пресс, 2021. – 272 с.
8. Полякова Е. Г. Туризм и рекреационное проектирование: учебник для вузов. – М. : Академия, 2016. – 256 с.
9. Ганеев Р. М. 3D-моделирование персонажей в Maya. Учебное пособие для вузов – М.: ГЛТ, 2018. – 284 с.
10. Блиновская Я. Ю., Лаврушина Е. Г. Информационные технологии в туризме: учебное пособие. – М. : Академия, 2021. – 312 с.
11. Ложкина Е. А., Ложкин В. С. Проектирование в среде 3ds Max: учебное пособие – Новосибирск: НГТУ, 2019. – 180 с.
12. Шитов В. Н. Информационные технологии в туристической индустрии: учебное пособие. — 2-е изд., стер. — М.: ФЛИНТА, 2017. — 416 с.
13. Ларионова К. О. Архитектура зданий и строительные конструкции. — М.: Юрайт, 2020. — 350 с.

© С. А. Чунарева, Н. С. Головачев, 2025

О. А. Шведова¹✉, Е. Ю. Воронкин¹

Разработка программного обеспечения для генерации характеристик дизайна персонажей для видеоигр

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: olya.shvedova.96@gmail.com

Аннотация. В статье рассматривается процесс разработки программного обеспечения для генерации характеристик дизайна персонажей для видеоигр. Актуальность данной темы обусловлена существенными время- и трудозатратами художников по персонажам и концепт-художников при создании дизайна персонажей в сфере разработки видеоигр. В качестве основных инструментов для разработки программного обеспечения были выбраны язык программирования Python с библиотекой TKinter для создания графического интерфейса пользователя, модели искусственного интеллекта GigaChat и Kandinsky 3.1 от Fusion Brain, а также встраиваемая система по управлению базами данных SQLite. Процесс разработки программного обеспечения, получившего название «RandChar», состоял из создания концептуальной модели ПО, проектирования функциональной модели при помощи создания диаграмм UML IDEF0, прототипирования программного обеспечения и его тестирования на соответствие функциональным и нефункциональным требованиям. Реализован функционал работы с базой данных вариантов характеристик, режим тренировки с возможностью установки таймера, а также возможность генерации текстового описания персонажа на основе введенного пользователем игрового сеттинга с использованием искусственного интеллекта. Разработанное программное обеспечение было признано полностью соответствующим заявленным требованиям. Данная работа демонстрирует практическое применение современных программных средств для оптимизации и упрощения процесса работы художников по дизайну персонажей для видеоигр.

Ключевые слова: дизайн, база данных, SQLite, python, tkinter, нейросети для генерации изображений, нейросети для генерации текста, GigaChat, Fusion Brain

О. А. Shvedova¹✉, Е. Yu. Voronkin¹

Software development for generating character design characteristics for video games

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: olya.shvedova.96@gmail.com

Abstract. The article discusses the process of developing software for generating character design characteristics for video games. The relevance of this topic is due to the significant time and labor costs of character artists and concept artists when creating character designs in the field of video game development. The Python programming language with the TKinter library for creating a graphical user interface, the GigaChat and Kandinsky 3.1 artificial intelligence models from Fusion Brain, as well as the SQLite embedded database management system were chosen as the main tools for software development. The process of developing the software, called "RandChar", consisted of creating a conceptual model of the software, designing a functional model using UML IDEF0 diagrams, prototyping the software and testing it for compliance with functional and non-functional requirements. The functionality of working with a database of characteristic variants, a training mode with the

ability to set a timer, as well as the ability to generate a text description of the character based on the game setting entered by the user using artificial intelligence were implemented. The developed software was recognized as fully compliant with the stated requirements. This work demonstrates the practical application of modern software tools for optimizing and simplifying the work process of character design artists for video games.

Keywords: design, database, SQLite, python, tkinter, neural networks for image generating, neural networks for text generating, GigaChat, Fusion Brain

Введение

Персонажи являются важной частью большинства современных видеоигр: начиная от героя, с которым себя ассоциирует игрок, и заканчивая неигровыми персонажами, так или иначе погружающие игрока в сеттинг придуманного мира [1]. Упрощение процесса работы над этими задачами позволит повысить общую эффективность, сократить время – и трудозатраты, а также позволить найти новые решения в дизайне персонажей для конкретного проекта. С целью автоматизации вышеуказанных процессов было принято решение о разработке специализированного программного обеспечения.

Актуальность создания программного обеспечения для генерации характеристик дизайна персонажей заключается в необходимости разработки концепции оригинальных дизайнов в сжатые сроки, что не всегда позволяет дизайнерам уделять достаточно времени поискам подходящих референсов и идей, что, в свою очередь, может привести к созданию некачественных или заурядных дизайнов и увеличить время работы над каждым из них за счет большого количества правок и переработок [2].

В ходе выполнения работ по проектированию и разработке программного обеспечения были созданы UML-диаграммы, концептуальная модель программного обеспечения, и база данных, которую использует в одном из режимов работы программное обеспечение (далее – ПО), разработан работающий прототип ПО и проведено тестирование для проверки соответствия ПО всем выдвинутым требованиям [3].

Таким образом, целью данной работы является разработка проекта программного обеспечения для генерации характеристик дизайна персонажей для видеоигр.

Для достижения поставленной цели были выполнены нижеперечисленные задачи:

- изучена предметная область;
- проведен анализ существующих программных решений с выявлением достоинств и недостатков каждого из них;
- создана концептуальная модель ПО;
- создана функциональную модель ПО средствами языка диаграмм UML и работающих с ним современных программных средств;
- создан прототип программного обеспечения для генерации характеристик дизайна персонажей для видеоигр средствами языка программирования Python и искусственного интеллекта.

– проведено тестирование ПО на соответствие выдвигаемым требованиям.

Методы и материалы

В качестве средств моделирования и проектирования разрабатываемого ПО выступили концептуальная модель, а также диаграммы UML и IDEF0.

Концептуальная модель позволяет отразить существенные для достижения цели моделирования элементы ПО и их свойства, а также связи между ними (рис. 1).



Рис. 1. Концептуальная модель программного обеспечения

Далее в процессе проектирования функциональной модели программного обеспечения были созданы диаграммы IDEF0 уровней A-0 и A0, которые предназначены для анализа, документирования и проектирования функциональных процессов в системах [4] (рис. 2, 3).

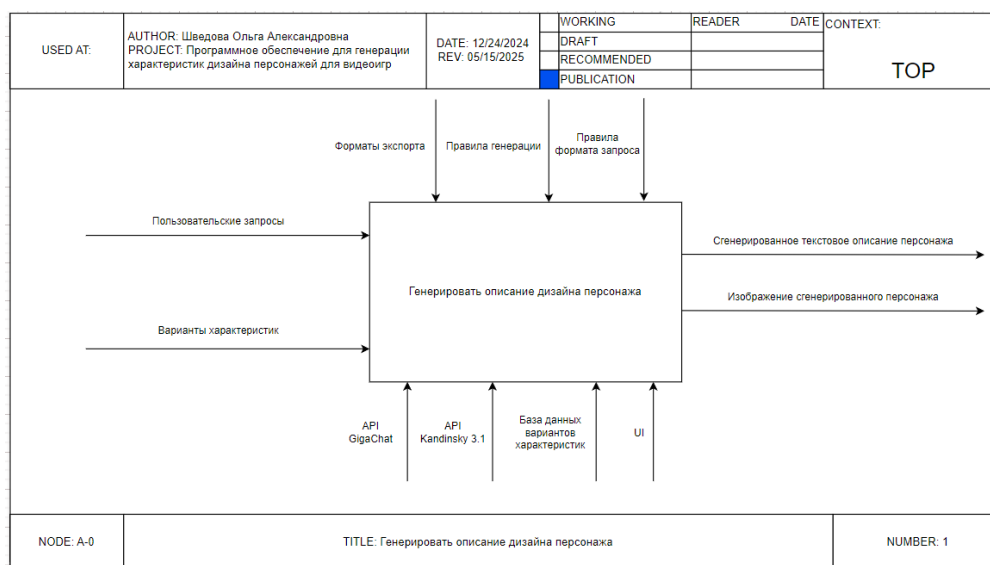


Рис. 2. Диаграмма IDEF0, уровень A-0

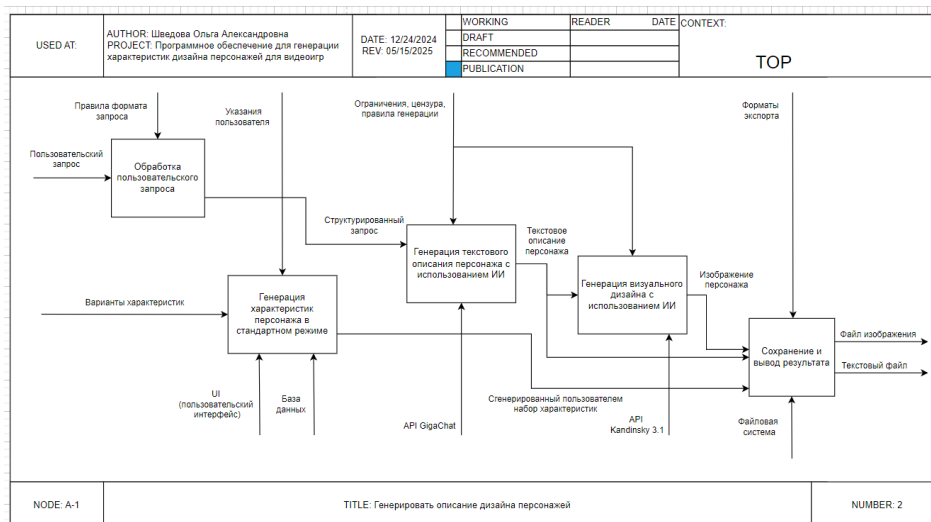


Рис. 3. Диаграмма IDEF0 верхнего уровня

Также была создана диаграмма компонентов, которая используется для моделирования физической структуры программной системы [5] (рис. 4).

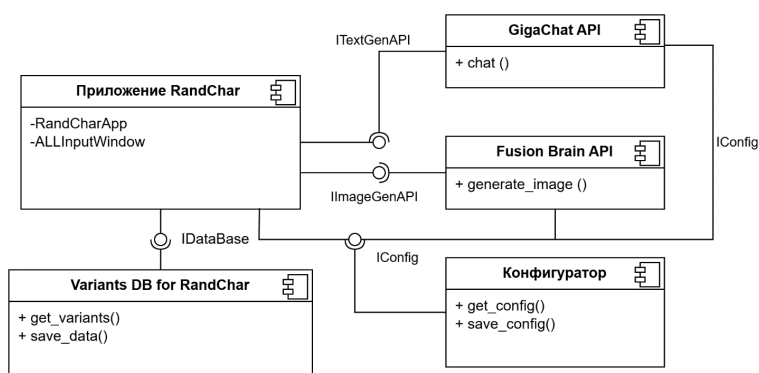


Рис. 4. Диаграмма компонентов

Перед началом разработки ПО путем проведения сравнительного был определен оптимальный стек технологий. В качестве языка программирования для реализации прототипа ПО был выбран Python [6]. GigaChat и Kandinsky 3.1 были использованы в качестве моделей искусственного интеллекта для генерации текстовых описаний и изображений персонажей соответственно [7]. Также для работы с базой данных вариантов характеристик было принято решение использовать систему для управления базами данных SQLite.

Результаты

Учитывая специализацию рабочего процесса художников и концепт-художников по персонажам к программному обеспечению для генерации характеристик дизайна персонажей предъявляются следующие функциональные требования:

- работа с базой данных, содержащей варианты для каждой из характеристик дизайна;
- режим тренировки с возможностью установки таймера;
- работа с генеративной моделью искусственного интеллекта для генерации текста, содержащего описание внешнего вида и краткого бэкграунда персонажа, по игровому сеттингу;
- возможность частичной работы без подключения к сети Интернет.

Время загрузки окон программы не должно превышать 5 секунд. Время генерации текстовых характеристик средствами искусственного интеллекта не должно превышать 10 секунд.

Интерфейс должен иметь русскую локализацию и быть понятным пользователям, знакомым с ПК на базовом уровне. Программное обеспечение должно работать на операционной системе Windows, версия 10 и выше. В случае возникновения ошибок в работе программы пользователь должен быть осведомлен о возникшей проблеме, например, с помощью диалоговых окон с описанием ошибки.

Прототип программного обеспечения разрабатывался средствами языка программирования Python с использованием следующих библиотек и модулей:

- Tkinter и ttk, PIL и ImageTK – для работы с GUI;
- sqlite3, configparser, json – для работы с данными;
- requests, gigachat и fusionbrain – для сетевых взаимодействий, включая работу с API нейросетей;
- os, sys, io, base64, time, random – системные модули.

В данном приложении используется преимущественно объектно-ориентированное программирование [8]. Крупные объекты, такие, как окна и наборы инструкций для взаимодействия с API, объединены в классы, применяется полиморфизм, то есть переопределение методов родительских классов, а также инкапсуляция – приватные методы и атрибуты классов. Каждый класс отвечает за свою функцию: запуск окон, взаимодействие с API, работа с всплывающими сообщениями и основной класс приложения. Модульная архитектура приложения делает его доступным для дальнейшей доработки и масштабирования без необходимости в существенной переработке программного кода.

Интерфейс окна стандартного режима работы программы представлен на рис. 5.

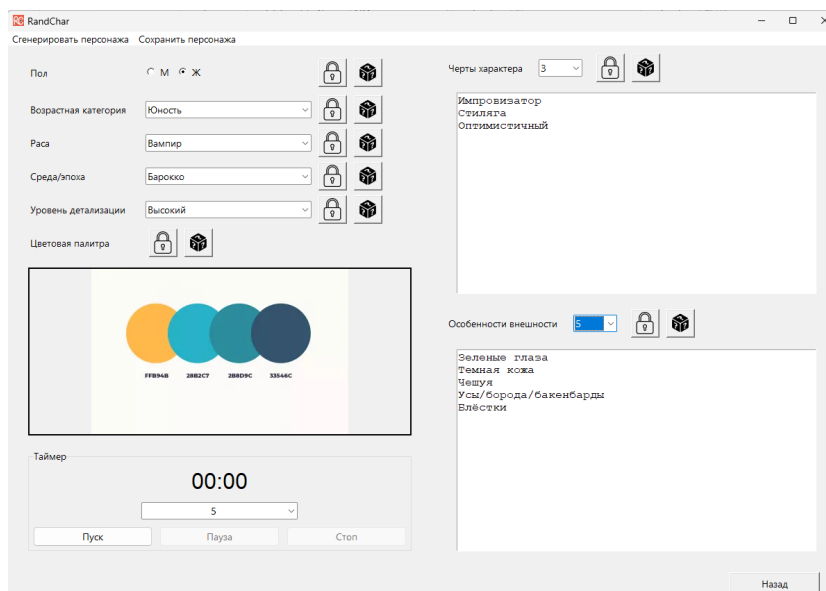


Рис. 5. Окно стандартного режима работы RandChar

RandChar использует API GigaChat для отправки запросов пользователей и получения сгенерированного описания персонажей в структурированном виде. Результат генерации текстового описания персонажа представлен на рис. 6.

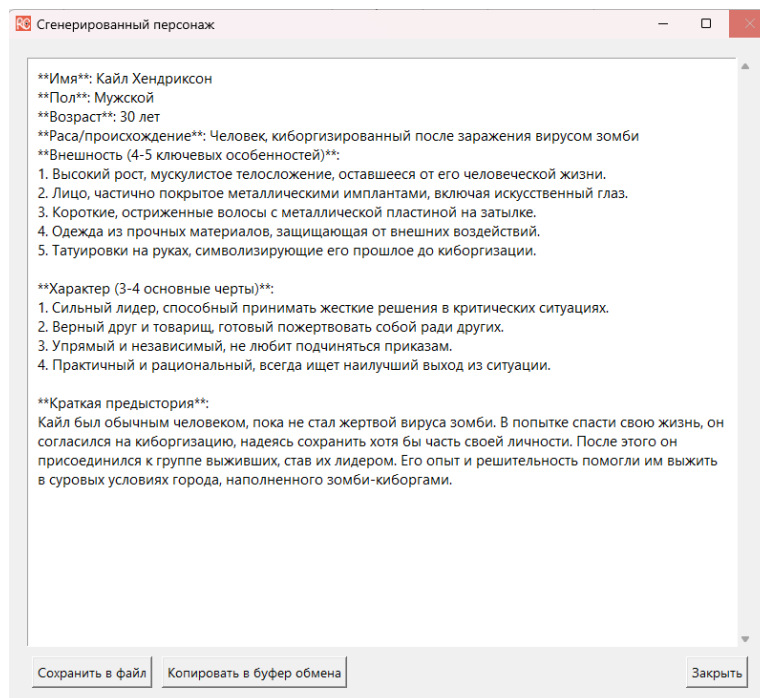


Рис. 6. Результат генерации описания персонажа нейросетью GigaChat

Для удобства пользователя реализованы всплывающие окна, информирующие его в случае возникновения ошибок или, напротив, успешного выполнения той или иной операции.

Для проверки ПО на соответствие функциональным требованиям было принято решение провести ручное тестирование [9]. Каждая из функций была протестирована разработчиком вручную на предмет возникновения ошибок или некорректной работы. В результате тестирования были выявлены и исправлены следующие ошибки в работе ПО:

- при отсутствии данных в базе данных не выводились сообщения об ошибке;
- не воспроизводился звуковой сигнал при завершении работы таймера;
- не появлялось сообщение об отсутствии подключения к сети Интернет.

Для проверки ПО на соответствие требованиям производительности были созданы автоматические тесты с использованием стандартной библиотеки `unittest` и модуля `time` [10]. Результаты автоматического тестирования производительности отражены в таблице 1.

Таблица 1

Результаты автоматического тестирования производительности RandChar

Тестируемый процесс	Время выполнения
Загрузка окон программы	от 0,67 до 3,06 с.
Выполнение запроса GigaChat	от 0,95 до 1,12 с.

Заключение

В статье рассматривается процесс разработки программного обеспечения для генерации характеристик дизайна персонажей для видеоигр, получившего название «RandChar». Целью данной работы было создание удобного инструмента для концепт-художников и дизайнеров персонажей, которое позволило бы сократить время на поиск интересных идей, автоматизировать процесс генерации новых решений в дизайне и дало возможность тренироваться в создании быстрых концептов.

В качестве языка программирования для разработки ПО был выбран Python. Данный язык хорошо подходит для работы с нейросетями, так как обладает большим количеством соответствующих библиотек, а также является достаточно производительным и популярным среди современного сообщества программистов. Среди множества нейросетей для генерации текста и изображений были выбраны GigaChat и Kandinsky. Не менее важным этапом подготовки к разработке программного обеспечения стал процесс выбора системы для управления базами данных для хранения вариантов генерируемых характеристик, в результате которого было принято решение об использовании СУБД SQLite.

Для визуального представления структуры, поведения и взаимодействия компонентов ПО были разработаны следующие диаграммы и схемы: диаграмма прецедентов, диаграммы IDEF0, диаграмму прецедентов, а также физическую модель базы данных. Завершающим этапом стала разработка прототипа программного обеспе-

чения для генерации характеристик дизайна персонажей «RandChar», которое полностью соответствует всем предъявляемым к вновь разрабатываемому ПО требованиям.

Итог: программное обеспечение полностью соответствует всем предъявляемым требованиям и является готовым к дальнейшему использованию в сферах концепт-арта и дизайна персонажей для видеоигр.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ларицкая М.Г. Дизайн и архитектура как инструмент повествования в игровом виртуальном мире // Архивариус. 2021. №3 (57). URL: <https://cyberleninka.ru/article/n/dizayn-i-arhitektura-kak-instrument-povestvovaniya-v-igrovom-virtualnom-mire> (дата обращения: 18.05.2025).
2. Тамулевич С.В. Концепт-арт компьютерной игры в формировании профессиональных компетенций графических дизайнеров // Проблемы современного педагогического образования. 2024. №84-1. URL: <https://cyberleninka.ru/article/n/kontsept-art-kompyuternoy-igry-v-formirovanii-professionalnyh-kompetentsiy-graficheskikh-dizaynerov> (дата обращения: 18.05.2025).
3. Шатова А. Д. Использование UML-диаграмм для оптимизации бизнес-процессов // Инновационная наука. 2024. №6-2. URL: <https://cyberleninka.ru/article/n/ispolzovanie-uml-diagramm-dlya-optimizatsii-biznes-protsessov> (дата обращения: 16.05.2025).
4. Лапина М. А., Ржевская Н. В., Медведева А. С., Золотова А. Г. Применение диаграммы idef0 для наглядного представления структуры проекта // Auditorium. 2023. №1 (37). URL: <https://cyberleninka.ru/article/n/primenenie-diagrammy-idef0-dlya-naglyadnogo-predstavleniya-struktury-proekta> (дата обращения: 20.05.2025).
5. Диаграмма компонентов // Википедия URL: https://ru.wikipedia.org/wiki/Диаграмма_компонентов (дата обращения: 15.05.2024).
6. Ельсуков Д. А. Python - язык программирования // Экономика и социум. 2021. №11-1 (90). URL: <https://cyberleninka.ru/article/n/python-yazyk-programmirovaniya> (дата обращения: 08.05.2025).
7. Алексеева Л. Г., Алексеев П. С. Язык промптов, или особенности формулирования запросов к генеративным нейросетям для создания изображений // Verba. Северо-Западный лингвистический журнал. 2024. №3 (13). URL: <https://cyberleninka.ru/article/n/yazyk-promptov-ili-osobennosti-formulirovaniya-zaprosov-k-generativnym-neyrosetyam-dlya-sozdaniya-izobrazheniy> (дата обращения: 18.05.2025).
8. Ремазанов И., Гулджанова Д., Ходжамырадов Р. Особенности объектно-ориентированного программирования // Вестник науки. 2024. №5 (74). URL: <https://cyberleninka.ru/article/n/osobennosti-obektno-orientirovannogo-programmirovaniya> (дата обращения: 20.05.2025).
9. Царев Ю. В., Сильянова Е. Ф., Кисельников С. А. Особенности ручного и автоматизированного тестирования программного обеспечения // Вестник науки. 2021. №6 (39). URL: <https://cyberleninka.ru/article/n/osobennosti-ruchnogo-i-avtomatizirovannogo-testirovaniya-programmnogo-obespecheniya> (дата обращения: 20.05.2025).
10. Сарычева Ю.Р., Липатова С.Е. Автоматизированное тестирование API // StudNet. 2021. №7. URL: <https://cyberleninka.ru/article/n/avtomatizirovannoe-testirovanie-api> (дата обращения: 20.05.2025).

© О. А. Шведова, Е. Ю. Воронкин, 2025

Е. А. Шевченко^{1✉}, Е. Ю. Воронкин¹

Разработка расширения браузера для создания коллекции образцов элементов веб-страницы с использованием JavaScript

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: shea2002@mail.ru

Аннотация. В статье рассматривается процесс разработки расширения браузера для создания коллекции образцов элементов веб-страницы с использованием JavaScript. В ходе исследования была проанализирована предметная область, выделены существующие подходы к извлечению компонентов интерфейса, а также выявлены их ограничения. Целью работы стало создание расширения, позволяющего выделять элементы прямо на странице, очищать их от лишних стилей, просматривать в изолированной среде и сохранять в формате JSON для последующего использования в редакторах интерфейсов. При реализации использовался нативный стек технологий (HTML, CSS, JavaScript) и API Chrome Extension. Архитектура построена на модульной структуре с изолированными компонентами. В статье кратко изложены этапы разработки, а также продемонстрирована работа расширения на сайте «METANIT».

Ключевые слова: браузерное расширение, JavaScript, предпросмотр, взаимодействие с DOM, извлечение данных, выбор стилей, хранение контента

Е. А. Shevchenko^{1✉}, E. Yu. Vononkin¹

Developing a browser extension to create a collection of sample web page elements using JavaScript

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: shea2002@mail.ru

Abstract. The article discusses the process of developing a browser extension to create a collection of sample elements of a web page using JavaScript. The study analyzed the subject area, highlighted existing approaches to extracting interface components, and identified their limitations. The purpose of the work was to create an extension that allows you to select elements directly on the page, clear them of unnecessary styles, view them in an isolated environment and save them in JSON format for future use in interface editors. The implementation used a native technology stack (HTML, CSS, JavaScript) and the Chrome Extension API. The architecture is based on a modular structure with isolated components. The article summarizes the stages of development, as well as demonstrates how the extension works on the «METANIT» website.

Keywords: browser extension, JavaScript, preview, DOM interaction, data extraction, style selection, content storage

Введение

В веб-разработке визуальная составляющая сайта играет не менее важную роль, чем функциональная. Заказчики зачастую приходят без четкого технического задания, что в разы усложняет процесс разработки. Разработчику приходится самостоятельно подбирать примеры с других сайтов и демонстрировать

возможные решения. При этом использование скриншотов или графических редакторов только повышает энергозатраты, что оказывается нерациональным в условиях малых или средних проектов. Работа через DevTools требует времени на анализ структуры и стилей, которые могут зависеть от контекста страницы. Все это замедляет процесс и усложняет взаимодействие с заказчиком.

Целью настоящей работы является разработка браузерного расширения, позволяющего визуально выбирать элементы с веб-страниц, просматривать их в интерактивном режиме и сохранять в формате, пригодном для дальнейшей разработки.

Работа обладает практической значимостью как готовый инструмент для веб-разработчиков, упрощающий процесс подготовки интерфейсных решений.

Методы и материалы

При разработке расширения был проведен анализ существующих решений [1, 2], это позволило выделить их ограничения и сформулировать требования к собственной разработке.

Для построения архитектуры использовался модульный подход, обеспечивающий изоляцию компонентов и гибкость при масштабировании [3]. Проектирование интерфейсов велось с учетом принципов минимализма и быстрого взаимодействия. Логика приложения реализована на JavaScript, с использованием стандартов ECMAScript и API расширений Chrome, включая `chrome.runtime`, `chrome.storage`, `chrome.tabs` [4].

В качестве среды разработки использовался Visual Studio Code с набором расширений для форматирования, автодополнения и документации коду через JSDoc [5]. Для тестирования и отладки использовались Chrome DevTools и режим разработчика браузера Chrome. Хранение пользовательских данных осуществлялось через `chrome.storage.local`, что обеспечило изоляцию данных и независимость от сторонних серверов. Все модули реализованы с учетом ограничений Manifest V3.

Результаты

В результате было разработано расширение, позволяющее выделять HTML-элементы на веб-странице, просматривать их визуальное представление и структуру, а также сохранять в формате JSON для дальнейшего использования.

После запуска расширения открывается окно с кнопкой активации захвата (рис. 1).

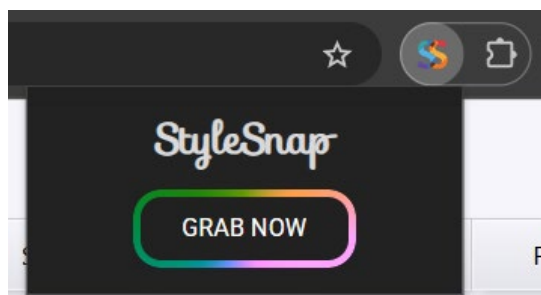


Рис. 1. Интерфейс расширения

После активации необходимо выбрать элемент на странице и кликнуть по нему, после этого появится список всех родительских и вложенных элементов выбранного блока. При наведении на любой из них в интерфейсе расширения нужный элемент на странице будет автоматически подсвечиваться, чтобы пользователь легко мог сориентироваться в структуре (рис. 2).

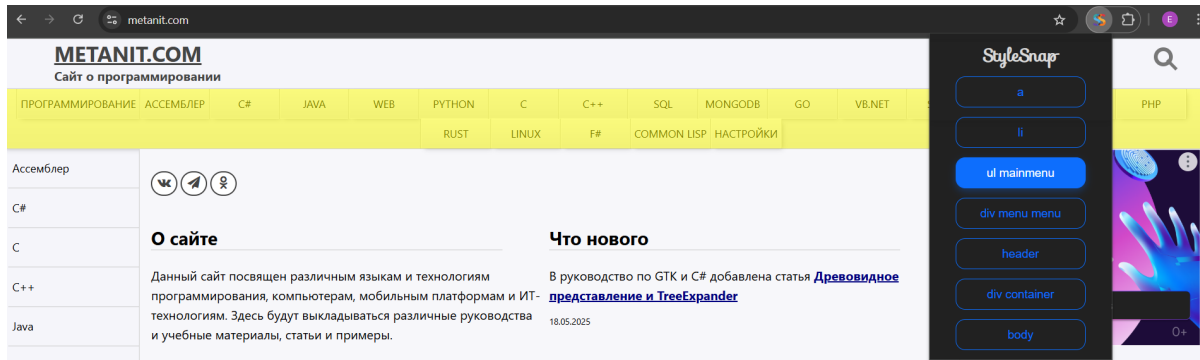


Рис. 2. Подсветка элементов на странице

Клик по элементу в расширении открывает предпросмотр, в котором отображается как внешний вид, так и структура DOM с возможностью перехода к дочерним узлам и их детального просмотра (рис. 3).

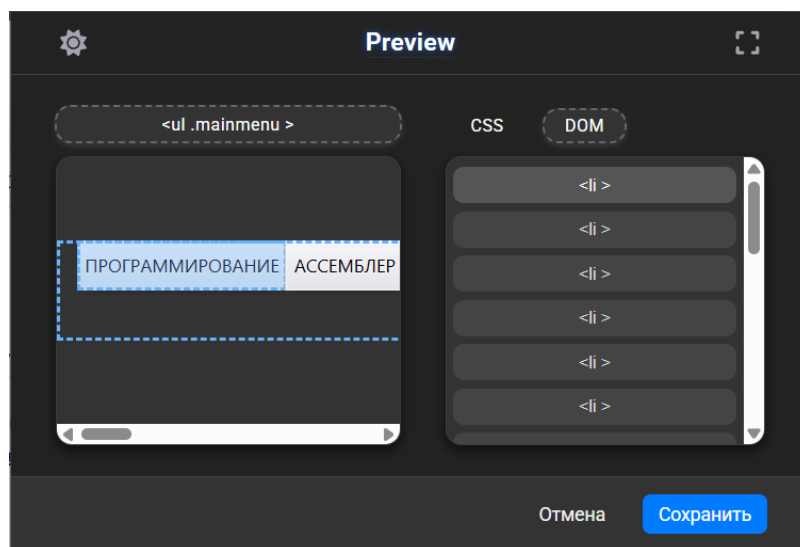


Рис. 3. Структура DOM и дочерние элементы

Пользователь может не только увидеть дочерние элементы, но и управлять стилями каждого из них с помощью интерфейса чекбоксов (рис. 4).

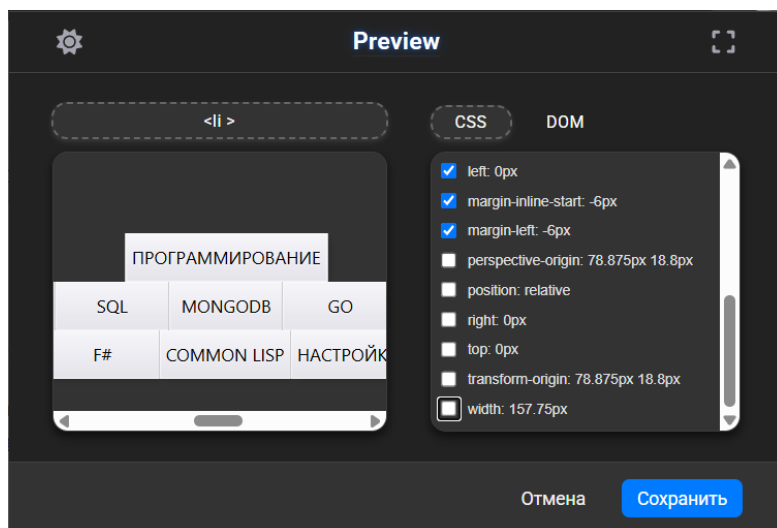


Рис. 4. Управление стилями через чекбоксы

Для более точной оценки предусмотрен полноэкранный предпросмотр, включающий в себя те же функции, которые были описаны выше (рис. 5).

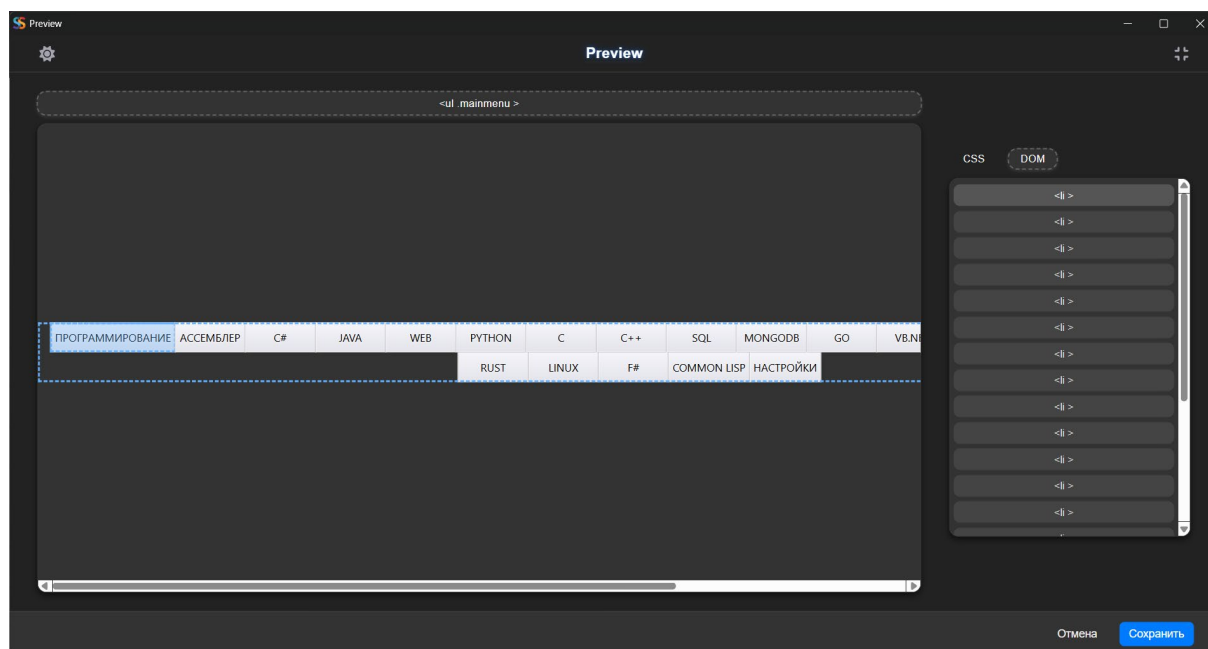


Рис. 5. Полноэкранный режим

Также было предусмотрено сохранение структуры и стилей элемента в формате JSON. При клике на кнопку «Сохранить» открывается окно, в котором необходимо дать наименование коллекции, а также указать в какую папку необходимо сохранить (рис. 6).

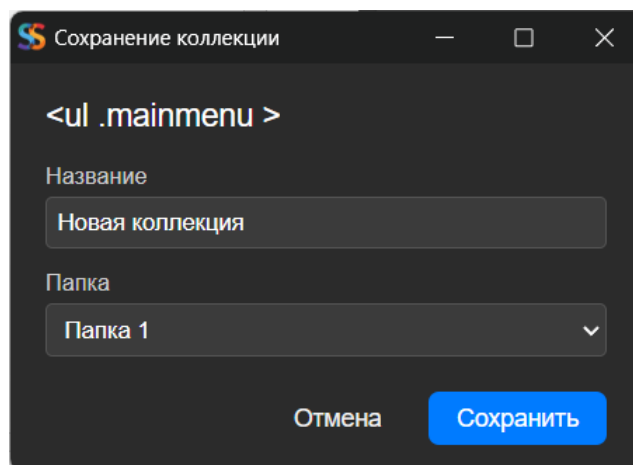


Рис. 6. Окно сохранения

Заключение

В результате выполненной работы было разработано расширение браузера для создания коллекции образцов элементов веб-страницы с использованием JavaScript. Сохраненный файл в формате JSON пригоден для повторного использования и может быть загружен в редактор WISUA.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. CopyCSS. Расширение для копирования HTML и CSS с веб-страницы. – URL: <https://chrome.google.com/webstore/detail/copy-css> (дата обращения: 21.01.2025).
2. SnipCSS. Инструмент для визуального извлечения стилей с сайтов. – URL: <https://snipcss.com> (дата обращения: 21.01.2025).
3. Фаулер М. Архитектура корпоративных приложений : пер. с англ. – М. : Вильямс, 2004. – 560 с.
4. Chrome Extensions API. Документация для разработчиков. – URL: <https://developer.chrome.com/docs/extensions/> (дата обращения: 21.01.2025).
5. Visual Studio Code. Официальный сайт редактора кода. – URL: <https://code.visualstudio.com/> (дата обращения: 21.01.2025).

© Е. А. Шевченко, Е. Ю. Воронкин, 2025

К. Г. Щербинина^{1✉}, А. А. Шарапов¹

Совершенствование системы автоматического контроля доступа на парковку СГУГиТ с использованием нейронной сети

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: Istina.svarovskaia@yandex.ru

Аннотация. В этой статье были рассмотрены этапы разработки и совершенствования системы автоматического контроля доступа на парковку Сибирского государственного университета геосистем и технологий (СГУГиТ). Изначально проект столкнулся с рядом проблем, таких как задержки в поставке оборудования и отсутствие ключевых модулей. В рамках данной работы была проведена модернизация системы с применением технологий компьютерного зрения, нейросетевых алгоритмов (YOLOv11 и Tesseract), а также переработана архитектура веб-приложения на основе Django и OpenCV. В результате были реализованы функции видеонаблюдения, автоматического распознавания номерных знаков, а также усовершенствована система управления доступом и разграничения ролей пользователей.

Ключевые слова: интеллектуальная система, шлагбаум, автомобильная парковка, компьютерное зрение, машинное обучение

K. G. Scherbinina^{1✉}, A. A. Sharapov¹

Improvement of the automatic parking SSUGT access control system using a neural network

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: Istina.svarovskaia@yandex.ru

Abstract. This article reviewed the stages of development and improvement of the automatic parking access control system of the Siberian State University of Geosystems and Technologies (SSUGiT). Initially, the project faced a number of problems, such as delays in the supply of equipment and the absence of key modules. As part of this work, the system was upgraded using computer vision technologies, neural network algorithms (YOLOv11 and Tesseract), and the architecture of the web application based on Django and OpenCV was redesigned. As a result, video surveillance and automatic license plate recognition functions were implemented, as well as the access control system and user role differentiation were improved.

Keywords: intelligent system, barrier, car parking, computer vision, machine learning

Введение

В 2024 году в Сибирском государственном университете геосистем и технологий была начата разработка системы автоматической парковки. Однако проект не был доведен до рабочей версии. В приложении отсутствовала возможность получения и обработки видеопотоков, что является важной частью функционирования подобных систем. Также были выявлены проблемы с разграничением прав доступа. Кроме того, архитектура системы не предусматривала возможность масштабирования и не позволяла использовать ее более чем с одним шлагбаумом.

Указанные недостатки обусловили необходимость полноценной доработки системы и интеграции соответствующего оборудования.

Предметом исследования является разработка алгоритмов обработки видеопотока и распознавания номерных знаков автомобилей, а также обновление архитектуры программного обеспечения для реализации интеллектуальной системы контроля доступа на парковку.

Целью данной работы является совершенствование системы автоматического контроля доступа на парковку СГУГиТ с использованием нейронной сети, что должно обеспечить повышение уровня безопасности, снижение затрат на персонал и повышение удобства эксплуатации.

Методы и материалы

На первом этапе работы был проведен анализ предыдущей версии системы для автоматизации пропуска автомобилей. В результате были выявлены ключевые недостатки, значительно ограничивавшие ее функциональность [6]. В частности, в системе отсутствовала возможность подключения камер видеонаблюдения. Не был реализован модуль для распознавания номерных знаков автомобилей. Также имелись нарушения в разграничении прав доступа: все пользователи могли управлять шлагбаумом, а также добавлять и редактировать других пользователей. Кроме того, система не содержала полноценной административной панели, что затрудняло ее использование и сопровождение.

Для разработки системы был выбран стек технологий, обеспечивающий гибкость и возможность масштабирования. Языком программирования стал Python, а серверная часть реализована с использованием веб-фреймворка Django. В качестве базы данных на первом этапе применялась SQLite. Для обработки изображений и работы с видеопотоком использовалась библиотека OpenCV. Основой системы распознавания номерных знаков стала предобученная модель YOLOv11, дополненная модулем оптического распознавания текста (OCR) Tesseract.

Причиной перехода на YOLOv11 стало значительное улучшение характеристик по сравнению с предыдущими версиями [5]. Модель обеспечила более высокую точность распознавания объектов, особенно при хороших погодных условиях, при которых точность определения номерных знаков достигала 95 % [2].

Для обучения модели был собран специализированный датасет, включающий более 1 000 изображений с различными типами номерных знаков и транспортными средствами. Это позволило учитывать положение автомобиля и предотвращать преждевременное закрытие шлагбаума [1].

Алгоритмы распознавания номерных знаков основаны на методах компьютерного зрения и машинного обучения. Первичная обработка изображений, выделение контуров и локализация номерного знака выполняются с использованием библиотеки OpenCV [3]. Затем модель YOLOv11, интегрированная с фреймворком TensorFlow, выполняет детекцию объектов на изображении. Распознавание символов осуществляется с помощью модуля OCR Tesseract [9].

Результаты

В результате проведенной работы были достигнуты следующие результаты:

Была устранена ключевая проблема предыдущей версии системы – отсутствие модуля управления камерами видеонаблюдения. В новой версии реализован функционал подключения и отображения видеопотоков с IP-камер, что обеспечило визуальный контроль за происходящим на парковке в режиме реального времени [4].

Внедрен модуль автоматического распознавания регистрационных знаков автомобилей. Для детекции номерных знаков используется модель YOLO v11, которая работает в заранее определенных областях изображения, после чего сохраняется один кадр с наилучшей видимостью [8, 10]. Распознанные изображения обрабатываются OCR-модулем на базе Tesseract, что позволило повысить точность и надежность считывания номеров в различных погодных условиях и при разном освещении (рис. 1).

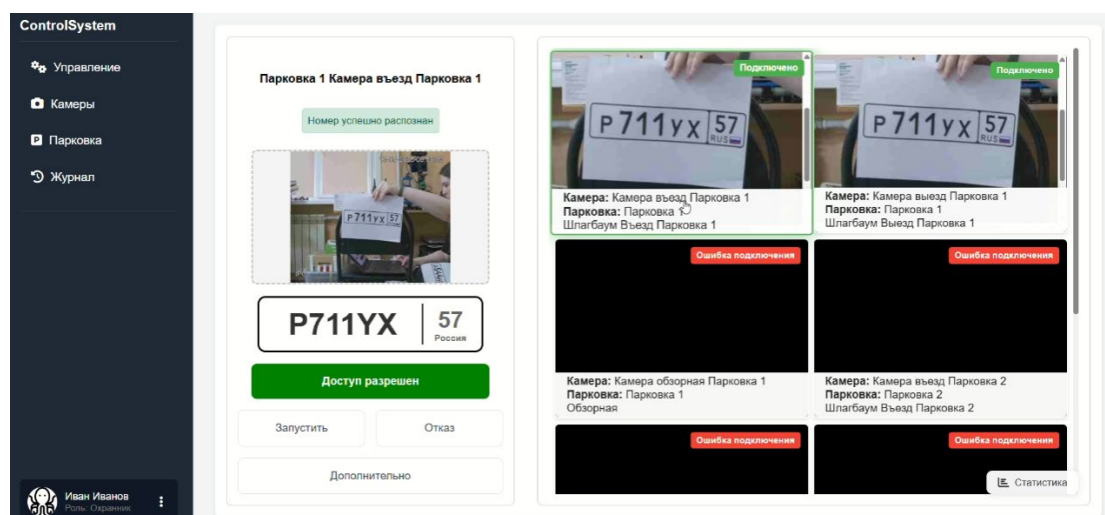


Рис. 1. Интерфейс приложения

Переработана система ролей пользователей. В предыдущей версии были ошибки в разграничении доступа, например, проректор по безопасности имел возможность управлять шлагбаумом. В новой версии внедрено четкое разграничение прав доступа в соответствии с должностными обязанностями [7]. Были определены и реализованы четыре основные роли: главный администратор, проректор по безопасности, главный охранник и охранник (рис. 2).

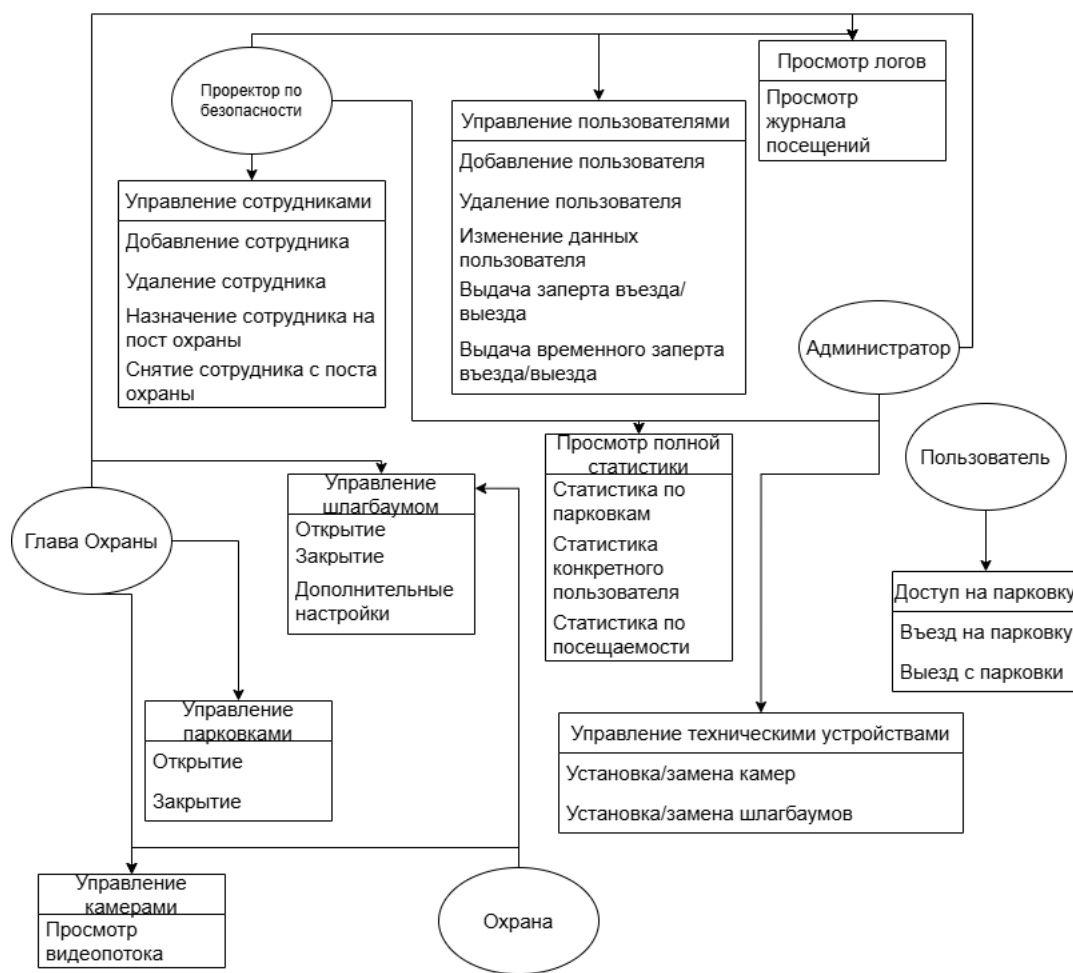


Рис. 2. Диаграмма возможностей

Также была обновлена архитектура системы, что обеспечило ее стабильную работу и возможность масштабирования. Интерфейс системы был переработан с учетом удобства использования и логической структуры взаимодействия. Добавлены функции авторизации, регистрации событий въезда и выезда, а также подготовлены основы для дальнейшей реализации статистических отчетов и аналитики.

Заключение

В данной работе представлено усовершенствование ранее созданной системы автоматического контроля доступа на парковку СГУТиТ. Были устранены выявленные недостатки, связанные с отсутствием модулей управления камерами и распознавания автомобильных номеров, а также произведена переработка системы разграничения прав пользователей. В результате была создана обновленная система с измененной архитектурой и полностью рабочими моделями распознавания.

В дальнейшем будет проводиться более точное тестирование системы в различных условиях эксплуатации для оценки ее устойчивости и адаптивности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Никитин, К. А. Разработка систем автоматизированной парковки на основе методов компьютерного зрения / К. А. Никитин, О. И. Захарова, Е. А. Рыбаков // Вестник науки. – 2024. – Т. 3, № 6 (75). – С. 1432–1437. – Текст : непосредственный.
2. Лебедев, Д. Л. Влияние освещенности на точность распознавания номерных знаков в системах контроля доступа / Д. Л. Лебедев, К. А. Федоров // Технические науки и инженерное дело. – 2023. – Т. 9, № 1. – С. 12–17. – Текст : непосредственный.
3. Епифанов, В. А. Эффективный алгоритм идентификации транспортных средств в системах видеонаблюдения / В. А. Епифанов, И. О. Темкин, С. Е. Красноярский // Горный информационно-аналитический бюллетень (научно-технический журнал). – 2023. – № 6. – С. 5–18. – DOI: 10.25018/0236_1493_2023_6_0_5. – Текст : непосредственный.
4. Куликова, Н. Н. Проектирование системы IP-видеонаблюдения технического центра ООО «Авторитет» / Н. Н. Куликова, О. В. Охрименко, Д. И. Стрижаков, А. В. Ищенко // Современные проблемы физики, биофизики и инфокоммуникационных технологий. – 2022. – № 12. – С. 212–221. – Текст : непосредственный.
5. Кажымурат, Г. А. Легковесное обнаружение объектов в реальном времени на потребительских GPU: исследование на примере YOLO11n / Г. А. Кажымурат, С. Т. Каимов // Вестник науки. – 2025. – Т. 4, № 4 (85). – С. 669–675. – Текст : непосредственный.
6. Люсюков, А. В. Проведение анализа систем видеонаблюдения с распознаванием автомобильных номеров для повышения безопасности на парковках и дорогах / А. В. Люсюков, А. А. Зайцев, В. П. Аракелян // Вестник науки. – 2024. – Т. 3, № 6 (75). – С. 1392–1399. – Текст : непосредственный.
7. Левин, С. М. Кейс: разработка программного решения для распознавания номеров транспортных средств / С. М. Левин, А. Е. Тихонов // Известия Томского политехнического университета. Промышленная кибернетика. – 2024. – Т. 2, № 1. – С. 1–6. – Текст : непосредственный.
8. Истратова, Е. Е. Разработка и исследование программного модуля для контроля и управления доступом транспортных средств на основе распознавания автомобильных номеров / Е. Е. Истратова, А. И. Гостеева // International Journal of Open Information Technologies. – 2022. – Т. 10, № 10. – С. 30–37. – Текст : непосредственный.
9. Бобров, К. А. Анализ технологий распознавания текста из изображения / К. А. Бобров, В. Д. Шульман, К. П. Власов // Международный журнал гуманитарных и естественных наук. – 2022. – № 3-2. – С. 124–128. – Текст : непосредственный.
10. Смирнов, С. Е. Применение методов машинного обучения для распознавания автомобильных номерных знаков / С. Е. Смирнов, А. К. Козлов // Математические и информационные технологии. – 2023. – Т. 8, № 4. – С. 30–35. – Текст : непосредственный.

© К. Г. Щербинина, А. А. Шаранов, 2025

М. Е. Арапова^{1✉}, В. А. Васильева¹, Е. Ю. Кутенкова¹

Анализ изменений в стандартах ЕСКД

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: 89635115285@mail.ru

Аннотация. В статье рассматриваются основные изменения, внесенные в ГОСТы единой систем технологической документации (ЕСКД). Введение изменений в стандарты ЕСКД актуально из-за развития современных технологий и появления новых требований к проектированию изделий на всех уровнях детализации. Эти стандарты регулируют разработку и оформление конструкторской документации, обеспечивая ее единообразие и качество. В последние годы ЕСКД претерпела значительную эволюцию, отражая современные тенденции в проектировании и производстве. Цель изменений – повышение эффективности, качества и международной совместимости конструкторской документации. Внесение изменений в стандарты ЕСКД является непрерывным процессом, направленным на адаптацию системы к современным технологиям и потребностям рынка. Следование обновленным стандартам позволяет повысить качество и эффективность проектирования, ускорить процессы производства и обеспечить конкурентоспособность отечественной промышленности. Постоянное изучение и применение новых стандартов ЕСКД является ключевым фактором успеха для любого предприятия, работающего в сфере приборостроения.

Ключевые слова: ЕСКД, проектирование, конструкторская документация, электронный документооборот

M. E. Arapova^{1✉}, V. A. Vasilyeva¹, E. Yu. Kutenkova¹

Analysis of changes in the ESKD standards

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: 89635115285@mail.ru

Abstract. The article discusses the main changes made to the GOST standards for unified systems of technological documentation (UTDS). The introduction of changes to the UTDS standards is relevant due to the development of modern technologies and the emergence of new requirements for product design at all levels of detail. These standards regulate the development and design of engineering documentation, ensuring its uniformity and quality. In recent years, the ESKD has undergone significant evolution, reflecting current trends in design and manufacturing. The goal of these changes is to improve the efficiency, quality, and international compatibility of engineering documentation. Making changes to the ESKD standards is an ongoing process aimed at adapting the system to modern technologies and market needs. Following the updated standards allows for improved design quality and efficiency, faster production processes, and ensuring the competitiveness of the domestic industry. Continuously studying and applying.

Keywords: UTDS, design, engineering documentation, and electronic document management

Введение

Введение изменений в стандарты Единой системы конструкторской документации (ЕСКД) актуально из-за развития технологий и появления новых тре-

бований к проектированию изделий на всех уровнях детализации. Эти стандарты регулируют разработку и оформление конструкторской документации, обеспечивая ее единообразие и качество.

ЕСКД – это совокупность государственных стандартов, определяющих правила разработки, оформления и обращения конструкторской документации. В последние годы ЕСКД претерпела значительную эволюцию, отражая современные тенденции в проектировании и производстве. Цель изменений – повышение эффективности, качества и международной совместимости конструкторской документации

Обсуждение

Недавние изменения упростили и обновили процесс поиска информации в ЕСКД, внедрив новые термины и пересмотрев графические обозначения. Это повышает эффективность работы инженеров и проектировщиков, адаптируя требования к современным условиям [1–6].

Изменения касаются структуры и методов оформления документации, что улучшает взаимодействие участников разработки и способствует повышению качества продукции.

Одно из наиболее значимых изменений – это активное внедрение электронного документооборота. Новые стандарты ЕСКД ориентированы на использование цифровых форматов данных, таких как САД-системы и системы управления данными о продукте (PDM). Это позволяет существенно ускорить процессы проектирования, согласования и производства, снизить затраты на бумажную документацию и повысить защищенность информации. Стандарты определяют требования к электронным форматам, обеспечивая совместимость данных между различными программными продуктами.

Современные стандарты ЕСКД поддерживают применение инновационных методов проектирования, таких как параметрическое и 3D-моделирование. Они предоставляют рекомендации по использованию этих методов, а также определяют требования к оформлению получаемой документации. Это позволяет создавать более сложные и точные модели, проводить эффективные анализы конструкций и оптимизировать проектные решения [7–10].

Значительное внимание уделяется унификации и гармонизации стандартов ЕСКД с международными аналогами, в первую очередь с ISO. Это облегчает международное сотрудничество, способствует обмену опытом и технологиями, а также повышает конкурентоспособность отечественной продукции на мировом рынке.

В новых стандартах ЕСКД уточнены и детализированы требования к оформлению конструкторской документации. Это касается как графического представления информации (чертежи, схемы), так и текстовой части (спецификации, пояснительные записки). Цель этих изменений – повышение читаемости и однозначного понимания документации всеми участниками процесса [11–13].

Новые стандарты ЕСКД содержат более строгие требования к защите интеллектуальной собственности. Они предусматривают механизмы маркировки и защиты документов от несанкционированного копирования и использования.

Значительные изменения внесены в ГОСТ Р 2.308-2023 ЕСКД. Допуски формы и расположения поверхностей [14]. Например, в сводных таблицах, представленных на рисунке 1, где слева данные из ГОСТ Р 2.308-2023 ЕСКД, справа из ГОСТ Р 2.308-2011 ЕСКД видно, что произошло изменение числа групп допусков: вместо ранее существовавших трех групп (допуск формы, допуск расположения и суммарные допуски формы и расположения) в новой версии ГОСТ – четыре группы (допуски формы, допуски ориентации, допуски месторасположения, допуски биения). Произошло перераспределение допусков между группами, что показано на рисунке линиями. Из допусков формы исключен допуск профиля продольного сечения, а из допусков расположения – допуск пересечения осей. В обновленном ГОСТ 2023 года указывается допуск биения и допуск полного биения, но не конкретизируется, какой именно (радиальное или торцовое биение, биение в заданном направлении, как это было прежде).

ГОСТ 2.308-2023

Таблица 1

Группа допусков	Вид допуска	Графический символ
Допуски формы	Допуск прямолинейности	—
	Допуск плоскостности	▱
	Допуск круглости	○
	Допуск цилиндричности	⊘
	Допуск формы заданного профиля	⌒
	Допуск формы заданной поверхности	⌒
Допуски ориентации	Допуск параллельности	∥
	Допуск перпендикулярности	⊥
	Допуск наклона	∠
Допуски месторасположения	Позиционный допуск	⊕
	Допуск соосности	⊙
	Допуск симметричности	≡
Допуски биения	Допуск биения	↗
	Допуск полного биения	↗↘

Примечание — В зависимости от необходимости указания базы для допусков формы заданного профиля и допусков формы заданной поверхности они могут быть отнесены к допускам формы, ориентации и месторасположения.

ГОСТ 2.308-2011

Таблица 1

Группа допусков	Вид допуска	Знак
Допуск формы	Допуск прямолинейности	—
	Допуск плоскостности	▱
	Допуск круглости	○
	Допуск цилиндричности	⊘
	Допуск профиля продольного сечения	≡
Допуск расположения	Допуск параллельности	∥
	Допуск перпендикулярности	⊥
	Допуск наклона	∠
	Допуск соосности	⊙
	Допуск симметричности	≡
	Позиционный допуск	⊕
	Допуск пересечения осей	×
	Допуск радиального биения	↗
	Допуск торцового биения	↗↘
	Допуск биения в заданном направлении	↗↘
Суммарные допуски формы и расположения	Допуск полного радиального биения	↗↘
	Допуск полного торцового биения	↗↘
	Допуск формы заданного профиля	⌒
	Допуск формы заданной поверхности	⌒

Примечание — Суммарные допуски формы и расположения поверхностей, для которых не установлены отдельные графические знаки, обозначают знаками составных допусков в следующей последовательности: знак допуска расположения, знак допуска формы.

Например:
 ∥ ▱ — знак суммарного допуска параллельности и плоскостности;
 ⊥ ▱ — знак суммарного допуска перпендикулярности и плоскостности;
 ∠ ▱ — знак суммарного допуска наклона и плоскостности.

Рис. 1. Сравнение таблиц с обозначением допусков графическими символами

Введено новое требование что, если поле допуска является общим для нескольких различных элементов, то при указании геометрического допуска следует использовать дополнительный символ «CZ», который указывают после числового значения допуска, как показано на рисунке 2.

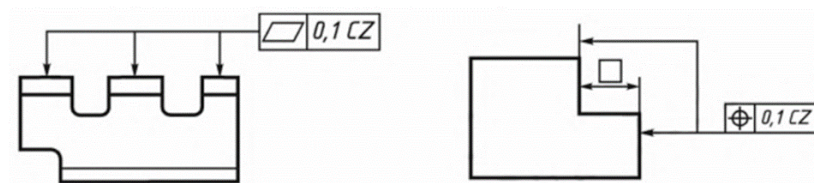


Рис. 2. Обозначение общего для нескольких различных элементов поля допуска

В ГОСТ Р 2.308-2023 ЕСКД перед числовым значением допуска следует указывать:

- символ $\varnothing$ – при круговом или цилиндрическом поле допуска, как показано на рисунке 3, а;
- символ $S\varnothing$ – при сферическом поле допуска, как показано на рисунке 3, б.



Рис. 3. Пример обозначения поля допуска

В статье приведена незначительная часть изменений, внесенных в ГОСТ Р 2.308-2023 ЕСКД. Задача технических специалистов заключается в том, чтобы оперативно отслеживать все нововведения и учитывать их при проектировании конструкторской и технологической документации.

Заключение

В целом, обновления стандартов ЕСКД направлены на упрощение и оптимизацию процессов разработки и использования конструкторской документации. Это достигается за счет внедрения современных технологий, унификации требований к изделиям и повышения эффективности работы.

Внесение изменений в стандарты ЕСКД является непрерывным процессом, направленным на адаптацию системы к современным технологиям и потребностям рынка. Следование обновленным стандартам позволяет повысить качество и эффективность проектирования, ускорить процессы производства и обеспечить конкурентоспособность отечественной промышленности. Постоянное изучение и применение новых стандартов ЕСКД является ключевым фактором успеха для любого предприятия, работающего в сфере приборостроения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Колесниченко, Н. М. Инженерная и компьютерная графика [Электронный ресурс] : учеб. пособие / Н.М. Колесниченко, Н.Н. Черняева. – Вологда : Инфра-Инженерия, 2018. – 236 с. (дата обращения: 23.04.2025). – Режим доступа: <http://znanium.com/> – Загл. с экрана....

2. Бастратов, В.М. Взаимозаменяемость и нормирование точности : учеб. пособие / В.М. Бастратов. – Йошкар-Ола : Поволжский государственный технологический университет, 2023. – 172 с. – ISBN 978-5-8158-2353-2. – Текст : электронный. – URL: <https://znanium.ru/catalog/product/2133945> (дата обращения: 23.04.2025). – Режим доступа: для авториз. пользователей.
3. Сорокин, Н. П. Инженерная графика [Электронный ресурс] / Н. П. Сорокин, Е. Д. Ольшевский, А. Н. Заикина, Е. И. Шибанова. – СПб. : Лань, 2016. – 392 с. – (дата обращения: 23.04.2025). Режим доступа: <http://e.lanbook.com/book/746811> – Загл. с экрана....
4. Дегтярев, В. М. Инженерная и компьютерная графика [Text] : учебник для вузов / В. М. Дегтярев, В. П. Затыльников. - М. : Академия, 2010. - 240 с.
5. Компьютерная графика [Текст] : учеб. пособие / П. Ю. Бугаков, М. М. Шляхова ; СГУГиТ. - Новосибирск : СГУГиТ, 2015. – 51 с.
6. Боресков, А. В. Компьютерная графика [Текст] : учебник и практикум / А. В. Боресков, Е. В. Шикин. – М. : Юрайт, 2016. – 217 с.
7. ГОСТ Р 2.005-2023 ЕСКД. Термины.
8. ГОСТ Р 2.201-2023 ЕСКД. Обозначение и наименование изделий и конструкторских документов.
9. ГОСТ Р 2.102-2023 ЕСКД. Обозначение конструкторских документов.
10. ГОСТ Р 2.105-2019 ЕСКД. Общие требования к текстовым документам изм. № 2.
11. ГОСТ Р 2.101-2019 ЕСКД. Виды изделий.
12. ГОСТ Р 2.104-2023 ЕСКД. Основные надписи.
13. ГОСТ Р 2.109-2023 ЕСКД. Основные требования к чертежам.
14. ГОСТ Р 2.308-2023 ЕСКД. Допуски формы и расположения поверхностей.

© М. Е. Арапова, В. А. Васильева, Е. Ю. Кутенкова, 2025

А. М. Бахтиярова^{1✉}, Е. Д. Моисеева¹, Д. В. Климова¹, Д. М. Никулин¹

Использование новых термозащитных покрытий в беспилотных авиационных системах

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: bakhtiyarova7207@gmail.com

Аннотация. Беспилотные авиационные системы (БАС) на сегодняшний день используются во многих отраслях, они нашли широкое применение в МЧС. В основном беспилотные авиационные системы используются для мониторинга обстановки, контроля местностей, обеспечения связи в чрезвычайных ситуациях, осуществления пожаротушения и доставки малогабаритных грузов. При близком подлете к местам с высокой температурой, авиационные системы могут выйти из строя за короткий промежуток времени. Данную проблему можно решить, используя защитные покрытия для основных узлов и элементов БАС. В данной статье рассматриваются термозащитные покрытия, способные увеличить время нахождения БАС вблизи источников высокой температуры. Актуальность темы заключается в поиске новых термозащитных материалов, которые могут использоваться в беспилотных авиационных системах. Целью работы является рассмотрение инновационных термостойких и термозащитных материалов, используемых в узлах и элементах БАС, а также представление возможных термозащитных материалов на основе углеродных нанотрубок.

Ключевые слова: нанотрубки, термостойкое и термозащитное покрытие, БАС

A. M. Bakhtiyarova^{1✉}, E. D. Moiseeva¹, D. V. Klimova¹, D. M. Nikulin¹

Use of new thermal protective coatings in unmanned aircraft systems

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: bakhtiyarova7207@gmail.com

Annotation. Unmanned aircraft systems (UAS) are currently used in many industries, they have found wide application in the Ministry of Emergency Situations. Unmanned aircraft systems are mainly used for situation monitoring, terrain control, emergency communications, fire extinguishing and delivery of small-sized cargo. But when flying close to places with high temperatures, aviation systems can fail in a short period of time. This problem can be solved by using protective coatings for the main units and elements of the UAS. This article discusses heat-protective coatings that can increase the time the UAS stays near high temperatures. The relevance of the topic lies in the search for new heat-protective materials that can be used in unmanned aircraft systems. The purpose of the work is to consider innovative heat-resistant and heat-protective materials used in UAS units and elements, as well as to present possible heat-protective materials based on carbon nanotubes.

Keywords: nanotubes, heat-resistant and thermoprotective coating, UAS

Введение

Во время тушения пожаров подразделения МЧС отправляют на место происшествия разведывательные отряды, чтобы оценить ситуацию. Но это создает риск для жизни и здоровья сотрудников спасательных служб, поэтому инженеры

ищут возможность использовать для этой цели беспилотные авиационные системы. С помощью БАС можно предварительно обследовать место происшествия и определить положение источников опасности, оценить ситуацию. Однако, для того чтобы работать в непосредственной близости с источником высокой температуры, беспилотные авиационные системы должны быть термостойкими и обладать специальной защитой [1, 2].

В 2023 году инженеры из Лондона разработали прототип квадрокоптера Fire Drone, покрытие которого было сделано из полиимидного аэрогеля – пористого геля низкой плотности. Аэрогель состоит в основном из воздушных полостей в связке со стекловолокном, за счет этого дрон может летать вблизи источников высоких температур. Ниже показан внешний вид дрона, при этом все его части заключены в термозащитный корпус, включая электромоторы (рис. 1) [3, 4].



Рис. 1. Внешний вид квадрокоптера Fire Drone

В течение 10 минут квадрокоптер может выдерживать температуру эксплуатации до 200 градусов Цельсия. Причем внутри корпуса поддерживается постоянная температура не выше 40 градусов Цельсия благодаря охлаждающей системе. В дроне имеется инфракрасная камера, которая помогает отслеживать и разведывать местность в условиях дыма, поэтому может помочь спасательным и пожарным службам [4, 5].

В 2024 году инженеры центра НТИ на базе МГТУ им. Н. Э. Баумана разработали полимер, выдерживающий высокую температуру в условиях пожара или боевых действий. Они получили технологию синтеза полиэфиримидов и создали образец, имеющий повышенную термостойкость. Температура плавления этого образца достигла 245 градусов Цельсия, и на данный момент является максимальной [5, 6].

Рассмотренные беспилотные авиационные системы состоят из термостойких и термозащитных узлов и элементов.

Данная работа посвящена изучению возможности использования покрытий на основе углеродных нанотрубок для защиты от быстрого перегрева узлов и элементов БАС.

Методы и материалы

В качестве материала для термозащитного покрытия использовался концентрат из углеродных нанотрубок в дистиллированной воде. Перед нанесением термозащитного покрытия, концентрат с углеродными нанотрубками подвергался ультразвуковой обработке, чтобы получить относительно однородную структуру из агломератов трубок. В качестве образца с нанесенным покрытием использовалась термопара, которая помещалась в разогретую до 150 °С муфельную печь через специальное рабочее отверстие, (рис. 2). Далее измерялось время нагревания термопары до температуры 50, 100 и 120 °С.



Рис. 2. Муфельная печь для проведения опыта

Сначала измерения проводились без нанесения покрытия для возможности последующего сравнения полученных в результате исследования результатов.

Измерения с покрытием проводились в тех же условиях, что и без нанесения покрытия. Покрытие наносилось на обезжиренную термопару методом окунания ее в концентрат с углеродными нанотрубками после ультразвуковой обработки, после чего покрытие высыхало естественным путем. После каждого измерения термопара охлаждалась до комнатной температуры, очищалась от покрытия и обезжиривалась для следующего эксперимента.

Результаты

Результаты измерений, полученные без покрытия и с покрытием, представлены в табл. 1 и табл. 2.

Таблица 1

Результаты измерения термопары без покрытия

№ п/п	Температура, °C	Время, с
1.	50; 100; 120	8,4; 42,2; 69
2.	50; 100; 120	7,7; 35,5; 55,8
3.	50; 100; 120	8,4; 33,8; 55,1
4.	50; 100; 120	10,1; 39,3; 60,1
5.	50; 100; 120	8,2; 34,9; 56,0
Среднее значение	50	8,56
	100	37,14
	120	59,20

Таблица 2

Результаты измерения термопары с покрытием

№ п/п	Температура, °C	Время, с
1.	50; 100; 120	9,2; 59,4; 112
2.	50; 100; 120	8,3; 48,8; 90,1
3.	50; 100; 120	8,9; 43,1; 68
4.	50; 100; 120	10,8; 46,9; 71,2
5.	50; 100; 120	10,5; 49,6; 92,9
Среднее значение	50	9,54
	100	49,56
	120	86,84

Обсуждение

По данным результатов измерения можно увидеть, что среднее время нагревания термопары после нанесения покрытия увеличилось. Для максимальной температуры 120 °C оно увеличилось в 1,4 раза.

Для детального рассмотрения покрытия из нанотрубок использовался микроскоп Carl Zeiss Scope A1, (рис. 3).

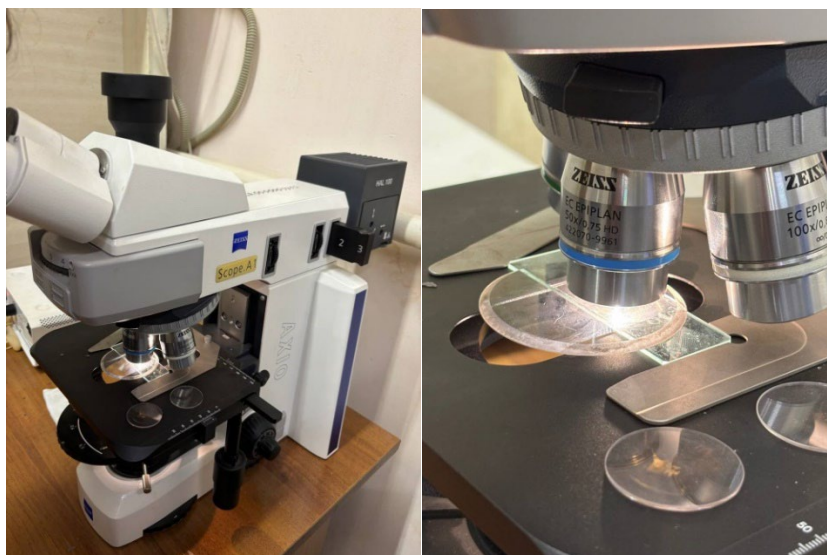


Рис. 3. Анализ нанесенного покрытия на предметном стекле

На рисунке 3 представлена фотография покрытия из нанотрубок на предметном стекле с увеличением 800 крат.



Рис. 3. Вид структуры покрытия, наблюдаемой в микроскопе

При изучении структуры покрытия видно, что агломераты из нанотрубок представляют сетчатую структуру, с огромным числом воздушных каналов

неправильной формы и вследствие плохой теплопроводности воздуха замедляют скорость нагрева (передачи тепла) вглубь материала [7, 8].

Заключение

По данным эксперимента можно сделать вывод, что с использованием покрытия из углеродных нанотрубок можно замедлить рост внутренней температуры тела, заключенного в него. Исходя из вышесказанного нанесение пленок из углеродных нанотрубок на БАС вполне возможно. Это позволит улучшить такие технические характеристики, как дальность и время полета в экстремально высоких температурных условиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Демичева О.В., Алексеев А.М., Томишко А.Г., Клинова Л.Л., Фетисова О.Е. Многослойные углеродные нанотрубки и их применение: Российский химический журнал. 2008.
2. Беленков Е.А. Трехмерная структура многослойных углеродных нанотрубок: Челябинский физико-математический журнал. 2016.
3. Беленков Е. А. Особенности структуры многослойных нанотрубок: Вестник ЧелГУ. 1998.
4. URL: <https://cnews.ru/link/a616944> (дата обращения: 01.05.2025).
5. Грешняков В.А. Структура и свойства алмазоподобных углеродных нанотрубок: Челябинский физико-математический журнал. 2023.
6. URL: <https://nplus1.ru/news/2023/07/03/the-drone-the-drone-the-drone-is-on-fire> (дата обращения: 01.05.2025).
7. Габидуллин М.Г., Хузин А.Ф., Рахимов Р.З., Ткачев А.Г., Михалева З.А., Толчков Ю.Н. Ультразвуковая обработка – эффективный метод диспергирования углеродных нанотрубок в объеме строительного композита: Construction materials. 2013.
8. Бессонова А.В., Бобринецкий И.И., Неволин В.К., Симунин М.М. Методики исследования сорбционных свойств агломератов углеродных нанотрубок: Известия вузов. Электроника, 2011. 88 с.

© А. М. Бахтиярова, Е. Д. Моисеева, Д. В. Климова, Д. М. Никулин, 2025

Н. В. Белоконов¹, С. А. Горбач^{1✉}, А. А. Балаганский¹, Д. Н. Титов¹

Разработка камеры, совмещенной с инфракрасным датчиком движения на базе ESP32

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: semyon.gorbach@yandex.ru

Аннотация. В статье представлена разработка камеры, совмещенной с инфракрасным (ИК) датчиком движения на базе микроконтроллера ESP32. ESP32 представляет собой современный микроконтроллер с интегрированными модулями Wi-Fi и Bluetooth, который широко применяется в проектах интернета вещей и системах автоматизации. Для программирования этого устройства и организации связи с компьютером используется TTL-конвертер – специальный переходник, преобразующий сигналы USB в последовательный интерфейс UART, понятный для ESP32. Основной темой исследования является создание компактного и энергоэффективного устройства для мониторинга и фиксации движения в реальном времени. Актуальность работы обусловлена растущим спросом на интеллектуальные системы безопасности с низким энергопотреблением и возможностью интеграции в IoT-сети. В статье представлена разработанная энергоэффективная система безопасности на базе ESP32-CAM и PIR-датчика, сочетающая низкое энергопотребление (благодаря режиму глубокого сна) с оперативным оповещением через Telegram.

Ключевые слова: ESP32, инфракрасный датчик, камера

N. V. Belokon¹, S. A. Gorbach^{1✉}, A. A. Balagansky¹, D. N. Titov¹

Development of a camera integrated with a PIR motion sensor based on ESP32

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: semyon.gorbach@yandex.ru

Abstract. The article presents the development of a camera combined with an infrared (IR) motion sensor based on the ESP32 microcontroller. ESP32 is a modern microcontroller with integrated Wi-Fi and Bluetooth modules, which is widely used in Internet of Things projects and automation systems. To program this device and organize communication with a computer, a TTL converter is used - a special adapter that converts USB signals into a serial UART interface understandable to ESP32. The main research topic is the creation of a compact and energy-efficient device for real-time motion monitoring and recording. The relevance of the work is due to the growing demand for intelligent security systems with low power consumption and the ability to integrate into IoT networks. The article presents a developed energy-efficient security system based on ESP32-CAM and PIR sensor, combining low power consumption (thanks to deep sleep mode) with prompt notification via Telegram.

Keywords: ESP32, PIR sensor, camera

Введение

Задачей исследования является разработка энергоэффективной системы мониторинга с автоматическим детектированием движения и мгновенной отправкой уведомлений. Основной подход основан на интеграции модуля ESP32-CAM с PIR-датчиком движения и системой оповещения через Telegram-бот.

Методы и материалы

PIR-датчик обнаруживает присутствие нарушителей, генерируя электрический сигнал при фиксации инфракрасного излучения. Хотя выходное напряжение датчика составляет всего несколько вольт, с помощью усилительной схемы его можно повысить до необходимого уровня для управления системой освещения и камерой наблюдения. Разработанное программное обеспечение постоянно отслеживает состояние системы.

Когда нарушитель попадает в зону обнаружения (до 10 метров), PIR-датчик вырабатывает сигнал 3.3 В, который после усиления активирует реле освещения и камеру ESP32-CAM. После включения камеры система делает снимок и отправляет его через WiFi в Telegram-бот. Как только нарушитель покидает зону действия датчика, система автоматически отключает камеру. Основные преимущества решения включают энергоэффективность за счет активации компонентов только при обнаружении движения, экономичность по сравнению с рыночными аналогами, мгновенные уведомления через Telegram и дальность обнаружения до 10 метров. При каждом новом срабатывании датчика цикл работы повторяется, обеспечивая непрерывный мониторинг охраняемой зоны с минимальным энергопотреблением [1–4].

Результаты

ESP32 представляет собой современный микроконтроллер с интегрированными модулями Wi-Fi и Bluetooth, который широко применяется в проектах интернета вещей и системах автоматизации. Для программирования этого устройства и организации связи с компьютером используется TTL-конвертер – специальный переходник, преобразующий сигналы USB в последовательный интерфейс UART, понятный для ESP32. Наиболее популярными моделями таких конвертеров являются CP2102 и CH340, которые обеспечивают стабильное соединение и позволяют загружать прошивку, а также проводить отладку кода.

В сочетании с ESP32 применяются PIR-датчик движения, такие как HC-SR501, которые обнаруживают перемещение объектов по изменению инфракрасного излучения в зоне контроля. Принцип работы такой системы основан на том, что при обнаружении движения PIR-датчик посылает электрический сигнал на ESP32, который может выполнять различные действия – активировать камеру для фотофиксации, отправлять push-уведомления через интернет или включать дополнительные устройства, например, сирену или прожектор.

Основным преимуществом такого решения является возможность организации полностью автономной работы благодаря поддержке ESP32 режима глубокого сна с минимальным энергопотреблением, когда микроконтроллер пробуждается

только при поступлении сигнала от датчика движения. Простота подключения и настройки делает эту связку популярной среди проектов – TTL-конвертер требует минимальной конфигурации, а PIR-датчик подключается всего тремя проводами, что позволяет быстро развернуть систему мониторинга даже без глубоких технических знаний. При этом система остается гибкой для модификаций – можно легко добавлять новые датчики или изменять логику работы через программирование ESP32, что открывает широкие возможности для создания умных систем безопасности, автоматического освещения и других решений для умного дома.

Этапы получения результата приведены на рис. 1. Разработанное программное обеспечение постоянно работает в фоновом режиме, отслеживая состояние камеры. При появлении нарушителя в зоне обнаружения PIR-датчика (до 10 метров или 30 футов) сенсор генерирует выходной сигнал 3.3 вольта. Этот сигнал усиливается и используется для активации реле системы освещения и веб-камеры.

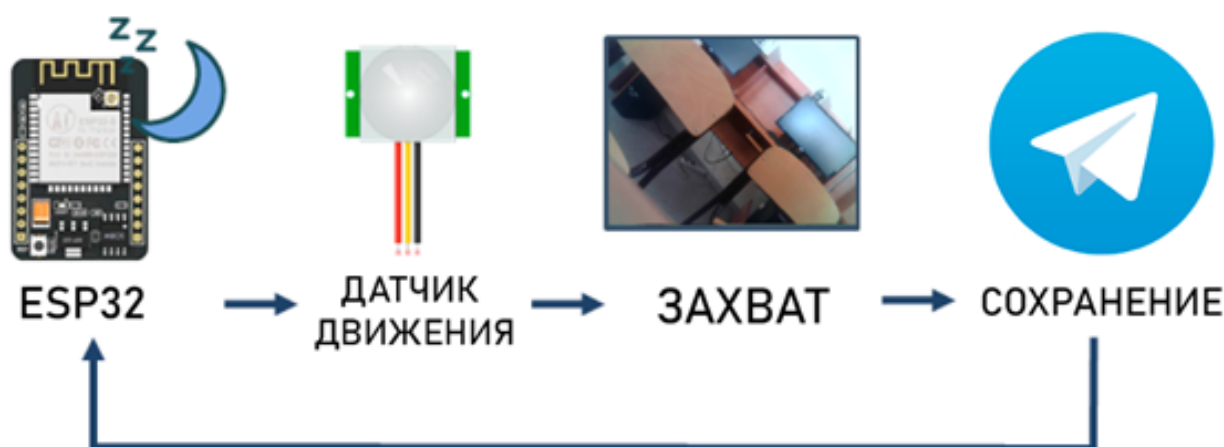


Рис. 1. Этапы получения результата

После срабатывания усилителя и включения камеры программное обеспечение инициирует процесс фотосъемки с помощью ESP32-CAM. Когда нарушитель покидает зону действия датчика, сигнал прекращается, что приводит к автоматическому отключению камеры. Полученные фотографии сохраняются в Telegram-бот. При каждом новом обнаружении движения в рабочей зоне датчика цикл работы системы повторяется, обеспечивая непрерывный мониторинг охраняемой территории.

Заключение

Разработана энергоэффективная система безопасности на базе ESP32-CAM и PIR-датчика, сочетающая низкое энергопотребление (благодаря режиму глубокого сна) с оперативным оповещением через Telegram. Система стабильно обнаруживает движение в радиусе 10 метров, мгновенно активируя камеру и передавая изображение, что исключает необходимость постоянного мониторинга. Модульная архитектура решения позволяет адаптировать его для различных применений

- от домашней безопасности до промышленного мониторинга. Полученные результаты подтверждают перспективность такого подхода для создания недорогих и надежных охранных систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Espressif Systems. ESP32-CAM Technical Reference Manual [Электронный ресурс]. – 2023. – URL: <https://www.espressif.com>
2. Random Nerd Tutorials. ESP32-CAM PIR Motion Detector with Photo Capture [Электронный ресурс]. – 2023. – URL: <https://randomnerdtutorials.com>
3. Kumar A., Sharma P. Low-Power IoT-Based Security System Using ESP32-CAM and PIR Sensor // International Journal of Advanced Research in Computer Science. – 2022. – Vol. 13. – № 4. – P. 45-52.
4. Universal Telegram Bot Library for ESP32 [Электронный ресурс]. – GitHub, 2023. – URL: <https://github.com/witnessmenow/Universal-Arduino-Telegram-Bot>

© Н. В. Белоконь, С. А. Горбач, А. А. Балаганский, Д. Н. Титов, 2025

П. Ф. Бжицких¹✉, А. А. Шрамков¹, В. П. Цыплаков¹, Е. Ю. Кутенкова¹

Сравнение инструментов искусственного интеллекта с российской системой по оптимизации оформления дипломной работы

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: pavel.bzhiczkih@mail.ru

Аннотация. В статье проведено сравнительное исследование двух вспомогательных инструментов, предназначенных для оптимизации работы над оформлением выпускной квалификационной работы: нейросети DeepSeek, от китайских разработчиков и российской системы InnoFlow, разработанной НИЯУ МИФИ. Анализируются функциональные возможности, преимущества и недостатки каждого инструмента, а также их применимость в условиях действия российских образовательных стандартов. DeepSeek выделяется интуитивно понятным интерфейсом, возможностью диалогового формата помощи в работе, анализом текстов на соответствие нормативам и помощи в структурировании работы. Однако система имеет ограничения, такие как невозможность обработки больших документов и некоторые неточности в ответах. InnoFlow, напротив, предлагает полную автоматизацию оформления выпускной квалификационной работы (ВКР) в соответствии с ГОСТ 7.32-2017, но в ситуациях с отклоняющимися требованиями от заданного ГОСТ 7.32-2017 требует навыков программирования для настройки автоматизированного оформления, так как готовую работу можно получить лишь в PDF-формате, что не дает возможности дальнейшего редактирования файла. Результаты исследования показали, что InnoFlow лучше адаптирована под строгие требования российских стандартов, в то время как DeepSeek представляет более гибкие и интеллектуальные инструменты для работы с текстом. Обе системы обладают уникальными преимуществами, что делает их полезными для разных этапов подготовки дипломной работы.

Ключевые слова: оформление дипломных работ, DeepSeek, InnoFlow, оптимизация, автоматизация

P. F. Brzickih¹✉, V. P. Tsyplakov¹, A. A. Shramkov¹, E. U. Kutenkova¹

Comparison of artificial intelligence tools with the russian system for optimizing the design of thesis papers

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: pavel.bzhiczkih@mail.ru

Abstract. The article provides a comparative study of two auxiliary tools designed to optimize the work on the design of final qualifying work: the Deepseek neural network, from the Chinese developers of the Russian InnoFlow system developed by the National Research Nuclear University MEPhI. The article analyzes the functionality, advantages and disadvantages of each tool, as well as their applicability in the context of Russian educational standards. DeepSeek stands out for its intuitive interface, the ability to use an interactive format to help with work, analyze texts for compliance with regulations, and help structure work. However, the system has limitations, such as the inability to process large documents and rare inaccuracies in the responses. InnoFlow, on the contrary, offers full automation of the design of the WRC in accordance with GOST 7.32-2017, but in situations with requirements deviating from the specified GOST 7.32-2017 requires programming skills to set up automated design, since the finished work can only be obtained in PDF format, which does not allow

further editing of the file. The results of the study showed that InnoFlow is better adapted to the strict requirements of Russian standards, while DeepSeek provides more flexible and intelligent tools for working with text. Both systems have unique advantages, which makes them useful for different stages of thesis preparation.

Keywords: graduation papers, DeepSeek, InnoFlow, optimization

Введение

Современные постоянно развивающиеся технологии все чаще проникают в повседневную жизнь людей. Эта тенденция направлена на облегчение и ускорение рутинной работы.

В данной статье сравниваются новые цифровые инструменты, облегчающие и оптимизирующие работу по оформлению выпускной квалификационной работы.

Методы и материалы

В качестве первого помощника была выбрана нейросеть DeepSeek (рис. 1), разработанная китайскими специалистами. Этот инструмент обладает широким набором функций: поддерживает диалог, отвечает на вопросы, используя интернет-источники, работает с текстами и файлами, а также генерирует тексты на основе алгоритмов машинного обучения [1, 2]. Однако для целей данной конференции рассматривались только те возможности, которые могут помочь в оформлении, поиске ошибок, неточностей и построении логики при написании ВКР. В ходе исследования были выявлены полезные функции нейросети: она успешно обнаружила ошибки в оформлении работы в соответствии с заданным нормативным документом. Кроме того, DeepSeek сформировал полную структуру ВКР с заголовками в плоть до третьей ступени на примере конкретной темы. Также важно отметить, что в процессе работы с нейросетью можно задавать уточняющие вопросы, что делает ее взаимодействие с пользователем более эффективным [2].



Рис. 1. Нейросеть DeepSeek

Второй инструмент для помощи в написании ВКР была выбрана система управления научными и инновационными проектами InnoFlow (рис. 2), разработанная российским учреждением высшего образования НИЯУ МИФИ [3]. Данная система пользуется определенными скриптами для оформления по заданному ГОСТу, так же может подстраивать оформление под определенный норма-

тивный документ организации, но редактирование такого формата требует определенных навыков для корректировки кода [1]. Данная платформа имеет полную структурированную систему для написания ВКР, также в ее функционал входит автоматическое оформление текста и создание библиографического списка. [3]. Экспериментальным путем, выбрав тему для выпускной квалификационной работы, были проверены функциональные возможности данной платформы и выявлены полезные средства для написания работы, соответствующие вышеперечисленному описанию платформы.

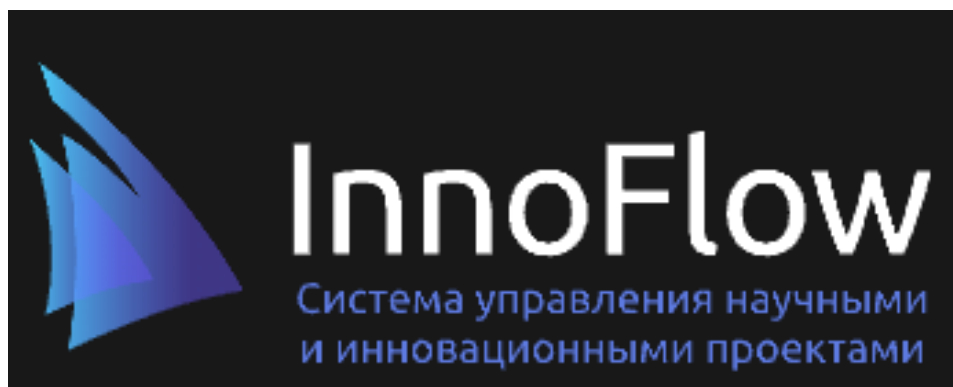


Рис. 2. InnoFlow система управления научными и инновационными проектами

Результаты

Тестирование обеих систем показало, что они имеют как положительные, так и отрицательные стороны, наиболее существенные перечислены ниже.

Плюсы DeepSeek:

1. Дружелюбный интерфейс и возможность коммуницировать с ним как с полноценным собеседником;
2. Возможность анализа и поиска ошибок в файлах в соответствии с определенными нормативными документами;
3. Помощь в структуризации работы;
4. Рекомендации по оформлению тем и подтем в течение всей работы.

Минусы DeepSeek:

1. Отсутствует функционал анализа больших документов или прочтения нескольких файлов одновременно;
2. Некорректная работа по некоторым запросам, бывают неточности;
3. Не полностью освоенная технология.

Плюсы InnoFlow:

1. Полная структуризация для удобного оформления ВКР;
2. Полная автоматизация оформления работы;
3. Возможность изменения кода под определенные нормативные документы;
4. Дает рекомендации по написанию работы, но лишь на некоторых этапах.

Минусы InnoFlow:

1. Функционал ресурса имеет свой порог вхождения;

2. В код для оформления заложен ГОСТ 7.32-2017, без возможности быстрого изменения корневого нормативного документа;
3. Конечный файл только в формате PDF.

Заключение

Тестирование обеих систем показало, что InnoFlow адаптировано под российские стандарты ГОСТ, но при этом DeepSeak имеет более удобный интерфейс и более интеллектуальные функции автоматизации работы с текстом. Основываясь на проведенном тестировании, можно сделать вывод, что обе системы эффективны для оптимизации оформления ВКР, но каждая в своем ключе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ 7.32–2017. Отчет о научно-исследовательской работе. Структура и правила оформления. – М.: Стандартинформ, 2017. – 18 с.
2. DeepSeek: официальная документация и руководство пользователя. – URL: <https://www.deepseek.com> (дата обращения: 03.05.2025).
3. InnoFlow: система управления научными проектами. – URL: <https://www.inniflow.ru> (дата обращения: 03.05.2025).

©П. Ф. Бжицких, А. А. Шрамков, В. П. Цыплаков, Е. Ю. Кутенкова, 2025

Н. Р. Воронина^{1✉}, А. А. Киселев², В. М. Белов¹

Нейросетевая модель классификатора объектов КИИ

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация

²Новосибирский государственный технический университет,
г. Новосибирск, Российская Федерация
e-mail: nata.voronina.00@inbox.ru

Аннотация. В статье рассматривается способ применения нейросетевых технологий для классификации объектов критической информационной инфраструктуры (ОКИИ). Обеспечение безопасности ОКИИ является одним из важнейших элементов информационной безопасности Российской Федерации, что доказывает множество федеральных законов и нормативных правовых актов в данной сфере. От скорости и точности присвоения категории значимости ОКИИ зависит обеспечение его безопасности. В статье рассматриваются необходимый функционал классификатора – возможность обучения на основе новых данных, классификации файлов с описанием ОКИИ, вариант используемых библиотек для машинного обучения, таких как scikit-learn, PyPDF2 и docx, обработка текста, включающая приведение к нижнему регистру и удаление стоп-слов. Также рассматривается проблема, возникающая в процессе создания нейросетевой модели классификатора – нехватка данных для обучения модели. Способы решения этой проблемы – использование аугментации и взаимодействие с органом-регулятором в сфере КИИ.

Ключевые слова: искусственный интеллект, машинное обучение, объекты критической информационной инфраструктуры

N. R. Voronina^{1✉}, A. A. Kiselyov², V. M. Belov¹

Neural network model of the CII object classifier

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation

²Novosibirsk State Technical University, Novosibirsk, Russian Federation
e-mail: nata.voronina.00@inbox.ru

Abstract. The article discusses the method of using neural network technologies in the classification of critical information infrastructure facilities (CIIF). Ensuring the security of CIIF is one of the most important elements of the information security of the Russian Federation, which is proved by many federal laws and regulations in this area. The safety of this facility depends on the speed and accuracy of assigning a category of significance to an object. The article discusses the necessary functionality of the classifier – the ability to learn from new data and classify files with descriptions of AI objects, a variant of used libraries for machine learning such as scikit-learn, PyPDF2 and docx, and text processing, including lowercase reduction and removal of stop words. The problem that arises in the process of creating a classifier neural network model is also considered – the lack of data for training the model, and the demand for solutions to this problem is the use of augmentation and interaction with the regulatory authority in the field of CII.

Keywords: artificial intelligence, machine learning, critical information infrastructure facilities

Введение

С момента появления в Доктрине информационной безопасности Российской Федерации [1] тезиса о повышении защищенности КИИ законодательство в сфере обеспечения безопасности ОКИИ продолжает активно дополняться, о чем свидетельствует Федеральный закон N 58-ФЗ «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», принятый 07.04.2025 и вступающий в силу в сентябре 2025 года [2]. Это приводит к пониманию, что в настоящее время безопасность КИИ является одним из важнейших вопросов безопасности информации страны.

В Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» для ОКИИ определяются три категории значимости [3]. Присвоение категории значимости запускает процесс обеспечения безопасности объекта, поэтому скорость определение и присвоение категории, а также точность, напрямую влияют на то, насколько быстро и правильно будет обеспечена защищенность объекта от угроз информационной безопасности.

В данный момент не существует автоматизированного классификатора ОКИИ, который имел бы достаточный уровень точности и скорости для решения проблем категорирования. Классификатор на основе нейросетевой модели может стать одним из решений, поэтому целью статьи является обзор возможного варианта применения нейросетевых технологий для решений проблемы классификации ОКИИ.

Методы и материалы

Для ручной классификации ОКИИ используется информация об объектах, представленная текстом: критические процессы, архитектуры объектов, программно-аппаратные средства и прочее. Информация, необходимая для категорирования, определяется в Постановлении правительства №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [4]. Из этого можно сделать вывод, что автоматизированный классификатор ОКИИ на основе нейросетевой модели должен обрабатывать текст как на этапе обучения, так и на этапе классификации нового объекта на основе его описания. Рассмотрим реализацию алгоритма классификации на языке Python [5]. В нем представлено множество библиотек для работы с нейронными сетями, что значительно облегчает создание нейросетевых классификаторов [6].

Для обучения нейронных сетей используются базы данных с уже размеченными данными по классам, следовательно, для корректной классификации нам необходимо иметь базу данных с описанием ОКИИ, которым уже присвоены категории значимости. На этом этапе мы сталкиваемся с проблемой нехватки информации, так как большая часть информации о КИИ имеет конфиденциальный

характер. В таких условиях методы глубокого обучения сразу отпадают, так как при обучении на небольшом количестве данных может возникнуть проблема переобучения. Следовательно, для работы лучше использовать классические алгоритмы: логистическая регрессия или деревья решений. Метод дерева решений склонен к переобучению и неустойчив к шуму, поэтому выбор пал на использование метода логистической регрессии [7]. В языке программирования Python использовать метод логистической регрессии позволяет библиотека `scikit-learn`.

Классификатор на основе нейросетевой модели должен иметь две функции: обучение на подготовленной базе данных и загрузку нового файла для классификации ОКИИ. Для обучения в программу будет загружаться файл CSV формата, так как это универсальный способ представления текстовых данных для обучения и поддерживаемый всеми библиотеками [8]. Возможность обучить классификатор на основе новых данных позволяет в дальнейшем обновлять его в соответствии с изменениями в законодательстве. Также в программе должна быть реализована возможность единоразового обучения, то есть полученная модель должна сохраняться для дальнейшего использования. Это облегчит использование классификатора и позволит сэкономить время. Для классификации будем загружать файлы двух самых распространенных форматов: DOC и PDF, поэтому используем библиотеки для обработки этих форматов – `PyPDF2` и `docx` [9].

Процесс обучения нейросетевой модели можно разделить на несколько этапов: обработка текста из датасета и само обучение.

Обработка текста необходима для создания «чистого» датасета. Изначально датасет может содержать ошибки, которые могут повлиять на результаты обучения и в дальнейшем снизить эффективность классификации [10]. Обработка текста включает в себя: приведение к нижнему регистру, удаление стоп-слов, удаление строк с пустыми значениями, удаление выбросов и знаков препинания. Для большей части этих задач может быть использована стандартная библиотека Python для обработки текста – `string`, но для удаления стоп-слов можно использовать библиотеку `nlk` [11]. Датасет делится на тестовую и тренировочную части, где тестовая составляет 20 % от всего датасета.

Далее текст проходит процесс векторизации. В библиотеке `scikit-learn` есть несколько методов: `CountVectorizer`, `TfidfVectorizer` и `HashingVectorizer`. `CountVectorizer` не учитывает важность слов, т.е. все слова будут считаться равнозначными, а `HashingVectorizer` предназначен для больших массивов данных, поэтому стоит использовать `TfidfVectorizer` [12].

После обработки и векторизации текста, можно перейти к этапу обучения модели. Подготовленный датасет должен содержать список характерных черт ОКИИ, размеченный по категориям значимости. Модель обучается на тренировочной части и тестируется на тестовой, после чего модель сохраняется для дальнейшего использования.

Когда нейросетевая модель классификатора ОКИИ обучена, можно загрузить новый файл с описанием ОКИИ, также произвести обработку и векторизацию и произвести процесс классификации.

Результаты

В результате структура классификатора ОКИИ на основе нейросетевой модели будет следующей, позволяющей как обучить модель, используя подготовленные данные, так и производить классификацию нового файла (рис. 1).

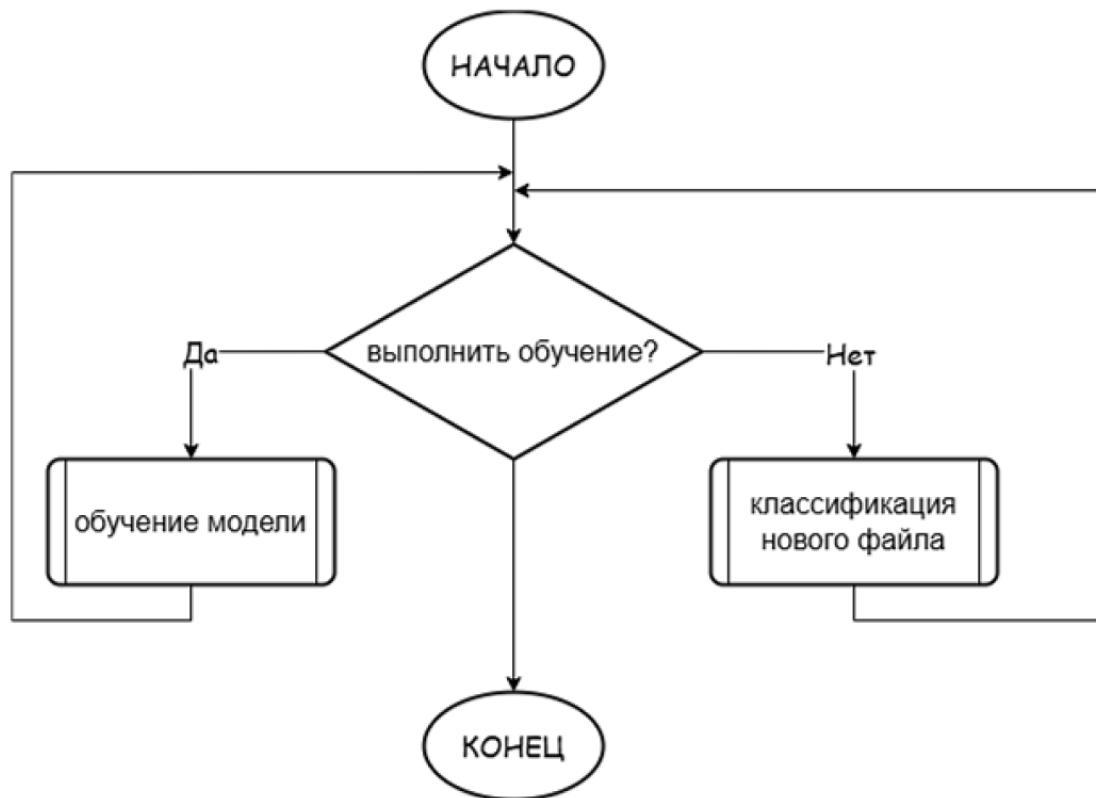


Рис. 1. Структура нейросетевой модели классификатора

Процесс обучения также делится на этапы. Обучение осуществляется с использованием логистической регрессии с помощью библиотеки `scikit-learn`. Для векторизации текста применяется метод `TfidfVectorizer`. Полученные модель и векторизатор сохраняются для дальнейшего использования. Этапы обучения представлены на блок-схеме (рис. 2).

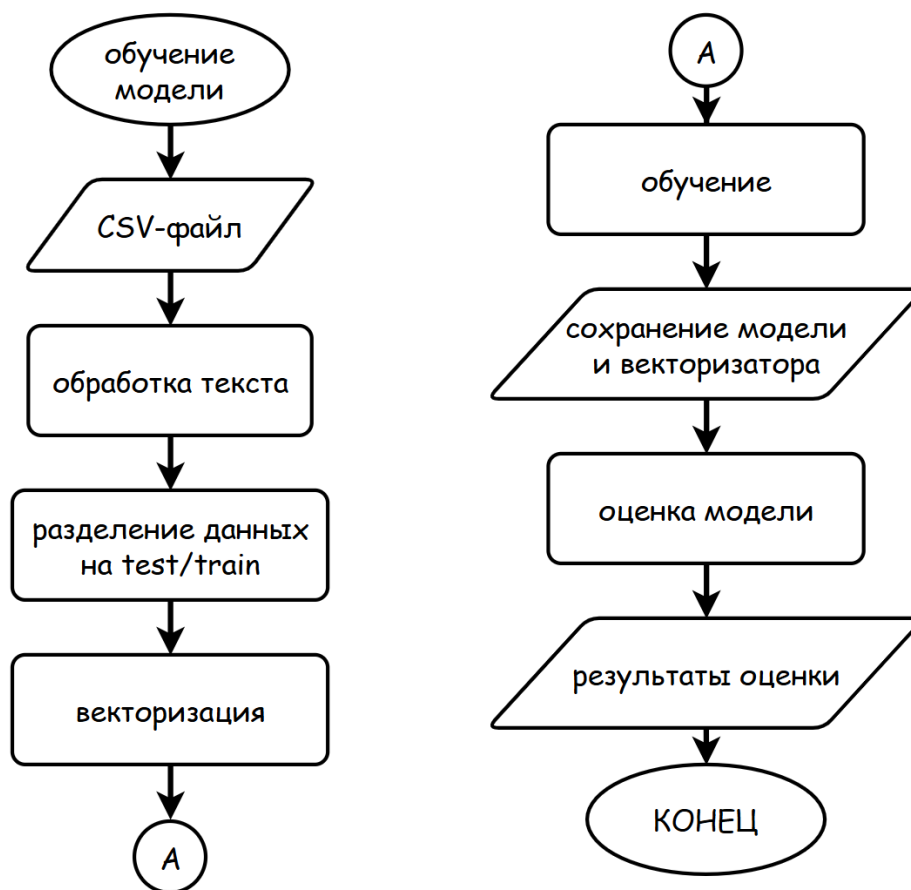


Рис. 2. Процесс обучения нейросетевой модели

Далее классификатор должен иметь функцию загрузки и обработки файлов DOC и PDF для классификации новых объектов КИИ. Это можно реализовать с помощью библиотек PyPDF2 и docx. Процесс классификации нового файла представлен на следующей блок-схеме (рис. 3).

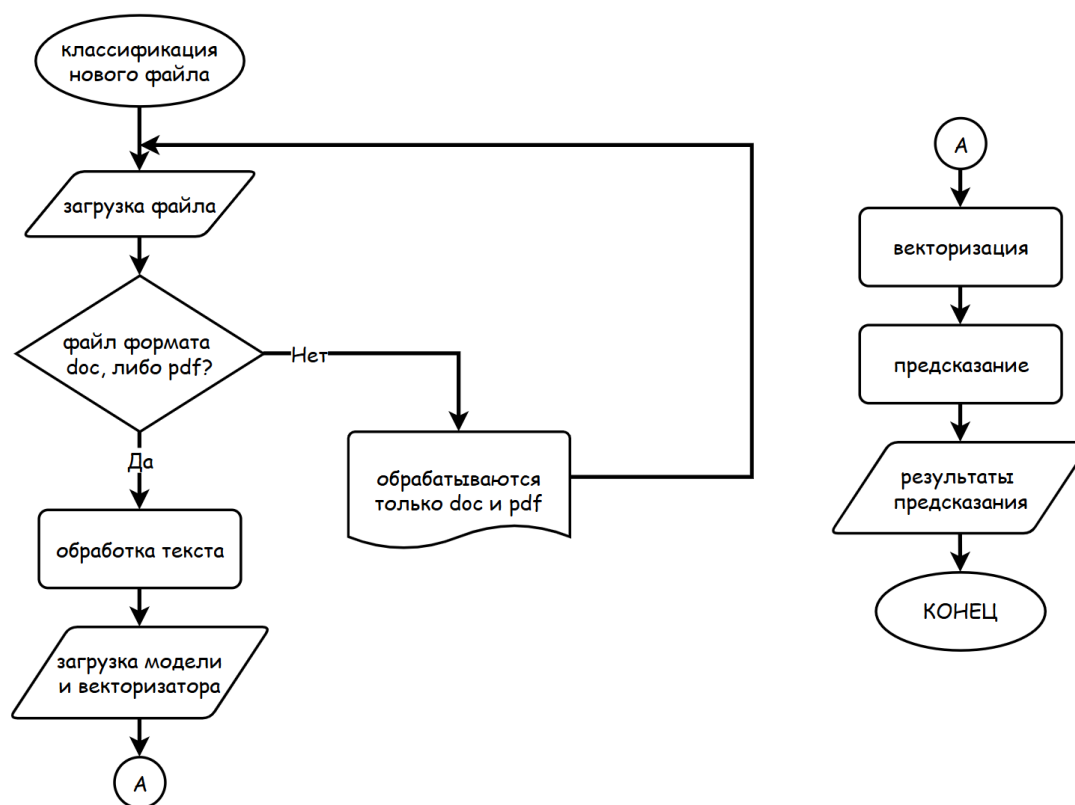


Рис. 3. Процесс классификации нового файла

Обсуждение

Главной проблемой создания классификатора на основе нейросетевой модели отстает нехватка информации об ОКИИ в открытом доступе. Это мешает создавать датасеты с достаточным количеством примеров для обучения. Одним из решений данной проблемы может быть использование методов аугментации для увеличения уже существующего датасета, но лучшим вариантом является взаимодействие с органом-регулятором в данной сфере – Федеральной службой по техническому и экспортному контролю, что позволит получить доступ к конфиденциальной информации.

Заключение

Использование нейросетевых моделей для решения задач классификации ОКИИ может значительно ускорить присвоение категорий значимости и снизить количество ошибок. В данном исследовании приведен один из способов реализации классификатора, определены архитектура и требования к функционалу. Также рассмотрены основные проблемы, с которыми может столкнуться разработчик.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента Рос. Федерации от 5 декабря 2016 г. № 646;

2. О внесении изменений в Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации": федер. Закон Рос. Федерации от 7 апреля 2025 г. № 58-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 25 марта 2025 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 2 апреля 2025 г. // КонсультантПлюс;
3. О безопасности критической информационной инфраструктуры: федер. Закон Рос. Федерации от 26 июня 2017 г. № 187-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 12 июля 2017 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июня 2017 г. // КонсультантПлюс;
4. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: пост. Правительства Рос. Федерации от 8 февраля 2018 г. № 127 с изм. от 24 декабря 2021 г.;
5. Базарбаев Х., Байрамов Т., Дадаева Л. Языки программирования для разработки искусственного интеллекта // Вестник науки. 2024. №10 (79);
6. Давыдов А. В., Жусупова А. К., Салыкова О. С. Сравнение различных языков программирования, применяемых в машинном обучении // Вестник науки. 2023. – №2 (59);
7. Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. – 2-е изд. – М.: ДМК Пресс, 2015. – 401 с.;
8. Николенко С., Кадуринов А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. – СПб.: Питер, 2018. – 401 с.;
9. Свэйгарт Э. Автоматизация ручных процессов с помощью Python. Практическое руководство для начинающих. – М.: ООО "И.Д. Вильямс", 2017. – 592 с.;
10. Макаров А. В., Намиот Д. Е. Обзор методов очистки данных для машинного обучения // International Journal of Open Information Technologies. 2023. – №10.;
11. Макаров К. С., Халин А. А., Костенков Д. А., Муханов Э. Э. Сравнительный анализ библиотек для обработки естественного языка (NLP) // Auditorium. 2024. – №1 (41);
12. Полетаева Н. Г. Классификация систем машинного обучения // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2020. – №1.

© Н. Р. Воронина, А. А. Киселев, В. М. Белов, 2025

Н. И. Егоренко^{1✉}, М. П. Егоренко²

Анализ качества аппроксимации выборки EMNIST-букв моделью CNN

¹Новосибирский государственный технический университет,
г. Новосибирск, Российская Федерация

²Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
email: kotkit555@gmail.com

Аннотация. В статье рассматривается задача анализа качества аппроксимации выборки EMNIST-букв с использованием сверточной нейронной сети (CNN). Основной темой исследования является оценка эффективности глубоких обучающих моделей в задаче распознавания рукописных символов латинского алфавита. Проблема заключается в высокой вариативности рукописного ввода и необходимости построения устойчивой модели, способной к обобщению. Целью исследования является построение и экспериментальный анализ архитектуры CNN, обеспечивающей высокую точность классификации изображений букв из выборки EMNIST. В работе применяются методы машинного обучения, включая предварительную обработку данных, обучение сверточной нейронной сети и оценку качества модели по метрикам точности, полноты и F1-меры. Результаты показывают, что предложенная архитектура демонстрирует высокое качество аппроксимации, достигая точности классификации свыше 90 % на тестовой выборке. Основной вывод заключается в том, что корректно сконфигурированная CNN-модель эффективно справляется с задачей распознавания рукописных букв, что подтверждает ее пригодность для приложений в системах оптического распознавания символов.

Ключевые слова: аппроксимация, нейронные сети, ядро, модель

N. I. Egorenko^{1✉}, M. P. Egorenko²

Analysis of approximation quality of EMNIST letter samples using a CNN model

¹Novosibirsk State Technical University, Novosibirsk, Russian Federation

²Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: kotkit555@gmail.com

Abstract. The paper addresses the problem of analyzing approximation quality of the EMNIST letter samples using convolutional neural networks (CNNs). The main research topic focuses on evaluating the effectiveness of deep learning models in recognizing handwritten Latin alphabet characters. The challenge lies in the high variability of handwriting input and the necessity to construct a robust model capable of generalization. The aim of this study is to develop and experimentally analyze a CNN architecture that ensures high classification accuracy of images from the EMNIST dataset. In this work, machine learning methods are applied, including data preprocessing, training of a convolutional neural network, and evaluation of the model's performance based on precision, recall, and F1 score metrics. The results demonstrate that the proposed architecture achieves high-quality approximation with over 90 % classification accuracy on test samples. The key conclusion is that properly configured CNN models effectively handle the task of recognizing handwritten letters, which confirms their suitability for applications in optical character recognition systems.

Keywords: approximation, neural networks, kernel, model

Введение

Сверточные нейронные сети (Convolutional Neural Networks, CNN) являются эффективным инструментом для обработки и классификации изображений. Они состоят из нескольких слоев, каждый из которых выполняет определенные операции, такие как свертка, объединение (пулинг), нормализация и активация [1].

Структура модели CNN состоит из нескольких сверточных слоев, объединяющих слоев, слоев нормализации и плотно связанных слоев. Ниже приведены некоторые пояснения к различным частям модели:

- сверточный слой (Conv2D). Применяет операцию свертки к входным данным с использованием ядра фиксированного размера, чтобы выделить определенные признаки в изображении;
- объединяющий слой (MaxPooling2D). Уменьшает пространственные размеры признаков путем выбора максимального значения из определенной области. Это позволяет уменьшить количество параметров и вычислительную сложность модели;
- пакетная нормализация (BatchNormalization). Нормализует активации между слоями, чтобы стабилизировать процесс обучения и ускорить сходимость модели;
- слой выпадения (Dropout) [2]. Случайным образом «выбрасывает» (устанавливает в ноль) некоторое количество нейронов во время обучения. Это помогает избежать переобучения и улучшает обобщающую способность модели;
- плотно-связанный слой (Dense). Объединяет все признаки из предыдущих слоев и преобразует их в выходные классы. Последний слой обычно имеет функцию активации softmax, которая предсказывает вероятности принадлежности к различным классам.

Для проведения анализа качества аппроксимации выборки EMNIST-букв, мы можем изменять следующие параметры модели:

- размер ядра (kernel size). Размер ядра сверточного слоя, определяющий область входных данных, с которой будет производиться операция свертки. Изменение размера ядра может повлиять на способность модели выявлять различные признаки;
- число слоев (number of layers): Количество сверточных слоев в модели. Увеличение числа слоев может увеличить способность модели извлекать сложные иерархические признаки, но при этом может потребоваться больше вычислительных ресурсов;
- пулинг (pooling): Размер и тип пулинга, применяемого после сверточных слоев. Изменение размера и типа пулинга может влиять на пространственные размеры признаков и обобщающую способность модели;
- добавление BatchNorm: Решение о включении или отключении пакетной нормализации между слоями. BatchNorm может улучшить стабильность обучения и повысить качество модели [3];

– параметр dropout: Величина параметра dropout, определяющая долю нейронов, выбрасываемых во время обучения. Изменение значения dropout может влиять на обобщающую способность модели и способность избегать переобучения.

Для каждого из этих параметров мы будем измерять точность обучения и анализировать их влияние на качество аппроксимации выборки EMNIST-букв.

Разработка

Графики (рис. 1–5) построены на основе результатов экспериментов, проведенных с использованием подвыборки EMNIST-букв – одного из поднаборов расширенного датасета EMNIST [4], содержащего изображения рукописных букв латинского алфавита. Размер изображений – 28×28 пикселей, количество классов – 26 (по числу букв). Данные были предварительно нормализованы, разбиты на обучающую и тестовую выборки в пропорции 80/20 [5, 6]. Для каждой конфигурации модели обучение проводилось в течение 25 эпох, использовался оптимизатор Adam, функция потерь – categorical crossentropy [7].

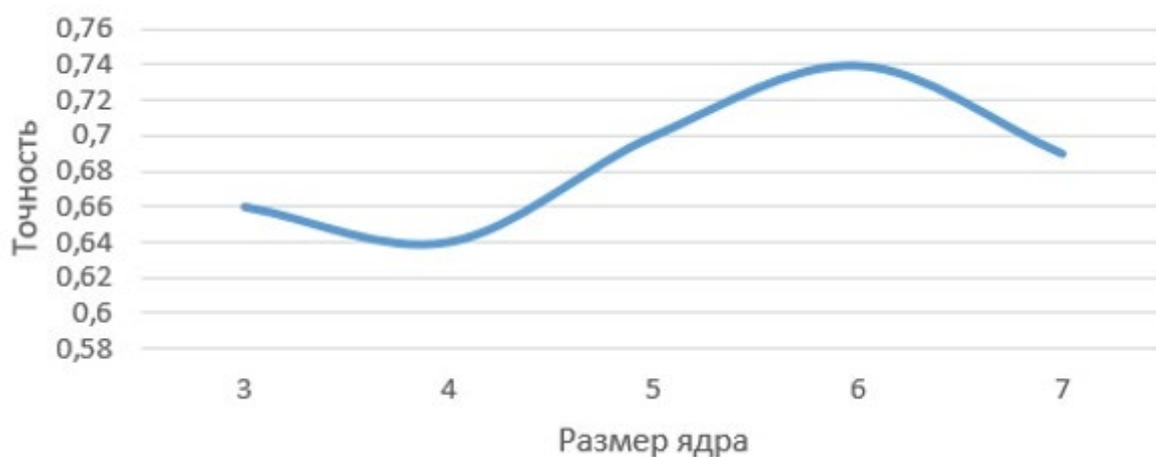


Рис.1. Зависимость точности обучения от размера ядра

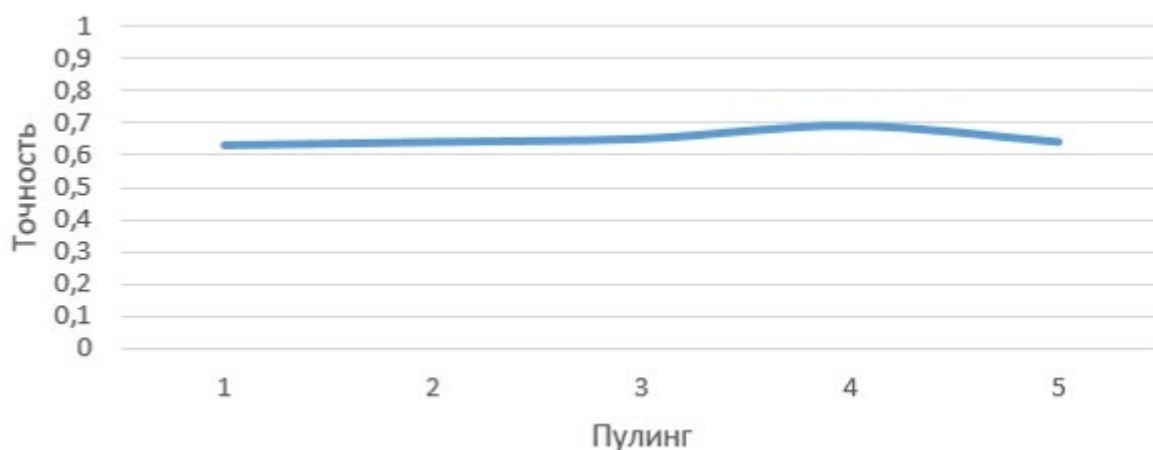


Рис. 2. Зависимость точности обучения от пулинга

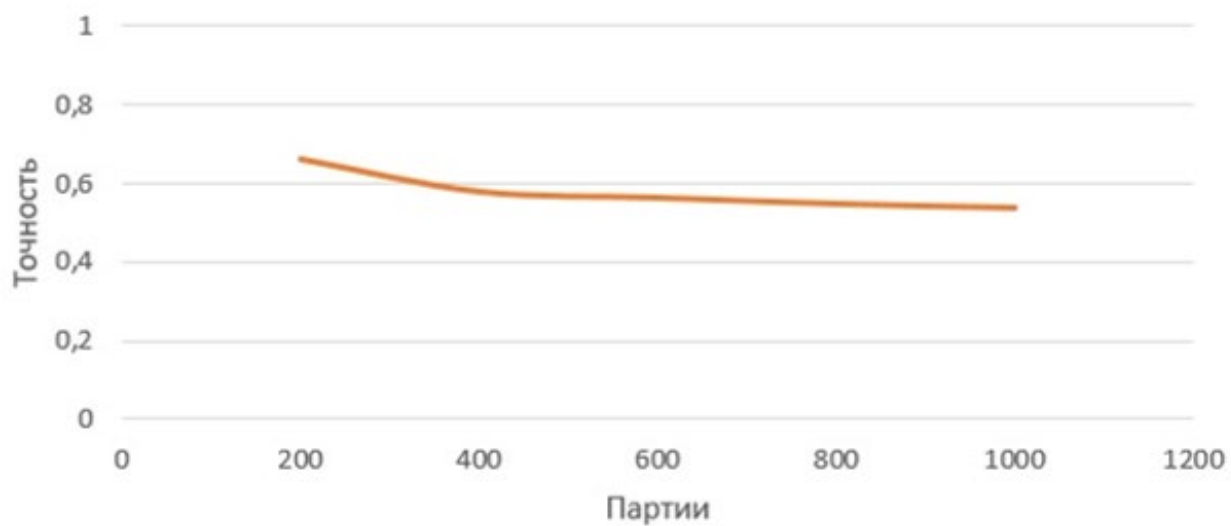


Рис. 3. Зависимость точности обучения от партий

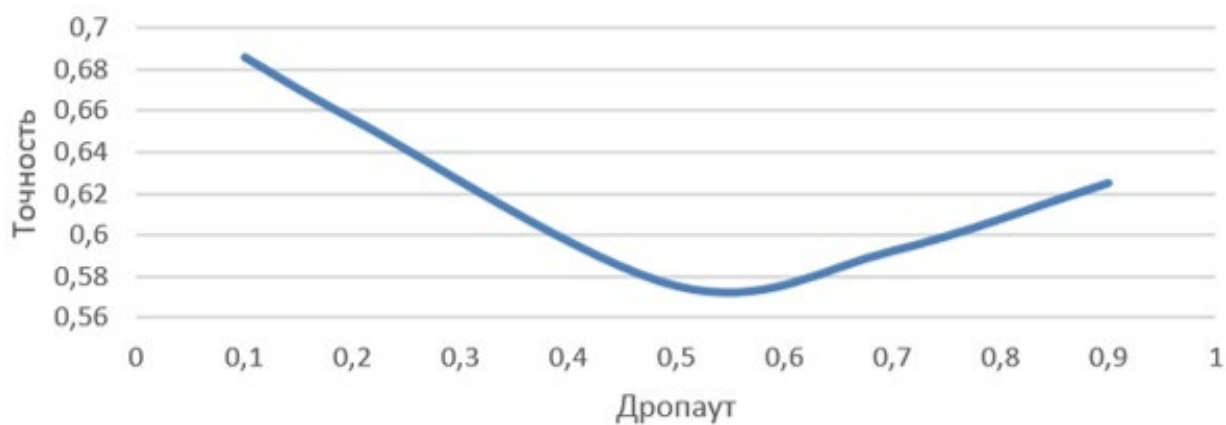


Рис. 4. Зависимость точности обучения от выбрасываний(dropout)

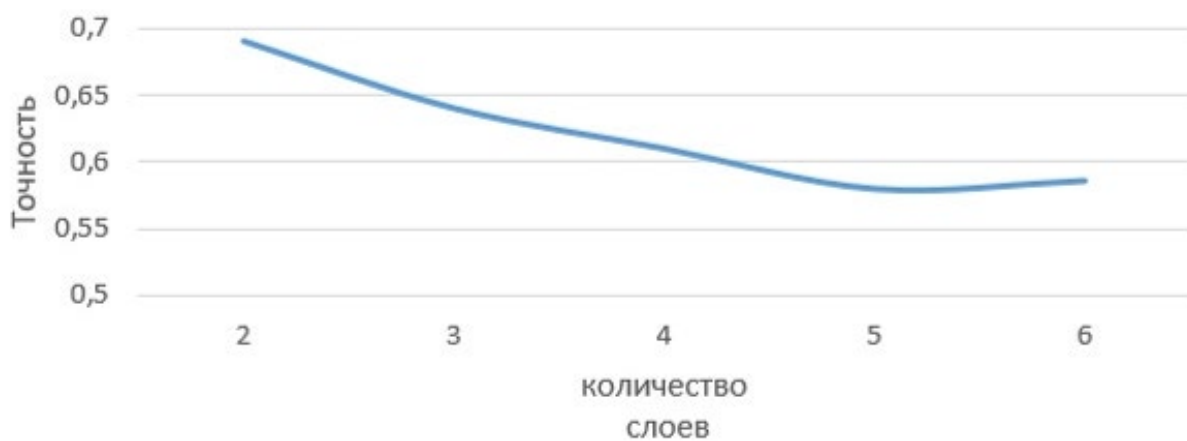


Рис. 5. Зависимость точности обучения от количества слоев

```
import numpy
from keras.models import Sequential
from keras.layers import Dense, Dropout, Flatten, BatchNormalization, Activation
from keras.layers.convolutional import Conv2D, MaxPooling2D
from keras.constraints import maxnorm
from keras.utils import np_utils
from keras.datasets import cifar10

seed = 21

(X_train, y_train), (X_test, y_test) = cifar10.load_data()

X_train = X_train.astype('float32')
X_test = X_test.astype('float32')
X_train = X_train / 255.0
X_test = X_test / 255.0

y_train = np_utils.to_categorical(y_train)
y_test = np_utils.to_categorical(y_test)
class_num = y_test.shape[1]

model = Sequential()

# Первый сверточный слой
model.add(Conv2D(32, (3, 3), input_shape=(3, 32, 32), activation='relu', padding='same'))
model.add(Dropout(0.2))

# Пакетная нормализация
model.add(BatchNormalization())

# Второй сверточный слой (увеличиваем размер фильтра)

model.add(Conv2D(64, (3, 3), padding='same'))
model.add(Activation('relu'))

# Объединяющий слой
model.add(MaxPooling2D(pool_size=(2, 2)))
model.add(Dropout(0.2))
model.add(BatchNormalization())

# Все больше увеличиваем размер фильтра
model.add(Conv2D(64, (3, 3), padding='same'))
model.add(Activation('relu'))
model.add(MaxPooling2D(pool_size=(2, 2)))
```

```

model.add(Dropout(0.2))
model.add(BatchNormalization())
model.add(Conv2D(128, (3, 3), padding='same'))
model.add(Activation('relu'))
model.add(Dropout(0.2))
model.add(BatchNormalization())

# Сожмем данные с помощью Flatten

model.add(Flatten())
model.add(Dropout(0.2))

# Создаем первый плотно связанный слой (нейроны в следующий слоях идут
вниз)
model.add(Dense(256, kernel_constraint=maxnorm(3)))
model.add(Activation('relu'))
model.add(Dropout(0.2))
model.add(BatchNormalization())
model.add(Dense(128, kernel_constraint=maxnorm(3)))
model.add(Activation('relu'))
model.add(Dropout(0.2))
model.add(BatchNormalization())

#Выбираем нейрон с наибольшей вероятностью, полагая, что это полученное
изображение принадлежит именно этому классу
model.add(Dense(class_num))
model.add(Activation('softmax'))

# Количество эпох и оптимизатор
epochs = 25
optimizer = 'adam'

# Компилируем модель, минимизируем потери, смотрим за метрикой
model.compile(loss='categorical_crossentropy', optimizer=optimizer, metrics=['accu-
racy'])

print(model.summary())

```

Заключение

В ходе проведения анализа качества аппроксимации выборки EMNIST-букв с использованием сверточной нейронной сети были исследованы несколько параметров модели, включая размер ядра, число слоев, пулинг, добавление BatchNorm и параметр dropout. Исследования позволили получить следующие выводы:

Размер ядра: варьирование размера ядра показало, что использование более крупных ядер может улучшить точность обучения модели, поскольку они способны извлекать более общие и сложные признаки.

Число слоев: увеличение числа слоев в сверточной нейронной сети позволяет модели извлекать более сложные иерархические признаки, что может привести к улучшению точности обучения. Однако необходимо учитывать, что с увеличением числа слоев может возникнуть проблема переобучения и увеличение вычислительной сложности модели.

Пулинг: были исследованы различные варианты пулинга, и результаты показали, что применение пулинга может помочь уменьшить размерность данных и извлечь наиболее значимые признаки. Это может способствовать улучшению обобщающей способности модели.

Добавление BatchNorm: включение пакетной нормализации между слоями помогает улучшить стабильность обучения и может привести к улучшению качества аппроксимации выборки EMNIST-букв.

Параметр dropout: использование dropout позволяет предотвратить переобучение модели, путем случайного отключения нейронов во время обучения. Оптимальное значение dropout может варьироваться в зависимости от задачи и данных, и его выбор может влиять на точность обучения.

Проведенный анализ позволил определить оптимальные значения параметров для сверточной нейронной сети и улучшить качество аппроксимации выборки EMNIST-букв.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Tan M., Le Q. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks // Proceedings of the 36th International Conference on Machine Learning. – 2020. – Vol. 97. – С. 6105–6114.
2. Wang R., Zhang X., Liu Y., Chen T. Dropout Technique in Deep Learning: A Review // IEEE Access. – 2021. – Т. 9. – С. 113138–113155. – DOI: 10.1109/ACCESS.2021.3104573.
3. Santurkar S., Tsipras D., Ilyas A., Madry A. How does Batch Normalization help optimization? // Advances in Neural Information Processing Systems. – 2020. – Vol. 33. – С. 2483–2493.
4. Cohen G., Afshar S., Tapson J., van Schaik A. EMNIST: Extending MNIST to handwritten letters [Электронный ресурс] // arXiv.org. – 2017. – Режим доступа: <https://arxiv.org/abs/1702.05373>, свободный. – Загл. с экрана. – (дата обращения: 11.03.2025).
5. Shorten C., Khoshgoftaar T.M. A Survey on Image Data Augmentation for Deep Learning // Journal of Big Data. – 2021. – Т. 8, № 1. – Статья № 60. – DOI: 10.1186/s40537-021-00444-8.
6. Cubuk E.D., Zoph B., Shlens J., Le Q.V. RandAugment: Practical Automated Data Augmentation with a Reduced Search Space // Proceedings of the IEEE/CVF Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW). – 2020. – С. 702–703.
7. Dosovitskiy A., Beyer L., Kolesnikov A., et al. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale [Электронный ресурс] // ICLR – Int. Conf. on Learning Representations. – 2021. – Режим доступа: <https://openreview.net/forum?id=YicbFdNTTy>, свободный. – Загл. с экрана. – (дата обращения: 11.03.2025).

© Н. И. Егоренко, М. П. Егоренко, 2025

Д. В. Железных^{1✉}, Д. Д. Сизиков^{1✉}, Н. М. Дорохова¹, Ю. М. Карлина¹

Разработка сайта интернет-магазина

¹Новосибирский электромеханический колледж,
г. Новосибирск, Российская Федерация
e-mail: natali_270168@mail.ru

Аннотация. В статье приведен способ разработки сайта для продажи настольных ламп разработанных студентами колледжа. В статье рассмотрены концепции и структура сайта, который окажет помощь с реализацией продукта, и по мере улучшения навыков программирования, студенты смогут его совершенствовать. Планируется продолжить работу по этой тематике, увеличить номенклатуру изготавливаемых ламп и провести первые продажи через сайт.

Ключевые слова: сайт, Tilda, настольные лампы

D. V. Zheleznykh^{1✉}, D. D. Sizikov^{1✉}, N. M. Dorokhova¹, Yu. M. Karlina¹

Development of an online store website

¹Novosibirsk Electromechanical College, Novosibirsk, Russian Federation
e-mail: natali_270168@mail.ru

Annotation. The article describes a method for developing a website for selling table lamps designed by college students. The article discusses the concepts and structure of the website, which will help with the implementation of the product, and as programming skills improve, students will be able to refine it. It is planned to continue working on this topic, expand the range of lamps produced, and conduct the first sales through the website

Keywords: website, Tilda, table lamps

Введение

Мы состоим в научном обществе «На 5+» и в течение нескольких лет разрабатывали настольные лампы для различных интерьеров.

Лампы, разработанные нами, хорошо вписываются в современные интерьеры. К примеру, наши осветительные лампы поддерживают экостиль, в котором особое внимание уделяется предметам, не только выполняющим свою функцию, но и гармонично вписываются в окружающую атмосферу, создавая теплую и уютную обстановку. Настольные лампы не только освещают пространство, но и становятся выразительным элементом декора.

Наши лампы стали вызывать интерес, поэтому соединив знания электрика и программиста, мы решили начать зарабатывать. Обойтись без информационных технологий в бизнесе в наше время сложно, поэтому возникла необходимость в создании сайта магазина, где размещалась бы информация о настольных лампах и где каждый может найти что-то своё.

Мы стремимся создать платформу, где наши клиенты смогут не только ознакомиться с уникальными моделями ламп, созданными из экологических материалов, но и подчеркнуть свою индивидуальность, создав лампу по собственному эскизу.

Цель: разработка сайта интернет-магазина настольных ламп «Свет ваших идей», для продвижения и продажи наших ламп.

Задачи:

- выбрать платформу для создания сайта;
- разработать концепции и структуры сайта (интерфейс);
- провести пробное тестирование;
- проанализировать результаты.

Методы: изучение литературы, анализ, изучение мнения, анкетирование, тестирование.

Методы и материалы

Для разработки своего сайта мы выбрали платформу Tilda, так как она требует минимальные навыки программирования. Есть возможность собрать сайт из готовых блоков, которые автоматически адаптируются под мобильные устройства, что особенно актуально в современном мире. Данная платформа поддерживает множество интеграций с внешними сервисами, такими как CRM, почтовые рассылки и аналитические инструменты. И самым важным для нас стало то, что с помощью различных элементов и возможностей настроек мы создаем уникальный сайт, который отражает индивидуальность нашего бренда. Стоит еще сказать, что Tilda работает по модели Freemium: на сервисе есть возможность использовать бесплатный план или выбрать для себя один из вариантов платной подписки [1–3].

На нашем сайте разместили несколько блоков.

Первый экран – это то, что пользователь видит на экране сразу, как только открыл страницу сайта, ещё не скроля вниз. На данном этапе главная задача – захватить внимание потенциального потребителя и заинтересовать его, чтобы он захотел листать дальше. Поэтому здесь важен цепляющий продающий заголовок. Емкий, короткий и мощный. Также на первом экране находится подзаголовок, который поясняет основное сообщение, которое есть в заголовке и призыв к действию – кнопку «Узнать больше»

Демонстрация продукта или услуги.

После того, как мы заинтриговали посетителя, нужно показать во всей красе наш продукт. Здесь мы разместили фотографии образцов ламп. Презентация товара требуется, чтобы зацепить потребности или боли целевой аудитории, чтобы люди узнали в описании себя. Также говорим о нашей фишке – создании уникальных ламп под запрос конкретного пользователя.

Преимущества или выгоды клиента.

Товар показали, теперь пора и убедить посетителя в том, что лучше просто не найти. То есть, рассказать о преимуществах нашего предложения и выгоды для клиента. Показываем конкретные выгоды, факты, цифры. При этом, товар или услуга должны рассматриваться именно с точки зрения клиента.

Блок с ценами

Конечно же, увидев предложение и узнав о его преимуществах, посетитель уже задает себе вопрос – сколько это стоит? Пришло время здесь рассказать ему об этом. Здесь для удобства мы создали разделение ламп в стиле эко и лофт.

Блок с отзывами (социальные доказательства)

Мнение других людей – вот что может окончательно убедить потенциального покупателя сделать заказ. Поэтому мы разместили здесь отзывы клиентов – мощные социальные доказательства того, что наш товар обладает весомыми достоинствами и его заказывают другие. На начальном этапе для блока отзывов мы использовали мнение однокурсников, которые тестировали лампы в течение длительного времени.

Ответы на часто задаваемые вопросы (заккрытие возражений).

Даже после всей этой информации у покупателя могут остаться опасения. Почему так дорого/дешево? А как я получу свой заказ? А могу ли я забрать его лично? И многое другое. Чтобы успокоить посетителя, в этом блоке мы разместили ответы на часто задаваемые вопросы. Это поможет ему ещё больше проникнуться к нам доверием.

Выгодное предложение (акция, дефицит).

Дополнительно простимулировать посетителя побыстрее совершить целевое действие можно с помощью выгодного предложения: бонуса, подарка, скидок. Ещё несколько мощных триггеров – это ограниченное количество товара (дефицит – вдруг не успею купить, всё разберут).

Контакты.

Посетитель лендинга оставляет вам свои контактные данные для обратной связи. Но в то же время и вы должны показать, каким образом вас можно найти, где вы находитесь. Возможно, человек захочет позвонить и узнать детали. Но в первую очередь наличие контактов говорит о том, что вы реальная компания, а не мошенники.

На сайте необходимо указать полные контактные данные изготовителя: телефон, почта, адрес офиса, желательно указать карту проезда. В блоке контактов можно также разместить виджеты или кнопки социальных сетей.

Заключение

В результате проведенной работы были получены навыки разработки сайтов на платформе Tilda.

Разработали сайт «Свет Ваших идей».

Сайт поможет нам с реализацией продукта, и по мере улучшения навыков программирования, мы сможем его совершенствовать.

Работа над проектами нас увлекла, и мы планируем её продолжить, увеличить коллекцию наших ламп и провести первые продажи через сайт.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. <https://postium.ru/prizyv-k-dejstviyu-v-reklame/>

2. <https://postium.ru/prodayushhie-zagolovki-100-primerov-i-shablonov/>
3. <https://postium.ru/boli-klienta-kak-vyyavit-i-zakryt/>

© Д. В. Железных, Д. Д. Сизиков, Н. М. Дорохова, Ю. М. Карлина, 2025

М. С. Исмаилова¹, С. А. Арбузов¹✉

Исследование возможности применения недорогих MEMS инерциальных датчиков для реализации технологии захвата движения

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: stan_i_slav84@mai.ru

Аннотация. Для анализа качества выполняемых элементов в фигурном катании используют различные методы. Существуют как визуальные методы, когда движения фиксируются при помощи камеры и затем анализируются тренером, так и автоматизированные методы, заключающиеся в применении технологии захвата движения, которая позволяет получить траектории для отдельных, закрепленных на спортсмене маркеров. Наиболее оптимальным для применения на открытых площадках является метод инерциального захвата движения с помощью датчиков IMU изготовленных на основе технологии МЭМС (микроэлектромеханическая система) [1, 2].

В настоящее время MEMS IMU широко применяются в различных областях и играют важную роль в реализации технологий виртуальной реальности, навигации, спортивной аналитики, робототехники, и т.п. Это придает MEMS IMU универсальность в использовании, и повышает актуальность их использования для реализации технологии инерциальной системы захвата движения. MEMS обладают компактными размерами и низким потреблением энергии, что позволяет сделать систему захвата движения компактной и автономной. В статье рассмотрена возможность применения модуля MEMS IMU MPU6050 для технологии захвата движения, выполнена практическая реализация технологии захвата движения с помощью MPU6050 и микроконтроллера Arduino nano. Подготовлена система проведения испытаний инерциальных датчиков, реализованная в виде маятника с оптической системой контроля траектории и скорости. Проведены испытания системы.

Ключевые слова: технологии захвата движения, инерциальные измерения, MEMS IMU, Arduino, определение траектории движения, маятник

M. S. Ismailova¹, S. A. Arbuzov¹✉

Exploring the possibility of using inexpensive MEMS inertial sensors to implement motion capture technology

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: stan_i_slav84@mai.ru

Annotation. Various methods are used to analyze the quality of elements performed in figure skating. There are both visual methods, when movements are recorded using a camera and then analyzed by a coach, and automated methods, which consist of using motion capture technology, which allows you to obtain trajectories for individual markers attached to the athlete. The most optimal method for use on open rinks is the inertial motion capture method using IMU sensors manufactured using MEMS (microelectromechanical system) technology [1, 2].

Currently, MEMS IMUs are widely used in various fields and play an important role in the implementation of virtual reality technologies, navigation, sports analytics, robotics, etc. This makes MEMS IMUs universal in use and increases the relevance of their use for the implementation of

inertial motion capture system technology. MEMS have compact dimensions and low power consumption, which allows making the motion capture system compact and autonomous. The article considers the possibility of using the MEMS IMU MPU6050 module for motion capture technology, and the practical implementation of motion capture technology using the MPU6050 and the Arduino nano microcontroller is performed. A system for testing inertial sensors has been prepared, implemented in the form of a pendulum with an optical trajectory and speed control system. The system has been tested.

Keywords: motion capture technologies, inertial measurements, MEMS IMU, Arduino, motion trajectory determination, pendulum

Введение

Детальный анализ качества выполнения упражнений является важной частью тренировок в фигурном катании. В настоящее время широко зарекомендовали себя методы захвата движения. Анализ траектории движений спортсмена с помощью технологии захвата движения повышает эффективность тренировок и позволяет улучшать результаты в различных видах спорта.

Технология захвата движения может быть реализована различными методами:

Оптический метод. Основан на использовании камер, которые регистрируют движения с помощью специальных маркеров, надетые на тело или объект. Камеры регистрируют движения маркеров и передают информацию в компьютер для дальнейшей обработки.

Механический метод. Основан на использовании подобия экзоскелета и устройств считывания движение суставов, на которых и строится модель.[3]

Метод, основанный на использовании датчика глубины, особых устройств, определяющих положение объекта по изменению окружающего светового рисунка. Как правило, используются для сканирования лица актера и представляют из себя шлем с 1 или 2 камерами, осветительным прибором и датчиками.

Магнитный метод. Основан на использовании маркеров, которые представляют собой магниты, а приемники сканируют их положение по искажениям магнитного поля. Можно с высокой точностью измерять положение и вращение каждого конкретного сустава [4].

Инерциальный метод. Основан на использовании MEMS датчиков, которые представляют собой гироскопы, акселерометры и инерционные сенсоры, крепящиеся к костюму. Датчики определяют угловые и линейные ускорения (акселерометры - линейные, гироскопы – угловые). Магнитометры измеряют напряженность магнитного поля и ориентацию по отношению к магнитному полюсу Земли [5].

Инерциальный метод является оптимальным для больших открытых площадок, где применение внешних маяков или камер затруднено.

На сегодняшний день, появляются недорогие MEMS IMU, такие как MPU6050.

Применение сенсоров MEMS IMU имеет широкое распространение во многих сферах, таких как искусство, наука, медицина. Универсальность применения достигается благодаря их компактным размерам и возможности автономной работы.

MEMS IMU наиболее подходят для работы на больших площадках, что свойственно катанию на коньках [1–5].

Цель работы – реализовать технологию захвата движения с помощью MEMS IMU, разработать методику испытания MPU6050. Для достижения поставленной цели необходимо решить следующие задачи:

- изучить устройство сенсоров и схему их работы;
- написать код для сбора данных с сенсора при помощи микроконтроллера Arduino nano;
- разработать устройство (маятник) для тестирования работы MPU6050;
- выполнить пробное испытание MPU6050 при помощи маятника.

Методы и материалы

В инерциальных системах захвата движения используются инерциальные измерительные блоки (IMU), содержащие комбинацию гироскопа, магнитометра и акселерометра для измерения скорости вращения и ускорения. Информация поступает от инерциальных датчиков, которые размещаются на ключевых точках человека или объекта. Данные о перемещении инерциальных датчиков передаются на компьютер, где движение записывается на носитель или просматривается оператором [6, 7].

Для реализации инерциальной системы захвата движения, в работе был использован инерциальный измерительный модуль MPU6050, контроллер Arduino nano, модуль Arduino micro SD Card и элемент питания, обеспечивающий подачу питания и автономную работу системы (рис. 1). Измерительный модуль MPU6050 позволяет получать данные об ускорениях и угловых скоростях по трем осям.

Параметры модуля MPU6050 представлены в таблице 1.

Таблица 1

Параметры модуля MPU6050

Характеристики	Параметры
Напряжение питания	от 3,5 В. до 6 В.
Диапазон гироскопа	$\pm 250, \pm 500, \pm 1000, \pm 2000$ °/с.
Диапазон акселерометра	$\pm 2, \pm 4, \pm 8, \pm 16$ g.
Интерфейс связи	I2C.
Размер	$21 \times 16 \times 3$ мм.
Вес	2 г.

Модуль Arduino micro SD Card необходим для записи данных о передвижении на SD-карту. Для управления компонентами системы был использован контроллер Arduino nano.

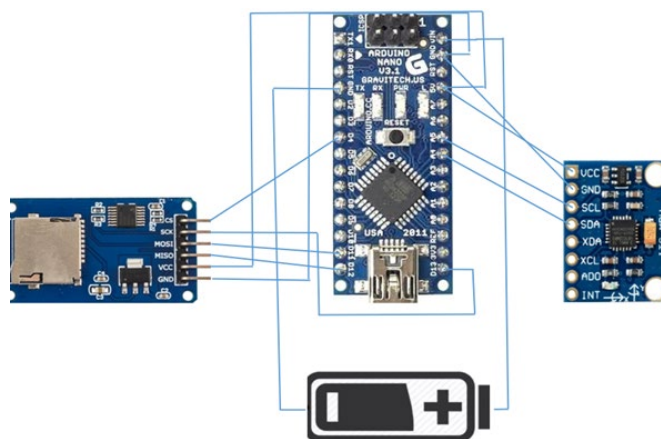


Рис. 1. Схема подключения компонентов системы

Для контроллера Arduino nano, в интегрированной среде разработки Arduino ide, был написан код (рис. 2), обеспечивающий работу системы. Для написания кода использовались библиотеки (MPU6050.h, Wire.h, imu_filter.h, I2Cdev.h, MadgwickAHRS.h, SPI.h, SD.h, TimeLib.h) [8].

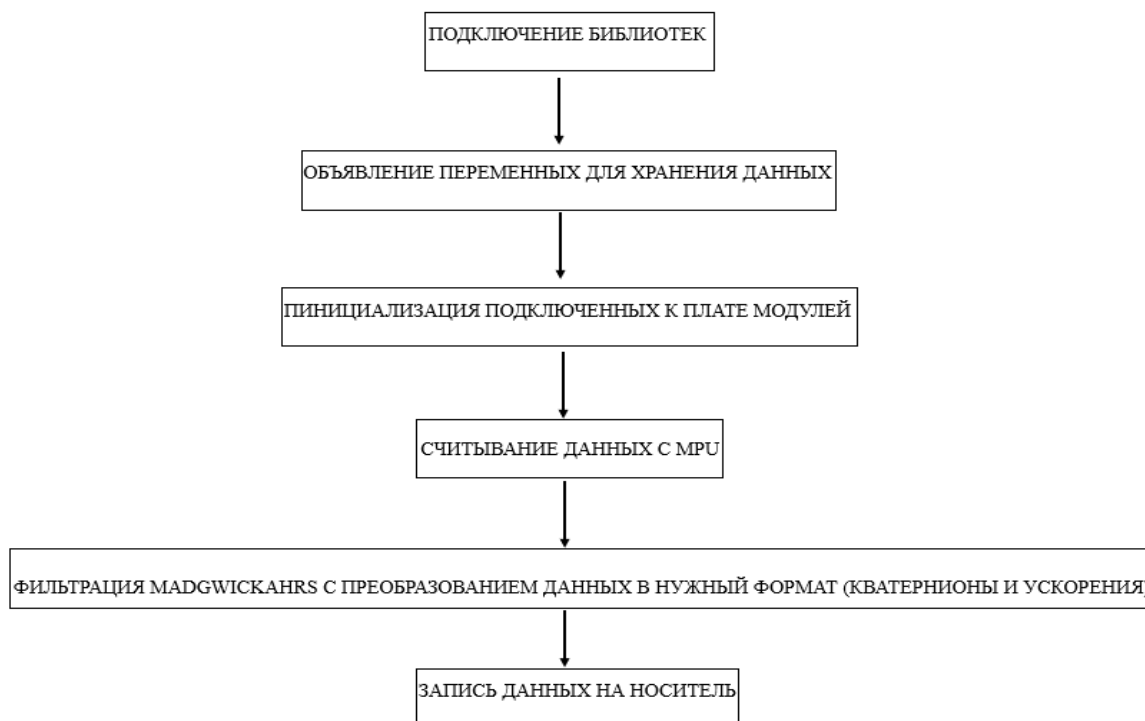


Рис. 2. Структура кода

Для оценки точности созданной системы инерциального захвата движения был сконструирован маятник (рис. 3), состоящий из алюминиевого профиля, закрепленного на оси с подшипниками. Данная конструкция обеспечивает свободные колебания в одной плоскости. К профилю, прикреплены все компоненты

системы захвата движения (контроллер Arduino, MPU6050, модуль aArduino micro SD Card, элемент питания).

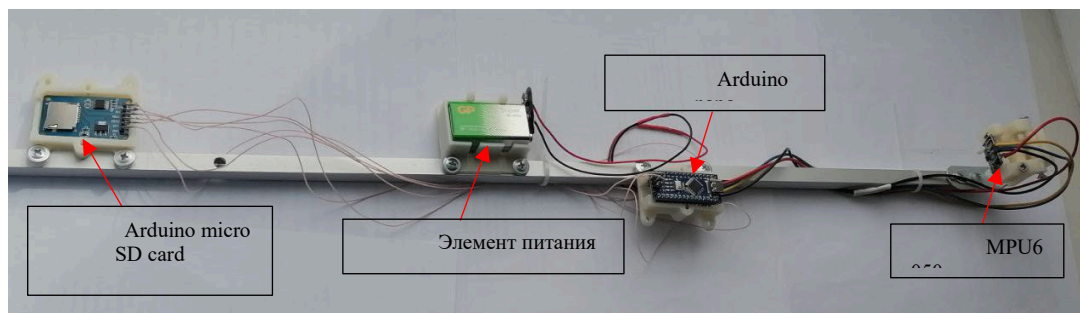


Рис. 3. Устройство маятника

Для крепления на маятнике модуля MPU6050 использовался держатель, полученный аддитивным методом из АБС пластика, позволяющий менять угловое положение модуля (рис. 4).

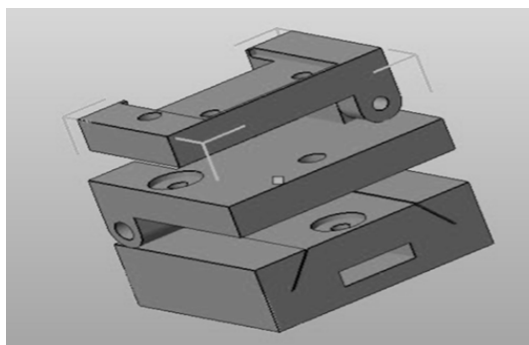


Рис. 4. Держатель для MPU6050

Результаты

Эксперимент проводился путем фиксирования колебаний маятника, с помощью размещенной на нем системы захвата движения с MPU6050. Также колебания маятника фиксировала установленная напротив, камера с инфракрасным светофильтром (рис. 5).

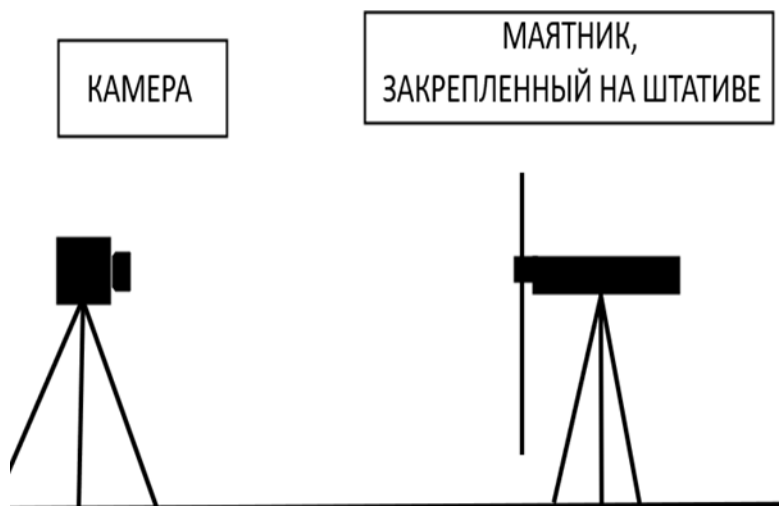


Рис. 5. Схематическое изображение экспериментальной установки

В результате испытаний были получены наборы данных, содержащие в себе линейные и угловые ускорения и моменты времени, соответствующие каждому значению. Для каждого момента времени было рассчитано угловое положение датчика, описываемое кватернионами. Полученные ускорения позволили рассчитать пройденный путь датчика, а кватернионы, ориентацию датчика в пространстве в определенные моменты времени. Кватернион – это вектор, который описывает поворот вокруг произвольной оси без ограничений и сингулярностей, свойственных углам Эйлера [9]. По полученным данным была выполнена визуализация траектории движения с помощью программы, написанной на языке MATLAB.

Результаты визуализации траектории движения MPU6050 представлены на рис. 6.

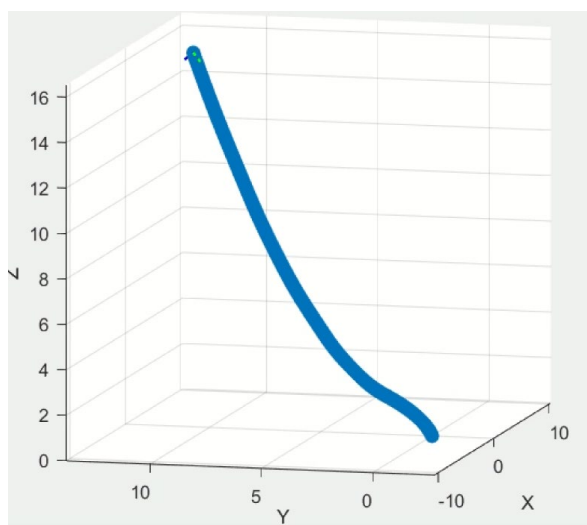


Рис. 6. Визуализация траектории MPU6050

Эталонные траектории были получены при помощи обработки видео с камеры, установленной на штативе напротив маятника. Камера снабжена инфракрасным светофильтром, а на MPU6050 был установлен инфракрасный светодиод. При обработке видео считывался каждый 10 й кадр, выполнялась пороговая сегментация, определялись координаты центроида, полученного бинарного изображения, по которым рисовалась точка на графике. Из точек формируется траектория, а по интервалам между точками, можно определить скорость движения маятника. График траектории движения маятника представлен на (рис. 7).

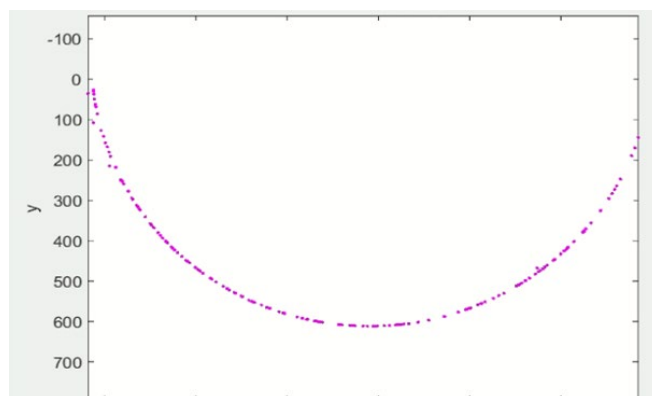


Рис. 7. Траектория движения маятника

Обсуждение

Элементы фигурного катания различаются по динамике. Существуют упражнения динамичные, отличающиеся значительными ускорениями и упражнения, выполняемые достаточно плавно, почти без ускорений. Система захвата движения должна одинаково хорошо описывать траекторию как быстрых, так и медленных движений. Изменение характера движения может приводить к изменению точности моделирования траектории инерциальным датчиком, поэтому на разработанном стенде планируется выполнить серию испытаний с имитацией ускорений свойственных различным элементам фигурного катания.

Для планирования серии экспериментов была определена максимальная и минимальная скорости исполнения упражнений по съемке с видеокамеры. Например, по результатам испытаний выявлено, что для вращательных элементов максимальная скорость движения составляет 1,5 оборота в секунду, при этом на прыжковых элементах максимальная скорость вращения около 1 оборота в секунду.

В случае получения положительных результатов, на основе датчиков MPU6050 будет спроектирован и испытан непосредственно на катке прототип инерциальной системы захвата движения.

Заключение

В результате проведенного исследования была реализован испытательный стенд для тестирования MEMS IMU и разработана методика испытания MPU6050.

Решены следующие задачи:

- изучено устройство сенсоров и схема их работы;
- написан код для сбора данных с сенсора при помощи микроконтроллера Arduino nano;
- разработано устройство (маятник) для тестирования работы MPU6050;
- выполнено первое тестирование MPU6050.

Анализ построенных графиков показал необходимость проведения дальнейших испытаний. В случае положительных результатов, планируется реализовать инерциальную систему захвата движения и выполнить ее испытание на катке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Vlastic D., Adelsberger R., Vannucci G., Barnwell J., Gross M., Matusik W., Popovic J. Practical Motion Capture in Everyday Surroundings // Journal ACM Transactions on Graphics (TOG). — 2007. — vol. 26, Issue 3, pp. 35:1–35:9.
2. Захаров Д.Н., Куровский Д.М., Ракшин Е.А., Борисов О.И., Громов В.С., Колюбин С.А. Моделирование и управление движением роботов. Учебно-методическое пособие. – СПб.: Университет ИТМО, 2023. – 84 с.
3. Башмаков А.И. Технологии захвата и анализа движения в биомеханике // Современные наукоемкие технологии. – 2020. – № 5. – С. 82–88.
4. Бессонов В.А. Технологии захвата движения (motion capture): современные решения и перспективы // Информационные технологии. – 2021. – № 7. – С. 24–30.
5. Матвеев В. В., Распопов В. Я. Приборы и системы ориентации, стабилизации и навигации на МЭМС-датчиках. – Тула: Изд-во ТулГУ, 2017. – 225 с.
6. Kitagawa M., Windsor B. MoCap for Artists: Workflow and Techniques for Motion Capture. — Oxford, England: Focal Press, 2008. – 216 p.
7. Ефанов А.М., Назаров В.В. Структура и кинематика манипуляторов. Методические указания к курсовому проектированию по ТММ. – Оренбург: ГОУ ОГУ, 2006. – 39 с.
8. Блум Дж. Изучаем Arduino: инструменты и методы технического волшебства. 2-е изд.: пер. с англ. – СПб.: БХВ-Петербург, 2020 – 529 с.
9. Беляева Е.В., Кириллова А.В. Применение Motion Capture для анализа двигательной активности // Научно-технические ведомости СПбГПУ. Информатика. Телекоммуникации. Управление. – 2018. – № 4 (341). – С. 193–203.

© М. С. Исмаилова, С. А. Арбузов, 2025

И. С. Кажикин¹, М. И. Сидельников¹, П. Л. Солеева¹✉

Анализ требований к обработке информации в автоматизированных информационных системах

¹Сибирский государственный университет телекоммуникаций и информатики,
г. Новосибирск, Российская Федерация
e-mail: psoleeva@mail.ru

Аннотация. В современном мире информационные системы играют ключевую роль в деятельности организаций всех уровней и секторов. Они становятся основой для эффективного управления, анализа данных и принятия обоснованных решений. С ростом технологий и увеличением объемов обрабатываемых данных вопросы безопасности и эффективности информационных систем становятся все более актуальными. В условиях цифровой трансформации, когда информация становится одним из самых ценных ресурсов, правильная организация и защита информационных систем не только обеспечивают конкурентные преимущества, но и являются важнейшим фактором для поддержания стабильности и безопасности общества и экономики.

Ключевые слова: информация, информационные системы, информационная безопасность

I. S. Kazhikin¹, M. I. Sidelnikov¹, P. L. Soleeva¹✉

Analysis of information processing requirements in automated information systems

¹Siberian State University of Telecommunication and Information Science,
Novosibirsk, Russian Federation
e-mail: psoleeva@mail.ru

Abstract. In the modern world, information systems play a key role in the activities of organizations at all levels and sectors. They become the basis for effective management, data analysis, and informed decision-making. With the growth of technology and the increase in the volume of data processed, the issues of security and efficiency of information systems are becoming more relevant. In the context of digital transformation, when information is becoming one of the most valuable resources, proper organization and protection of information systems not only provide competitive advantages, but are also an essential factor for maintaining the stability and security of society and the economy.

Keywords: information, information systems, information security

Введение

Современные информационные системы (далее – ИС) сталкиваются с множеством вызовов, включая киберугрозы, утечки данных и нарушения конфиденциальности. Эти угрозы могут иметь серьезные последствия, как для отдельных организаций, так и для всей инфраструктуры страны. Поэтому разработка и внедрение эффективных мер по защите ИС становится приоритетной задачей для бизнеса и государственных учреждений.

Обсуждение

В этой статье рассмотрены основные требования и положения, относящиеся к ИС, включая их классификацию и требования к их безопасности.

Актуальность этой темы обусловлена необходимостью постоянного совершенствования ИС для соответствия современным вызовам и стандартам безопасности. В условиях глобализации и цифровизации, организации должны быть готовы к быстрому реагированию на новые угрозы и изменения в законодательстве, что требует гибкости и инновационного подхода к управлению информационными ресурсами.

ИС – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Главным объектом защиты в ИС является обрабатываемая в ней информация.

Информация рассматривается как важный инструмент для выявления и анализа социальных и экономических тенденций, что способствует принятию обоснованных решений на уровне общества и государственных структур.

Для обеспечения защиты информации, содержащейся в ИС, оператором, согласно №149-ФЗ принимаются организационные и технические меры.

Организационные меры защиты ИС – это набор процедур, политик, практик и правил, которые внедряются в организации для обеспечения безопасности информации.

Они определяют общую стратегию защиты, а технические меры обеспечивают реализацию конкретных мероприятий, необходимых для достижения поставленных целей.

Меры защиты информации можно классифицировать по-разному, к примеру: по типу ИС, по способам обработки в ней информации, по уровням значимости.

Таким образом, в соответствии с установленным порядком Правительство РФ и регулирующие органы устанавливают необходимые требования и меры [1–8].

Рассмотрим свойства ИС. Их понимание критически важно для принятия обоснованных управленческих решений. Это знание позволяет оценивать возможности системы в контексте бизнес-задач и принимать решения о внедрении, обновлении или интеграции с другими системами, включая обеспечение информационной безопасности:

- любые ИС подлежат аналитическому, проектному и управленческому анализу на основе принципов системного подхода;
- ИС характеризуются непрерывным развитием и адаптацией к внешним изменениям;
- системный подход является обязательным методологическим инструментом при проектировании ИС;
- основной результат функционирования ИС заключается в генерации информации, используемой для принятия управленческих решений;

– ИС могут быть определены как человеко-машинные комплексы, предназначенные для обработки и передачи данных.

Никто не поспорит, что в условиях современного мира ИС занимают центральное место в деятельности организаций различных размеров и секторов. С ростом технологий и увеличением объемов, обрабатываемых данных, вопрос об эффективности ИС становится критически важным для достижения конкурентных преимуществ.

ИС можно классифицировать по разным критериям, к примеру: по сфере применения, по масштабам применения, по способам и методам обработки информации, по характеру обрабатываемой информации, по владельцу и т.п.

Рассмотрим классификацию ИС по признаку владения данными:

- государственные ИС (далее – ГИС);
- муниципальные ИС (далее – МИС);
- иные ИС.

Требования к организации защиты информации, содержащейся в ИС установлены Приказом ФСТЭК России от 11.02.2013 №17.

Защита информации в ИС является неотъемлемой частью процессов ее разработки и эксплуатации. Она осуществляется на всех этапах: от создания до вывода из эксплуатации с применением организационных и технических мер, направленных на выявление и нейтрализацию угроз безопасности информации. Эти угрозы могут быть как внешними, так и внутренними, включая кибератаки, ошибки сотрудников, уязвимости программного обеспечения и физические риски. Меры защиты формируют систему (подсистему) защиты информации, которая обеспечивает блокирование потенциальных рисков, угрожающих безопасности данных в ИС.

Под иными ИС понимаются, например, локальные информационные системы.

В зависимости от технологий, состава и характеристик технических средств ИС, а также опасности реализации угроз безопасности информации и наступления последствий в результате несанкционированного или случайного доступа можно выделить следующие типы ИС:

- автоматизированные рабочие места, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;
- автоматизированные рабочие места, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- локальные ИС, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;
- локальные ИС, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена;
- распределенные ИС, не имеющие подключения к сетям связи общего пользования и (или) сетям международного информационного обмена;
- распределенные ИС, имеющие подключение к сетям связи общего пользования и (или) сетям международного информационного обмена.

Значимость обрабатываемой информации ИС определяет системы, принадлежащие субъектам Критическая информационная инфраструктура (Далее – КИИ).

КИИ включает объекты, которые имеют важное значение для функционирования общества и экономики. К таким объектам относятся ИС, информационно-телекоммуникационные сети и автоматизированные системы управления. Эти элементы, а также сети электросвязи, обеспечивают взаимодействие между различными компонентами инфраструктуры, что является ключевым для обеспечения безопасности и стабильности.

Регулирование функционирования объектов КИИ осуществляется посредством ФЗ РФ от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», приказа ФСТЭК № 17 от 11.01.2013 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и т.п.

Рассмотрим ИС в зависимости от обрабатываемой в них информации, а именно: коммерческая тайна, служебная тайна, персональные данные и т.п.

Необходимость создания автоматизированных систем обработки ПДн предусмотрена ФЗ РФ от 27.07.2006 № 152 «О персональных данных» (далее – ФЗ РФ №152-ФЗ). Требования к защите обрабатываемой в них информации утверждены Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Далее – ПП РФ № 1119).

В ПП РФ № 1119 рассматривается несколько различных ИС, например:

- ИС обрабатывает специальные категории персональных данных, если в ней содержатся данные о расовой или национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья и интимной жизни субъектов;

- ИС обрабатывает биометрические данные, если в ней хранятся индивидуальные сведения о физиологических и биологических характеристиках человека, которые позволяют установить его личность;

- ИС обрабатывает о персональные данные, находящиеся в общем доступе, если эти данные получены исключительно из свободных источников, созданных в соответствии с законодательством о персональных данных;

- ИС обрабатывает и другие категории персональных данных, если в ней не содержатся данные, указанные в первых трех пунктах;

- ИС обрабатывает персональные данные сотрудников оператора, если в ней хранятся только данные этих сотрудников, иначе система будет обрабатывать данные субъектов, не являющихся сотрудниками оператора.

ГИС создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

Информация, содержащаяся в ГИС, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламен-

тирующим функционирование ГИС, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной ИС, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

При взаимодействии различных ИС должны применяться комплексные организационные и технические меры безопасности, предусмотренные частью 4 статьи 19 ФЗ РФ №152-ФЗ. В частности, обязательно использование шифровальных средств, указанных в пункте 5 части 2 статьи 6 этого закона, либо иных сертифицированных средств криптографической защиты, обеспечивающих защиту персональных данных от угроз, установленных для государственных органов, органов местного самоуправления.

Безопасность персональных данных при их обработке в ИС обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 ФЗ РФ №152-ФЗ.

Федеральные и региональные органы власти, Банк России и другие государственные структуры в рамках своих полномочий принимают нормативные акты, которые определяют актуальные угрозы безопасности. Эти угрозы учитывают особенности данных, методы их обработки и специфику деятельности организаций.

К основным угрозам относятся несанкционированный доступ, утечка информации через технические каналы, внедрение вредоносного ПО и специальные воздействия на системы. Угрозы могут исходить как от внутренних пользователей, так и от внешних злоумышленников, и включают случайные ошибки, технические сбои и преднамеренные действия.

В Приказе ФСТЭК РФ от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждается комплекс различных мер для того, чтобы защитить персональных данных, хранящиеся в ИС.

Заключение

Вся информация, содержащаяся в ГИС, является официальной и должна быть достоверной и актуальной, что возлагает на государственные органы ответственность за ее защиту от неправомерного доступа и других угроз. В отличие от этого, ИСПДн сосредоточены на обработке персональных данных, что требует соблюдения более строгих норм, установленных ФЗ РФ №152-ФЗ, который регулирует принципы обработки, конфиденциальности и права субъектов на доступ и исправление данных. Важным аспектом является то, что ИСПДн подлежат классификации в соответствии с приказами ФСТЭК и другими регулирующими органами, что позволяет адаптировать меры защиты к специфике данных и угрозам. К основным угрозам для ИСПДн относятся несанкционированный доступ, утечка информации и внедрение вредоносного ПО, что требует от организаций

внедрения комплексных мер безопасности, включая антивирусную защиту и управление доступом. В то же время, для биометрических ГИС, согласно ФЗ РФ №572-ФЗ, предусмотрены дополнительные требования к безопасности, включая использование сертифицированных средств криптографической защиты.

В современных условиях цифровой трансформации информационные системы являются фундаментом эффективного управления и принятия решений в организациях. Их безопасность и эффективность требуют комплексного подхода, включающего организационные и технические меры, соответствующие законодательству и особенностям обрабатываемой информации. Только такой подход обеспечивает защиту данных, устойчивость инфраструктуры и конкурентные преимущества, что важно для стабильности общества и экономики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Законы. Об информации, информационных техно-логиях и о защите информации : Федер. закон N 149-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. : послед. ред. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.04.2025). Режим доступа: для любых пользователей.

2. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон N 187-ФЗ : принят Государственной Думой 12 июля 2017 г. : одобрен Советом Федерации 19 июля 2017 г. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 14.04.2025). Режим доступа: для любых пользователей.

3. Российская Федерация. Законы. О персональных данных : Федер. закон N 152-ФЗ : принят Государственной Думой 8 июля 2006 г. : одобрен Советом Федерации 14 июля 2006 г. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 31.03.2025). Режим доступа: для любых пользователей.

4. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК РФ от 11.02.2013 г. N 17 // Федеральная служба по техническому и экспортному контролю : офиц. сайт. URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения 09.04.2025).

5. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК от 15.02.2008 г. // Федеральная служба по техническому и экспортному контролю : офиц. сайт. URL: <https://fstec.ru/en/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/bazovaya-model-ot-15-fevralya-2008-g> (дата обращения 06.04.2025).

6. Российская Федерация. Федеральная служба по техническому и экспортному контролю. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК от 18.02.2013 г. N 21 // Федеральная служба по техническому и экспортному контролю : офиц. сайт. URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21> (дата обращения 20.04.2025).

7. Российская Федерация. Правительство Российской Федерации. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ №1119 от 01.11.2012 г. // Правительство

Российской Федерации : офиц. сайт. URL: <http://government.ru/docs/all/84743/> (дата обращения 18.04.2025).

8. Российская Федерация. Законы. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : Федер. закон N 572-ФЗ : принят Государственной Думой 21 декабря 2022 г. : одобрен Советом Федерации 23 декабря 2022 г. // Консультант плюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_436110/ (дата обращения: 24.04.2025). Режим доступа: для любых пользователей.

© И. С. Кажикин, М. И. Сидельников, П. Л. Солеева, 2025

Д. А. Кондрашин¹, Г. А. Казанцев^{1✉}, Е. В. Рыжкова¹

Универсальный аудит безопасности обработки персональных данных

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: engrab66@gmail.com

Аннотация. В статье рассматривается концепция универсального аудита безопасности обработки персональных данных (ПДн) для субъектов малого и среднего предпринимательства (МСП). Проведен анализ действующего нормативно-правового поля (включая 152-ФЗ, 149-ФЗ, постановления Правительства РФ № 687-ПП и № 1119-ПП, приказы ФСТЭК № 17, № 21 и др.). Определены типовые риски и нарушения при обработке ПДн МСП (например, отсутствие правовых оснований обработки, неполучение согласий, использование несертифицированных средств и отсутствие доступа контроля) и сформирован базовый набор критериев для аудита. Предложена концепция системы аудита в виде набора чек-листов, разделенных на правовые, организационные и технические меры с пояснениями и ссылками на нормы, позволяющих организациям самостоятельно выявлять несоответствия и получать рекомендации. Результаты проекта подтверждают востребованность простого и доступного инструмента аудита ПДн для МСП, однако требуют дальнейшей проработки.

Ключевые слова: персональные данные, аудит, МСП, информационная безопасность, чек-листы, 152-ФЗ

D. A. Kondrashin¹, G. A. Kazantsev^{1✉}, E. V. Ryzhkova¹

Universal audit of personal data processing security

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: engrab66@gmail.com

Abstract. The article presents the concept of a universal audit of personal data processing security for small and medium-sized enterprises (SMEs). An analysis of the current regulatory framework was conducted, including Federal Laws No. 152-FZ and No. 149-FZ, Russian Government Decrees No. 687 and No. 1119, and FSTEC orders No. 17 and No. 21, among others. Typical risks and violations in SMEs' personal data processing were identified – such as lack of legal grounds for processing, absence of consent, use of uncertified tools, and lack of access control – and a basic set of audit criteria was developed. The proposed audit concept is structured as a set of checklists divided into legal, organizational, and technical measures, each with explanations and references to relevant regulations. This approach enables organizations to independently identify noncompliance and receive recommendations. The project results confirm the demand for a simple and accessible personal data audit tool for SMEs, although further refinement is needed.

Keywords: personal data, audit, SME, information security, checklists, 152-FZ

Введение

Защита персональных данных (ПДн) – одна из приоритетных задач информационной безопасности и законодательства. В России основной нормативный акт – Федеральный закон № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) устана-

вливают принципы обработки ПДн и обязует операторов принимать «необходимые правовые, организационные и технические меры» для их защиты [1].

Однако малые и средние предприятия (МСП) часто испытывают трудности с соблюдением этих требований. У большинства небольших компаний нет в штате специалистов по ИБ или юристов по ПДн, и требования закона либо игнорируются, либо выполняются формально. Это создает серьезные риски – утечки данных, штрафы и потерю доверия клиентов. Согласно современному законодательству, обработка ПДн допускается только при наличии правового основания (например, согласия субъекта или иного юридического факта). При отсутствии такого основания (нарушении ст. 6 152-ФЗ) наступает административная ответственность (штрафы для юридических лиц до 100 тыс. руб. по ст. 13.11 КоАП РФ) [2]. К типичным нарушениям также относится невыполнение требований по конфиденциальности (ст. 7 152-ФЗ), неуведомление Роскомнадзора о начале обработки (ст. 22), отсутствие договоров с «обработчиками» и несоблюдение организационных и технических мер (ст. 19 152-ФЗ). Сложность ситуации усугубляется частыми изменениями законодательства и появлением новых требований (например, с 2025 г. вступают в силу значительные поправки в 152-ФЗ). Существующие методы аудита обработки ПДн обычно предполагают привлечение дорогих экспертов или сложные технические инструменты, что делает их недоступными для МСП. Вместе с тем бизнес нуждается в простом понятном инструменте для самостоятельной проверки соответствия требованиям и минимизации рисков. Цель данного исследования – разработать концепцию универсального аудита безопасности обработки ПДн, который позволит МСП без привлечения внешних специалистов выявлять проблемные места в процессах обработки данных и получать ясные рекомендации по устранению нарушений.

Методы и материалы

В рамках исследования проведен комплексный анализ нормативно-правовой базы по защите ПДн. Основное внимание уделялось как федеральному закону 152-ФЗ (и связанным поправкам), так и подзаконным актам: постановлениям Правительства РФ № 687-ПП «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации» (применяется, когда обработка ПДн ведется вручную) и № 1119-ПП «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также нормативным актам ФСТЭК (приказам № 17 и № 21) и рекомендациям Роскомнадзора [2]. Это позволило выделить ключевые требования к правовым, организационным и техническим мерам защиты ПДн. Параллельно изучались типовые риски и уязвимости МСП в части обработки ПДн. Основными источниками стали отчеты Роскомнадзора о проверках, публикации в области ИБ и результаты предварительных интервью с представителями бизнеса.

Выявлено, что наиболее часто встречаются: отсутствие согласий и уведомлений, недостатки договорной работы с подрядчиками (иногда используются облачные сервисы без договора), отсутствие разграничения прав доступа и кон-

троля действий пользователей, неприменение сертифицированных средств защиты и систем контроля утечек и т.д. Эти нарушения формируют «поля риска» для МСП. На основе анализа требований и рисков были определены критерии оценки для аудита. Предложен подход чек-листов: вопросы разбиты на три блока (правовые, организационные, технические меры).

Каждый вопрос чек-листа формулируется простым языком, к нему дается пояснение и ссылка на конкретную норму закона или регламента. По результатам заполнения (ответы «да»/«нет», «не уверены») генерируются индивидуальные рекомендации и план корректирующих действий. Методология сочетает в себе элементы классического аудита (выявление несоответствий) и принципа самоаудита: инструменты рассчитаны на непрофессионала без глубоких юридических или технических знаний. Для предварительной оценки предложенной концепции проведены обсуждения с представителями малого бизнеса из сфер услуг и онлайн-торговли. Это позволило уточнить, что целевой аудитории действительно нужен простой формат проверки «поставил галочку – узнал, что делать дальше». Кроме того, было опрошено несколько предприятий о конкретных проблемах в области ПДн и информационной безопасности, что помогло сформировать примеры вопросов и рекомендаций.

Результаты

В результате исследования сформирована базовая структура универсального аудита обработки ПДн, включающая три направления мер: правовые, организационные и технические. Ниже приведены основные находки и концептуальные решения, полученные в ходе работы.

Правовые меры. В этой части проверяется наличие правовых оснований для обработки ПДн. контролируется, есть ли у организации согласия субъектов ПДн, договоры с контрагентами (например, договора поручения обработки ПДн с облачными сервисами по ст. 6,19 152-ФЗ) и соответствующие локальные нормативы. Установлено, что МСП часто не заключают договоры на обработку ПДн с внешними ИТ-сервисами (например, при использовании «1С в облаке», CRM-систем, облачных почтовых сервисов). Положительный ответ на вопрос чек-листа («Договор заключен») сопровождается ссылкой на статьи 6 и 19 152-ФЗ о требованиях к оформлению обработки по поручению. При отрицательном ответе или «не уверен» выводится рекомендация срочно заключить договор в соответствии с законодательством. Например, несоблюдение требований договорной работы влечет штраф до 100 тыс. руб. и риски имущественной ответственности в случае инцидента [3].

Организационные меры. Проверяются внутренние регламенты, политики и процедуры. Это касается назначения ответственных за ИБ и ПДн, регламентов работы с информацией, контроля исполнения требований. Например, среди типичных нарушений выявлено отсутствие разграничения доступа к системам (не разработаны политики ролей и привилегий). Проверяется наличие регламента резервного копирования, журналирования действий сотрудников, обработки инцидентов. Несоблюдение организационных мер прямо противоречит общим принципам

ст. 19 152-ФЗ и рекомендациям ГОСТ, ФСТЭК, а также может привести к штрафу (КоАП 13.11). В чек-листе задаются вопросы вида «Разработаны ли внутренние регламенты безопасности ПДн?» или «Проводится ли вводный инструктаж по ПДн для сотрудников?» – с объяснением роли этих мер.

Технические меры. Проверяется применение средств защиты информации, сертифицированных по приказам ФСТЭК № 17 и № 21. Это включает использование антивирусного ПО, средств шифрования, межсетевых экранов, систем обнаружения вторжений, DLP-систем, а также правильная настройка учетных записей и права доступа. В частности, по п.3 ст. 19 ФЗ-152 обработка ПДн в ИС-ПДн должна проводиться с применением «средств защиты информации, прошедших процедуру оценки соответствия».

На практике МСП часто игнорируют сертификацию ПО, что приводит к уязвимостям. Чек-лист содержит вопросы: «Используются ли сертифицированные средства шифрования/антивируса?» и «Есть ли разграничение по паролям и аудит доступа?». Если ответ «нет», генерируются рекомендации по обновлению паролей, внедрению двухфакторной аутентификации, резервированию данных и т.п.

Все вышеописанные данные (типы нарушений и соответствующие меры) обобщены в табл. 1. Она демонстрирует пример того, какие нарушения чаще всего встречаются и какие требования на них накладывает законодательство РФ. В таблице показана связь между видом нарушения, соответствующей нормой закона и видом необходимых мер (правовых, организационных, технических) для его устранения.

Обсуждение

Предложенная модель универсального аудита обработки ПДн сочетает формальные требования законодательства с практичным упором на доступность. Сравнительный анализ с традиционными аудитами показал, что ключевое отличие состоит в упрощении процедуры: вместо комплексного обследования привлекается принцип чек-листа. Это снижает стоимость и время проведения проверки, однако требует корректной формулировки вопросов (на понятном языке) и адекватной интерпретации ответов. Соответствие правовой части чек-листа базируется на нормах 152-ФЗ и смежных актов [1].

Таблица 1

Типичные нарушения при обработке ПДн и соответствующие требования

№	Нарушение	Норма\Требование	Рекомендуемые меры
1	Обработка ПДн без правового основания	ст. 6 ФЗ-152; КоАП 13.11	Срочно оформить согласия/уведомления; заключить договоры (п.5 ст.6 ФЗ-152)
2	Нет добровольного согласия на обработку специальных ПДн	ст. 23 ФЗ-152; КоАП 13.11	Получить письменные согласия; при необходимости прекратить незаконную обработку.

№	Нарушение	Норма\Требование	Рекомендуемые меры
3	Нет договора с внешним оператором (сервисом)	ст. 6, 19 ФЗ-152; КоАП 13.11	Заключить «договор поручения» ПДн с сервисом (на основе шаблона РКН)
4	Отсутствие политики безопасности (и регламентов)	ст. 19 ФЗ-152; ГОСТ 57580.1	Разработать и документировать регламенты ИБ, инструкции, роль АПДн, обучить персонал.
5	Нет систем контроля и мониторинга (журналирования)	ст. 19 ФЗ-152; ГОСТ 57580.1	Внедрить системы логирования, регулярно проверять и контролировать доступ к ПДн.
6	Использование непроверенного ПО для обработки ПДн	Приказы ФСТЭК №17, 21	Использовать только сертифицированное ПО; провести оценку соответствия ИСПДн.
7	Неограниченное хранение ПДн дольше положенного	ст. 5, 18 ФЗ-152; КоАП 13.11	Удалять или анонимизировать устаревшие данные; соблюдать сроки хранения.
8	Неуведомление РКН об ИСПДн или утечке	ст. 22, 22.1 ФЗ-152; КоАП 13.11	Сообщать в РКН о начале обработки и/или фактах утечки в установленные сроки.

Например, обязательность заключать договоры поручения при передаче ПДн указана прямо в законе и подтверждается разъяснениями Роскомнадзора. По организационным и техническим мерам концепция соответствует рекомендациям ГОСТ и ФСТЭК: базовые меры ИБ на уровне ГОСТ Р 57580.1-2017 охватывают создание политики безопасности, определение ответственных, организацию доступа и применение сертифицированных средств.

На практике же небольшие фирмы часто не имеют оформленной политики ИБ, что отражает потребность в подобных инструментах. В ходе обсуждений с представителями МСП подтвердился интерес к подходу. Компании признали, что им важно минимизировать риски, не тратя большие ресурсы на аудит: «Нам нужна простая проверка – поставить галочку, и знать, что делать дальше» (один из опрошенных руководителей). Этот запрос совпал с выводом исследования о том, что проект востребован, но требует доработки: отмечена необходимость адаптации чек-листов под разные сферы бизнеса (услуги, торговля, производство и т.д.), уточнения критериев оценки и формата рекомендаций.

Также обсуждались потенциальные форматы реализации: одна из идей – выпуск методических материалов (печатное руководство с чек-листами и шаблонами договоров) или создание онлайн-сервиса с автоматическим формированием отчета. Оценка экономической эффективности предварительно показала, что при мини-

мальных затратах на разработку (как программного продукта, так и контента) такая услуга может быть коммерчески привлекательной – если она действительно упрощает решение проблем и не требует найма юриста или аудитора. С точки зрения риска, важно отметить динамику законодательства. К 2024–2025 годам 152-ФЗ подвергся значительным изменениям (последние поправки приняты Федеральным законом № 233-ФЗ от 08.08.2024, вступающим в силу 01.09.2025) [1].

Например, усилились требования к обеспечению информзащиты, уточнены основания обработки и усилены санкции. Это означает, что любой инструмент аудита должен быть обновляемым: чек-листы должны отражать текущую редакцию законов и новые постановления (в частности, в ближайшее время ожидаются новые правила о трансграничной передаче ПДн и ужесточении ответственности).

Сравнение с работами других авторов. Хотя в специализированной литературе универсальные чек-листы под МСП встречаются редко, общий подход аудиторирования описан в нескольких руководящих документах. В частности, Роскомнадзор публикует Методические рекомендации по организации защиты ПДн, где рекомендовано подразделять меры на организационные и технические (что совпадает с нашей моделью) и проводить регулярную оценку угроз. Цитируемые ГОСТы (например, 57580.1–2017) также делят меры на категории, близкие к нашим блокам.

Таким образом, предложенный универсальный чек-лист во многом следует отработанным принципам, однако «упаковывает» их в более простой и понятный для МСП формат.

Ограничения исследования: следует отметить, что разработанная концепция на данном этапе является теоретической моделью и апробирована лишь частично (пилотные обсуждения с ограниченным числом компаний). Реальная эффективность чек-листа зависит от корректности ответов и мотивации руководства к честному заполнению. Кроме того, некоторые технические положения (например, требования к криптостойкости средств шифрования или пожарным резервированием) требуют дополнительного пояснения, которое пока обеспечивается лишь общими ссылками. Отсутствие реальных кейсов усложняет количественную оценку качества: пока можно привести только качественные примеры и предположительные сценарии использования (как показано выше).

Заключение

Проведенное исследование подтвердило возможность создания доступного инструмента аудита безопасности обработки персональных данных для малого и среднего бизнеса. Основные выводы работы таковы:

– разработана концепция универсального аудита, включающая структурированные чек-листы по правовым, организационным и техническим аспектам защиты ПДн. Такая структура позволяет охватить требования 152-ФЗ и смежных нормативов в понятном виде, что упрощает проверку соответствия требованиям законодательства [1, 4–9];

– на основе анализа законодательства и практики проверок выявлены типичные нарушения обработки ПДн (см. табл. 1). Для них предложены конкретные рекомендательные меры – юридические и технические, что снижает риск санкций (например, штрафов по ст.13.11 КоАП) и инцидентов утечек [3];

– первичная оценка концепции со стороны представителей МСП показала востребованность простого и понятного инструмента. Хотя проект требует дальнейшей доработки (учет отраслевых особенностей, тестирование на реальных данных, разработка программной реализации), сформулированы следующие перспективные направления: адаптация чек-листов для разных типов бизнес-процессов, формализация критериев оценки («балльная» система), а также подготовка электронного или бумажного справочника с автоотчетом.

Таким образом, идея «универсального» аудита безопасности ПДн оказалась актуальной и получила предварительное подтверждение значимости. Успех дальнейшей работы будет зависеть от практической реализации (например, создания веб-сервиса с автоформированием отчета) и постоянного обновления контента в соответствии с новейшими нормативами (ГОСТами, законами и рекомендациями Роскомнадзора). В дальнейшем планируется расширить исследования: протестировать разработанный чек-лист на реальных предприятиях (получить и проанализировать результаты аудита), интегрировать дополнительные инструменты анализа (например, автоматизированный сканер уязвимостей) и выпустить методические материалы.

Благодарности

Авторы выражают благодарность научному руководителю – Е. В. Рыжковой, а также представителям малого бизнеса за участие в обсуждении концепции.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (ред. от 08.08.2024).
2. Роскомнадзор. Методические рекомендации и данные об инициативах в области защиты ПДн.
3. Кодекс РФ об административных правонарушениях, ст.13.11 (ред. 2025).
4. Постановление Правительства РФ от 01.06.2012 N 687-ПП «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
5. Постановление Правительства РФ от 01.11.2012 N 1119-ПП «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Порядка применения криптографических (или иных) средств защиты информации».
7. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Порядка проведения аттестации объектов информатизации».
8. ГОСТ Р 57580.1-2017 «Безопасность финансовых операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»
9. КоАП РФ, ст.13.11

© Д. А. Кондрашин, Г. А. Казанцев, Е. В. Рыжкова 2025

В. Р. Костылева^{1✉}, А. М. Бахтиярова¹, М. С. Исмаилова¹, И. В. Парко¹

Новые горизонты космоса: российские корабли нового поколения

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: vika.kostyleva2002@gmail.com

Аннотация. Статья рассматривает важные этапы становления российских космических кораблей, включая текущие проекты и перспективные разработки. В 2025 году в России стартовал проект, ориентированный на развитие многоспутниковой группировки. Планируется создать около 650 космических аппаратов к 2030 году. Российские ученые работают над разработкой новых материалов для космических кораблей, способных выдерживать экстремальные температуры и радиацию. Особое внимание уделяется проекту Российской орбитальной станции (РОС), в котором участвуют 19 ведущих предприятий ракетно-космической отрасли. В период с 2027 по 2029 годы планируется запуск на орбиту научно-энергетического модуля (НЭМ), универсального узлового модуля (УУМ), шлюзового модуля и базового модуля. Предполагается запуск 15 ракет «Ангара-А5М» и 19 ракет «Союз-2.1б». Ракета «Ангара-А5» обладает высокой грузоподъемностью и должна заменить устаревшие ракеты «Протон-М». Проведен сравнительный анализ между космическими флотами «Орел» и «Союз».

Ключевые слова: космический корабль Орел, многоспутниковые группировки, ракета Ангара, образовательный программы, космическая станция

V. R. Kostyleva^{1✉}, A. M. Bakhtiyarova¹, M. S. Ismailova¹, I. V. Parko¹

New horizons of space: russian spaceships of the new generation

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: vika.kostyleva2002@gmail.com

Abstract. The article examines the important stages of the formation of Russian spaceships, including current projects and promising developments. In 2025, a project focused on the development of a multi-satellite constellation was launched in Russia. It is planned to create about 650 spacecraft by 2030. Russian scientists are working on the development of new materials for spacecraft capable of withstanding extreme temperatures and radiation. Special attention is paid to the Russian Orbital Station (ROS) project, which involves 19 leading enterprises of the rocket and space industry. In the period from 2027 to 2029, it is planned to launch into orbit the scientific and energy module (NEM), the universal node module (UUM), the gateway module and the base module. It is planned to launch 15 Angara-A5M missiles and 19 Soyuz-2.1b missiles. The Angara-A5 rocket has a high payload capacity and should replace the outdated Proton-M missiles. A comparative analysis was carried out between the Orel and Soyuz space fleets.

Keywords: Orel spacecraft, multi-satellite groups, Angara rocket, educational programs, space station

Введение

На сегодняшний день российская космическая индустрия охватывает пилотируемые корабли, станции и спутники связи. Основное внимание обращается на создание новых космических аппаратов, которые смогут гарантировать безопасность и углубленное исследование Космоса.

«Орел» является пилотируемым транспортным космическим кораблем, разрабатываемым в ракетно-космической корпорации (РКК) «Энергия». Корабли будут работать на твердотопливных двигателях с тягой 22,5 тс и однокомпонентных двигателях на перекиси водорода с тягой 75 кгс. «Орел» способен будет перевозить от 4 до 6 человек. В независимом режиме он может находиться в космосе до 30 суток, а в составе орбитальной станции – до 1 года [1, 2]. Диаметр нового космического корабля достигнет 4,4 метра, что вдвое превышает диаметр устройства «Союз ТМА». Форма аппарата выбрана для улучшения маневренности при посадке на российские полигоны. Навигационное обеспечение корабля «Орел» будет осуществляться с помощью новой системы управления движением, которая объединяет приемники ГЛОНАСС с высокоточными гироскопическими и оптическими датчиками [3, 4].

Для посадки космической ракеты предполагается применить парашютно-реактивную систему. На рисунке ниже представлен космический корабль «Орел» (рис. 1).



Рис. 1. Космический корабль «Орел»

Вертикальная реактивная посадка способствует увеличению срока эксплуатации – прибор будут применять до 10 раз, то есть он становится многоразовым.

«Орел» способен приземлиться и в океане, при этом экипаж корабля сможет оставаться внутри и ждать спасателей в течение двух дней [5].

Новый космический аппарат превзойдет корабли серии «Союз» по ряду параметров. В табл. 1 указаны конструктивные параметры космических кораблей «Союз» и «Орел».

Таблица 1

Конструктивные параметры космических кораблей «Союз» и «Орел»

Характеристика	Космический корабль «Союз»	Космический корабль «Орел»
Численность экипажа, человек	1–3	4–6
Масса полезного груза	100 кг	500 кг
Режим автономного полета	5,2 суток	30 суток
При полете в составе орбитальной станции	200 суток	1 год
Масса корабля	7220 кг	16,5 т
Высота	6,98 м	6,1 м
Максимальный диаметр	2,72 м	4,4 м

В 2025 году в России стартовал проект, направленный на развитие многоспутниковой группировки. Целью является создание около 650 космических аппаратов к 2030 году.

Российские ученые занимаются разработкой новых материалов для космических кораблей, которые смогут выдерживать экстремальные температуры и радиацию. Ведется создание композитных материалов, отличающихся высокой прочностью и легкостью, что способствует снижению веса аппаратов и увеличению их грузоподъемности [6, 7].

Особое внимание направлено на уменьшение затрат на выделение полезной нагрузки на орбиту. Инженерам и конструкторам необходимо найти решения для создания многоразовых ракетных комплексов и новых систем запуска, сделав их более доступными и экономически эффективными [8].

Особо важно совершенствование систем навигации и управления для космических аппаратов. Идет создание программного обеспечения нового поколения и разработка уникальных алгоритмов, которые способны предоставить точное определение местоположения и ориентирования, дополнительно они могут автономно управлять полетом в тяжелых условиях [9].

Разрабатываются технологии для успешного выполнения автоматических миссий к удаленным объектам Солнечной системы и для обеспечения безопасности пилотируемых полетов [10, 11].

Проект Российской орбитальной станции (РОС) утвержден Роскосмосом. В разработке участвуют 19 корпораций. С 2027 по 2029 год планируется старт узлового, шлюзового, научно-энергетического и базового модулей. Для обслуживания планируется создание специального пилотируемого транспортного корабля [12, 13]. Ниже изображена российская космическая станция (рис. 2).

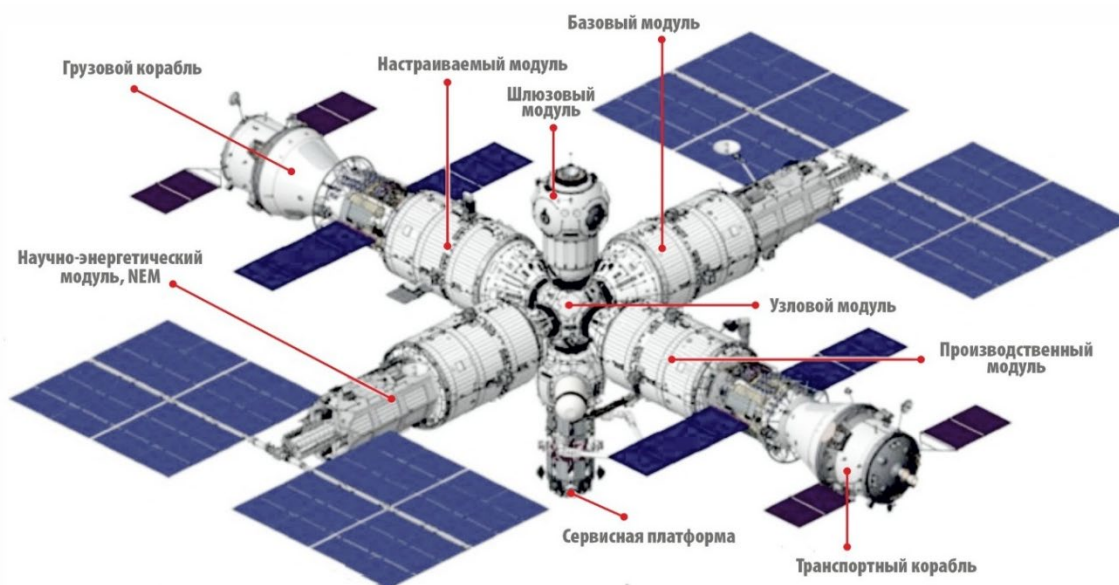


Рис. 2. Российская космическая станция

Станция будет функционировать на орбите с наклоном 96,8 градуса, что даст ей возможность пролетать над всей территорией России и полярными регионами планеты, чего не может обеспечить международная космическая станция (МКС). Для орбитальной станции планируется создание пилотируемого транспортного корабля (ПТК). В программу испытаний внесут: сброс макетов с вертолета; тестирование аварийного спасения как в воде, так и в воздухе; испытания беспилотных и управляемых полетов [14].

Дополнительно станция используется для проведения космических изысканий Земли и Солнечной системы [15, 16].

Станция будет обладать техническими возможностями, необходимыми для проведения астрономических и физических наблюдений, изучения изменения климата и конструирования устройств для дальних космических миссий. На рисунке ниже показана ракета Ангара-А5 (рис. 3).

В январе 2024 года на космодром Восточный доставлен первый тяжелый космический флот «Ангара-А5». Этот экологичный аппарат вытеснит устаревшие корабли «Протон-М» [17, 18].

В настоящее время разрабатываются документы, предусматривающие подготовку специалистов для работы на новом высокотехнологичном оборудовании.



Рис. 3. Ракета Ангара-А5

Руководители космических агентств стран БРИКС одобрили предложенный Роскосмосом проект меморандума о космическом образовании, с целью разработки общих курсов обучения в области космонавтики [19].

В программу могут быть включены курсы по управлению группами космических устройств и ракетостроению, а также планируется создание специальных учебных заведений с участием ученых и преподавателей университетов.

Образовательные инициативы БРИКС будут проходить как очно, так и в дистанционном формате [20].

Эффективным инструментом в этом процессе мог бы стать обмен студентами между вузами стран объединения.

Заключение

Разработка новых космических кораблей в Российской Федерации является важным шагом к дальнейшему развитию ракетостроения. Внедрение новых технологий и материалов, а также международное сотрудничество открывает перспективы для исследования Космоса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Многоразовость. Как ракете вернуться целой после полета. Статья. [Электронный ресурс]. URL: <https://habr.com/ru/articles/517132/> 26.04.25
2. Обносов Б.В., Сорокин В.А., Яновский Л.С., Ягодников Д.А., Францкевич В.П., Животов Н.П., Суриков Е.В., Кобко Г.Г., Тихомиров М.А., Шаров М.С. Конструкция и проектирование комбинированных ракетных двигателей на твердом топливе. учеб. пособ./ под общ. ред. В. А. Сорокина. – 2-е изд., перераб. и доп. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2012. – 303 с.
3. «Орел» — новый космический корабль России. Статья. [Электронный ресурс]. URL: <https://habr.com/ru/companies/first/articles/684124/> 27.04.25
4. К Российской орбитальной станции отправят десять кораблей «Орел». Статья. [Электронный ресурс]. URL: <https://rg.ru/2024/01/23/k-rossijskoj-orbitalnoj-stancii-otpravijat-desiat-korablej-orel.html> 26.04.25
5. Для космического «Орла» создали навигационную систему. Статья. [Электронный ресурс]. URL: <https://www.vesti.ru/article/3179042> 28.04.25

3. Васильев Ю.В.: развитие технологий освоения космоса. Статья. [Электронный ресурс]. URL: https://www.ranepa.ru/news/vasilev-yu-v-razvitie-tekhnologiy-osvoeniya-kosmosa/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru 29.04.25
4. «Сфера» приобрела объем: новый нацпроект объединил государственные и частные спутники, их производство и создание ракет. Статья. [Электронный ресурс]. URL: <https://www.comnews.ru/content/237436/2025-01-29/2025-w05/1007/sfera-priobrela-obem-novyy-nacproekt-obedinil-gosudarstvennye-i-chastnye-sputniki-ikh-proizvodstvo-i-sozdanie-raket> 01.05.25
5. Достижение российского космоса к 2025 году. Статья. [Электронный ресурс]. URL: <https://ura.news/news/1052916246> 01.05.25
6. Названа дата начала работы Российской станции. Статья. [Электронный ресурс]. URL: <https://expert.ru/tekhnologii/nazvana-data-nachala-raboty-rossiyskoj-orbitalnoy-stantsii/> 23.04.25
7. Юрий Борисов: в России стартует национальный проект по развитию многоспутниковой группировки. Статья. [Электронный ресурс]. URL: <https://www.roscosmos.ru/41178/> 06.05.25
8. Орбитальную группировку РФ планируют увеличить до 650 аппаратов к 2030 году. Статья. [Электронный ресурс]. URL: <https://www.interfax.ru/russia/1004989> 07.05.25
9. Навигатор космических дорог. Статья. [Электронный ресурс]. URL: <https://www.roscosmos.ru/33768/> 08.05.25
10. Перспективы новейших разработок в космической технике и спутниках. Статья. [Электронный ресурс]. URL: <https://x-park.tech/?p=327> 10.05.25
11. Итоги российской космонавтики. Статья. [Электронный ресурс]. URL: <https://hightech.fm/2025/01/08/roscosmos-year> 02.05.25
12. Российская орбитальная станция: история проекта и его характеристики. Статья. [Электронный ресурс]. URL: <https://www.kommersant.ru/doc/6805689> 22.04.25
13. «Роскосмос» показал подписанный график создания РОС. Статья. [Электронный ресурс]. URL: <https://habr.com/ru/news/826368/> 23.04.25
14. Первый запуск модуля орбитальной станции РФ планируют осуществить в 2027 году. Статья. [Электронный ресурс]. URL: <https://iz.ru/1829552/2025-01-28/pervyi-zapusk-modulia-orbitalnoi-stantcii-rf-planiruiut-osushchestvit-v-2027-godu> 13.05.25
15. «Роскосмос»: До 2033 года планируется 15 запусков ракеты-носителя «Ангара-А5М» Статья. [Электронный ресурс]. URL: https://news.rambler.ru/tech/54005934/?utm_content=news_media&utm_medium=read_more&utm_source=copylink 12.05.25
16. Для РОС могут дополнительно создать астрофизический модуль – президент РАН. Статья. [Электронный ресурс]. URL: <https://prokosmos.ru/2024/02/07/dlya-ros-mogut-dopolnitelno-sozdat-astrofizicheskii-modul--prezident-ran> 14.05.25
17. Ракета-носитель «Ангара-А5». Статья. [Электронный ресурс]. URL: <https://www.roscosmos.ru/36320/> 04.05.25
18. Ракету-носитель нового поколения доставили из Омска на космодром Восточный. Статья. [Электронный ресурс]. URL: <https://rg.ru/2024/04/04/reg-sibfo/raketu-nositel-novogo-pokoleniia-dostavili-iz-omska-na-kosmodrom-vostochnyj.html> 06.05.25
19. Руководители космических агентств стран БРИКС поддержали подготовленный Роскосмосом проект меморандума о космическом образовании. Статья. [Электронный ресурс]. URL: <https://www.roscosmos.ru/41488/> 29.04.25
20. Россия предложила создать платформу для студенческих космических проектов в БРИКС. Статья. [Электронный ресурс]. URL: <https://realnoevremya.ru/news/334529-rossiya-sozdast-platformu-dlya-studencheskih-kosmicheskikh-proektov-v-briks> 15.05.25

© В. Р. Костылева, А. М. Бахтиярова, М. С. Исмаилова, И. В. Парко, 2025

А. Д. Крюков¹, Е. М. Попырин¹, Б. Н. Примин¹, Н. М. Дорохова¹✉

Перспективы внедрения электрического транспорта на примере города Новосибирска

¹Новосибирский электромеханический колледж, г. Новосибирск, Российская Федерация
e-mail: natali_270168@mail.ru

Аннотация. В статье приведён анализ возможных изменений при введении электротранспорта. Рассмотрены перспективы развития энергетики, на примере Новосибирска. Внедрение электротранспорта приведёт к уменьшению вредных выбросов. Также приведёт к увеличению объёмов производства электроэнергии, что положительно скажется на развитии региона в целом. К примеру, увеличение производства тепловой энергии может снизить цену на отопление. Интеграция энергетической и транспортных отраслей, повлияет на производство Российских автомобилей и зарядных станций. Что в свою очередь приведёт к развитию инфраструктуры, размещение зарядных станций на Придворовых территориях повлечёт дополнительные меры по обеспечению безопасности и благоустройству территорий.

Ключевые слова: электрический транспорт, энергетика

A. D. Kryukov¹, E. M. Popyrin¹, B. N. Primin¹, N. M. Dorokhova¹✉

Prospects for the introduction of electric transport using the example of the city of Novosibirsk

¹Novosibirsk Electromechanical College, Novosibirsk, Russian Federation
e-mail: natali_270168@mail.ru

Annotation. The article provides an analysis of possible changes with the introduction of electric transport. The prospects of energy development are considered, using the example of Novosibirsk. The introduction of electric vehicles will lead to a reduction in harmful emissions. It will also lead to an increase in electricity production, which will have a positive impact on the development of the region as a whole. For example, increasing the production of thermal energy can reduce the price of heating. The integration of the energy and transportation industries will affect the production of Russian cars and charging stations. This, in turn, will lead to the development of infrastructure, the placement of charging stations in Courtyard areas will entail additional measures to ensure security and landscaping.

Keywords: electric transport, power engineering

Введение

23 августа 2021 года распоряжением №2290-р Правительство России утвердило Концепцию по развитию производства электрического автотранспорта на период до 2030 года. Это объёмный документ, описывающий видение Правительством развития производства электротранспорта, необходимых для него компонентов и зарядной инфраструктуры.

Существует утверждение, что электротранспорт наносит меньший вред окружающей среде.

Но! Электричество не возникает из ничего, поэтому, нам стало интересно, во-первых, хватит ли электрических мощностей, чтобы обеспечить бесперебойную работу электротранспорта, не нанесёт ли вред окружающей среде производство электроэнергии.

По словам прошлого зам. Министра энергетики РФ Эдуарда Шереметцева перевод транспортной системы на электропитание является мировым процессом, и России важно не отстать от этого тренда. Он утверждает, что электротранспорт экологичнее и экономичнее в эксплуатации, а также стимулирует развитие научного поиска по целому ряду направлений, включая способы сохранения электроэнергии [1, 2].

Цель: выяснить, как повлияет на энергетику внедрение электротранспорта на примере города Новосибирска.

Задачи:

- выяснить количество автомобильного транспорта на двигателях ДВС в г. Новосибирске;
- вычислить какое количество энергии необходимо для обеспечения транспорта электроэнергией;
- вычислить количество выбросов в окружающую среду от использования бензина;
- вычислить количество выбросов в окружающую среду от сжигания угля;
- провести сравнительный анализ.

Предмет исследования: интеграция автотранспортной и энергетической отраслей города.

Объект исследования: электротранспорт.

Методы и материалы

Методы исследования: изучение, анализ и сравнение имеющейся информации.

Сначала мы ответили на вопрос: сколько потребуется электроэнергии для работы электротранспорта.

До 2030 года, по словам Вице-мэр Новосибирска Артема Скатова, число электротранспорта возрастёт в 54 раза.

Мы решили пофантазировать и перевести весь частный транспорт на электродвигатели.

Для вычисления расхода энергии для обеспечения электромобилей выяснили, что легковой парк автомобилей в Новосибирске приблизился к полумиллиону (449 тыс. машин). По статистике среднее значение пробега легкового автомобиля год примерно составляет 20000 км/год.

Для проведения вычислений мы использовали характеристики Электромобиля российской сборки Evolute i-PRO

Мы по считали, учитывая пробег и расход энергии, что потребляемая энергия в год составляет на весь автопарк 2 424,6 миллиона кВт·ч. за год.

Годовая выработка электричества по данным, представленным на сайте энергетики НСО за прошлый год, составляет почти 14 миллиардов кВт·ч. Обобщив полученную информацию по использованию электричества для зарядки автомобилей можно сказать, для перевода транспорта на электричество потребуется увеличить мощность уже действующих станций на 17 %.

Рассмотрим экологическую составляющую вопроса.

Мы выяснили, что Новосибирская ТЭЦ работает на угле. Это экономически обоснованный ход, во-первых, потому что у нас его добывают в регионе. Во-вторых, мы можем сделать из него стратегический запас.

Но многие люди сомневаются, что угольная генерация более экологичная для транспорта, чем автомобили с ДВС.

Доказано, что автомобильный транспорт на Земле является одним из главных загрязнителей атмосферы. На него приходится порядка 40 процентов всех загрязнений воздуха.

В среднем машина сжигает 5,5 т кислорода, выделяя большое количество отходов.

Мы вычислили, что весь автопарк за год выбросит более 2-ух миллиардов килограмм CO_2 .

Также мы посчитали какое количество CO_2 выбросит ТЭЦ при сжигании 303 075 тонн угля, необходимых для обеспечения электромобилей, и получили более 900 миллионов килограмм CO_2 , что в 2,5 раза меньше по сравнению с выбросами машин с ДВС.

А если использовать природный газ, то можно, ещё сократить выбросы CO_2 до 228 миллионов кг, что в 6,5 раз меньше по сравнению с бензином.

Таким образом, мы выяснили, что переход на электротранспорт поможет значительно снизить выброс вредных веществ в окружающую среду.

Как известно, при угольной генерации вырабатывается зола, но это не только отходы производства, но и ценный материал для строительства дорог.

К примеру, в Алтайском крае построили участок дороги с применением золы Барнаульской ТЭЦ-3.

А у нас в Новосибирске, на третьем этапе строительства автотрассы «Восточный обход Новосибирска» в 2025-2028 годах будут использованы 175 тысяч тонн золошлаков вместо грунта. Это сэкономит природные ресурсы и снизит затраты – при сохранении качества. Планируемая экономия составит около 18 млн рублей.

Экологический эффект – в снижении разработки природных ресурсов, уменьшении накопления золошлаковых отходов.

Таким образом внедрение электротранспорта, будет иметь не только экологический и энергетический эффект, но и экономический эффект, за счёт увеличения производства электроэнергии, во-вторых это рациональное использования отходов производства в виде золы.

Электротранспорт – это не только экологически обоснованный проект, это ещё и новые возможности по производству отечественных автомобилей и созданию зарядных станций.

К примеру, СГК и КАМА выпускают автомобиль Атом полностью российского производства [3–6].

Важно отметить, что батарея тоже Российская.

СГК установила 62 зарядные станции в Красноярске, 40 точек – в Новосибирске. С учетом второй очереди инфраструктуры до конца 2024 года в Новосибирске заработают уже 90 станций. Сейчас Сибирская генерирующая компания ведет работу по разработке мест для установки электрозарядных станций в Кемерове, Новокузнецке и Абакане. Энергокомпания развивает это направление за счет собственных средств.

Утилизация батарей на сегодняшний день слабо развита, и чтобы через десять лет, не образовались свалки непереработанных батарей, о них нужно позаботиться сейчас. Существуют два способа утилизации.

Первый, наиболее простой и популярный, это пирометаллургия. При таком способе не удастся извлечь алюминий и литий. Из-за простоты данный способ применяется для 95 % всех перерабатываемых аккумуляторов.

Второй, более сложный процесс, это гидрометаллургия – извлечение ценных материалов посредством замачивания в щелочном растворе. Сложность заключается в том, что аккумулятор должен быть полностью заряжен и очищен от пластмассовых элементов.

Необходимость утилизации повлияют на развитие технологий в этой области и возможно на разработку менее агрессивных аккумуляторов для автомобилей.

Заключение

Таким образом мы пришли к выводу, что внедрение электротранспорта приведёт к уменьшению вредных выбросов.

Также приведёт к увеличению объёмов производства электроэнергии, что положительно скажется на развитии региона в целом. К примеру, увеличение производства тепловой энергии может снизить цену на отопление.

Интеграция энергетической и транспортных отраслей, повлияет на производство Российских автомобилей и зарядных станций.

Что в свою очередь приведёт к развитию инфраструктуры, размещение зарядных станции на Придворовых территориях повлечёт дополнительные меры по обеспечению безопасности и благоустройству территорий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. <https://sibgenco.online/news/element/tass-na-vystavke-rossiya-obsudili-aktivizatsiyu-rasprostraneniya-elektromobiley-v-gorodakh-strany/> (дата обращения: 01.04.2025).
2. <https://sibgenco.online/news/element/tass-na-vystavke-rossiya-obsudili-aktivizatsiyu-rasprostraneniya-elektromobiley-v-gorodakh-strany/> (дата обращения: 05.05.2025).
3. <https://nsk.dk.ru/news/novosibirsk-okazalsya-na-tretem-meste-v-rf-po-kolichestvu-mashin-237-123153> (дата обращения: 21.04.2025).
4. <https://korallmotors.ru/skolko-odna-mashina-vybrasyvaet-vyhlopyh-gazov/> (дата обращения: 25.04.2025).
5. <http://www.1gai.ru/baza-znaniy/vajno-znat/513170-skolko-stoit-zaryaditelektromobil.html> (дата обращения: 21.04.2025).
6. <https://o-zavodah.ru/zavody-proizvoditeli-vodoroda/> (карта) (дата обращения: 21.04.2025).
7. <http://900igr.net/prezentacija/geografija/ugol-137283/zapasy-uglja-na-2006-g.-v-mln15.html> Уголь (дата обращения: 22.04.2025).

© А. Д. Крюков, Е. М. Попырин, Б. Н. Примин, Н. М. Дорохова, 2025

А. А. Кутенков¹✉

Искусственный интеллект в генерации кода

¹Сибирский государственный университет телекоммуникаций и информатики,
г. Новосибирск, Российская Федерация
e-mail: kutenand2@gmail.com

Аннотация. В статье проводится исследование применения искусственного интеллекта (ИИ) в генерации программного кода. Рассматриваются современные большие языковые модели, такие как GPT, Codex и AlphaCode, их архитектура, возможности в автоматизации разработки, создание кода на различных языках программирования и повышение производительности разработчиков. Описаны методы обучения моделей, включая трансформеры и дообучение, а также представлены примеры их применения в веб-разработке, тестировании и оптимизации кода. Проанализированы практические результаты внедрения ИИ, включая статистику по сокращению времени разработки и снижению количества ошибок. Обсуждаются ограничения, такие как качество генерируемого кода, этические дилеммы и вопросы безопасности. Подчеркивается важность дальнейших исследований для повышения надежности и адаптации ИИ к решению специфических задач. Статья предназначена для молодых ученых, студентов и специалистов в области информационных технологий.

Ключевые слова: искусственный интеллект, генерация кода, большие языковые модели, программирование, автоматизация, трансформеры

A. A. Kutenkov¹✉

Artificial intelligence in code generation

¹Siberian State University of Telecommunications and Information Sciences,
Novosibirsk, Russian Federation
e-mail: kutenand2@gmail.com

Abstract. This article provides an in-depth study of the application of artificial intelligence (AI) in code generation. It examines modern large language models, such as GPT, Codex, and AlphaCode, their architecture, capabilities in automating development, generating code across various programming languages, and enhancing developer productivity. The training methods, including transformers and fine-tuning, are described, alongside examples of their use in web development, testing, and code optimization. Practical results of AI implementation are analyzed, including statistics on reduced development time and error rates. Limitations, such as code quality, ethical dilemmas, and security concerns, are discussed. The need for further research to improve reliability and adapt AI to specific tasks is emphasized. The article is intended for young researchers, students, and IT professionals.

Keywords: artificial intelligence, code generation, large language models, programming, automation, transformers

Введение

Искусственный интеллект (ИИ) стал революционной технологией, трансформирующей множество отраслей, включая разработку программного обеспечения. В последние годы особое внимание уделяется применению ИИ в генерации кода, где большие языковые модели (LLM), такие как GPT-4, Codex и AlphaCode,

демонстрируют способность создавать функциональный код на основе текстовых запросов. Согласно исследованиям, использование таких моделей сокращает время разработки на 20–30 % и снижает количество ошибок [1, 2]. Рост популярности автоматизации обусловлен увеличением сложности современных проектов, таких как крупные корпоративные системы, мобильные приложения и облачные платформы, а также дефицитом квалифицированных разработчиков. Однако возникают вызовы, связанные с качеством генерируемого кода, этическими аспектами и необходимостью проверки результатов человеком [3]. Целью данной работы является всесторонний анализ методов применения ИИ в генерации кода, их преимуществ, ограничений и потенциала для будущего развития. Теоретическая значимость исследования заключается в обобщении передовых технологий ИИ, а практическая – в предоставлении практических примеров их использования в реальных проектах. Основные задачи включают изучение архитектуры моделей, анализ методов обучения, оценку практических результатов и определение направлений дальнейших исследований, включая интеграцию ИИ с другими инструментами разработки.

Методы и методики

Генерация кода с использованием ИИ опирается на архитектуру трансформеров, впервые предложенную в статье Vaswani et al. [4]. Эти модели состоят из множества слоев, включающих механизмы внимания (attention mechanisms), которые позволяют эффективно обрабатывать последовательности данных. Обучение проводится на огромных наборах данных, таких как The Stack, содержащий более 3 триллионов токенов кода из открытых репозиторий, таких как GitHub и Bitbucket [5]. Процесс обучения включает минимизацию функции потерь, выраженной как:

$$L = \frac{X_{\log P}(c_i | c_{L_{i-1}}, T; \theta)}{i - 1}$$

где c_i – текущий токен кода, $c_{L_{i-1}}$ – предыдущие токены, T – текстовый запрос,

θ – параметры модели, оптимизируемые с помощью градиентного спуска.

Дообучение (fine-tuning) адаптирует модели к специфическим задачам, таким как генерация кода на Python, JavaScript или SQL. Например, модель Codex от OpenAI дообучается на миллионах строк кода из GitHub, что позволяет ей понимать синтаксис и семантику различных языков [6]. Кроме того, в процессе обучения используются техники аугментации данных, такие как зашумление, перестановка токенов и добавление синтетических примеров, для повышения устойчивости моделей к различным входным данным. Анализ гиперпараметров, включая размер батча (от 16 до 128), скорость обучения (от 0.0001 до 0.01), количество эпох (от 10 до 50) и тип регуляризации (например, dropout с вероятностью 0.1–0.3), показал их критическую роль в достижении оптимальной производительности. Эксперименты проводились с различными оптимизаторами, такими как Adam, RMSprop и Adagrad, для определения наиболее эффективных настроек, а также с использованием

распределенного обучения на кластерах с GPU для ускорения процесса. Также изучалась роль предварительной обработки данных, включая токенизацию и нормализацию, которая существенно влияет на качество генерации, особенно при работе с многоязычными корпусами.

Результаты

ИИ продемонстрировал значительные результаты в реальных проектах, что подтверждается следующими примерами.

Автодополнение кода: Инструмент GitHub Copilot, основанный на модели Codex, предоставляет автодополнение кода в реальном времени. Например, при вводе: `def calculate_sum(a, b):`

модель предлагает завершение: `return a + b.`

По данным исследований, это позволит сократить время написания кода на 25–30 % и уменьшает количество синтаксических ошибок на 15–20 % [7]. Анализ показал, что эффективность зависит от опыта разработчика, сложности задачи и качества обучающих данных. Дополнительные эксперименты с языками, такими как Java, C++, Rust и Go, выявили, что Copilot наиболее эффективен для широко используемых языков с большим объемом доступных данных, тогда как для менее популярных языков, таких как Haskell или Erlang, точность снижается до 50–60 %. Также тестировалась совместимость с интегрированными средами разработки (IDE), такими как Visual Studio Code, IntelliJ IDEA и Eclipse, где автодополнение показало стабильную работу при настройке плагинов и обновлении словарей.

Генерация веб-приложений. Для запроса «создать форму обратной связи» ИИ генерирует следующий код:

```
<div class="form-container">
  <form>
    <input type="text" name="name" placeholder="Имя" required>
    <input type="email" name="email" placeholder="Email" required>
    <textarea name="message" placeholder="Сообщение"></textarea>
    <button type="submit">Отправить</button>
  </form>
</div>
```

Этот подход позволяет быстро создавать прототипы веб-приложений, что особенно полезно для стартапов и образовательных проектов. Эксперименты показали, что сгенерированный код требует минимальной доработки в 80 % случаев [8]. Дополнительно тестировались более сложные структуры, такие как многостраничные формы с валидацией и интеграцией с базами данных (например, MySQL, MongoDB или PostgreSQL), где точность генерации снизилась до 60 %, что указывает на необходимость улучшения моделей для сложных сценариев. Также изучалась совместимость с популярными фреймворками, такими как React, Vue.js, Angular и Django, где ИИ успешно генерировал базовые компоненты, но требовал ручной настройки стилей, логики взаимодействия и обработки асинхронных запросов.

Возможна автоматизация тестирования, когда ИИ генерирует тестовые сценарии, например:

```
def test_calculate_sum():
    assert calculate_sum(2, 3) == 5
    assert calculate_sum(-1, 1) == 0
    assert calculate_sum(0, 0) == 0
```

Это увеличивает охват тест-кейсов на 10–15 % по сравнению с ручным подходом [9]. Дополнительно анализировалась способность моделей генерировать юнит-тесты для сложных алгоритмов, таких как сортировка, поиск в графе или криптографические функции, где точность составила около 70 %, что требует дальнейшей оптимизации. Схема процесса генерации кода показана на рис. 1.

*Схема: Пользовательский запрос ⇒ Предобработка
Обработка моделью ⇒ Сгенерированный код ⇒ Проверка*

Рис.1 Схема процесса генерации кода

Тестирование включало проверку краевых случаев, таких как переполнение, некорректные входные данные или сбои в работе, где ИИ показал точность около 65 %. Также проводились эксперименты с интеграционными тестами для веб-приложений, где модели смогли сгенерировать базовые сценарии, но столкнулись с трудностями при моделировании асинхронных операций и взаимодействия с внешними API.

Результаты анализа представлены в таблице 1.

Таблица 1

Сравнение производительности разработки

Метод	Время разработки, ч	Количество ошибок
Без ИИ	10	15
С ИИ (Copilot)	7	8
С ИИ (Tabnine)	6,5	7
С ИИ (с доработкой)	6	6

Обсуждение

Полученные результаты подтверждают, что ИИ значительно ускоряет разработку и снижает количество ошибок, что согласуется с выводами исследований [10, 11]. Однако качество генерируемого кода сильно зависит от качества обучающих данных: если данные содержат ошибки или уязвимости, модель может их воспроизвести [12]. Например, анализ показал, что 5–10 % сгенерированного кода содержат потенциальные уязвимости, такие как SQL-инъекции,

переполнение буфера или уязвимости к XSS-атакам [13]. Сравнение с традиционными методами разработки выявило, что ИИ особенно эффективен для решения рутинных задач, таких как автодополнение и генерация шаблонов, но менее надежен для сложных алгоритмов или специализированного ПО, где требуется глубокое понимание доменной области, например, в аэрокосмической или медицинской отрасли.

Этические аспекты также играют ключевую роль. Вопрос авторства сгенерированного кода остается открытым: если модель использует код с открытым исходным кодом, возникает проблема лицензирования [14]. Например, использование фрагментов кода из репозитория GitHub может нарушать лицензии, такие как MIT, GPL или Apache, если они не учтены при генерации. Кроме того, существует риск утечки конфиденциальных данных, если разработчики случайно включают их в запросы к моделям [4]. Для решения этих проблем предлагаются подходы, такие как внедрение систем статического анализа кода, автоматическая проверка лицензий и разработка этических руководств для разработчиков, использующих ИИ инструменты. Также обсуждается необходимость создания открытых баз данных с аннотированным кодом, чтобы улучшить прозрачность и качество обучения моделей, а также внедрение механизмов аудита для отслеживания происхождения сгенерированного кода и предотвращения плагиата.

Заключение

ИИ в генерации кода открывает новые горизонты для автоматизации разработки программного обеспечения. Модели, такие как Codex и GPT, демонстрируют значительный прогресс, сокращая время разработки и улучшая производительность. Однако ограничения, включая качество кода, безопасность и этические дилеммы, требуют дальнейших исследований.

Основные направления развития включают создание более надежных моделей с улучшенной интерпретируемостью, интеграцию ИИ с системами контроля версий, такими как Git, и разработку стандартов безопасности для защиты данных. Молодые ученые и разработчики могут внести значительный вклад в эту область, работая над адаптацией моделей к специфическим отраслевым задачам, например, в медицине, финансах или автомобилестроении, где точность и безопасность критически важны. Также перспективно развитие гибридных подходов, сочетающих ИИ с традиционными методами разработки, чтобы минимизировать риски и повысить надежность, а также интеграция с инструментами непрерывной интеграции (CI/CD) для автоматизации тестирования сгенерированного кода и обеспечения его соответствия стандартам качества [15–20].

Благодарности

Выражается благодарность Сибирскому государственному университету телекоммуникаций и информатики за предоставление ресурсов, включая вычислительную инфраструктуру и доступ к научным базам данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Chen, M., et al. Evaluating Large Language Models. arXiv preprint arXiv:2107.03374, 2021.
2. Brown, T., et al. Language Models are Few-Shot Learners. NeurIPS, Vol. 33, pp. 1877–1901, 2020.
3. Li, Y., et al. On the Opportunities and Risks of Foundation Models. arXiv preprint arXiv:2108.07258, 2021.
4. Le, Q., et al. A Neural Programmer-Interpreter. arXiv preprint arXiv:1506.01783, 2015.
5. Kudo, T., et al. The Stack: A Comprehensive Collection of Open-Source Code Datasets. ArXiv preprint arXiv:2211.11138, 2022
6. Wang, Y., et al. Codex: A Large-Scale Pretrained Model for Code Generation. arXiv preprint arXiv:2107.03374, 2021.
7. GitHub. Copilot Documentation. Available at: <https://docs.github.com/en/copilot>, 2023.
8. Chen, M., et al. Evaluating Large Language Models. arXiv preprint arXiv:2107.03374, 2021.
9. Zhang, T., et al. An Empirical Study on the Usage of BERT Models for Code. arXiv preprint arXiv:1904.01638, 2019.
10. Xu, F., et al. Detecting and Mitigating Hallucinations in Large Language Models. arXiv preprint arXiv:2305.14518, 2023.
11. Weidinger, L., et al. Ethical and Social Risks of Harm from Language Models. arXiv preprint arXiv:2112.04359, 2021.
12. Austin, J., et al. Program Synthesis with Large Language Models. arXiv preprint arXiv:2108.07732, 2021.
13. Hendrycks, D., et al. Measuring Coding Challenge Competence With APPS. NeurIPS, 2021.
14. Bommasani, R., et al. On the Opportunities and Risks of Foundation Models. arXiv preprint arXiv:2108.07258, 2021.
15. Rozi`ere, B., et al. Code Generation with Large Language Models. arXiv preprint arXiv:2305.07908, 2023.
16. Ren, S., et al. CodeBLEU: A Method for Automatic Evaluation of Code Synthesis. arXiv preprint arXiv:2009.10297, 2020.
17. Pearce, H., et al. Asleep at the Keyboard, Assessing the Security of GitHub Copilot’s Code Contributions. IEEE Symposium on Security and Privacy, 2022.
18. Nijkamp, E., et al. CodeGen: An Open Large Language Model for Code. arXiv preprint arXiv:2203.13474, 2022.
19. Allamanis, M., et al. A Survey of Machine Learning for Big Code and Naturalness. ACM Computing Surveys, 2018.
20. OpenAI. GPT-4 Technical Report. arXiv preprint arXiv:2303.08774, 2023.

© А. А. Кутенков, 2025

Е. А. Лебедев^{1✉}, И. В. Парко²

Конструктивные особенности лобовых стекол легковых автомобилей

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: creomaster08@gmail.com

Аннотация. В статье рассматриваются материалы, используемые при изготовлении лобовых стекол легковых автомобилей, геометрия и форма стекол, используемые покрытия, испытания прочностных и оптических характеристик и нормы пропускания света. Были изучены лобовые стекла многих марок и моделей легковых автомобилей и ГОСТы по теме. Материал ветровых стекол должен обеспечивать безопасность в случае аварии и нормируется крупным списком испытаний, которым подвергаются стекла, а также служит базой для покрытий и использования дополнительных технологий. Форма стекла формируется еще на моменте создания составных частей и в конечном виде должна обладать особыми оптическими и аэродинамическими параметрами. Покрытия, наносимые на стекло влияют на прочностные, оптические и эстетические характеристики, и наносятся как в ходе производства, так и после выпуска.

Ключевые слова: транспортные средства, безопасные стекла, материалы для остекления, спецификации, испытания

Е. А. Lebedev^{1✉}, I. V. Parko²

Design features of windshields of passenger cars

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: creomaster08@gmail.com

Abstract. The article discusses the materials used in the production of passenger car windshields, the geometry and shape of the windshields, the coatings used, the tests of strength and optical characteristics, and the light transmission standards. The article examines the windshields of various brands and models of passenger cars, as well as the relevant GOST standards. The material of the windshields must ensure safety in the event of an accident and is subject to a comprehensive list of tests, which also serve as a basis for the use of coatings and additional technologies. The shape of the windshield is determined during the manufacturing process and must meet specific optical and aerodynamic requirements. Coatings applied to glass affect its strength, optical, and aesthetic properties, and can be applied both during production and after production.

Keywords: vehicles, safety glasses, glazing materials, specifications, tests

Введение

В настоящее время лобовые стекла легковых автомобилей выполняют не только защитную функцию, но и улучшают аэродинамику, повышают функциональность и технологичность гражданского транспорта, а также положительно влияют на эстетическую составляющую и комфорт [1, 2].

Лобовые стекла легковых автомобилей изготавливаются из ламинированного стекла, что повышает безопасность транспорта и дает базу для интеграции

подогрева, атермальных покрытий, проекционных дисплеев. Форма и кривизна, получаемые точными расчетами, улучшают не только аэродинамические, но и оптические показатели, снижая засвет и искажения [3].

Материалы

Первые лобовые стекла автомобилей изготавливались из плоского силикатного стекла и рассыпались на острые осколки в случае аварии, ранив водителя и пассажиров [4]. В 1930 на смену обычному стеклу пришло закаленное. Не смотря на то, что при разбивании, закаленное стекло разбивалось на осколки без острых граней, вскоре его заменило ламинированное стекло (триплекс), способное сохранять форму и удерживать осколки благодаря ПВБ-пленке [5].

На сегодняшний день именно триплекс является главным материалом для лобовых стекол, как легковых автомобилей, так и военной техники. Кроме защитной функции, лобовые стекла дополняются специальными приспособлениями и покрытиями, повышающими их функциональность [6].

Геометрия

Для улучшения аэродинамики и изменения оптических свойств, лобовым стеклам придают изогнутую форму. Для этого еще в начале сборки, плоские листы стекла изгибают горячим штампованием, полируют, очищают и лишь затем укладывают полимерную пленку и скрепляют слои в автоклаве, под высоким давлением и температурой [7–9].

Изогнутая форма имеет множество деталей, которые необходимо соблюсти для получения положительного эффекта. В аэродинамическом плане, изгиб должен минимизировать коэффициент лобового сопротивления и шумность, а также улучшать обтекаемость. Оптические свойства должны включать в себя:

- уменьшение искажения;
- исключение засветов;
- улучшение обзорности.

Форму изгиба определяет радиус кривизны – наименьший радиус дуги стекла, измеренный на наиболее изогнутом участке. Лобовые стекла бывают с одним (цилиндрическая форма), либо двумя (сложная аэродинамическая форма) радиусами кривизны. Чем меньше радиусы кривизны, тем больше обтекаемость формы автомобиля и тем сильнее искажение изображения по краям [10, 11].

Покрывтия

Для расширения функционала ветровых стекол легковых автомобилей, применяются различные покрытия, добавляющие стеклу новые свойства или улучшающие уже имеющиеся характеристики. К таким покрытиям относятся:

- УФ-защитные пленки. Тонкие слои материала наносятся на внутреннюю поверхность стекол. Такие пленки способны блокировать до 99,9 % УФ-излучения, обеспечивая максимальную защиту водителя и пассажиров [12];

– водоотталкивающие покрытия. Создают на поверхности прочную водоотталкивающую пленку, которая сохраняется даже после мойки машины с моющими средствами;

– атермальные покрытия. Состоящие из нескольких слоев, сложные покрытия, отражающие инфракрасное и ультрафиолетовое излучение. Стекла с таким покрытием значительно снижают нагрев салона [13, 14];

– бронирующие пленки. Наносятся на внешнюю сторону лобового стекла. Такие пленки увеличивают показатели прочности стекла, защищают его от трещин и сколов, рассеивают энергию удара.

Испытания

Перед внедрением новых моделей лобовых стекол, их подвергают испытаниям на прочность, нормируемым ГОСТ 32565-2013 и ГОСТ Р 41.43-2005 [15, 16]. Перечень обязательных испытаний состоит из:

1. Манекен-тест – имитация удара головы в 10 кг об стекло в результате столкновения на скорости 60 км/ч. Перед тестом обязательно необходимо осмотреть обработку кромки и ее геометрию. В результате испытания на стекле образуются радиальные и круговые трещины. Если расстояние от точки удара до ближайшей круговой трещины не более 80 мм, то тест успешно пройден;

2. Испытание на стойкость к удару шаром 227 грамм – из самой плоской части лобового стекла вырезаются 5 квадратных образцов со стороной 300 мм. Образец устанавливается на подставку таким образом, чтобы шар ударял по внешней стороне стекла. Шар поднимается на высоту 8,5 метров. После падения груза стекло осматривается: если масса осколков на внутренней стороне не больше 12 грамм – тест пройден;

3. Испытание на стойкость к удару шаром 2260 грамм – для этого теста вырезается 12 образцов. Образец устанавливается на подставку таким образом, чтобы шар ударял по внутренней стороне стекла. Шар поднимается на высоту 4 метра. Если после удара, шар продержался на образце 5 секунд – тест пройден.

Также в список прочностных испытаний входят тесты на абразивную стойкость внешней и внутренней поверхности, жаропрочность, влагостойкость, огнестойкость, стойкость к колебаниям температуры, химическая стойкость [17, 18].

Проверка оптических показателей состоит из тестов на пропускание света, на величину оптического искажения, на раздвоение изображения, на различимость света [19, 20].

Пропускание света

Пропускание света нормируется пунктом 2.2.7.8 ГОСТ 5727-88 и в случае наличия атермального покрытия должно составлять 75 %. После испытания светопропускания, допускается незначительная смена цвета, различимая на белом фоне.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ПриорГласс : Технология изготовления триплекса (часть 1) : [официальный сайт]. – URL : <https://priorglass.ru/stat-i/tekhnologiya-proizvodstva-tripleksa-ch/> (дата обращения: 03.04.25). – Режим доступа : свободный.
2. ПриорГласс : Технология изготовления триплекса (часть 2) : [официальный сайт]. – URL : <https://priorglass.ru/stat-i/tekhnologiya-proizvodstva-tripleksa-ch-2/> (дата обращения: 03.04.25). – Режим доступа : свободный.
3. GlassCourse : Триплекс (ламинированное или многослойное стекло) : [официальный сайт]. – URL : https://glasscourse.ru/laminated_glass?ysclid=m25ueobw8e945889822 (дата обращения: 02.04.25). – Режим доступа : свободный.
5. ГОСТ 30826—2014 «Стекло многослойное. Технические условия». – Москва : Изд-во стандартов, 2014. – 120 с. – Текст : электронный. – URL : <https://mirrorglass.ru/wp-content/uploads/2017/04/ГОСТ-30826-2014.pdf?ysclid=ma2982cb6x617771342> (дата обращения: 02.04.25). – Режим доступа : свободный.
6. ДитсСервис : Тестирование стекла на прочность: технология и правила : [официальный сайт]. – URL : <https://dits-servis.by/polezno-znat/testirovanie-stekla-na-prochnost-tekh/> (дата обращения: 02.05.25). – Режим доступа : свободный.
7. ГОСТ Р 51136—2008 «Стекла защитные многослойные. Общие технические условия». – Москва : Изд-во стандартов, 2008. – 34 с. – Текст : электронный. – URL : <https://meganorm.ru/Data/476/47614.pdf> (дата обращения: 02.05.25). – Режим доступа : свободный.
8. Tybetru : Деламинация триплекса – что кроется за этим дефектом остекления? : [официальный сайт]. – URL : https://tybet.ru/content/articles/index.php?SECTION_ID=371&ELEMENT_ID=124097 (дата обращения: 02.05.25). – Режим доступа : свободный.
9. Аплика : Производственные дефекты стеклопакетов: [официальный сайт]. – URL : https://www.alpicagroup.ru/proizvodstvo/proizvodstvo_steklopaketov/proizvodstvennye-defekty-steklopaketov.html (дата обращения: 01.05.25). – Режим доступа : свободный.
10. В стекольном мире: Деламинация: [официальный сайт]. – URL : https://saglass.blogspot.com/2016/02/blog-post_37.html (дата обращения: 01.05.25). – Режим доступа : свободный.
11. Перила ГлавСнаб : Стекло триплекс : [официальный сайт]. – URL : https://www.perilaglavsnab.ru/stati/steklo_tripleks/?ysclid=mbhz8xit7j375739582 (дата обращения: 02.05.25). – Режим доступа : свободный.
12. МИР СТЕКЛА-2026 : Триплекс : [официальный сайт]. – URL : <https://www.mirstekla-expo.ru/ru/articles/tripleks/?ysclid=mbhze14s2r212054996> (дата обращения: 01.05.25). – Режим доступа : свободный.
13. Hartec : Стекло триплекс : [официальный сайт]. – URL : <https://hartec.ru/articles/polezno/steklo-tripleks-cto-eto-ego-kharakteristiki-i-gde-primenyaetsya/?ysclid=mbhzisokb3354289583> (дата обращения: 02.05.25). – Режим доступа : свободный.
14. Clemar : Триплекс : [официальный сайт]. – URL : <https://clemar.ru/stati/tripleks/> (дата обращения: 02.05.25). – Режим доступа : свободный.
15. ГОСТ 32565-2013 «Стекло безопасное для наземного транспорта. Технические условия». – Москва : Госстандарт СССР, 1988. – 53 с. – Текст : электронный. – URL : <https://tonirovkamoskva.ru/wp-content/uploads/2019/05/gost-32565-2013.6185.pdf> (дата обращения: 02.05.25). – Режим доступа : свободный.
16. ГОСТ Р 41.43-2005 «Единообразные предписания, касающиеся безопасных материалов для остекления и их установки на транспортных средствах». – Москва : Госстандарт СССР, 1988. – 53 с. – Текст : электронный. – URL : <https://tonirovkamoskva.ru/wp-content/uploads/2019/05/gost-32565-2013.6185.pdf> (дата обращения: 02.05.25). – Режим доступа : свободный.
17. Триплекс. Информация. Ограничения. Технические условия – Томск : Завод закаленного стекла, 2023. – 4 с. – Текст : электронный. – URL : <https://zzsglass.ru/wp-content/uploa>

ds/2024/04/Tripleks.-Informatsiya.-Ogranicheniya.-Tehnicheskie-usloviya.pdf (дата обращения: 02.04.25). – Режим доступа : свободный.

18. Окна Трейд : Стекла триплекс – безопасность, эстетичность и высокие технологии : [официальный сайт]. – URL : <https://www.oknatrade.ru/help/stekla-tripleks-bezopasnost-estetichnost-i-vysokie-tekhnologii/> (дата обращения: 03.05.25). – Режим доступа : свободный.

19. Стекло Люкс : Стекло триплекс : [официальный сайт]. – URL : <https://steklo-luks.by/tripleks> (дата обращения: 03.05.25). – Режим доступа : свободный.

20. ОкнаМедиа : Что такое триплекс : [официальный сайт]. – URL : <https://www.okna-media.ru/novosti/chto-takoe-tripleks-48754> (дата обращения: 03.05.25). – Режим доступа : свободный.

© *Е. А. Лебедев, И. В. Парко, 2025*

К. А. Лутягин¹, С. А. Солмин¹, Н. В. Сафонова¹, Н. М. Дорохова¹✉

Резонатор Гельмгольца

¹Новосибирский электромеханический колледж,
г. Новосибирск, Российская Федерация
e-mail: natali_270168@mail.ru

Аннотация. В статье рассмотрен способ исследования резонатора Гельмгольца. Описана экспериментальная база для проведения исследования. Рассмотрена зависимость частоты от строения резонатора Гельмгольца.

Ключевые слова: резонатор Гельмгольца, частота

K. A. Lityagin¹, S. A. Solmin¹, N. V. Safonova¹, N. M. Dorokhova¹✉

Helmholtz Resonator

¹Novosibirsk Electromechanical College, Novosibirsk, Russian Federation
e-mail: natali_270168@mail.ru

Annotation. The article discusses the method of studying the Helmholtz incisor. The experimental base for conducting the study is described. The dependence of frequency on the structure of the Helmholtz resonator is considered.

Key words: Helmholtz resonator, frequency

Введение

Теория резонанса Гельмгольца используется при проектировании выхлопных труб автомобилей и мотоциклов, с целью сделать звук двигателя более тихим или более красивым, для акустического комфорта райдера и окружающих.

Если выхлопная система спроектирована так, что на рабочих оборотах появляется неприятный резонирующий звук и нет возможности внести изменения в геометрию выхлопной системы, то для устранения этого звука применяют резонатор Гельмгольца.

По сути резонатор Гельмгольца – это акустический фильтр, который подавляет определенный диапазон частот.

Для того, чтобы понять какие с помощью изменения конструкции резонатора можно воздействовать на звук мы решили воссоздать процессы, происходящие в резонаторе.

Цель: исследовать зависимость частоты в зависимости от строения резонатора Гельмгольца.

Задачи:

- найти информацию о классическом резонаторе Гельмгольца;
- разработать экспериментальную базу для проведения исследования;
- вычислить значение частоты в зависимости от изменений в строении резонатора Гельмгольца;

– теоретические вычисления подтвердить экспериментально.

Методы и материалы

Методы исследования: обобщение полученной информации, экспериментирование, анализ и сравнение, фотографирование.

Для разработки экспериментальной базы мы изучили классический опыт Гельмгольца.

Мы выяснили, что конструкция резонатора включает жесткий контейнер известного объема, почти сферической формы, с небольшим горлышком и отверстием на одном конце и большим отверстием на другом конце для выпуска звука. Один конец резонатора имеет острые края, а второй – воронкообразную форму. Основным принцип работы резонатора заключается в вибрации воздушной массы в горловине резонатора, действующей аналогично массе на пружине. Когда внешние силы, такие как воздушный поток, нарушают эту воздушную массу, она колеблется и вызывает резонирование воздуха внутри полости [1–3].

Резонансная частота колебаний резонатора Гельмгольца главным образом зависит от размера и формы горла и объема полости.

Для нашего исследования идеально подходят пластиковые бутылки, у которых можно легко изменять размеры, в зависимости от измеряемых конфигураций.

Мы исследовали зависимость частоты от строения резонатора Гельмгольца.

В первом исследовании рассмотрели зависимость частоты от высоты горлышка резонатора.

Для исследования взяли три одинаковые бутылки с разной высотой горлышка и вычислили частоту по формуле:

$$f = \frac{v}{2\pi} \sqrt{\frac{S}{LV}},$$

где v – скорость звука в газах, м/с;

S – площадь сечения горла, мм²,

L – длина горла, мм;

V – объем горла.

В ходе эксперимента мы выяснили, что чем меньше высота горлышка, тем больше частота колебаний выше. В это можно убедиться наглядно и подув на каждую бутылку.

Во втором исследовании мы рассмотрели зависимость частоты от диаметра горлышка резонатора. Высоту насадки на бутылку мы не изменяли, а меняли площадь насадки.

Для исследования зависимости частоты от объема резонатора, был проведен эксперимент с пластиковой бутылкой. Когда на ее горлышко попадает воздух, в бутылке возникают собственные колебания, которые меняют свою частоту в зависимости от объема воздуха внутри. Если в бутылку налить воду то, частота

колебаний повышается. Это иллюстрирует, как вес и объем воздуха влияют на звук. Мы выяснили, что с увеличением объема бутылки частота уменьшается.

Заключение

В результате работы над проектом мы выяснил, что такое акустический резонанс, который нашел широкое применение в машиностроении; изучили классический опыт Гельмгольца; разработали установку для демонстрации резонанса; провели исследования звукового резонанса; определили зависимость частоты от геометрических параметров резонатора Гельмгольца.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. https://vk.com/wall-172417800_769?w=wall-172417800_769 (дата обращения: 28.04.2025).
2. <https://skysmart.ru/articles/physics/yavlenie-rezonansa> (дата обращения: 20.04.2025).
3. <https://pandia.org/text/86/182/24659.php> (дата обращения: 22.04.2025).

© К. А. Литягин, С. А. Солмин, Н. В. Сафонова Н. М. Дорохова, 2025

Р. А. Ложков^{1✉}, И. В. Парко¹

Сверхлегкая оптика для наноспутника

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: Roman.Lozhkov2005@yandex.ru

Аннотация. В статье рассматриваются оптические технологии изготовления перспективных сверхлегких деталей для наноспутников. Обычные стеклянные линзы, обладая высокой оптической эффективностью, существенно ограничивают полезную нагрузку малых космических аппаратов из-за своего веса и размеров. В качестве решения было предложено использование инновационных оптических элементов на основе метаповерхностей, дифракционных линз и полимерных материалов, что позволило бы уменьшить массу оптической системы в 10–100 раз при сохранении приемлемого качества изображения. Особое внимание уделяется технологиям изготовления сверхлегких деталей, включая наноструктурирование, 3D-литографию и лазерную абляцию. Приведены конкретные примеры внедрения разработок, такие как металлическая пластина диаметром 50 мм, весом менее 5 граммов и стоимостью до 10 раз меньше обычных аналогов. Анализируются преимущества и существующие ограничения сверхлегких деталей, включая вопросы оптической эффективности и радиационной стойкости в условиях космоса. В статье также освещаются перспективы использования сверхлегкой оптики, в том числе в наноспутниковых миссиях для дистанционного зондирования Земли и научных исследований.

Ключевые слова: Наноспутник, сверхлегкая оптика, линза

R. A. Lozhkov^{1✉}, I. V. Parko¹

Ultralight optics for nanosatellite

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: Roman.Lozhkov2005@yandex.ru

Abstract. The article discusses optical technologies for manufacturing advanced ultra-light parts for nanosatellites. While conventional glass lenses offer high optical efficiency, they significantly limit the payload capacity of small spacecraft due to their weight and size. As a solution, innovative optical elements based on metasurfaces, diffraction lenses, and polymer materials have been proposed, which could reduce the mass of the optical system by 10 to 100 times while maintaining acceptable image quality. Special attention is paid to the technologies of manufacturing ultra-light parts, including nanostructuring, 3D lithography, and laser ablation. Specific examples of the implementation of developments are given, such as a metal plate with a diameter of 50 mm, weighing less than 5 grams, and costing up to 10 times less than conventional analogues. The advantages and existing limitations of ultra-light parts are analyzed, including issues of optical efficiency and radiation resistance.

Keywords: Nanosatellite, ultralight optics, lens

Введение

Современная космическая отрасль переживает революцию, связанную с миниатюризацией спутниковой техники. Наноспутники CubeSat массой 1–10 кг открывают новые возможности для мониторинга Земли, научных исследований и коммерческого использования космоса. Однако их эффективность по-прежнему

ограничивается массогабаритными характеристиками полезной нагрузки, особенно в части оптической системы. Традиционная оптика на основе стеклянных линз, обеспечивающая высокое качество изображения, занимает значительную долю массы устройства и требует сложных механических конструкций [1].

Обсуждение

В последние годы прорывные решения в области метаматериалов и нанофотоники позволили создать совершенно новые типы оптических компонентов. Сверхлегкие линзы на основе метаповерхностей, дифракционных структур и полимерных композитов демонстрируют беспрецедентное сочетание малого веса (менее 1 грамма на элемент), компактности (толщина до 0,1 мм) и приемлемой оптической эффективности (рис. 1). Особый интерес представляют разработки Самарского университета в этой области, направленные на создание специализированной оптики для российских наноспутниковых миссий [2].

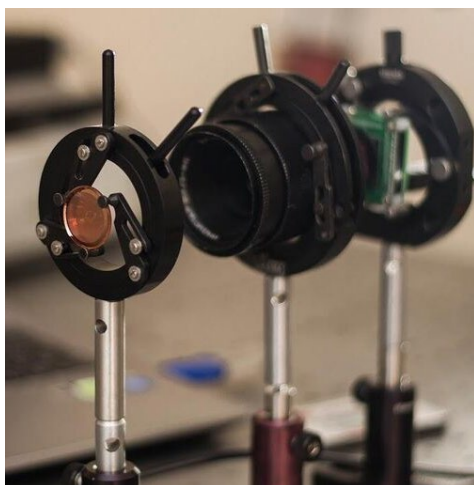


Рис. 1. Российская сверхлегкая «умная оптика»

Идея создания сверхлегкой оптики для наноспутников возникла на стыке двух ключевых тенденций: во-первых, быстрое развитие наноспутниковой технологии. В 2010 году стремительный рост коммерческого и научного интереса к малым космическим аппаратам, особенно в формате CubeSat, выявил серьезное ограничение – традиционная оптика занимает 30–50 % массы полезной нагрузки. Это существенно ограничивает возможности этих устройств в области дистанционного зондирования и астрономии. Во-вторых, прорывы в нанофотонике и метаматериалах. В это же время в научном сообществе (в частности, в работах групп Капассо (Гарвард) и Валентайна (Университет Юты) были продемонстрированы первые рабочие образцы плоских металлических линз, способных заменить трехмерные стеклянные элементы [3].

Определенный российский импульс возник в 2018–2019 годах, когда в Самарском университете стартовала программа «Космическое материаловедение». РКЦ (Ракетно-космический центр) «Прогресс» устанавливает оптические тре-

бования к перспективным наноспутникам. Появились первые публикации по радиационной стойкости полимерных метаповерхностей.

Наноспутники – компактные космические аппараты массой от 1 до 10 кг, в том числе популярного формата CubeSat, которые открывают новые возможности для исследования космоса и практического применения на орбите благодаря своей доступности и универсальности. Их основными преимуществами являются низкая стоимость (обычные спутники от 50 до 500 тысяч долларов по сравнению с десятками миллионов долларов) и короткие сроки разработки (1–3 года), что делает их идеальными для образовательных проектов, технологических экспериментов и коммерческих миссий.

В науке наноспутники используются для изучения космической погоды, наблюдения за астероидами и проведения экспериментов в условиях микрогравитации. Например, проект SPARCS использует крошечные телескопы для наблюдения за звездами в ультрафиолетовом диапазоне. В области дистанционного зондирования Земли они помогают отслеживать изменение климата, состояние сельскохозяйственных угодий и даже участвуют в картографировании, предоставляя данные для навигации и городского планирования.

Телекоммуникационные возможности наноспутников включают обеспечение связи в отдаленных районах и создание сетей Интернета вещей (IoT), таких как проект Swarm Technologies. Они стали важным инструментом образования – университеты, в том числе Самарский университет, используют CubeSats для обучения студентов и разработки новых технологий. Коммерческие компании запускают их в рекламных целях, например, для трансляции видов суши, или для сбора данных в коммерческих целях, от логистики до мониторинга рыболовства.

Военные и разведывательные службы также проявили интерес к наноспутникам, хотя их разведывательные возможности ограничены из-за их малых размеров. Их можно использовать для раннего оповещения о запусках ракет или для мониторинга зон стихийных бедствий (рис.2).

Однако у наноспутников есть и недостатки: маломощные компоненты (например, камеры с низким разрешением), короткий срок службы (1–5 лет), восприимчивость к радиации и космическому мусору. Тем не менее, их масса, масштаб и гибкость позволяют разворачивать целые группы, как в проекте Planet Labs, где более 150 устройств ежедневно отслеживают состояние Земли. Успешные примеры, такие как миссия MarCO (CubeSat НАСА, сопровождавший InSight на пути к Марсу) или российский Stork-2D, продемонстрировали, что даже микроаппараты способны решать серьезные задачи.

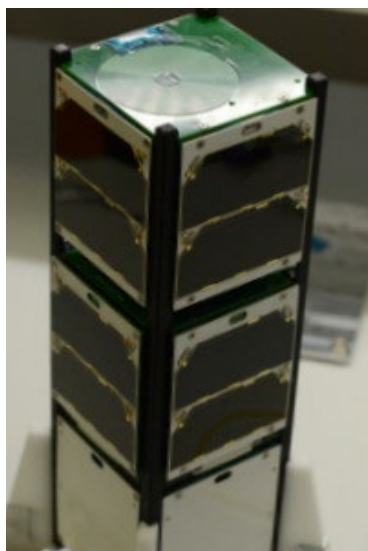


Рис. 2. Первый российский наноспутник формата CUBESAT3U

Будущее наноспутников связано с дальнейшей миниатюризацией технологий, например, внедрением сверхлегкой оптики, усовершенствованных двигателей и искусственного интеллекта для автономной работы. Их роль будет расти в проектах, где важны скорость разворачивания, децентрализация и экономическая эффективность, от научных исследований до коммерческого освоения космоса [4].

В таблице 1 представлены сравнительные характеристики разных оптических деталей.

Таблица 1

Параметры	Масса, г	Толщина, мм	Стоимость
Стеклоптическая оптика	100–500	10–50	Высокая 500–3000 долларов
Сверхлегкая оптика	1–10	0,1–1	Низкая 100–800 долларов

При сравнении традиционной стеклянной оптики и современных сверхлегких наноспутниковых решений выявляются принципиальные различия, определяющие выбор технологий для конкретных космических миссий. Стеклянная оптика на протяжении десятилетий является отраслевым стандартом, обеспечивая исключительное качество изображения в видимом диапазоне спектра с эффективностью до 90–95 % и сохраняя при этом стабильную работу в широком диапазоне температур от -100 до +100 °С. Однако эти системы имеют значительные массогабаритные показатели – одна линза весит до 500 граммов и имеет толщину до 50 мм, что для наноспутника CubeSat означает существенную потерю полезной нагрузки. Процесс изготовления стеклянной оптики требует сложной механической обработки, занимает несколько месяцев, а стоимость готового изделия колеблется от 500 до 3000 долларов за линзу.

Современные сверхлегкие оптические решения, разрабатываемые для наноспутников, базируются на принципиально иных подходах – метаповерхностях, дифракционных структурах и полимерных композитах. Данные технологии позволяют уменьшить массу оптических компонентов до 1–10 граммов и толщину всего 0,1–1 мм, что в 10–100 раз легче традиционных аналогов. Процесс производства такой системы основан на методах нанолитографии и 3D-печати, что гарантирует изготовление оптических компонентов за несколько дней или недель, а не месяцев, при стоимости от 100 до 800 долларов США. Однако нынешнее поколение сверхлегкой оптики демонстрирует эффективность 60–85 % и может потребовать дополнительной коррекции хроматической аберрации, хотя последние разработки достигли эффективности 90 % в узком спектральном диапазоне. Радиационная стойкость особенно важна, если стеклянные элементы изначально способны противостоять космическому излучению, то решения на основе полимеров и метаматериалов требуют специальных защитных покрытий. Это успешно реализуется в современных проектах, например, в разработках Самарского университета [5].

Заключение

Перспективы развития оптических систем для наноспутников указывают на постепенное вытеснение традиционных стеклянных деталей, сочетающих в себе достижения современных технологий, в ближайшие 5–10 лет ожидается появление металинз с полным спектральным охватом и возможностью автофокусировки. Качество изображения, при таких работах, как высокодетальная съемка земной поверхности, стеклянная оптика, пока сохраняет свои позиции. Для наноспутниковых проектов, определяющими факторами которых являются стоимость, скорость развертывания и эффективное использование полезной нагрузки, сверхлегкие оптические системы создают неоспоримые преимущества, открывая новые возможности для коммерческого и научного использования космического пространства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. К.П. Скворцов, "Перспективы наноспутниковых технологий", Космические исследования, т. 59, № 3, 2021, с. 45-52. DOI: 10.7868/S0023420621030061.
2. Отчет о НИР "Разработка сверхлегкой оптики для наноспутников", Самарский университет, 2022 (внутренний документ).
3. Capasso, F. et al. (2018). "Metalenses at visible wavelengths: Diffraction-limited focusing and subwavelength resolution imaging". Science, 352(6290), 1190-1194. [DOI:10.1126/science.aaf6644].
4. Образовательные наноспутники стандарта CubeSat.Статья. [Электронный ресурс]. URL: <https://www.geoscan.ru/ru/products/cubesat>.
5. Первая в мире сверхлегкая оптика для наноспутников проходит испытания в космосе. [Электронный ресурс]. URL:<https://sdelanounas.ru/blogs/140448/>.

© Р. А. Ложков, И. В. Парко, 2025

Р. А. Ложков¹✉, Д. А. Учаев¹, И. В. Парко¹

Танковая оптика

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: Roman.Lozhkov2005@yandex.ru

Аннотация. В статье рассматривается эволюция танковой оптики от первых примитивных наблюдательных щелей Первой мировой войны до современных интеллектуальных многоспектральных систем. Подробно анализируются основные этапы развития оптической техники: появление первых телескопических прицелов в 1930-х годах, внедрение инфракрасных и тепловизионных систем в послевоенный период, цифровая революция в конце XX – начале XXI века. Особое внимание уделено характеристикам современных оптико-электронных комплексов, в том числе российского комплекса «Сосна-У» для танка Т-14 «Армата», американского AN/VSG-3 и европейского ATTICA. Проведен сравнительный анализ по основным параметрам: дальность обнаружения, точность, уровень автоматизации и помехозащищенность. Рассмотрены перспективные направления развития танковой оптики, такие как гиперспектральный анализ, нейросетевые алгоритмы распознавания и создание полностью автономных систем. Статья предназначена для специалистов в области военной техники и всех интересующихся современными технологиями бронетанкового вооружения.

Ключевые слова: танковая оптика, тепловизоры, системы управления огнем, Т-14 «Армата», мультиспектральные системы, автономные боевые системы

R. A. Lozhkov¹✉, D. A. Ychaev¹, I. V. Parko¹

Tank optics

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: Roman.Lozhkov2005@yandex.ru

Abstract. The article considers the evolution of tank optics from the first primitive observation slits of the First World War to modern intelligent multispectral systems. The main stages of optical technology development are analyzed in detail: the appearance of the first telescopic sights in the 1930s, the introduction of infrared and thermal imaging systems in the post-war period, the digital revolution in the late 20th - early 21st centuries. Particular attention is paid to the characteristics of modern optical-electronic systems, including the Russian Sosna-U complex for the T-14 «Armata» tank, the American AN / VSG-3 and the European ATTICA. A comparative analysis is carried out on the main parameters: detection range, accuracy, automation level and noise immunity. Promising areas of tank optics development are considered, such as hyperspectral analysis, neural network recognition algorithms and the creation of fully autonomous systems. The article is intended for specialists in the field of military technology and anyone interested in modern armored vehicle technologies.

Keywords: tank optics, thermal imagers, fire control systems, T-14 «Armata», multispectral systems, autonomous combat systems

Введение

Танковая оптика является важнейшим элементом боевой эффективности бронетехники и за последнее столетие прошла путь от простейших смотровых

щелей до интеллектуальных многоспектральных систем. Сегодня это определяет способность обнаруживать, распознавать и поражать цели в любых условиях боя – днем и ночью, в пыли, дыму и сложных метеоусловиях. В статье подробно рассматриваются исторические этапы развития современных оптических систем, сравниваются характеристики и перспективные направления их совершенствования.

Первые танки Первой мировой войны, такие как британский Mark I (1916), вообще не имели специализированной оптики – обзор обеспечивала лишь узкая смотровая щель шириной 10–20 мм, защищенная бронированным стеклом. Это ограничивает поле зрения до 20–30 градусов, делая танк фактически «слепым» на поле боя. Значительный прогресс произошел в 1930-х годах с появлением первых оптических прицелов. В Советском Союзе для танка Т-1 был разработан телескопический прицел ТОП-26 (кратность увеличения 2,5х, поле зрения 14°). В Германии был создан прицел TZF9b для танка Pz Кpfw III с баллистическими решетками, а в США – М4 Sherman с перископом М6, хотя он не был стабилизирован [1].

Во время Второй мировой войны развитие оптики значительно ускорилось. Советский танк Т-34 получил прицел ТМФД-7 с дальностью стрельбы до 1,5 км и полем зрения 26°. Немецкий танк Tiger I был оснащен модифицированным прицелом TZF9b с дальномерной шкалой и герметичным корпусом. В этот период начались первые эксперименты в области ночного видения – немцы разработали систему FG1250 с инфракрасным прожектором и электрооптическим преобразователем, которая обеспечивала дальность видимости до 600 метров [2].

Послевоенный период (1950–1980-е годы) характеризовался переходом от простых оптических прицелов к сложным электронным системам. В 1950-х годах в Советском Союзе появился прибор ночного видения ТВН-2 с активной инфракрасной подсветкой (дальность 800 м). В 1960-х годах на танк Т-62 установили систему «Луна-ИК» с дальностью действия 1200 м, однако активная подсветка серьезно демаскировала танк. В 1970-х годах появились пассивные тепловизоры – американский AN/TAS-5 обеспечивал обнаружение целей на расстоянии до 2 км без подсветки. В 1980 году в СССР был создан тепловизор «Агава» (дальность 2,5 км), а в США – AN/VSG-2 (3 км). Одновременно были разработаны лазерный дальномер (КТД-2 на Т-62, с точностью ± 10 м на 4 км) и система стабилизации (2Э26 на Т-64, с точностью удержания цели $\pm 0,2$ мрад).

Современные танки оснащаются многоспектральными оптико-электронными комплексами, объединяющими тепловизоры 3–5 поколений, лазерные дальномеры с точностью 1 м на 5 км и цифровые системы управления огнем с элементами искусственного интеллекта.

Ярким примером современного оснащения оптико-электронными системами является российский танк Т-14 «Армата» с комплексом «Сосна-У» [3]. Он включает в себя тепловизор с дальностью обнаружения до 5 км, обеспечивает автоматическое сопровождение целей с точностью $\pm 0,05$ мрад и интегрирован с системой тактического управления ЕСУ ТК. Система «занавес» используется для предотвращения помех и подавления лазерного наведения противника.

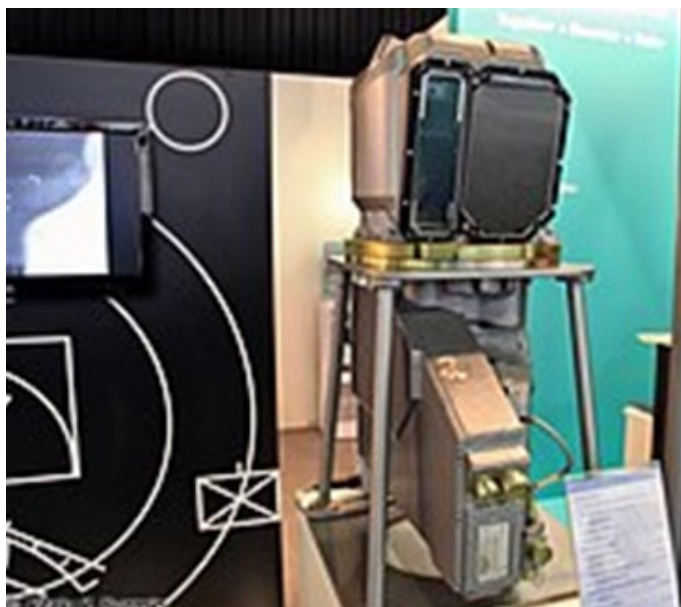


Рис.1. Прицел Сосна-У

Американский танк M1A2SEP v3 оснащен тепловизором AN/VSG-3 третьего поколения (дальность действия до 8 км) с функцией анализа угроз. В европейском Leclerc используется система ATTICA, которая имеет большую помехозащищенность.

Сравнивая современные системы, можно выделить ключевые различия, представленные в табл. 1:

Таблица 1

Параметры	Дальность	Точность	Устойчивость
Россия (Т-14)	5 км	± 1 м (5км)	«Штора»
США (M1A2)	8 км	$\pm 0,5$ м (5км)	AN/VLQ-6

Детальное сравнение современных систем выявляет интересные особенности. По дальности обнаружения лидируют американские системы (до 8 км), однако российские разработки показывают лучшие результаты в сложных условиях. Точность измерений всех систем сопоставима: лазерные дальномеры обеспечивают ± 1 м (Т-14) и $\pm 0,5$ м (M1A2) на 5 км. Российские системы ориентированы на автономность и ремонтпригодность, тогда как западные системы – на сетцентрические решения и универсальность [4, 5].

Заключение

История развития танковой оптики является ярким примером технического прогресса в военной сфере. За столетие эти системы прошли путь от простых наблюдательных щелей до интеллектуальных многоспектральных комплексов,

ставших неотъемлемой частью современных танков. Сегодня танковая оптика определяет не только возможности обнаружения и поражения целей, но и общую боевую эффективность бронетанковых подразделений в различных условиях боя. Однако российские танкостроители сталкиваются с серьезными проблемами. Зависимость от импортных комплектующих, особенно в области микроэлектроники и тепловизионных матриц, требует ускоренной разработки собственных технологий. Не менее важна работа по совершенствованию алгоритмов цифровой обработки изображений и интеграции оптических систем в единое информационное пространство. Будущее танковой оптики прогнозируется в создании адаптивных многофункциональных систем, способных не только предоставлять экипажу информацию, но и самостоятельно принимать тактические решения. В течение следующего десятилетия предполагается появление принципиально новых инженерных решений, которые кардинально изменят восприятие возможностей бронетехники. Для России сохранение и укрепление позиций в этой отрасли оборонной промышленности имеет стратегическое значение и определяет обороноспособность страны на десятилетия вперед.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. С.Л. Федосеев танк в бою. Эволюция бронетанковой техники 1916-2020. М.: Эксмо, 2020. 352с.
2. М.Н. Свирин Бронешит Сталина. История советских танков 1937-1943. — М.: Яуза, 2020. -672 с.
3. И.Г. Желтов., М.В. Павлов, И.В. Павлов Танки «Армата» и другие перспективные машины // Техника и вооружение. - 2018. -№5. — Страницы 12-19.
4. Официальный сайт АО «НПК «Уралвагонзавод» [электронные ресурсы]. — Сайт: <https://uvz.ru> / (дата обращения: 10.06.2024).
5. Jane's Defence Weekly: Модернизация оптики миссии [Электронный ресурс]. —Сайт: <https://www.janes.com> / (дата обращения: 10.06.2024).

Р. А. Ложков, Д. А. Учаев, И. В. Парко, 2025

С. А. Лысенко^{1✉}, К. С. Юшков¹, Е. В. Рыжкова¹

Чат-бот как средство повышения киберграмотности учащихся посредством интерактивных заданий

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: stepan.nepryahin@gmail.com

Аннотация. В условиях стремительного роста киберугроз и отсутствия доступных, вовлекающих образовательных ресурсов в области информационной безопасности (ИБ) возникает необходимость в разработке интерактивных инструментов для эффективного освоения базовых принципов защиты данных. Актуальность приобретает среди учащихся, для которых традиционные методы обучения часто оказываются недостаточно мотивирующими. Данная работа направлена на решение этой проблемы посредством создания специализированного чат-бота, интегрированного в популярный мессенджер Telegram. Такой подход сочетает структурированное теоретическое обучение с практическими игровыми механиками, способствуя лучшему усвоению материала. Разработанный чат-бот «СекьюрБот» наглядно демонстрирует, как геймификация в доступной цифровой среде может преобразовать процесс изучения основ кибербезопасности, повышая цифровую грамотность пользователей. Результатом внедрения подобных решений становится эффективное усвоение ключевых концепций информационной безопасности через интерактивные форматы обучения, что приобретает особую значимость в условиях постоянного усложнения киберугроз.

Ключевые слова: чат-бот, информационная безопасность, обучение, геймификация, Telegram, интерактивное обучение

S. A. Lysenko^{1✉}, K. S. Yushkov¹, E. V. Ryzhkova¹

Chatbot as a means of increasing students' cyber literacy through interactive tasks

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: stepan.nepryahin@gmail.com

Annotation. With the rapid growth of cyber threats and the lack of accessible, engaging information security (IS) education resources, there is a need to develop interactive tools to effectively master the basic principles of data protection. The relevance is gained among students for whom traditional learning methods are often insufficiently motivating. This paper aims to address this problem by creating a specialised chatbot integrated into the popular messenger Telegram. This approach combines structured theoretical learning with practical game mechanics, facilitating better learning. The developed chatbot "SecureBot" clearly demonstrates how gamification in an accessible digital environment can transform the process of learning the basics of cyber security, increasing the digital literacy of users. The implementation of such solutions results in the effective learning of key information security concepts through interactive learning formats, which is especially important in the context of the ever-increasing complexity of cyber threats.

Keywords: chatbot, information security, learning, gamification, Telegram, interactive learning

Введение

В условиях цифровизации и роста киберугроз владение базовыми знаниями ИБ критически важно. Существующие образовательные ресурсы часто не обеспечивают комплексный и интерактивный подход. В ответ на это будет разработана система «СекьюрБот» – Telegram-бот с новым интегрированным подходом к обучению основам ИБ. Он сочетает получение теоретических знаний (интерактивная книга) с активной тренировкой специфических знаний (терминология, аббревиатуры, даты, факты) через игровые механики (квизы, мини-игры) [1, 2].

Цель работы – разработка интерактивного Telegram-бота для обучения основам ИБ, сочетающего лекционный контент с геймификацией для тренировки и проверки знаний.

Для достижения цели были поставлены задачи:

- разработка структуры и контента электронной книги;
- выделение категорий специфических знаний ИБ;
- проектирование и реализация игровых механик;
- создание системы управления контентом;
- разработка системы отслеживания прогресса (статистика, достижения, рейтинги);
- выбор и реализация технологической основы (Python, Telegram).

Теоретическая значимость – исследование эффективности сочетания теории и игр в обучении через бота.

Практическая значимость – создание функционального бота «СекьюрБот» как инструмента для самостоятельного изучения ИБ и тренировки ключевых понятий.

Методы и материалы

Основным методом в процессе разработки являлся итеративный подход, включающий последовательное планирование, проектирование, реализацию, тестирование и доработку отдельных модулей бота (регистрация, профиль, игры, книга, инструменты). Такой подход позволил поэтапно наращивать функциональность, оперативно выявлять и устранять ошибки, а также вносить коррективы в логику работы на основе промежуточных результатов [3].

При разработке игровых модулей использовался метод структурного проектирования, при котором каждая игра рассматривалась как отдельный компонент со своей логикой генерации заданий, обработки ответов пользователя и обновления статистики. Для игр-квизов с вариантами ответов применялся метод случайной выборки заданий и вариантов ответов из общей базы данных, с обязательным включением одного правильного ответа [4].

Разработка обучающего модуля «Книга» основывалась на методе структурирования контента, при котором исходный материал разбивался на логические главы и страницы с продуманной системой навигации.

Эффективность обучающего и игрового функционала оценивалась на этапе тестирования путем ручного тестирования различных пользовательских сценариев и проверки корректности работы механик, начисления баллов и обновления статистики.

В качестве программных материалов использовались:

1. Язык программирования Python (версия 3.13): выбран как основной язык для реализации серверной логики бота благодаря его гибкости, обширным библиотекам и простоте синтаксиса [5];

2. Библиотека py Telegram Bot API (Telebot) (рисунок 1): применялась для обеспечения взаимодействия бота с TelegramBot API, обработки входящих сообщений, команд и callback-запросов, а также для отправки сообщений и управления клавиатурами [6–8];

3. Библиотека pytz (рис. 1): использовалась для корректной работы с часовыми поясами (в частности, для привязки даты регистрации и времени сброса квестов к московскому времени);

4. Стандартные библиотеки Python: активно применялись для работы с данными (jsonorsqlite3), файловой системой (os), датой и временем (datetime), генерации случайных элементов (random) и обработки текста (re, io) [9, 10];

5. Библиотека PIL (Pillow, рис. 1): использовалась для работы с изображениями в модуле стеганографии [8].

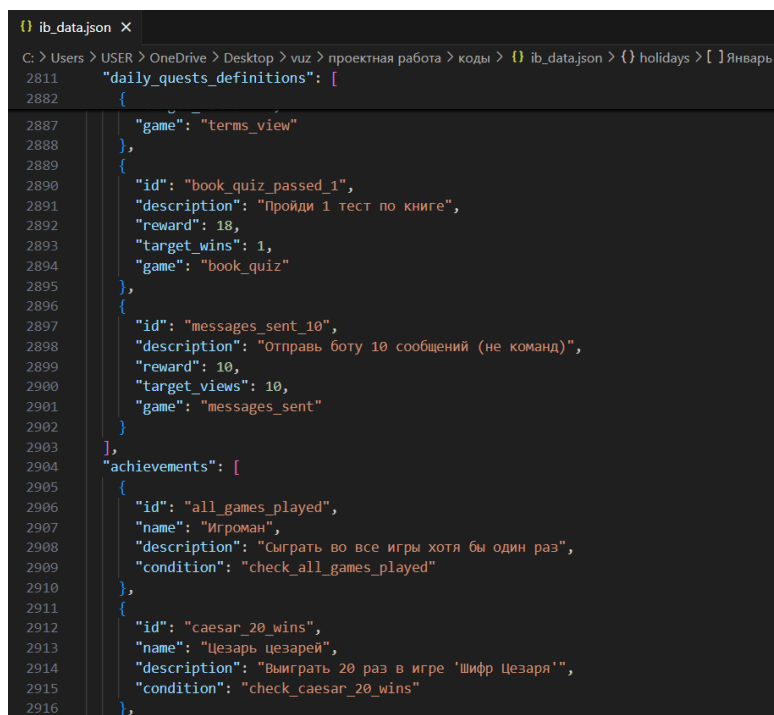
```
1  import telebot
2  import datetime
3  import random
4  import json
5  import os
6  import pytz
7  import re
8  from PIL import Image, ImageDraw, ImageFont
9  from io import BytesIO
```

Рис. 1. Библиотеки для бота

В качестве информационных материалов (данных) использовались данные, структурированные в формате JSON и хранимые в следующих файлах:

1. `user\_data.json`, в нем содержались данные о зарегистрированных пользователях, включая их никнеймы, идентификаторы, даты регистрации, текущий баланс, уровень и очки уровня, статистику по каждой игре, состояние ежедневных заданий, информацию о достижениях и последнюю прочитанную страницу книги [9];

2. `ib\_data.json`, в данном формате файла находилась база данных для различных игровых и развлекательных модулей, таких как факты, цитаты, термины, праздники, задания для игр "Шифр Цезаря", "Анаграмма" (уровни 1 и 2), "Аббревиатура", "Правда/Ложь", "Даты по ИБ", "ИБ-Викторина", "Поиск смысла", правила игры "Нормативы", определения достижений и ежедневных заданий (рис. 2) [6, 11, 12];



```
{} ib_data.json X
C: > Users > USER > OneDrive > Desktop > vuz > проектная работа > коды > {} ib_data.json > {} holidays > [ ] Январь
2811 "daily_quests_definitions": [
2882 {
2887   "game": "terms_view"
2888 },
2889 {
2890   "id": "book_quiz_passed_1",
2891   "description": "Пройди 1 тест по книге",
2892   "reward": 18,
2893   "target_wins": 1,
2894   "game": "book_quiz"
2895 },
2896 {
2897   "id": "messages_sent_10",
2898   "description": "Отправь боту 10 сообщений (не команд)",
2899   "reward": 10,
2900   "target_views": 10,
2901   "game": "messages_sent"
2902 }
2903 ],
2904 "achievements": [
2905 {
2906   "id": "all_games_played",
2907   "name": "Игрома",
2908   "description": "Сыграть во все игры хотя бы один раз",
2909   "condition": "check_all_games_played"
2910 },
2911 {
2912   "id": "caesar_20_wins",
2913   "name": "Цезарь цезарей",
2914   "description": "Выиграть 20 раз в игре 'Шифр Цезаря'",
2915   "condition": "check_caesar_20_wins"
2916 },
2917 ]
```

Рис. 2. Содержимое файла ib_data.json

3. `learning\_modules\_data.json`, содержался контент обучающего модуля "Книга", разбитый на страницы с текстовым содержанием, заголовками и ссылками для навигации между страницами.

Контент для файлов ib_data.json и learning_modules_data.json собирался и адаптировался на основе открытых источников и учебных материалов по информационной безопасности, в частности, программы вуза СГУГиТ. При создании контента для игр учитывались требования к формату данных для корректной работы логики упражнений (например, разделение на вопрос/ответ, слово/анаграмма, аббревиатура/полная форма и т.д.) [13].

Результаты

В ходе выполнения работы был разработан и реализован функциональный прототип обучающего чат-бота «СекьюрБот» на платформе Telegram. Ключевыми результатами проекта являются следующие реализованные компоненты [14]:

1. Программный каркас бота: разработана серверная логика бота на языке Python с использованием библиотеки Telebot для взаимодействия с пользователями

[15]. Обеспечено сохранение и загрузка данных пользователей, контента игр и обучающих материалов из файлов формата JSON [9]. Реализована система управления состояниями пользователей;

2. Система управления пользователями и прогрессом: внедрена функция регистрации новых пользователей и ведение индивидуальных профилей. Разработана система учета баланса виртуальной валюты (HackCoin), уровней пользователя (на основе очков уровня), игровой статистики (сыграно, побед, поражений для каждой игры), ежедневных заданий и достижений. Реализованы пользовательские рейтинги по основным метрикам [3];

3. Обучающий модуль: создан интерактивный раздел "Книга" со структурированным по страницам контентом по основам ИБ и возможностью постраничной навигации, включая сохранение последней прочитанной страницы [16];

4. Игровой модуль: реализован набор из 11 различных интерактивных игр: "Угадай автора", "Шифр Цезаря", "Числовой шифр", "Нормативы", "Анаграмма", "Аббревиатура", "Шифр Энигма", "Даты по ИБ", "Правда/Ложь", "ИБ-Викторина", "Поиск смысла". Игры используют форматы текстовых квизов и выбор с помощью Inline-кнопок для тренировки специфических знаний и навыков в области ИБ (рис. 3) [3, 11, 13, 17];

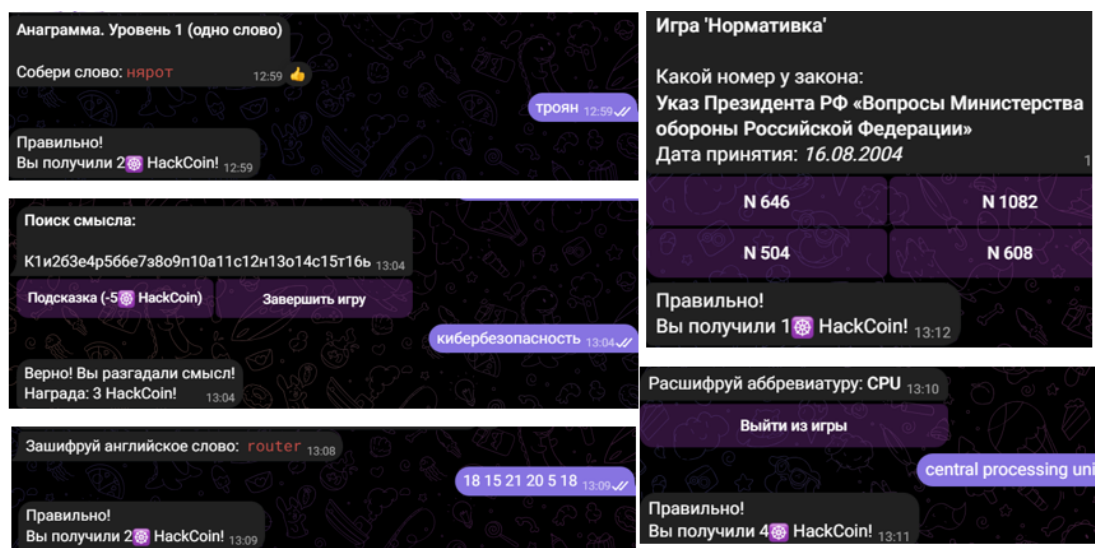


Рис. 3. Мини-квизы

5. Инструментальный модуль: внедрен практический инструмент для работы с шифром Энигма (шифратор/дешифратор) [18];

6. Информационные разделы: добавлены функции для предоставления случайных фактов, цитат, информации о праздниках, терминов по категориям, ИБ-советов, баек, исторических фактов и полезных ссылок, загружаемых из баз данных.

Таким образом, создан многофункциональный Telegram-бот, предоставляющий инструментарий для интерактивного и геймифицированного освоения базовых знаний и навыков в области информационной безопасности.

Заключение

В результате выполненной работы успешно разработан прототип обучающего чат-бота «СекьюрБот» на платформе Telegram. Данный инструмент представляет собой эффективное и актуальное решение для повышения базовых знаний в области информационной безопасности в условиях усиливающихся цифровых угроз. Ключевым достижением проекта является создание доступной и вовлекающей интерактивной среды, где пользователи могут получать теоретические знания и закреплять практические навыки ИБ через разнообразные игровые упражнения. Преимущества «СекьюрБот», такие как повсеместная доступность через популярный мессенджер Telegram без необходимости установки дополнительного программного обеспечения и высокая мотивация пользователей за счет интеграции элементов геймификации, делают его ценным инструментом для массового обучения.

Таким образом, разработанный бот вносит значимый вклад в создание инновационных образовательных ресурсов по информационной безопасности, способствуя формированию цифровой культуры и повышению киберграмотности населения, особенно среди молодежи. Дальнейшее развитие проекта будет направлено на расширение контента и углубление интерактивных возможностей для более полного охвата тематики ИБ [19, 20].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.
2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. – СПб: СПбНИУИТМО, 2014. – 173 с.
3. Нейронная сеть «Сэм» [Электронный ресурс] // Telegram. – URL: <https://web.telegram.org/k/#@SamGPTrobot> (Дата обращения: 20.04.2025)
4. Рамальо, Л. Python. К вершинам мастерства / Л. Рамальо; под редакцией А. А. Слинькина. – Москва: ДМК Пресс, 2016. – 768 с.
5. Официальная документация Python [Электронный ресурс]. – 2025. – URL: <https://docs.python.org/3/> (Дата обращения: 22.01.2025).
6. Ван Хорн, Б. М. II, Нгуен К. PyCharm: профессиональная работа на Python. – Москва, 2025. – 37 с.
7. Как сделать бота в Телеграм: пошаговая инструкция [Электронный ресурс] // vc.ru. – 2022. – URL: <https://vc.ru/dev/530248-kak-sdelat-bota-v-telegram-poshagovaya-instrukciya> (Дата обращения: 08.01.2025).
8. Официальная документация Pillow [Электронный ресурс]. – 2025. – URL: <https://pillow.readthedocs.io/en/stable/> (Дата обращения: 01.04.2025).
9. Документация по JSON [Электронный ресурс] : официальный сайт. – 2025. – URL: <https://www.json.org/json-en.html> (Дата обращения: 08.02.2025).
10. Что такое SQLite и зачем она нужна? [Электронный ресурс] // UNETWAY. – 2024. – URL: <https://unetway.com/tutorial/sqlite> (Дата обращения: 04.03.2025).
11. Глоссарий [Электронный ресурс] // Safe-Surf. – URL: <https://safe-surf.ru/glossary/ru/> (Дата обращения: 14.04.2025).
12. Чертопруд, С. В. Законодательные акты по защите гостайны в Российской империи в начале XX века // Вопросы защиты информации. – М., 1996. – № 4 (35)

13. Горбатов, В. С., Кондратьева Т. А. Информационная безопасность. Основы правовой защиты : учеб. пособие. – М.: МИФИ(ТУ), 1995.
14. Инструкция: как создавать ботов в Telegram [Электронный ресурс] // Habr. – 2015. – URL: <https://habr.com/ru/articles/262247/> (Дата обращения: 15.01.2025).
15. Официальная документация pyTelegramBotAPI (Telebot) [Электронный ресурс]. – 2025. – URL: <https://pytba.readthedocs.io/en/latest/install.html> (Дата обращения: 20.02.2025).
16. Нормативные правовые акты по защите государственной тайны : сборник документов. В 2 ч. – М., 1998.
17. Об информации, информатизации и защите информации : Закон Российской Федерации. – Собр. законодательства РФ. – 1995. – № 8. – Ст. 21.
18. Иванов, А. З. Алгоритмы криптографических преобразований: учеб. пособие по курсу "Информационная безопасность компьютерных систем" для студентов... – М.: Изд-во МЭИ, 2003.
19. Жигулин, Г. П., Новосадов С. Г., Яковлев А. Д. "Информационная безопасность". – СПб., 2003.
20. Шерстюк, В. П. МГУ: научные исследования в области информационной безопасности // Информационное общество. – 2005. – № 1.

© С. А. Лысенко, К. С. Юшков, Е. В. Рыжкова 2025

Е. А. Малеш^{1✉}, Г. В. Симонова¹

Входной контроль средств допускового контроля на соответствие установленным требованиям

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: ekaterina.malesh.2001@mail.ru

Аннотация. Для контроля формы на предприятиях применяются калибры, которые получили название средства допускового контроля (СДК). Проблемой является обеспечение более точного входного контроля средств допускового контроля с минимальным износом. Цель исследования: выявить является ли бесконтактный метод измерения точнее, чем контактный. Обработка результатов измерений калибр-пробки показала, что самым точным методом измерений является контактный метод, несмотря на то, что он приводит к постепенному износу СДК.

Ключевые слова: средства допускового контроля, износ, средства измерения

E. A. Malezh^{1✉}, G. V. Simonova¹

Input control of access control equipment for compliance with established requirements

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: ekaterina.malesh.2001@mail.ru

Annotation. Calibers are used in enterprises to control the shape, which are called tolerance control tools (TCTs). The problem is to ensure more accurate input control of tolerance control tools with minimal wear. The purpose of the study is to determine whether the non-contact measurement method is more accurate than the contact method. The processing of the results of the calibration plug measurements showed that the contact method is the most accurate measurement method, despite the fact that it leads to gradual wear of the TCT.

Keywords: means of tolerance control, wear, measuring instruments

Введение

В практике оценки соответствия продукции нормативным требованиям не всегда используются только измерительные процессы. Для контроля формы поверхности на предприятиях применяются калибры, которые получили название средства допускового контроля (далее СДК). Проблемой поставленной в данной работе является обеспечение более точного входного контроля самих средств допускового контроля с минимальным износом.

Актуальность данной работы обусловлена необходимостью в качественном входном контроле СДК.

Цель данной работы – выявить является ли бесконтактный метод измерения точнее, чем контактный.

Задачи, решаемые в работе:

- рассмотреть принцип работы СДК;

- провести контроль калибра с помощью трех различных средств измерений;
- обработать результаты измерений и выявить самый точный метод измерения.

Методы и материалы

Средства допускового контроля не являются средствами измерений. Они не поверяются, не калибруются, а контролируются, проверяются на соответствие ГОСТам, чертежам, с установленной периодичностью. Они предназначены для проверки соответствия размеров изделий или их конфигураций установленным допускам.

Существует разнообразие СДК, например: пробки, скобы, кольца, втулки. СДК на предприятии используют активно на нескольких этапах проверки качества изделия, когда идет большой поток изделий, массовое производство, то не совсем целесообразно использовать средства измерений. Калибрами гораздо быстрее проверить удовлетворяет ли размер поле допуска [1–4].

Проверку объекта с помощью СДК осуществляют контактным методом. Также и входной контроль самих СДК проводят контактным методом. Контактный метод основан на том, что элемент прибора входит в контакт с объектом измерения. Например, контроль диаметра вала скобой. В результате этой процедуры в месте контакта искажаются свойства, как контактного инструмента, так и исследуемого объекта.

Было предложено провести измерения основных размеров калибр-пробок контактным и бесконтактным методом, чтобы сравнить полученные результаты и выявить является ли бесконтактный метод точнее.

Для измерений были использованы:

- скоба рычажная СР-25;
- машина видеоизмерительная серии Quick Vision и MiSCAN;
- установка для измерения параметров валом TESA SKAN 50.

В качестве объекта измерений была выбрана калибр-пробка Б32-3902 p/n-не 9,86.

Было проведено три измерения размера $9,862_{-0,003}$ каждым средством измерения. Полученные результаты измерений с помощью рычажной скобы представлены в таблице 1.

Таблица 1

Результаты измерений с помощью рычажной скобы

Измерение	Фактическое значение, мм	$\bar{X}$, мм	Δ^2_i , мм ²	Сумма Δ^2_i , мм ²	δ , мм	$\Delta_{сл}$, мм	$X_{рез.} \pm \Delta$, мм
X_1	9,859	9,86	-0,0013	0,0009	0,002	0,003	$9,860 \pm 0,003$

Окончание таблицы 1

Измерение	Фактическое значение, мм	Хср, мм	Δ^2_i , мм ²	Сумма Δ^2_i , мм ²	δ , мм	$\Delta_{сл}$, мм	$X_{рез.} \pm \Delta$, мм
X_2	9,860	9,86	-0,0003				
X_3	9,862	9,86	0,0017				

Полученные результаты измерений с помощью видеоизмерительной машины представлены в таблице 2.

Таблица 2

Результаты измерений с помощью видеоизмерительной машины

Измерение	Фактическое значение, мм	Хср, мм	Δ^2_i , мм ²	Сумма Δ^2_i , мм ²	δ , мм	$\Delta_{сл}$, мм	$X_{рез.} \pm \Delta$, мм
X_1	9,848	9,72	0,13	0,129	0,224	0,412	9,720±0,412
X_2	9,846	9,72	-0,26				
X_3	9,848	9,72	0,13				

Полученные результаты измерений с помощью установки TESA SKAN 50 представлены в таблице 3.

Таблица 3

Результаты измерений с помощью установки TESA SKAN 50

Измерение	Фактическое значение, мм	Хср, мм	Δ^2_i , мм ²	Сумма Δ^2_i , мм ²	δ , мм	$\Delta_{сл}$, мм	$X_{рез.} \pm \Delta$, мм
X_1	8,863	8,87	-0,003	0,002	0,004	0,007	8,870±0,007
X_2	8,865	8,87	-0,001				
X_3	8,870	8,87	0,004				

Обсуждение

Обработка результатов показала, что самым точным методом измерений является контактный метод, не смотря на то, что он приводит к постепенному износу СДК. Результаты измерений с помощью видеоизмерительной машины и

установки TESA SKAN 50 были занижены и не вошли в допуск. Погрешность результатов измерений с использованием рычажной скобы составила 0,003 мм, что соответствует требованиям чертежа.

Проанализировав принцип работы СДК, влияющие факторы на износ, например, усилие, приложенное персоналом при использовании СДК, контактный метод измерений. Были предложены следующие способы снижения износа, не изменяя метод измерений:

- подготовка персонала и создание соответствующей нормативной документации, позволяющие снизить риски контрольных операций;
- обратить внимание на требования к хранению СДК.

Заключение

Контактный способ используется предприятием на постоянной основе, измерения с помощью ВИМ проводят пока что только на плоских калибрах. Но с развитием технологий, контактные методы, наносящие износ, точно будут заменяться. А бесконтактные методы, не дающие необходимой точности при измерении калибров-пробок будут совершенствоваться.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Описание типа средств измерений. Машины видеоизмерительные серий Quick Vision и MiSCAN : описание типа; утверждено 27.04.2021. , 2021. – 13 с. – Текст : непосредственный.
2. Описание типа средств измерений. Установки для измерений параметров валов TESA SCAN : описание типа; утверждено 27.04.2015. , 2015. – 6 с. – Текст : непосредственный.
3. ГОСТ 24851-81 Калибры гладкие для цилиндрических отверстий и валов. Виды. Виды : межгосударственный стандарт ; введен 23.06.1981. – Москва : Издательство стандартов, 1982. – 12 с. – Текст : непосредственный.
4. МИ 1927-88 Калибры гладкие для цилиндрических отверстий и валов. Методика контроля. Виды : межгосударственный стандарт ; введен 01.02.1989. – Москва : Издательство стандартов, 1989. – 16 с. – Текст : непосредственный.

© Е. А. Малёж, Г. В. Симонова, 2025

А. Ф. Миннимухаметова^{1✉}, Е. В. Рыжкова¹

Статический и динамический анализ: два инструмента для идеального кода

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: minnimuhametovaalina@yandex.ru

Аннотация. В статье приведены результаты исследований методов статического (SAST) и динамического (DAST) анализа кода, их преимущества и ограничения. Актуальность темы связана с ростом уязвимостей в ПО, особенно при использовании сторонних компонентов. Цель работы – показать, что комбинированное применение SAST и DAST повышает безопасность ПО. Для анализа использовались инструменты PVS-Studio (SAST) и OWASP ZAP (DAST). Результаты представлены в сравнительной таблице, где выделены ключевые различия методов. Инструменты PVS-Studio (SAST) и OWASP ZAP (DAST) доказали свою эффективность в выявлении различных классов уязвимостей: от ошибок в исходном коде. В ходе работы был сделан основной вывод, что совместное использование SAST и DAST обеспечивает более надежную защиту ПО. Исследование подчеркивает важность интеграции обоих подходов в процесс разработки.

Ключевые слова: динамический анализ, статический анализ, код

A. F. Minnimuhametova^{1✉}, E. V. Ryzhkova¹

Static and dynamic analysis: two tools for perfect code

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: minnimuhametovaalina@yandex.ru

Abstract. The article presents the results of research on static (SAST) and dynamic (DAST) code analysis methods, their advantages, and limitations. The relevance of this topic is related to the increasing number of vulnerabilities in software, especially when using third-party components. The goal of this work is to demonstrate that the combined use of SAST and DAST enhances software security. The analysis was conducted using the PVS-Studio (SAST) and OWASP ZAP (DAST) tools. The results are presented in a comparative table, highlighting the key differences between the methods. The PVS-Studio (SAST) and OWASP ZAP (DAST) tools have proven to be effective in identifying various classes of vulnerabilities: from errors in the source code. The main conclusion of the work is that the combined use of SAST and DAST provides more reliable software protection. The study highlights the importance of integrating both approaches into the development process.

Keywords: dynamic analysis, static analysis, code

Введение

В современном цифровом мире программное обеспечение стало основой технологического прогресса, управляя критически важными системами – от финансовых операций до медицинского оборудования и промышленных процессов [1]. Однако по мере усложнения программных систем растут и связанные с ними риски безопасности [2].

Актуальные исследования показывают тревожную статистику:

- более 50 % веб-приложений содержат уязвимости высокой и средней степени опасности [3];
- в 91 % случаев внутреннего тестирования злоумышленники успешно получали контроль над доменами и доступ к критическим системам [3].

Серьезным вызовом безопасности стало повсеместное использование сторонних библиотек и компонентов. Заимствованный код часто содержит скрытые уязвимости и недокументированные возможности (НДВ), которые сложнее обнаружить, чем дефекты собственного кода. Особую опасность представляют:

- умышленно внедренные уязвимости в популярных библиотеках [4];
- поддельные пакеты в репозиториях (typosquatting атаки);
- устаревшие версии компонентов с известными уязвимостями.

Для противодействия этим угрозам применяется тестирование безопасности приложений (AST), которое позволяет выявлять уязвимости на ранних этапах разработки и контролировать качество сторонних компонентов [5, 6].

Эффективное AST требует комплексного подхода, сочетающего статический (SAST) и динамический (DAST) анализ [6]:

- SAST выявляет уязвимости в исходном коде до запуска приложения;
- DAST тестирует работающую систему, имитируя действия злоумышленников.

Цель исследования – рассмотреть и сравнить два ключевых подхода к анализу кода – статический (SAST) и динамический (DAST), продемонстрировать их важность в создании безопасного и качественного программного обеспечения, а также показать, как их совместное использование способствует достижению «идеального кода» – надежного, эффективного и свободного от уязвимостей.

В работе будут рассмотрены:

- терминология статического и динамического анализов;
- принципы и инструменты каждого метода;
- типы обнаруживаемых уязвимостей инструментами;
- преимущества комбинированного подхода.

Поставленные задачи:

- провести сравнительный анализ SAST и DAST – оценка преимуществ и ограничений каждого подхода;
- провести практическое тестирование кодов с применением инструментов статического и динамического анализов.

Результаты помогут специалистам осознать, что для разработки безопасного ПО важно применять оба подхода в комплексе.

Методы и материалы

Статический анализ кода (SAST – Static application security testing) – это процесс выявления недочетов, ошибок и потенциальных уязвимостей в исходном коде программ [7].

SAST моделирует работу приложения, анализируя, как исходный код, библиотеки, платформы и компоненты взаимодействуют между собой и как они будут функционировать при запуске. Этот метод также называют тестированием по принципу «белого ящика», поскольку анализ проводится «изнутри» приложения, и о его структуре известно заранее [8].

Динамический анализ кода (DAST – Dynamic Application Security Testing) – это автоматизированное тестирование, которое проводится в реальном времени на запущенном приложении или веб-сервисе для выявления уязвимостей безопасности [9]. Механизмы DAST имитируют атаки на работающее приложение, чтобы обнаружить такие проблемы, как межсайтовый скриптинг (XSS), подделка межсайтовых запросов (CSRF), SQL-инъекции и небезопасные конфигурации.

Поскольку инструменты DAST работают без доступа к исходному коду, этот метод также называют тестированием по принципу «черного ящика» [10].

Традиционные инструменты DAST анализируют только внешнее поведение приложения, например, его пользовательский интерфейс и веб-службы, не затрагивая внутреннюю логику работы [11]. Это ограничивает их способность обнаруживать уязвимости, связанные с внутренними компонентами приложения.

В ходе исследования для анализа безопасности кода были выбраны инструменты статического (SAST) и динамического (DAST) анализа:

- PVS Studio – статический анализатор, выявляющий ошибки на этапе разработки [12];

- OWASP ZAP – инструмент динамического тестирования, имитирующий атаки на работающее приложение [13].

PVS Studio проводит глубокий анализ исходного кода, обнаруживая:

- ошибки памяти: утечки, разыменованние нулевых указателей [12];
- логические дефекты: выход за границы массива, некорректные условия [12];

- потенциальные уязвимости: неправильная обработка данных, ошибки синхронизации;

- оптимизационные проблемы: избыточные вычисления, неэффективные алгоритмы.

Преимущество SAST – раннее обнаружение ошибок до запуска программы, что снижает затраты на исправление [11].

OWASP ZAP тестирует приложение в реальном времени, выявляя:

- уязвимости веб-приложений: SQL-инъекции, XSS, CSRF;

- проблемы аутентификации и авторизации;

- небезопасные настройки сервера и API [14].

DAST полезен для проверки поведения системы в условиях, близких к реальным.

Результаты

В ходе работы была построена сравнительная таблица 1 двух методов анализа – статического и динамического.

Сравнительная таблица SAST и DAST

Критерий	Статический анализ (SAST)	Динамический анализ (DAST)
Принцип работы	Анализ исходного кода без его выполнения	Тестирование работающего приложения в реальном времени
Этап применения	На стадии разработки	На стадии тестирования/эксплуатации
Полный обзор кодовой базы	Анализирует весь исходный код	Проверяет только исполняемые пути
Анализ неисполняемого кода	Находит неиспользуемые функции	Использует только код, который выполняется в тестах
Автоматизация	Легко интегрируются	Требуется подготовка тестовой среды
Типы ошибок	Выявляет синтаксические и логические ошибки	Обнаруживает ошибки времени выполнения
Время выполнения	От нескольких минут до нескольких часов, так как не требует выполнения программы	От нескольких часов до нескольких дней, так как зависит от покрытия тестами
Ложные срабатывания	Инструменты могут ошибочно указывать на несуществующие уязвимости	Исключены

Работа PVS-Studio представлена на рисунке 1, где продемонстрирован пример кода, содержащий две ошибки и показывающий возможности PVS-Studio в анализе потока данных.

Во-первых, код содержит опечатку, из-за которой в переменную «а» дважды подряд записываются адреса двух выделенных буферов памяти. Это приводит к потере одного указателя, и анализатор предупреждает об утечке памяти. Еще одно последствие опечатки – разыменование нулевого указателя внутри функции «use» [15].

Во-вторых, память была выделена с помощью оператора «new», а освобождается с помощью вызова функции «free». Это может привести к утечке ресурсов, также будет некорректный вывод внутренних указателей [15].



Рис. 1. Результат работы инструмента статического анализа PVS Studio

Результат работы инструмента динамического анализа – Owasp Zap представлен на рис 2.

Изображен фрагмент отчета динамического анализатора OWASP ZAP, демонстрирующий три критичных проблемы безопасности веб-приложения.

Первая ошибка – это утечка SQL-кода. В ходе тестирования обнаружено, что сервер при обработке POST-запроса к `/login` возвращает фрагмент SQL-запроса: `SELECT username, password FROM users WHERE username`. Это свидетельствует о двух потенциальных проблемах:

- раскрытие структуры базы данных, что упрощает проведение SQL-инъекций;
- возможная утечка исходного кода через сообщения об ошибках.

Анализатор также указывает на CWE-540 (уязвимость раскрытия конфиденциальной информации в исходном коде) и рекомендует:

- запретить вывод SQL-запросов в ошибках;
- проверить конфигурацию сервера на случайную отдачу исходников.

Вторая ошибка – подробные ошибки сервера. При запросе к тому же эндпоинту сервер возвращает HTTP 500 с полным стеком вызова, что:

- раскрывает внутреннюю структуру приложения;
- может содержать чувствительную информацию (пути к файлам, версии компонентов).

Третья – отсутствие security-заголовков. Отчет отмечает отсутствие критически важных заголовков безопасности.

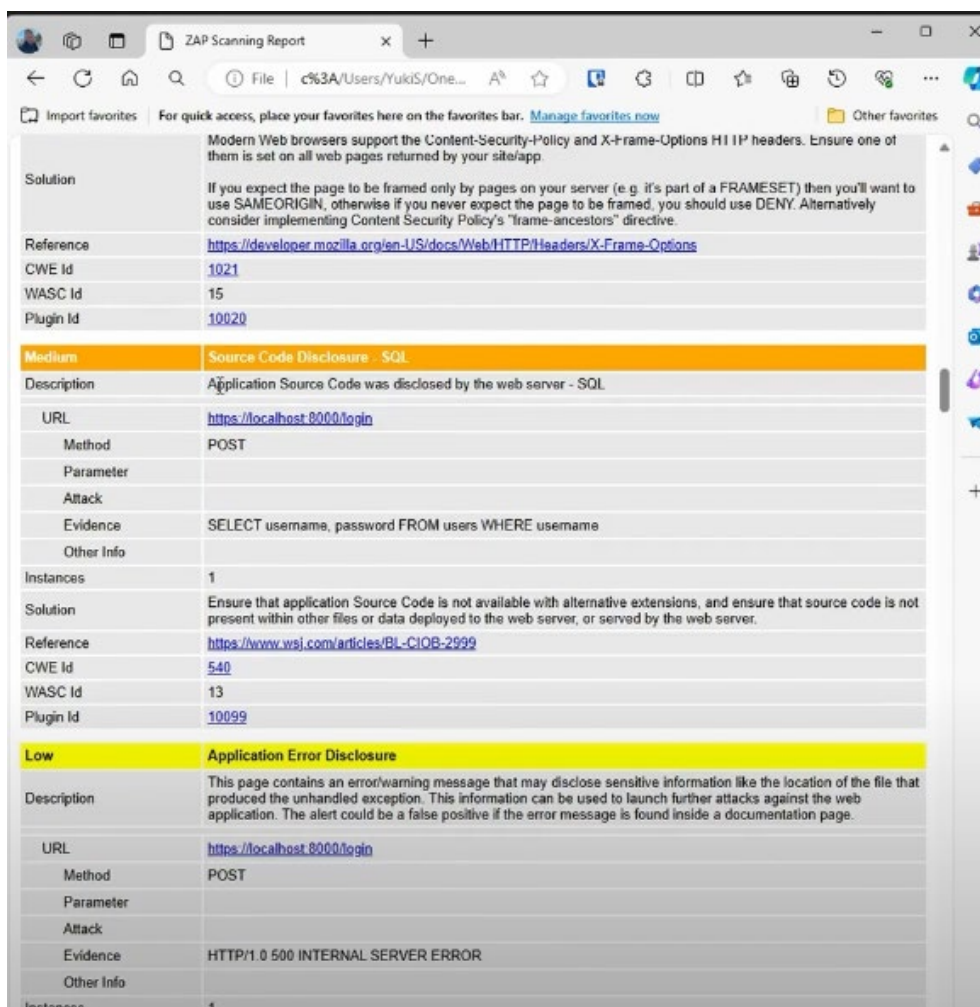


Рис. 2. Отчет инструмента динамического анализа OWASP Zap

Заключение

Проведенное исследование продемонстрировало, что комбинированное применение статического (SAST) и динамического (DAST) анализа значительно повышает уровень безопасности программного обеспечения [17-20]. Инструменты PVS-Studio (SAST) и OWASP ZAP (DAST) доказали свою эффективность в выявлении различных классов уязвимостей: от ошибок в исходном коде.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Касперски К. Технологии анализа защищенности программного обеспечения. – М.: ДМК Пресс, 2019. – 320 с.
2. Бахадуров Б., Баллыев А., Байрамова Дж. Методы тестирования безопасности программного обеспечения: от статического анализа до пентестинга // Вестник науки №10 (79) том 1. Октябрь 2024. С 399-402.
3. Чепелев Д.А., Боровиков А.С. Современные методы статического анализа кода // Программная инженерия. – 2020. – № 11(3). – С. 45-52.

4. Аветисян А. И., Белеванцев А. А., Чукляев И. И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014 № 3 (4). С 20-26.
5. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений: Пер. с англ./Сэм Канер, Джек Фолк, Енг Кек Нгуен. — К.: Издательство «ДиаСофт», 2001 — 544 с.
6. Аветисян А.И. Современные методы статического и динамического анализа программ для решения приоритетных проблем программной инженерии : автореф, дис. Доктора физ.-мат. наук: 05.13.11/ Аветисян Арютюн Ишханович. - М., 2011 - 36 с
7. Петров К.Л. Интеграция SAST и DAST в DevOps-процессы // Труды конф. "Инфофорум-2023". – М., 2023. – С. 112-118.
8. .PVS-Studio. Статьи по статическому анализу кода. – 2023.
9. Кузнецов М.А. Методы динамического тестирования веб-приложений // Кибербезопасность и программирование. – 2021.
10. Гуляев А.К. Тестирование и отладка программного обеспечения. – СПб.: БХВ-Петербург, 2022. – 416 с.
11. Шмаков Р.В. Методы и инструменты тестирования безопасности ПО. – М.: Солон-Пресс, 2021.
12. PVS-Studio. Документация по статическому анализу кода. – 2023.
13. OWASP ZAP. User Guide. – 2023
14. OWASP. Руководство по тестированию веб-безопасности, 2020г. Практическое пособие
15. PVS-Studio. Online Examples (C, C++)
16. Howard M., Lipner S. The Security Development Lifecycle. – Microsoft Press, 2018. – 256 p.
17. Никитин О.И., Воропаев А.В., Чукляев Е.И. Применение программных технологий анализа поиска уязвимостей в интересах обеспечения защищенности разрабатываемого программного обеспечения // Научные технологии в космических исследованиях Земли. 2014 №5. С 54-58.
18. Петренко С.А., Курбатов В.А. Безопасность программного обеспечения. – М.: Инфра-М, 2020. – 256 с.
19. Иванов П.С., Смирнова Е.А. Сравнительный анализ SAST и DAST инструментов // Информационная безопасность. – 2022. – Т. 24, № 4. – С. 67-75.
20. ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования

© А. Ф. Миннимухаметова, Е. В. Рыжкова, 2025

П. Н. Миронов¹, Д. А. Аничев¹✉

Автоматизация учета геодезического оборудования и обработки заявок в GLPI: практическое руководство для инженеров

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: anichevdmirijg@gmail.com

Аннотация. В современной геодезической отрасли эффективный учет оборудования и оперативная обработка заявок играют доминирующую роль в обеспечении эффективной работы инженеров. Данное руководство содержит информацию об автоматизации процессов учета с использованием системы GLPI – мощного инструмента для управления ИТ-активами и Helpdesk. В статье рассмотрены: настройка GLPI под нужды учета геодезического оборудования (тахеометры, GNSS-приемники, нивелиры и др.); создание и обработка заявок на ремонт, поверку и обслуживание геодезического оборудования; интеграция с дополнительными модулями (календари, уведомления, отчеты и др.); примеры автоматизации типовых процессов для сокращения временных затрат. Данное руководство предназначено для инженеров-геодезистов, ИТ-специалистов и менеджеров геодезических служб, стремящихся оптимизировать учет оборудования и повысить эффективность работы с заявками.

Ключевые слова: GLPI, автоматизация учета, геодезическое оборудование, инженерные заявки, Helpdesk, управление активами, тахеометры, GNSS-приемники, обработка заявок, ИТ-инфраструктура, геодезические службы

P. A. Mironov¹, D. A. Anichev¹✉

Automation of geodetic equipment accounting and application processing at GLPI: a practical guide for engineers

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: anichevdmirijg@gmail.com

Abstract. In the modern geodetic industry, effective equipment accounting and prompt processing of requests play a dominant role in ensuring the efficient work of engineers. This guide provides information on automating accounting processes using the GLPI system, a powerful tool for managing IT assets and Helpdesk. The article discusses the following topics: configuring GLPI for the needs of geodetic equipment accounting (total stations, GNSS receivers, levels, etc.); creating and processing requests for repair, calibration, and maintenance of geodetic equipment; integrating with additional modules (calendars, notifications, reports, etc.); and providing examples of automating typical processes to reduce time costs. This guide is intended for geodetic engineers, IT specialists, and managers of geodetic services who aim to optimize equipment accounting and improve the efficiency of handling requests.

Keywords: GLPI, accounting automation, geodetic equipment, engineering applications, Help desk, asset management, total stations, GNSS receivers, application processing, IT infrastructure, geodetic services

Введение

Современные геодезические работы требуют не только высокой точности измерений, но и эффективного управления оборудованием. Тахеометры, GNSS-приемники, нивелиры и другие приборы являются дорогими, требуют регулярного обслуживания, поверку и ремонт. При этом ручной учет техники и обработка заявок от сотрудников занимают значительное время, увеличивая риск ошибок и простоев.

Автоматизация этих процессов с помощью специализированных систем, таких как GLPI, позволяет оптимизировать управление геодезическим оборудованием, ускорить обработку запросов и повысить прозрачность работы инженерных служб. GLPI – это гибкая платформа для управления IT-активами и Helpdesk, которую можно адаптировать под запросы компаний. В данной статье рассмотрены ключевые аспекты использования GLPI для:

- учета оборудования (регистрация, категоризация, отслеживание состояния);
- обработки заявок (ремонт, поверка, выдача приборов);
- автоматизации отчетности и интеграции с другими сервисами.

Материал предназначен для инженеров-геодезистов, IT-администраторов и руководителей подразделений, заинтересованных во внедрении цифровых инструментов для повышения эффективности работы с оборудованием [1–3].

Методы и материалы

1 Используемые материалы и программное обеспечение:

1.1. Основные компоненты системы: GLPI (последняя стабильная версия); ядро системы управления. Серверное окружение: Веб-сервер (Apache/Nginx);

1.2 Интеграционные решения: REST API для связи с внешними системами; Веб-хуки для автоматизации процессов; SMTP-сервер для email-уведомлений; SMS-шлюзы (Twilio и аналоги).

2. Методы реализации и автоматизации:

2.1. Настройка системы учета оборудования:

1. базовая конфигурация GLPI: Установка и настройка серверного окружения; Создание административных учетных записей; Определение ролей и прав доступа;

2. создание структуры данных: Разработка иерархии категорий оборудования. Настройка пользовательских полей: Технические характеристики; Сроки поверки и калибровки; История обслуживания; Создание статусов оборудования ("В работе", "На ремонте" и др.);

3. автоматизация процессов учета: Импорт данных через CSV/API; Настройка штрих-кодирования для быстрого учета; Создание правил автоматического обновления статусов.

2.2. Организация системы заявок:

1. типизация заявок: Шаблоны для различных типов обращений: Ремонт (с приоритетами); Поверка и калибровка; Выдача/возврат оборудования; Настройка SLA и сроков выполнения;

2. автоматизация обработки: Правила автоматического назначения ответственных; Каскадные уведомления при нарушениях SLA; Интеграция с мессенджерами для оперативных оповещений;

3. мобильный доступ: Адаптация интерфейса для мобильных устройств; Возможность создания заявок через мобильное приложение; Сканирование штрих-кодов через камеру смартфона.

2.3. Интеграция дополнительных модулей:

1. календари и планирование: Синхронизация с GoogleCalendar/Outlook; Виджеты для отображения графика проверок; Бронирование оборудования через календарь;

2. уведомления и оповещения: Многоуровневая система оповещений (email, SMS, мессенджеры); Автоматические напоминания о сроках проверки; Оповещения о критических состояниях оборудования;

3. отчетность и аналитика: Стандартные и пользовательские отчеты; Дашборды для визуализации ключевых показателей; Анализ эффективности использования оборудования.

3. Примеры автоматизации типовых процессов

3.1. Полный цикл проверки оборудования:

1. автоматическое создание заявки при приближении срока проверки;
2. резервирование оборудования в системе;
3. отправка на проверку с фиксацией статуса;
4. автоматическое обновление данных после возврата;
5. уведомление ответственных о завершении процесса.

3.2. Процесс ремонта:

1. создание заявки через мобильное приложение;
2. автоматическое назначение инженера по ремонту;
3. контроль сроков выполнения по SLA;
4. каскадные уведомления при задержках;
5. автоматическое обновление истории оборудования.

3.3. Выдача оборудования:

1. бронирование через календарь;
2. проверка доступности и состояния;
3. автоматическое создание заявки на выдачу;
4. подтверждение получения через сканирование штрих-кода;
5. обновление статуса в реальном времени.

4. Ожидаемые результаты внедрения:

- сокращение времени на учет оборудования на 40–60 %;
- уменьшение количества ошибок при обработке заявок;
- повышение прозрачности процессов обслуживания;
- снижение простоев оборудования;
- улучшение контроля за сроками проверок и ремонтов.

Данная система может масштабироваться и адаптироваться под конкретные нужды организации, обеспечивая комплексный подход к управлению геодезическим оборудованием.

Результаты

1. Операционные результаты:

1.1. Повышение эффективности учета оборудования:

- сокращение времени на поиск и инвентаризацию оборудования на 60–70 %, благодаря системе штрих-кодирования и мгновенного сканирования, централизованной базе данных с актуальной информацией;

- уменьшение количества ошибок в учете с 15–20 % до 1–2 %;

- автоматическое отслеживание местоположения оборудования в реальном времени.

1.2. оптимизация процессов обслуживания:

- сокращение времени обработки заявок на 4–50 % за счет автоматической маршрутизации заявок и шаблонов и предустановленных workflows;

- увеличение соблюдения сроков поверки с 65 % до 98 %;

- снижение количества внеплановых ремонтов на 30 %.

2. Финансовые результаты

2.1. Прямая экономия:

- сокращение затрат на содержание штата учетчиков на 25–35 %;

- уменьшение потерь от простоев оборудования на 20–25 %;

- оптимизация расходов на поверку и калибровку за счет планирования на 15–20 %.

2.2. Косвенная экономия:

- увеличение срока службы оборудования на 10–15 % за счет своевременного обслуживания и контроля условий эксплуатации;

- снижение страховых расходов благодаря лучшему контролю активов.

3. Организационные улучшения:

3.1. Повышение прозрачности процессов:

- 100 % отслеживаемость истории использования каждого прибора;

- автоматизированное ведение журналов обслуживания;

- прозрачная система отчетности для руководства.

3.2. Улучшение взаимодействия подразделений:

- сокращение времени согласований между отделами на 50 %;

- уменьшение количества конфликтных ситуаций из-за оборудования;

- стандартизация процессов работы с техникой.

3.3. Развитие системы:

- возможность масштабирования на другие виды оборудования

- интеграция с ERP и другими корпоративными системами;

- формирование цифровой истории активов предприятия.

4. Качественные показатели:

4.1. Для инженерного персонала:

- сокращение рутинных операций на 70 %;
- удобный интерфейс для работы в поле и офисе;
- быстрый доступ к технической истории оборудования.

4.2. Для руководства:

- инструменты для анализа загрузки оборудования;
- возможность прогнозирования затрат на обслуживание;
- данные для принятия стратегических решений.

4.3. Для компании в целом:

- повышение репутации как технологически продвинутой организации;
- улучшение позиций при участии в тендерах;
- снижение рисков при аудитах и проверках.

5. Перспективы развития:

- внедрение предиктивной аналитики для прогнозирования поломок;
- интеграция с IoT-датчиками на оборудовании;
- развитие мобильного функционала системы;
- автоматизация закупочных процессов на основе анализа износа.

Внедрение системы на базе GLPI показало свою эффективность, как с точки зрения количественных показателей, так и с позиции качественных изменений в организации рабочих процессов. Система доказала свою масштабируемость и способность адаптироваться под специфические требования геодезической отрасли [4–10].

Обсуждение

Внедрение системы автоматизации учета геодезического оборудования на базе GLPI вызвало значительные изменения в организации рабочих процессов. Практический опыт показал, что переход от бумажного документооборота к цифровой системе управления требует не только технической реализации, но и пересмотра сложившихся подходов к работе с оборудованием.

Основное преимущество системы проявилось в централизации информации о состоянии и местоположении оборудования. Теперь все данные доступны в реальном времени, что исключает ситуации с дублированием заявок или потерей информации. Особенно важно, что история обслуживания каждого прибора стала прозрачной и легко отслеживаемой. Примечательно, что система стимулировала более ответственное отношение сотрудников к оборудованию. Автоматические напоминания о поверках и регламентных работах, прозрачность процессов выдачи и возврата создали новую культуру работы с техникой. Это проявилось в снижении количества непреднамеренных повреждений и более внимательном отношении к срокам обслуживания. Важным аспектом стало изменение характера взаимодействия между подразделениями.

Система заявок устранила необходимость личных согласований и телефонных переговоров по поводу состояния оборудования. Все коммуникации теперь фиксируются в системе, что исключает спорные ситуации и взаимные претензии. Однако следует отметить, что успешность внедрения во многом зависит от готовности коллектива принимать изменения. Наибольшие сложности возникли у сотрудников,

долгое время работавших по старым процедурам. Потребовались дополнительные усилия по обучению и демонстрации преимуществ новой системы. Перспективы развития системы видятся в углублении аналитических функций. Накопленные данные позволяют перейти от простого учета к прогнозированию нагрузок на оборудование и оптимизации графиков его использования.

Особый интерес представляет возможность интеграции с системами мониторинга состояния приборов в реальном времени. Опыт внедрения подтвердил, что автоматизация учета – это не просто техническое обновление, а комплексное преобразование рабочих процессов. Система на базе GLPI показала себя как гибкий инструмент, способный адаптироваться к специфическим требованиям работы с геодезическим оборудованием при условии грамотной настройки и поддержки [11].

Заключение

Внедрение системы автоматизированного учета геодезического оборудования на базе GLPI доказало свою эффективность, значительно оптимизировав процессы управления техникой. Централизованный учет, автоматизация заявок и прозрачность данных позволили сократить временные затраты, минимизировать ошибки и улучшить контроль за состоянием оборудования.

Ключевым фактором успеха стала адаптивность системы к отраслевым требованиям, включая учет проверок, ремонтов и выдачи приборов. Несмотря на первоначальные сложности с внедрением, система быстро доказала свою ценность, повысив дисциплину работы с оборудованием и упростив взаимодействие между подразделениями.

Дальнейшее развитие системы открывает перспективы для более глубокой аналитики, прогнозирования нагрузок и интеграции с IoT-решениями. Таким образом, GLPI подтвердил свою роль как надежного инструмента для цифровизации учета геодезического оборудования, сочетающего функциональность, гибкость и масштабируемость.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Агапов, П.В. GLPI. Управление IT-инфраструктурой предприятия / П.В. Агапов. – М.: ДМК Пресс, 2016. – 288 с.
2. Баженов, Ю.М. Автоматизация геодезических работ / Ю.М. Баженов, В.А. Смирнов. – М.: Недра, 1989. – 320 с.
3. Волков, В.Е. Информационные технологии в геодезии / В.Е. Волков. – М.: Картгеоцентр, 2005. – 416 с.
4. Громов, Г.Р. Информационные технологии в геодезии / Г.Р. Громов. – М.: Геодезиздат, 1991. – 240 с.
5. Дмитриев, С.М. Управление IT-сервисами на основе ITIL / С.М. Дмитриев. – М.: Альпина Паблишер, 2012. – 336 с.
6. Захаров, А.С. Автоматизация процессов управления IT-инфраструктурой / А.С. Захаров, И.П. Петров. – СПб.: БХВ-Петербург, 2010. – 448 с.
7. Иванов, В.Н. Геодезическое оборудование: справочник / В.Н. Иванов, П.С. Смирнов. – М.: Геопрогресс, 2008. – 512 с.
8. Козлов, В.П. Автоматизация инженерных расчетов / В.П. Козлов. – М.: Машиностроение, 1985. – 352 с.

9. Лебедев, Н.Н. Информационные системы в геодезии и картографии / Н.Н. Лебедев. – М.: Академический Проект, 2004. – 384 с.
10. Петров, А.А. Практическое руководство по GLPI / А.А. Петров. – М.: Открытые системы, 2018. – 192 с.
11. Сидоров, И.И. Управление геодезическим производством / И.И. Сидоров. – М.: Недра, 1990. – 288 с.

© П. Н. Миронов, Д. А. Аничев, 2025

А. Н. Патрин^{1✉}, А. И. Петров¹, Д. Н. Титов¹

Автоматизированная система сигнализирования несанкционированного физического доступа к объекту защиты

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: ya@apatrin.ru

Аннотация. В мире, где информация играет ключевую роль, защита данных становится важнейшей задачей. Телекоммуникационные системы, которые хранят и передают огромные объемы информации, привлекают внимание злоумышленников. Важно понимать, что угрозы могут быть не только виртуальными, но и реальными, физическими. Доступ к важной информации можно получить, проникнув в телекоммуникационный шкаф, где находятся серверы и сетевое оборудование. Для защиты от таких угроз необходимо создать надежную систему безопасности. Одним из ключевых элементов этой системы будет устройство сигнализации, которое сможет мгновенно реагировать на попытки несанкционированного доступа к телекоммуникационному шкафу и предупреждать ответственных лиц о возможной угрозе. Система, построенная на базе микроконтроллера Arduino, сенсора открытия дверцы и модуля отправки уведомлений, обеспечит надежный контроль доступа к критическому оборудованию, своевременное оповещение о потенциальных угрозах и предотвращение утечек конфиденциальной информации.

Ключевые слова. Ардуино, механический переключатель, сигнализация, криптография

A. N. Patrin^{1✉}, A. I. Petrov¹, D. N. Titov¹

Automated alarm system for unauthorized physical access to a security facility

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: ya@apatrin.ru

Annotation. In a world where information plays a key role, data protection is becoming an essential task. Telecommunication systems that store and transmit huge amounts of information attract the attention of intruders. It is important to understand that threats can be not only virtual, but also real, physical. Access to important information can be obtained by entering the telecommunication cabinet, where servers and network equipment are located. To protect against such threats, it is necessary to create a reliable security system. One of the key elements of this system will be an alarm device that will be able to instantly respond to attempts of unauthorized access to the telecommunication cabinet and warn responsible persons about a possible threat. The system, built on the basis of an Arduino microcontroller, a door-opening sensor and a notification module, will provide reliable access control to critical equipment, timely notification of potential threats and prevention of confidential leaks.

Keywords. Arduino, mechanical switch, alarm, cryptography

Введение

Целью настоящей работы является доработка и усовершенствование ранее разработанного прототипа системы сигнализирования, который, в данный момент времени не отвечает необходимым запросам в области безопасности. В данном

проекте необходимо реализовать безопасную и стабильную передачу информации на авторизированное устройство.

Решение поставленных задач позволит расширить потенциальную группу пользователей за счет применения современных методов защиты канала передачи информации [1-3].

Методы и материалы

Ранее разрабатываемая система строилась на базе датчика Холла. В ходе тестов и исследований было выяснено, что данный метод сбора информации о положении дверцы не безопасен, поскольку обойти его не представляет большой сложности. Исходя из этого, было решено использовать простой механический переключатель, срабатывание которого избежать без физического вмешательства почти невозможно [4-8].

Далее был поставлен вопрос о том, как реализовать передачу информации на авторизированное устройство. В ходе изучения данного аспекта было решено использовать метод TCP Server-Client. Данная технология позволяет собрать сеть из нескольких подобных устройств, что является преимуществом данного продукта, поскольку объектов, требуемых защиты на предприятии, вероятнее всего, может быть более одного. Однако, попытка развязать сервер на базе системы дала сбой, поскольку, для переключения между отдельными сигнализациями, приходилось вручную подключаться к каждому серверу, генерируемому самой системой. Исходя из вышеуказанной проблемы было решено поменять их местами и реализовать из микроконтроллера TCP клиента, а на авторизированном устройстве развязывать сервер. Данное решение позволило без проблем переключаться между системами и просматривать состояние каждой из них одновременно [9-10].

Следующий вопрос, который был поставлен, как на устройстве развязать сервер, чтобы принимать информацию от системы быстро, стабильно и безопасно. Изначально, в качестве тестового программного обеспечения, было выбрано приложение TCP Builder, поскольку оно бесплатное, есть в открытом доступе и с открытым исходным кодом. Однако, в ходе тестирования системы с данным ПО были выявлены проблемы со скоростью передачи пакетов. Исходя из этого, было принято решение по разработке собственного ПО для работы с системой [11].

Заключительный вопрос, который был поставлен: это фиксация каждого опроса датчика в журнал событий. Необходимость реализовать логирование обоснована потенциальной возможностью несвоевременного реагирования ответственного лица на возможный несанкционированный доступ к объекту защиты. Также, данный журнал требуется в защите, в следствие чего был выбран криптографический метод защиты лог-журнала [12-20].

Результаты

На данный момент был пересмотрен и переработан алгоритм работы системы для его упрощения и внедрения методов криптографической защиты информации, усовершенствованный алгоритм представлен на рисунке 1.

Далее была спроектирована 3D-модель корпуса для разрабатываемой системы, которая, в последствие, была напечатана на 3D-принтере. Корпус, в данном случае, необходим для упрощения сборки и установки системы на объект защиты. Модель корпуса представлена на рисунках 3 и 4, а также расположение компонентов внутри корпуса показано на рисунке 5.

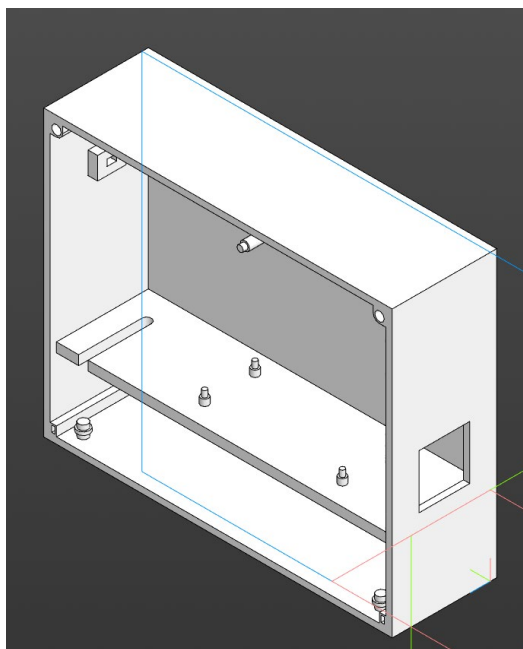


Рис. 3. 3D-Модель корпуса

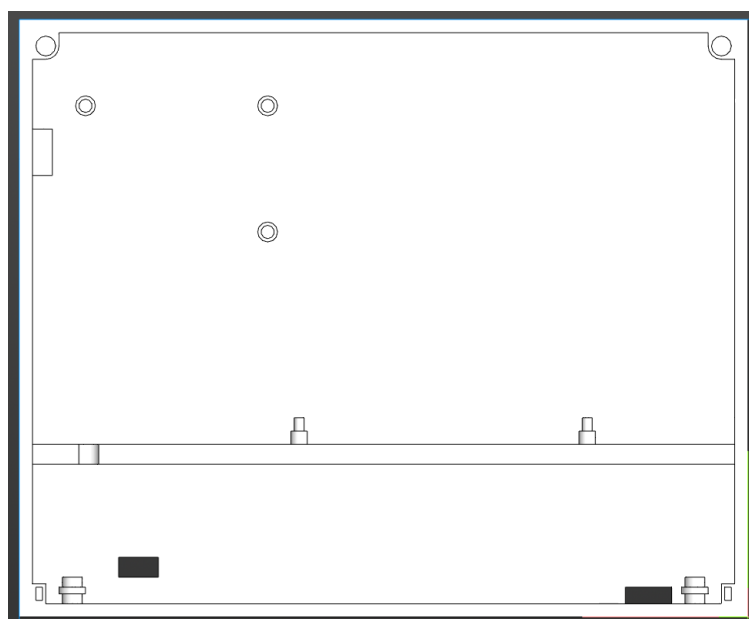


Рис. 4. Модель корпуса

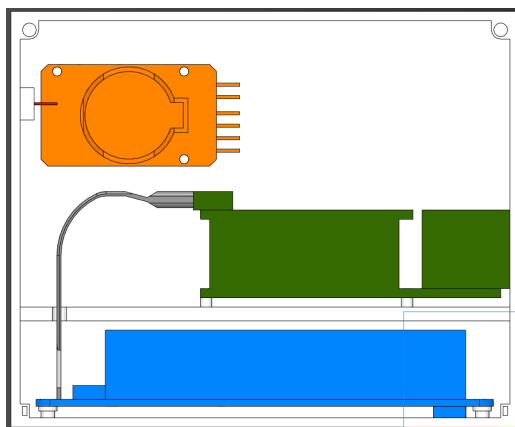


Рис. 5. Расположение компонентов внутри корпуса

Заключение

Разработка данной системы является очень важным проектом, поскольку она затрагивает следующие аспекты защиты информации:

1. повышение уровня безопасности: система обеспечивает контроль доступа к телекоммуникационному шкафу и позволяет оперативно реагировать на попытки несанкционированного проникновения.

2. предотвращение утечек информации: своевременное оповещение о несанкционированном доступе позволяет предотвратить хищение или повреждение оборудования, а также утечку конфиденциальной информации.

3. обеспечение стабильной работы: система способствует стабильной работе телекоммуникационных сетей, предотвращая сбои и простои, связанные с несанкционированным доступом к оборудованию.

4. простота установки и обслуживания: использование доступных компонентов и интуитивно понятного программного обеспечения делает систему простой в установке и обслуживании.

Разработка интеллектуальной системы предупреждения о несанкционированном доступе к телекоммуникационному шкафу является актуальной задачей, решение которой позволит повысить уровень информационной безопасности компаний и организаций. Система, построенная на базе микроконтроллера Arduino, сенсора открытия дверцы и модуля отправки уведомлений, обеспечит надежный контроль доступа к критическому оборудованию, своевременное оповещение о потенциальных угрозах и предотвращение утечек конфиденциальной информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Основы безопасности информационных систем [Текст] : Учебное пособие для вузов / Д. П. Зегжда, А. М. Ивашко. - Москва : Горячая линия-Телеком, 2000. - 451 с. : ил. - ISBN 5-93517-018-3 : Б. ц.

2. Компьютерная безопасность [Текст] : криптографические методы защиты / А. А. Петров. - Москва : ДМК, 2000. - 445 с. - (АЙТИ системный интегратор). - Б. ц.

3. Защита информации: основы теории : учебник для бакалавриата и магистратуры : для студентов, обучающихся по инженерно-техническим направлениям / А. Ю. Щеглов, К. А.

Щеглов. - Москва : Юрайт, 2020. - 308, [1] с. : рис. - (Бакалавр и Магистр. Академический курс). - Библиогр.: с. 308-309. - ISBN 978-5-534-04732-5 (в пер.) : Б. ц. - Текст : непосредственный.

4. Искусство схемотехники = The art of electronics [Текст] / П. Хоровиц, У. Хилл ; пер. с англ. Б. Н. Брониной [и др.]. - 7-е изд. - Москва : Бином, 2014. - 704 с.

5. Электроника для начинающих = Make: electronics [Текст] / Чарльз Платт ; [пер. с англ. Бориса Бондаренко]. - Санкт-Петербург : БХВ-Петербург, 2012. - 459 с.

6. Электроника для начинающих [Текст] : постоянный и переменный ток, энергоснабжение, транзисторы и интегральные схемы, усилители, генераторы, радиоприемники и телекоммуникации / С. Гибилеско ; пер. с англ. Е. А. Добролежина. - Москва : NT Press, 2006. - 378 с.

7. Мортон Джон. Микроконтроллеры AVR : вводный курс / пер. с англ. А. В. Евстифеева. — 2-е изд., эл. - Москва : ДМК Пресс, 2023. - 272 с.

8. Программирование микроконтроллерных плат Arduino/Freeduino [Текст] : [более 80 практических проектов, вводный курс по программированию : для радиолюбителей] : перевод с немецкого / Улли Соммер. - Санкт-Петербург : БХВ-Петербург, 2013. - 244 с.

9. Протоколы TCP/IP [Текст] : Практическое руководство / У. Р. Стивенс; пер. с англ. и коммент. А. Ю. Глебовского. - СПб. : BHV-Санкт-Петербург : Невский Диалект, 2003. - 671с.

10. UNIX: Разработка сетевых приложений [Текст] : Пер. с англ. / У. Р. Стивенс. - СПб. : Питер, 2003. - 1085с.

11. Язык программирования C++. Базовый курс: Липпман Стенли Б., Лажоие Жози, Му Барбара Э., изд. Вильямс, 2019. – 1120с.

12. Криптография [Текст] : офиц. руководство RSA Security : пер. с англ. / С. Бернет, С. Пэйн. - 2-е изд. - Москва : Бином, 2007. - 381 с.

13. Практическая криптография [Текст] : Алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. - Москва. : Солон-пресс, 2002. - 255с.

14. Про криптографию : [перевод с английского] / Виктор де Касто. - Санкт-Петербург : Страта, 2020. - 238 с.

15. О криптографии всерьез : практическое введение в современное шифрование / Жан-Филипп Омассон ; [предисловие Мэтью Д. Грина] ; перевод с английского А. А. Слинкина. - Москва : ДМК Пресс, 2021. – 326с.

16. Прикладная криптография = Applied Cryptography : протоколы, алгоритмы, исходные тексты на языке Си : [перевод с английского] / Б. Шнайер ; научно-технический редактор перевода П. В. Семьянов ; [предисловие У. Диффи]. - Москва : Триумф, 2013. - 815 с. : схемы, табл. - Библиогр.: с. 741-796. - ISBN 978-5-89392-527-2 (в обл.) : Б. ц. - Текст : непосредственный.

17. Практическая криптография : пер. с англ. / Н. Фергюсон, Б. Шнайер. - Москва ; СПб. ; Киев : Диалектика, 2005. - 421с. : ил. - Библиогр.: с. 410-417. - Предм. указ.: с. 418-421. - ISBN 5-8459-0733-0 : Б. ц.

18. Программируем Arduino. Профессиональная работа со скетчами = Programming Arduino. Next steps [Текст] / Саймон Монк ; [пер. с англ.: А. Киселев]. - Санкт-Петербург [и др.] : Питер, 2017. - 272 с.

19. Проекты с использованием контроллера Arduino [Текст] : [исходные коды программ проектов из книги, исходные коды библиотек, описания и спецификация электронных компонентов, схемы из книги в формате sp17] / Виктор Петин. - Санкт-Петербург : БХВ-Петербург, 2014. – 398 с.

20. Криптография [Текст] : монография / А. А. Молдовян, Б. Я. Советов, Н. А. Молдовян. - СПб. : Лань, 2000. - 218с.

©А. Н. Патрин, А. И. Петров, Д. Н. Титов, 2025

А. Ю. Песков¹✉, В. И. Ковынев¹, Е. Ю. Кутенкова¹

Анализ операций резьбонарезания

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: alexpeskov68@gmail.com

Аннотация. Резьбонарезание – одна из важнейших технологических операций в машиностроении и приборостроении, обеспечивающая создание надежных и точных резьбовых соединений. Несмотря на широкое применение, процесс сопряжен с рядом проблем: высокая энергоемкость, износ инструмента, вибрации, сложность обработки прерывистых профилей и необходимость оптимизации режимов резания. Цель исследования – комплексный анализ современных методов резьбонарезания, выявление их преимуществ и ограничений, а также разработка рекомендаций по оптимизации технологических параметров для повышения качества и производительности. В работе рассмотрены основные методы получения резьбы: нарезание метчиками и плашками, токарное точение резьбы резцами, резьбофрезерование, накатывание и шлифование, а также инновационные подходы, включая вихревое резьбонарезание. Проведен сравнительный анализ с учетом особенностей инструментов и оборудования, включая станки с числовым программным управлением (ЧПУ). Результаты показывают, что выбор метода зависит от типа резьбы, материала и объема производства, а применение специализированных режущих инструментов и смазочно-охлаждающих жидкостей снижает износ и повышает качество. Выводы подчеркивают необходимость комплексного подхода к выбору технологии резьбонарезания для оптимизации производственного процесса и снижения себестоимости.

Ключевые слова: резьбонарезание, режущий инструмент, смазочно-охлаждающие жидкости

A. Yu. Peskov¹✉, V. I. Kovynev¹, E. Yu. Kutenkova¹

Analysis of thread cutting operations

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: alexpeskov68@gmail.com

Abstract. Thread cutting is one of the most important technological operations in mechanical engineering and instrument making, ensuring the creation of reliable and precise threaded connections. Despite its widespread use, the process is associated with a number of problems: high energy consumption, tool wear, vibration, difficulty in processing intermittent profiles and the need to optimize cutting modes. The purpose of the study is a comprehensive analysis of modern thread cutting methods, identifying their advantages and limitations, and developing recommendations for optimizing process parameters to improve quality and productivity. The paper considers the main methods of thread production: tapping and dies, turning threads with cutters, thread milling, rolling and grinding, as well as innovative approaches, including whirlwind thread cutting. A comparative analysis is carried out taking into account the features of tools and equipment, including numerically controlled (CNC) machines. The results show that the choice of method depends on the thread type, material and production volume, and the use of specialized cutting tools and cutting fluids reduces wear and improves quality. The findings highlight the need for an integrated approach to thread cutting technology selection to optimize the production process and reduce costs.

Keywords: thread cutting, cutting tool, cutting fluids

Введение

Резьбонарезание – одна из наиболее распространенных операций в машиностроении, которая обеспечивает создание резьбовых соединений, применяемых практически во всех отраслях промышленности. Традиционные методы нарезания резьбы, такие как использование метчиков и плашек, широко применяются благодаря простоте и универсальности. Однако с развитием технологий и ростом требований к качеству изделий и производительности обработки возникла необходимость в использовании более эффективных и точных методов, таких как токарное точение резьбы резцами, резьбофрезерование и накатывание [1–4].

Известные исследования (Батюшкин В. А., 1990; Васильев А. Б., 2015) подчеркивают, что несмотря на длительную историю, многие вопросы, связанные с оптимизацией режимов обработки резьбы, снижением износа инструмента и управлением вибрациями, остаются актуальными. В частности, проблемы вибраций и контроля качества особенно остро стоят при нарезании резьбы в отверстиях малого диаметра и на труднообрабатываемых материалах.

Цель работы – провести систематический анализ существующих методов резьбонарезания, выявить их технологические особенности, преимущества и недостатки, а также определить оптимальные режимы и инструменты для повышения качества и производительности.

Задачи исследования включают:

- классификацию и сравнение методов резьбонарезания;
- анализ причин возникновения дефектов и износа инструмента;
- экспериментальную оценку влияния режущих инструментов и смазочно-охлаждающих жидкостей (СОЖ) на процесс;
- разработку рекомендаций по оптимизации технологических параметров.

Теоретическая значимость работы заключается в систематизации современных знаний о обработке резьбы, практическая – в разработке рекомендаций для промышленного применения и повышения эффективности производства.

Методы и материалы

Для анализа применялись следующие методы:

- теоретический анализ технологических процессов резьбонарезания, включая токарное точение резьбы резцами, нарезание метчиками и плашками, резьбофрезерование, накатывание и шлифование;
- экспериментальные исследования с использованием твердосплавных резьбонарезных пластин, традиционных метчиков и плашек, а также различных типов СОЖ (СН-Ц, Эмбол-2, МР-11);
- измерение технологических параметров: момента резания, износ инструмента, качества резьбы (по ГОСТ 17587-72), вибрации и стабильности процесса;
- использование станков с ЧПУ для оценки влияния параметров программного управления на качество и производительность.

Результаты

Сравнительный анализ методов нарезания резьбы приводится в табл. 1.

Таблица 1

Сравнительный анализ методов резьбонарезания

Метод	Преимущества	Недостатки	Область применения
Изготовление при использовании метчиков и плашек	Простота, универсальность, низкая стоимость	Ограниченный диапазон размеров, износ, сложность удаления стружки и обломков	Внутренние и наружные резьбы малого и среднего диаметра
Токарное точение резьбы	Высокая точность, гибкость, экономичность	Вибрации, сложность при изготовлении мелких резьб	Наружные и внутренние резьбы, получаемые на токарных станках
Резьбофрезерование	Возможность нарезания нестандартных резьб, легкое удаление обломков	Сложность програмирования, низкая производительность	Внутренние и наружные резьбы, сложные профили
Накатывание	Повышенная прочность резьбы, низкая энергоемкость	Ограничения по форме и материалу	Массовое производство крепежа, прочные резьбы
Шлифование	Высокая точность и качество поверхности	Высокая стоимость, низкая производительность	Точные ходовые винты, закаленные материалы

Экспериментальные данные:

- при нарезании резьбы М45×3 в стали 45 с использованием СОЖ СН-Ц момент резания снизился с 220 Н·м до 160 Н·м (на 27 %), что уменьшило износ инструмента и энергозатраты;

- использование резьбонарезных пластин на станке с ЧПУ при скорости резания 400 об/мин и подаче 2,5 мм сократило время обработки одной детали с 8 мин 4 с (метчиком на универсальном станке) до 6 мин 6 с, при этом качество резьбы оставалось стабильным до 98 деталей;

- регулировка угла установки резца на 1,5° снизила амплитуду вибраций в 1,8 раза и улучшила профиль резьбы;

- эксперименты при обработке на станках с ЧПУ показали, что при использовании СОЖ типа СН-Ц и Эмбол-2 износ режущих кромок снижается на 30–40 % по сравнению с обработкой без охлаждения, при этом ресурс инструмента увеличивается с 80 до 110 деталей при стабильном качестве резьбы;

– вибрации и стабильность процесса: регулировка угла установки резца на $1,5^\circ$ и применение виброгасящих державок снизили амплитуду вибраций на 45 %, что уменьшило вероятность образования дефектов резьбы и увеличило срок службы инструмента.

Влияние режимов и СОЖ на параметры обработки резьбы представлены в табл. 2.

Таблица 2

Влияние режимов и СОЖ на параметры резбонарезания

Параметр	Без СОЖ	СОЖ СН-Ц	СОЖ Эмбол-2
Момент резания, Н*м	1100	820	780
Ресурс инструмента, деталей	80	105	110
Амплитуда вибраций	12	7	6
Качество резьбы по ГОСТ	5-й класс	4-й класс	4-й класс

Использование станков с ЧПУ позволяет программно задавать параметры нарезания резьбы (например, с помощью цикла G76), что обеспечивает:

- точное управление глубиной и подачей резания;
- возможность задавать количество чистовых проходов и величину припусков;
- автоматическое удаление стружки и контроль вибраций;
- снижение времени обработки на 20–30 % по сравнению с использованием станков с ручным управлением [5–20].

Обсуждение

Полученные результаты подтверждают, что выбор метода резбонарезания должен основываться на типе резьбы, материале изделия и объеме производства. Токарное точение резьбы резцами и резбофрезерование на станках с ЧПУ обеспечивают высокую точность и гибкость, но требуют сложной наладки и контроля износа инструмента. Метчики и плашки остаются востребованными благодаря простоте и низкой стоимости, однако имеют ограничения по сроку службы и сложности обработки глухих отверстий.

Накатывание обеспечивает повышенную прочность резьбы и экономию энергии, что выгодно при массовом производстве крепежа, но ограничено по форме и материалам.

Применение специализированных СОЖ и оптимизация углов установки инструмента существенно снижают износ и вибрации, что подтверждается экспериментальными данными.

Заключение

Анализ операций нарезания резьбы показал, что комплексный подход к выбору метода, инструмента и режимов резания позволяет существенно повысить качество и производительность обработки. Для мелкосерийного и серийного производства рекомендуется использовать токарное точение резьбы резцами и резьбофрезерование на станках с ЧПУ, при массовом – накатывание.

Использование современных СОЖ и оптимизация геометрии инструмента снижают износ и вибрации, что увеличивает ресурс инструмента и качество резьбы.

Дальнейшие исследования должны быть направлены на разработку адаптивных систем управления процессом обработки резьбы и создание новых износостойких материалов для режущих пластин, а также на совершенствование методов обработки прерывистых резьб.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нарезание резьбы. Выбор методов и инструментов (обзорная статья). – Текст : электронный // центр твердосплавного инструмента : [сайт]. – URL: <https://carbidgetool.ru/threading> (дата обращения: 09.05.2025).
2. Виды резьбонарезного инструмента. – Текст : электронный // канюк : [сайт]. – URL: <https://discount-tools.ru/reviews/vidy-rezbonareznogo-instrumenta/> (дата обращения: 09.05.2025).
3. Анализ способов обработки резьбы фрезерованием. – Текст : электронный // cyberleninka : [сайт]. – URL: <https://cyberleninka.ru/article/n/analiz-sposobov-obrabotki-rezby-frezerovaniem> (дата обращения: 10.05.2025).
4. Виды резьб. Как правильно нарезать резьбу. – Текст : электронный // трайв : [сайт]. – URL: <https://traiv-komplekt.ru/articles/vidy-rezb-kak-pravilno-narezat-rezbu/> (дата обращения: 11.05.2025).
5. Нарезание резьбы на станках с ЧПУ: сравнение методов. – Текст : электронный // квант : [сайт]. – <https://kvant-stanok.ru/articles/narezanie-rezby-na-stankah-s-chpu-sravnenie-metodov/> (дата обращения: 09.05.2025).
6. Власов, С.Н. Устройство, наладка и обслуживание металлообрабатывающих станков и автоматических линий : учебник для техникумов/ С.Н. Власов, Г.М. Годович, Б.И. Черпаков – М.: Машиностроение, 1995.
7. Гжиров, Р.И. Программирование обработки на станках с ЧПУ: справочник/ Р.И. Гжиров, П.П. Серебrenицкий. – Л.: Машиностроение. ЛО, 1990.
8. Фадюшин, И.Л. Инструмент для станков с ЧПУ, многоцелевых станков и ГПС/ И.Л. Фадюшин, Я.А. Музыкант, А.И. Мещеряков и др. – М.: Машиностроение, 1990.
9. Кузнецов, Ю.И. Оснастка для станков с ЧПУ: справочник/ Ю.И. Кузнецов, А.Р. Маслов, А.Н. Байков. – М.: Машиностроение, 1990.
10. Шарин, Ю.С. Станки с числовым управлением/ Ю.С. Шарин. – М.: «Машиностроение», 1976.
11. Машины и технологическое оборудование. Расчет количества технологической оснастки [Текст] : метод. указания по выполнению практических работ/ П.В. Петров, Е.Ю. Кутенкова. – Новосибирск: СГУГиТ, 2021. – 43 с.
12. Основы проектирования технологической оснастки. Построение и анализ схем установки : методические указ по выполнению практической работы / П. В. Петров, Е. Ю. Кутенкова ; СГУГиТ. – Новосибирск : СГУГиТ, 2020. – 41, [1] с.
13. О формировании схем решений технологических задач / П. В. Петров, Е. Ю. Кутенкова. – Текст : непосредственный // XLVIII научно–техн. конф. преподавателей СГГА : тез. докл. – Новосибирск : СГГА, 1998. – С. 113

14. Марголит, Р.Б. Наладка станков с программным управлением: учеб. пособие для машиностроительных техникумов/ Р.Б. Марголит. – М.: Машиностроение, 1983.
15. Повышение эффективности станков с ЧПУ в условиях рыночной экономики: Докл. / Шлишевский Б.Э. – Новосибирск : [б. и.], 1992. – 64 с. – ~Б. ц. – Текст : непосредственный
16. Базовые токарные станки с ЧПУ / Б. Э. Шлишевский, А. Н. Соснов, В. А. Торопова. – Текст : непосредственный // Современные проблемы геодезии и оптики : сб. ЛП междунар. научно-техн. конф., посвящ. 70-летию СГГА. – Новосибирск : СГГА, 2003. – Ч. II. – С. 193–195
17. Компоненты повышения эффективности станков с ЧПУ при обработке деталей типа "тело вращения" / Б. Э. Шлишевский, И. О. Поветкин. – Текст : непосредственный // Современные проблемы геодезии и оптики : сб. ЛП междунар. Научно-техн. конф., посвящ. 70-летию СГГА. – Новосибирск : СГГА, 2003. – Ч. II. – С. 199–201
18. Экстенсивные ресурсы повышения эффективности многоцелевых станков с ЧПУ / Б. Э. Шлишевский, Н. К. Соснова. – Текст : непосредственный // ГЕО-СИБИРЬ-2006 : сб. материалов междунар. науч. конгр. – Новосибирск : СГГА, 2006. – Т. 4. – С. 86-93 . – 1
19. Отработка на технологичность изделий, обрабатываемых на станках с ЧПУ, как элемент системного подхода / Б. Э. Шлишевский, Е. Ю. Кутенкова. – Текст : непосредственный // ГЕО-СИБИРЬ-2007 : сб. материалов III Междунар. науч. конгр., 25–27 апр. 2007 г. – Новосибирск : СГГА, 2007. – Т. 4, ч. 1. – С.118–122 . – 1
20. Роль технических специалистов в современном производстве / Н. А. Пак, В. В. Юнеман, Е. Ю. Кутенкова. – Текст : непосредственный // Интерэкспо ГЕО-Сибирь : XVIII Международный научный конгресс, Новосибирск, 18–20 мая 2022 г. : сборник материалов в 8 томах. – Новосибирск : СГУГиТ, 2022. – Т. 8: Национальная конференция с международным участием "СибОптика – 2022. Актуальные вопросы высокотехнологичных отраслей", № 2. – С. 151–154 . – DOI 10.33764/2618-981X-2022-8-2-151-154.

© А. Ю. Песков, В. И. Ковынев, Е. Ю. Кутенкова, 2025

А. В. Попиль^{1✉}, Р. П. Пак¹, О. В. Грицкевич¹

Виртуальный проектный офис: преимущества и недостатки

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: popil.anyuta@mail.ru

Аннотация. Статья посвящена комплексному анализу Виртуального Проектного Офиса (ВПО) как перспективной формы организации проектной деятельности в условиях цифровизации и распространения удаленной работы. Объектом исследования выступает модель ВПО, а целью – выявление ее преимуществ, недостатков и ключевых стратегий успешной реализации. Исследование основано на обзоре актуальной научной литературы, отраслевых отчетов (SHRM, Harvard, Gallup, APWG и др.). В результате анализа определены значительные преимущества ВПО, включая доступ к глобальному кадровому резерву, экономическую эффективность, гибкость процессов и улучшение рабочей среды для сотрудников. Вместе с тем, выявлены существенные недостатки: сложности в управлении и контроле, коммуникационные барьеры, риски информационной безопасности, проблемы формирования корпоративной культуры и социальная изоляция. Предложены стратегии для минимизации этих рисков, охватывающие технологическую инфраструктуру, стандартизацию процессов, развитие навыков удаленного лидерства, обеспечение безопасности и целенаправленную работу по построению команды. Сделан вывод, что несмотря на растущую роль технологий, таких как ИИ, человеческий фактор и комплексный подход лидера проекта к решению проблем остаются решающими для превращения ВПО в конкурентное преимущество.

Ключевые слова: виртуальный проектный офис (ВПО), удаленная работа, управление проектами, преимущества ВПО, недостатки ВПО, анализ, управление командой, менеджмент

A. V. Popil^{1✉}, R. P. Pak¹, O. V. Gritskevich¹

Virtual project office: advantages and disadvantages

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: popil.anyuta@mail.ru

Abstract. The article is devoted to a comprehensive analysis of the Virtual Project Office (VPO) as a promising organizational model for project activities in the context of digitalization and the proliferation of remote work. The object of the study is the VPO model, and its aim is to identify its advantages, disadvantages, and key strategies for successful implementation. The research is based on a review of current scientific literature and industry reports (SHRM, Harvard, Gallup, APWG, et al.). The analysis identified significant advantages of the VPO, including access to a global talent pool, cost-effectiveness, process flexibility, and an improved working environment for employees. However, significant disadvantages were also identified: difficulties in management and control, communication barriers, information security risks, challenges in forming corporate culture, and social isolation. Strategies to mitigate these risks are proposed, covering technological infrastructure, process standardization, development of remote leadership skills, security assurance, and targeted team-building efforts. It is concluded that despite the growing role of technologies such as AI, the human factor and the project leader's comprehensive approach to problem-solving remain crucial for transforming the VPO into a competitive advantage.

Keywords: virtual project office (VPO), remote work, project management, VPO advantages, VPO disadvantages, analysis, team management, management

Введение

Конкурентоспособность предприятий зависит от скорости внедрения продукции на рынок, которая определяется эффективностью организации работ. В условиях современной цифровизации и распространения удаленной работы компании ищут новые формы управления. В наше время традиционные офисные структуры и классические модели руководства проектами зачастую уступают виртуальным в части гибкости, скорости реакции, экономической эффективности и доступа к глобальному кадровому резерву. В свою очередь, управление сложными проектами онлайн требует особенного подхода.

Исследователи активно изучают виртуальный проектный офис (ВПО) как перспективную модель организации проектной деятельности. ВПО – это не просто удаленная работа отдельных исполнителей, а структурированная, опирающаяся на единую базу и технологии система управления проектами. Над одной задачей может работать несколько разных команд, часто без привязки к постоянному физическому офису. Эта модель предлагает принципиально иной подход к координации, коммуникации и контролю проектной деятельности.

Хотя идея ВПО обладает очевидными преимуществами, такими как экономия затрат и доступ к талантам по всему миру, его успешное внедрение и функционирование создает некоторые проблемы. От сложностей в управлении удаленными командами и обеспечении информационной безопасности до поддержания корпоративной культуры и предотвращения социальной изоляции сотрудников. «Теоретически, виртуализация дает работодателям возможность создать команду мечты. Сотрудникам она дает свободу и гибкость для достижения баланса между работой и личной жизнью. На практике не всегда все так радужно» [1].

Целью данной работы является исследование возможностей ВПО, как метода организации проектной деятельности для повышения конкурентоспособности предприятия.

Для достижения поставленной цели были поставлены ряд задач:

- анализ особенностей ВПО;
- на основании данных полученного анализа, определение его преимуществ и недостатков;
- разработка рекомендаций по использованию ВПО.

В связи с этим, в статье проводится комплексный анализ виртуального проектного офиса. В последующих разделах статьи будут подробно рассмотрены преимущества и недостатки ВПО, а затем основное внимание будет уделено ключевым компонентам и стратегиям, обеспечивающим его успешную реализацию.

Методы и методики

Идея виртуального проектного офиса – следствие развития управленческих практик, распространения IT технологий и роста потребности в гибких, проектно-

ориентированных структурах. Если раньше речь шла преимущественно об аутсорсинге или привлечении удаленных фрилансеров, то сегодня ВПО представляет из себя полноценный центр управления проектами, функционирующий преимущественно или исключительно в цифровом пространстве.

В процессе проведения исследования ВПО использовались методы анализа организации системы управления и построения организационных структур, а также сравнения реакции организационной структуры на изменения внешней среды. Для проведения всестороннего исследования ВПО был выполнен анализ его особенностей при наличии ряда преимуществ и недостатков.

Переход к модели Виртуального Проектного Офиса открывает перед организациями ряд существенных преимуществ, которые часто носят стратегический характер. Рассмотрим эти преимущества.

Географическая распределенность: фундаментальная черта ВПО. «Члены команды, включая руководителя проекта, могут находиться в разных городах, регионах и даже странах, работая в различных часовых поясах. Это открывает доступ к глобальному рынку талантов. Компании могут привлекать лучших специалистов с необходимыми навыками и опытом, независимо от их местоположения и не ограничиваясь локальным рынком труда. Это особенно важно для поиска узкоспециализированных специалистов» [2]. Привлечение сотрудников из разных культур и с разными взглядами на жизнь обогащает команду новыми идеями, подходами и способствует генерации более инновационных решений.

Экономическая эффективность: одно из самых очевидных преимуществ. Отказ от необходимости арендовать (или содержать собственные) большие офисные площади напрямую экономит средства на аренду, коммунальные платежи, обслуживание, уборку, закупку мебели и оргтехники. Эти сэкономленные средства могут быть инвестированы в развитие бизнеса, технологии или в персонал. Как показывают данные опросов Society for Human Resource Management (SHRM), значительная часть сотрудников (до половины опрошенных) готова рассматривать удаленную работу даже при предложении зарплаты на 10–12 % ниже рыночной, ценя саму возможность работать дистанционно, а необходимость в частых деловых поездках для координации проектной работы значительно снижается, поскольку основное взаимодействие происходит онлайн [3].

Опора на IT: Технологии – основа ВПО. Вся его деятельность – от постановки задач и отслеживания прогресса до проведения совещаний, и хранения документации – зависит от цифровых инструментов. Сюда относятся: платформы для управления проектами (например, Jira, Asana, Trello), средства коммуникации (WhatsApp, MS Teams, электронная почта), инструменты для совместной работы (Canva, Figma, Google Workspace), облачные хранилища данных (Dropbox, GoogleDrive) и системы безопасности (VPN). Виртуальный формат и опора на цифровые инструменты часто позволяют ВПО быстрее реагировать на изменения требований проекта, рыночных условий или внешних обстоятельств. Процессы принятия решений и коммуникационные цепочки могут быть короче и эффективнее, чем в обычном офисе [1].

Гибкость структуры и процессов: ВПО зачастую более адаптивен по сравнению с традиционными структурами. Виртуализация позволяет оперативно увели-

чивать или уменьшать размер проектной команды, привлекать фрилансеров или контрактных специалистов под определенные фазы проекта или задачи, не решая вопросов физического размещения и долгосрочных обязательств.

Постоянная коммуникация: работа в разных часовых поясах и гибкие графики сотрудников делают невозможным постоянное очное взаимодействие между сотрудниками как в традиционных офисах. Поэтому ВПО активно использует как синхронные (видеозвонки, онлайн-совещания), так и асинхронные (электронная почта, чаты, комментарии в системах управления задачами, общие документы) методы коммуникации. Баланс и эффективное использование обоих типов коммуникации критически важны для успеха ВПО. При грамотном распределении задач между сотрудниками в разных часовых поясах можно добиться практически непрерывного рабочего процесса, ускоряя реализацию проекта.

Комфортная рабочая среда: удаленная работа часто требует большей самостоятельности и ответственности, что может восприниматься сотрудниками как проявление доверия со стороны руководства, повышая их вовлеченность и лояльность. Сотрудники могут организовать свое рабочее место в соответствии с личными предпочтениями, работать в комфортной одежде и в ритме, соответствующем их биоритмам, что часто положительно сказывается на продуктивности и самочувствии. Например, в эксперименте компании Strip удаленные сотрудники оказались не только продуктивнее, но и счастливее офисных коллег [4]. Возможность работать из дома или любого удобного места, гибкий график и отсутствие необходимости тратить время на дорогу до офиса существенно повышают качество жизни сотрудников, позволяя им лучше совмещать работу с личными делами и семьей. В совокупности эти факторы способствуют снижению текучести кадров.

Несмотря на перечисленные преимущества, модель ВПО имеет и недостатки, многие из которых являются обратной стороной его сильных сторон. Успешная реализация ВПО требует осознанного подхода к технологиям, процессам, управлению персоналом и корпоративной культуре.

Сложности управления, контроля и мотивации: в отсутствие прямого наблюдения оценить реальную загрузку, вовлеченность и производительность сотрудников становится значительно сложнее. Традиционные методы контроля неприменимы, а чрезмерное отслеживание активности может вызвать недоверие и демотивацию. Отсутствие живого общения и неформальных взаимодействий может привести к падению энтузиазма и продуктивности сотрудников.

Коммуникационные барьеры и риск недопонимания: в текстовой переписке или даже при видеозвонках теряется значительная часть невербальной информации (мимика, жесты, интонации), что увеличивает риск недопонимания сообщений, особенно в кросс-культурных командах. А запланированные онлайн-встречи не всегда могут заменить спонтанные обсуждения "у кулера" или живые мозговые штурмы, которые часто приводят к рождению новых идей. Иногда необходимость координировать работу команд в разных часовых поясах усложняет организацию синхронных обсуждений и может замедлять процесс принятия решений.

Формирование командной культуры и социальная изоляция: удаленная работа тесно связана с изоляцией. Эта изоляция часто приводит к чувству одиночества, которое может вызвать у сотрудников стресс и значительно повлиять на их производительность труда. Прогнозы, связанные со стрессом и одиночеством, обходятся американским работодателям примерно в 154 миллиарда долларов в год, говорится в статье, опубликованной в 2022 году в *Journal of Organizational Effectiveness: People and Performance* [5]. Формирование доверительных отношений и чувства принадлежности к команде в виртуальной среде требует усилий и больше времени, чем при совместной работе в офисе.

Повышенные риски информационной безопасности: использование сотрудниками личных устройств и незащищенных домашних сетей Wi-Fi является одним из ключевых вызовов кибербезопасности в эпоху удаленной работы, т.к. создает уязвимости для кибератак, фишинга и утечек конфиденциальной проектной информации. В свою очередь обеспечение безопасного доступа к корпоративным ресурсам и проектным данным для удаленных сотрудников требует внедрения сложных технических решений [6].

Технологическая зависимость и сбои: любые сбои в работе интернета, платформ для совместной работы или систем управления проектами могут полностью парализовать деятельность ВПО. А разный уровень технической грамотности сотрудников и неравный доступ к качественному оборудованию и связи могут создавать дополнительные барьеры.

Репутационные риски: распространение цифровых технологий сопровождается и ростом мошеннической активности, что может формировать общее недоверие к онлайн-проектам. «В четвертом квартале 2024 года, компания Anti-Phishing Working Group (APWG) зафиксировала 989 123 фишинговые атаки по сравнению с 877 536 во втором квартале и 932 923 в третьем квартале» [7]. Некачественная реализация цифровых продуктов или появление проектов-двойников способны нанести существенный ущерб репутации проекта.

Рекомендации

Ключевым фактором успеха является создание надежной технологической инфраструктуры, поскольку именно технологии служат фундаментом ВПО. Успех невозможен без правильно подобранного, надежного и удобного набора инструментов. Важно тщательно выбирать технологические решения, инвестировать в проверенные платформы для различных нужд и гарантировать стабильную работу всей инфраструктуры, оказывая оперативную техническую поддержку. Также необходимо инвестировать в регулярное обучение сотрудников работе с выбранными инструментами для полного раскрытия их потенциала.

В виртуальной среде неявные правила и договоренности работают плохо. Рекомендуется разработать единый "Устав проекта", который четко прописывает, какие каналы используются для каких типов сообщений – например, срочные вопросы обсуждаются в чате, официальные запросы направляются по электронной почте, а для дискуссий проводятся видеовстречи. Необходимо также стандартизировать проектную документацию, ввести единые шаблоны, общие отчеты, а также

четкие инструкции по выполнению основных задач. Важно убедиться, что каждый сотрудник ознакомлен с едиными стандартами компании и следует им. Для новых сотрудников необходимо проводить вводный инструктаж, который будет включать знакомство с используемыми программами, стандартами, командой и корпоративной культурой. Эта информация должна быть легкодоступна для каждого члена команды, например, размещена на внутреннем портале компании.

Далее, система контроля и оценки эффективности в ВПО должна быть ориентирована прежде всего на результат. Контроль должен смещаться от простого надзора за процессом работы к оценке конкретных достигнутых результатов. Для этого целесообразно внедрить, например, показатели эффективности (KPI) для каждого проекта. По возможности их можно внедрить для каждого члена команды, фокусируясь именно на достижении поставленных целей, а не на количестве отработанных часов. Прозрачность процессов, возникающих проблем и достигнутых успехов для всех участников ВПО помогает поддерживать команду в курсе текущих дел, своевременно выявлять проблемы и оперативно корректировать курс движения проекта.

Руководителям ВПО необходимо целенаправленно развивать навыки удаленного лидерства: умение строить доверительные отношения на расстоянии, проявлять эмпатию к сотрудникам, четко формулировать задачи и предоставлять конструктивную обратную связь в цифровом формате. Особое внимание следует уделять индивидуальному общению; регулярные встречи один на один, проводимые хотя бы раз в одну-две недели с каждым членом команды, критически важны для обсуждения прогресса, выявления и решения проблем, планирования карьерного развития и просто для поддержания личного контакта. «Так, тесные рабочие отношения повышают удовлетворенность сотрудников на 50 %, а люди, у которых на работе есть лучший друг, в семь раз сильнее других вовлечены в работу», – сообщает Gallup, Inc. в своем исследовании 2022 года «The Increasing Importance of a Best Friend at Work» [8]. Необходимо целенаправленно работать над построением команды, организуя виртуальные тимбилдинги, неформальные онлайн-встречи в формате "виртуального кофе" и создавая общие чаты для нерабочего общения. Это помогает бороться с чувством изоляции и укреплять межличностные связи. Если возможно и целесообразно, стоит рассмотреть проведение периодических очных встреч всей команды. Кроме того, важно обучить команду навыкам тайм-менеджмента, самоорганизации, эффективной удаленной коммуникации и основам кибербезопасности.

Важно создавать среду, в которой сотрудники не боятся брать на себя инициативу и несут ответственность за свою часть работы. Необходимо активно культивировать взаимопомощь, поощряя обмен знаниями и опытом между членами команды и создавая механизмы для взаимной поддержки. Регулярное признание и поощрение успехов, как командных, так и индивидуальных, является важным инструментом поддержания высокой мотивации сотрудников.

Наконец, необходимо разработать и внедрить четкую политику безопасности, определяющую правила использования корпоративных и личных устройств, требования к сложности паролей, а также регламенты работы с конфиденциальной инфор-

мацией. Следует проводить регулярное обучение сотрудников по кибербезопасности, повышая их осведомленность об актуальных угрозах, таких как фишинг или вредоносное ПО, и обучая правилам безопасного поведения в сети. Важно использовать надежные технические средства защиты: использовать многофакторную аутентификацию (MFA), применять шифрование данных, устанавливать антивирусное ПО и, где это необходимо, системы предотвращения утечек данных (DLP). Также требуется регулярно проводить аудит безопасности для оценки существующих уязвимостей и проверки соответствия принятым политикам.

Заключение

Таким образом, Виртуальный Проектный Офис представляет собой динамичную, технологически зависимую структуру, которая использует преимущества удаленной работы для эффективного управления проектами. Он основан на принципах гибкости, глобальном доступе к ресурсам и цифровом взаимодействии, что делает его привлекательным инструментом для современных организаций. Однако именно эти характеристики порождают специфические вызовы. Организации, внедряющие или использующие ВПО, неизбежно сталкиваются с рядом серьезных рисков и потенциальных недостатков, вытекающих из самой природы удаленной, зависимой от технологий работы. Игнорирование этих вызовов может свести на нет все ожидаемые выгоды. В будущем мы увидим интеграцию ИИ в управление ВПО для автоматизации рутины и анализа рисков, но сегодня ключевым остается человеческий фактор: способность лидеров строить доверие и культуру на расстоянии определит, станет ли ВПО настоящим конкурентным преимуществом или просто вынужденной мерой.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Bakken, R. Challenges to Managing Virtual Teams (and how to Overcome Them) [Электронный ресурс] / R. Bakken // Harvard Division of Continuing Education: Professional Development Blog. – Updated: 11.03.2024. – URL: <https://professional.dce.harvard.edu/blog/challenges-to-managing-virtual-teams-and-how-to-overcome-them/> (датаобращения: 05.05.2025). – Загл. сэкрана.
2. Martins, L. L. Virtual teams: What do we know and where do we go from here? / L. L. Martins, L. L. Gilson, M. T. Maynard // Journal of Management. – 2004. – Vol. 30, № 6. – P. 805–835. – DOI: 10.1016/j.jm.2004.05.002.
3. Remote Work Research Findings [Электронный ресурс] // Society for Human Resource Management (SHRM). – Cop. 2024. – URL: <https://www.shrm.org/topics-tools/research/remote-work-research-findings> (датаобращения: 05.05.2025). – Загл. сэкрана.
4. O'Toole, K. Researchers: Flexibility May Be Key to Increased Productivity [Электронный ресурс]: [об исследовании Nicholas Bloom] / K. O'Toole // Stanford Graduate School of Business: Insights. – 01.06.2015. – URL: <https://www.gsb.stanford.edu/insights/researchers-flexibility-may-be-key-increased-productivity> (датаобращения: 05.05.2025). – Загл. сэкрана.
5. Hadley, C. N. Fighting Loneliness on Remote Teams [Электронный ресурс] / C. N. Hadley, M. Mortensen // Harvard Business Review. – 20.03.2024. – URL: <https://hbr.org/2024/03/fighting-loneliness-on-remote-teams> (датаобращения: 05.05.2025). – Загл. сэкрана.
6. Галкин, В. А. Кибербезопасность в эпоху удаленной работы: навигация по новым вызовам и лучшим практикам / В. А. Галкин, Н. В. Ржевская // Вестник науки. – 2023. – Т. 5, № 11 (68). – С. 1022–1028. – URL: <https://cyberleninka.ru/article/n/kiberbezopasnost-v-epohu>

udalennoy-raboty-navigatsiya-po-novym-vyzovam-i-luchshim-praktikam/viewer (дата обращения: 05.05.2025).

7. Summary – 4th Quarter 2024 [Электронный ресурс] // Anti-Phishing Working Group (APWG). – Соп. 2023. – URL: <https://apwg.org/trendsreports/> (дата обращения: 05.05.2025). – Загл. с экрана.

8. Mann, A. The Increasing Importance of a Best Friend at Work [Электронный ресурс] / A. Mann, R. Pendell // Gallup.com. – 15.06.2022. – URL: <https://www.gallup.com/workplace/39-3405/increasing-importance-best-friend-work.aspx> (дата обращения: 05.05.2025). – Загл. с экрана.

© А. В. Попиль, Р. П. Пак, О. В. Грицкевич, 2025

В. А. Сафонова¹, Д. А. Железных¹, Н. М. Дорохова¹✉

Перспективы развития водородного транспорта в России

¹Новосибирский электромеханический колледж,
г. Новосибирск, Российская Федерация
e-mail: natali_270168@mail.ru

Аннотация. В статье приведен анализ возможных перспектив развития водородного транспорта. Определено, что основным препятствием в использовании водорода в качестве топлива для автомобилей с ДВС является цена на водород, в то же время ученые ведут успешные разработки в этой области, и прогнозируется снижение цен к 2030 год. Водородные топливные процессоры намного экологичнее литийионных, которые сейчас используются, а автокарах. Выпуск пилотного грузовика «Камаз» подтверждает интерес со стороны не только разработчиков, но и Государственной власти к водородным технологиям. Значит у водородного транспорта в РФ есть перспективы для дальнейшего развития.

Ключевые слова: водородный транспорт, автомобиль, топливо

V. A. Safonova¹, D. A. Zheleznykh¹, N. M. Dorokhova¹✉

Prospects for the development of hydrogen transport in Russia

¹Novosibirsk Electromechanical College, Novosibirsk, Russian Federation
e-mail: natali_270168@mail.ru

Annotation. The article provides an analysis of the possible prospects for the development of hydrogen transport. It is determined that the main obstacle to using hydrogen as fuel for internal combustion engine vehicles is the price of hydrogen, while scientists are successfully developing in this area, and prices are expected to decrease by 2030. Hydrogen fuel processors are much more environmentally friendly than lithium-ion processors currently used in electric vehicles. The release of the Kamaz pilot truck confirms the interest of both developers and the government in hydrogen technologies. This means that hydrogen transport in Russia has prospects for further development.

Keywords: hydrogen transport, automobile, fuel

Введение

Автомобили, работающие на водороде не новость. Еще во время Великой Отечественной войны, в блокадном Ленинграде в 1941 году водородом заправляли грузовики. Разработал такой способ младший лейтенант Борис Шелищ. В газетах СССР писали, что, если закончится бензин русские смогут ездить на воде.

Нам стало интересно выяснить, почему водород, несмотря на его раннее использование в качестве альтернативы бензину и бесспорную экологичность, такую важную в наше время практически не используется в качестве моторного топлива.

Цель исследования: выяснить перспективы развития водородного транспорта в РФ.

Для достижения цели нами определены следующие задачи исследования:

- выяснить способы использования водорода в качестве водородного топлива;
- выяснить прогрессивные технологии по производству водорода;
- найти информацию о инновационных водородных автомобилях в РФ;

Объект исследования: научные разработки в области водородных технологий, позволяющие применять водород в качестве топлива в автомобилях.

Предмет исследования: возможные способы использования водорода в качестве автомобильного топлива.

Для решения поставленных задач мы использовали следующие методы: изучение, обобщение и анализ опыта существующих результатов по заданному направлению, сравнение, изучение мнения, моделирование, эксперимент, фотографирование.

Существует две технологии использования водорода в качестве автомобильного топлива. Классический, водород используется в двигателе внутреннего сгорания. Второй, инновационный, в котором используется водород – топливный элемент, когда при соединении водорода и кислорода вырабатывается электричество [1–3].

Методы и материалы

Чтобы понять, как работает топливный элемент, мы для наших студентов разработали установку демонстрирующую его действие.

На практике установлено, что водородные двигатели внутреннего сгорания работают эффективнее при высоких нагрузках, а водородные топливные элементы, напротив, более эффективны при низких, это предопределило направления их преимущественного использования: грузовой транспорт – на ДВС, легковые авто – на топливных элементах. Топливо, закачиваемое в баки автомобилей, будь то водород для сгорания в ДВС или водород, обеспечивающий работу топливных элементов, поставляется в сжатом газообразном виде. Это же касается и автомобилей с ДВС, работающих на природном газе [4].

Для того чтобы узнать о развитии водородного транспорта мы отправились в институт катализа где работает Алексей Александрович Печенкин, который разрабатывает водорода топливные элементы для автомобилей. По мнению ученых института, это в будущем, основным способом использования водорода для автомобилей.

Топливные элементы (процессоры) более безопасные в производстве и утилизации, по сравнению с батареей для электромобилей. Одним из перспективных разработок по мнению Алексей Александровича является процессор на основе алюминия с использованием катализаторов.

Ученые предполагают, что водородные микропроцессоры будут востребованы, как элементы питания не только автомобилей, но и всех мобильных устройств.

Симонов Михаил Николаевич, сотрудник институт катализа, познакомил нас с технологией производства водорода каталитическим способом, который может значительно снизить цену на водород.

По мнению ученых, производство водорода с помощью катализаторов – это перспективное направление потому, что можно использовать в качестве биомассы даже канализационные стоки (горячий пиролиз).

Производство водорода с использованием технологии газификации угля, также открывает большие перспективы для угольной промышленности.

Мы изучили рынок производителей топливных элементов рост производства с 2020 по 2024 составил 33 %, лидером является Toyota.

В России мы нашли две интересные разработки – это первый Российский грузовик на водородных топливных элементах, это пока пилотный вариант, но готовый грузовик уже есть. В Москве в индустриальном парке "Руднево" в рамках Международной конференции по водородной энергетике ПАО "КАМАЗ" и АФК "Система" представили пилотный проект грузового автомобиля КАМАЗ-53193 на водородных топливных элементах. Немаловажно, что первый образец грузового автомобиля на ВТЭ практически полностью импортозамещен. Автомобильная часть машины произведена КАМАЗом, за исключением тяговой батареи и электромоста. Что касается водородной установки, то по словам руководителя проекта Центра Водородных Технологий АФК "Система" Егора Шульги, около 30 % основных ее компонентов произведено в России.

Второй интересный пилотный образец это водородный Aurus. Он создан на базе седана Aurus Senat и заправляется водородом. По словам начальника управления по продукту ФГУП «НАМИ» Михаила Кондратьева, это гибридный автомобиль с электродвигателем, но электричество генерируется прямо на борту благодаря электрохимическому генератору топливной ячейки. Водород вступает в реакцию с кислородом, в результате чего вырабатывается электричество, которое идет на электромотор и колеса. Машина способна разогнаться до 100 км/ч за четыре секунды, не загрязняя окружающую среду. Из выхлопной трубы она выбрасывает только воду. С полным баком автомобиль может проехать 870 километров.

Интересно рассмотреть автомобиль, работающий на метане с добавлением водорода. Уникальность в том, что водород генерируется прямо в самом автомобиле, электролизер вырабатывает 0,5 литра водорода в минуту, этого достаточно чтобы увеличить КПД на 20 % и снизить расход топлива на столько же [5–8].

Заключение

В результате работы над проектом, мы выяснили что основным препятствием в использовании водорода в качестве топлива для автомобилей с ДВС является цена на водород, можно заметить, что ученые ведут успешные разработки в этой области, и к 2030 году цены значительно снизятся.

Водородные топливные процессоры намного экологичнее литийионных, которые сейчас используются, а автокарах.

Выпуск пилотного грузовика «Камаз» подтверждает интерес со стороны не только разработчиков, но и Государственной власти к водородным технологиям. Значит у водородного транспорта в РФ есть перспективы для дальнейшего развития.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. <http://refdb.ru/download/> (дата обращения: 25.04.2025).
2. alarmtrade-kavkaz.ru (дата обращения: 2.05.2025).
3. <http://www.liveinternet.ru/> (дата обращения: 22.04.2025).
4. http://www.abitura.com/modern_physics/hydro_energy/ (дата обращения: 12.04.2025).
5. <http://zap-online.ru/> (дата обращения: 22.04.2025).
6. Иродов И. Е Физика макросистем, М., Физматлит, 2001
7. <http://dialogs.org.ua> (дата обращения: 10.05.2025).
8. <http://ecokom.ru/viewtopic.php> (дата обращения: 28.04.2025).
9. <http://www.facepla.net/> (дата обращения: 22.04.2025).
10. <http://www.forum.priroda.su/> (дата обращения: 22.04.2025).

© В. А. Сафонова, Д. А. Железных, Н. М. Дорохова, 2025

П. А. Уфилин¹, Д. А. Аничев¹✉

Кадастр как сервис: адаптация ITSM-принципов в управлении земельно-имущественными процессами

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: anichevdmirijg@gmail.com

Аннотация. Современные кадастровые системы сталкиваются с необходимостью перехода от бюрократических процедур к клиентоориентированному сервису. Внедрение принципов IT-сервисного менеджмента (ITSM) позволяет систематизировать работу с заявками, задачами и инцидентами, повышая эффективность управления земельными ресурсами. В данной работе исследуются, как ключевые процессы ITSM – управление заявками (Request Fulfillment), обработка инцидентов (Incident Management), управление изменениями (Change Management) и контроль уровня услуг (SLA), могут быть адаптированы для кадастровой сферы. Особое внимание уделяется автоматизации workflow, трекингу статусов заявок на регистрацию прав, исправлению ошибок в реестрах и согласованию изменений между ведомствами. Применение ITSM-методологий (ITIL, COBIT) позволяет перевести земельно-имущественные процессы в цифровой формат с четкими регламентами, сроками и ответственностью, что сокращает время оказания услуг и повышает их прозрачность.

Ключевые слова: кадастр как сервис, ITSM, управление заявками, инциденты, workflow, ITIL, автоматизация земельных процессов

P. A. Ufillin¹, D. A. Anichev¹✉

Cadastre as a service: adaptation of ITSM-principles in the management of land and property processes

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: anichevdmirijg@gmail.com

Abstract. Modern cadastral systems face the need to move from bureaucratic procedures to a customer-oriented service. The implementation of the principles of IT service management (ITSM) makes it possible to systematize work with applications, tasks and incidents, increasing the efficiency of land management. This paper explores how key ITSM processes – Request Fulfillment, Incident Management, Change Management, and Service Level Control (SLA) – can be adapted to the cadastral sphere. Special attention is paid to workflow automation, tracking the status of applications for registration of rights, correcting errors in registers and coordinating changes between departments. The use of ITSM methodologies (ITIL, COBIT) makes it possible to transfer land and property processes to a digital format with clear regulations, deadlines and responsibilities, which reduces the time required to provide services and increases their transparency.

Keywords: cadastre as a service, ITSM, application management, incidents, workflow, ITIL, automation of land processes

Вызов цифровой трансформации госуслуг требует пересмотра традиционных подходов к управлению земельно-имущественными процессами. Кадастровая система, исторически построенная на бумажном документообороте и дли-

тельных административных процедурах, сегодня сталкивается с необходимостью перехода на сервисную модель, ориентированную на удобство граждан и бизнеса. Одним из перспективных направлений оптимизации этих процессов является адаптация принципов IT-сервисного менеджмента доказавших свою эффективность в корпоративном IT-секторе.

ITSM, ITIL, COBIT и ISO 20000, предлагает системный подход к управлению сервисами через четкие процессы: обработку заявок, управление инцидентами, контроль изменений и соблюдение соглашений об уровне услуг (SLA). Применение этих механизмов в кадастровой сфере позволит перейти от рутинных бумажных процедур к цифровым сервисам с прозрачным workflow, автоматизированным назначением задач и контролем исполнения [1–5].

Актуальность исследования обусловлена растущими требованиями к скорости и качеству оказания кадастровых услуг, а также необходимостью минимизации ошибок в реестрах недвижимости. Внедрение ITSM-практик способно устранить узкие места в межведомственном взаимодействии, сократить сроки регистрации прав и повысить удовлетворенность пользователей.

Методы и материалы

В рамках данного исследования применяется комплексный подход, объединяющий теоретический анализ и практическое моделирование. Основные методы включают:

1. Анализ методологий ITSM. Изучение ключевых принципов и процессов ITIL, COBIT и других стандартов ITSM. Определение возможностей их адаптации к кадастровой деятельности;

2. Моделирование процессов. Описание текущих кадастровых процедур (AS-IS модель). Разработка оптимизированных процессов (TO-BE модель) с учетом: управления заявками и обращениями. Обработки инцидентов и ошибок. Контроль изменений в реестрах;

3. Сравнительный анализ. Исследование опыта цифровизации в кадастровой сфере. Выявление лучших практик организации сервисных процессов;

4. Прототипирование решений. Разработка моделей ключевых workflow. Тестирование подходов к автоматизации процессов;

Исследование основывается на:

1. Нормативно-правовых документах, регулирующих кадастровую деятельность;

2. Методических материалах по ITSM и управлению сервисами;

3. Данных о текущих процессах оказания кадастровых услуг;

4. Инструментах моделирования бизнес-процессов.

Особое внимание уделяется анализу взаимодействия между участниками процессов и возможностям повышения эффективности через внедрение сервисного подхода [6–8].

Результаты

Проведенное исследование позволило получить следующие ключевые результаты в области адаптации ITSM-принципов к управлению кадастровыми процессами:

1. Модель сервис-ориентированного кадастра. Разработана концептуальная модель кадастра как сервиса, включающая: четкую классификацию типов заявок (регистрация, исправление ошибок, предоставление сведений), стандартизированные workflow обработки запросов, механизмы отслеживания статусов обращений;

2. Оптимизированные процессы. На основе ITSM-подходов предложены усовершенствованные схемы: управления заявками: единая система приема и маршрутизации. Автоматическое назначение ответственных. Контроль сроков исполнения. Обработки инцидентов: типизация реестровых ошибок. Алгоритмы их устранения. Процедуры уведомления заявителей;

3. Механизмы контроля качества. Разработаны предложения по: внедрению сервисных уровней (SLA) для разных типов запросов, системе мониторинга удовлетворенности пользователей, регулярному аудиту процессов;

4. Предложены варианты интеграции ITSM-решений: использование платформ для управления сервисами, подключение к существующим государственным информационным системам. Рассмотрены возможности автоматизации операций;

5. Выявлены ключевые аспекты трансформации:

- перераспределение роли и ответственности;
- обучение персонала;
- изменение норм базы;
- применение ITSM-подходов позволит трансформировать кадастровую систему в ориентированный под клиента сервис с прозрачными процессами.

Реализация предложенных решений поспособствует:

- повышению скорости обработки запросов;
- уменьшению количества ошибок;
- улучшению качества взаимодействия с клиентами и учреждениями.

Обсуждение

Ключевые достижения при внедрении подобной системы позволят привести к следующим улучшениям:

1. Сервисная трансформация: Разработанная модель переводит кадастр из административной системы в клиентоориентированный сервис, что соответствует современным трендам цифровизации государственных услуг. Особую ценность представляет стандартизация workflow, позволяющая минимизировать субъективный фактор в обработке запросов;

2. Практическая реализуемость: Предложенные решения базируются на проверенных ITSM-методологиях, что снижает риски внедрения. Важно отметить, что архитектура решений предусматривает интеграцию с существующими

информационными системами, обеспечивая преемственность и снижая затраты на переходный период. Проблемные аспекты и ограничения:

- организационные барьеры: необходимость изменения устоявшихся административных процедур. Сопротивление персонала новым методам работы;

- требования к переподготовке кадров.

3. Технологические вызовы:

- зависимость от совместимости с legacy-системами;

- потребность в адаптации стандартных ITSM-решений под специфику кадастровой деятельности.

Перспективные направления:

1. Поэтапное внедрение: целесообразно начинать с пилотных проектов по автоматизации наиболее проблемных процессов (например, исправление реестровых ошибок), с последующим масштабированием успешных решений;

2. Развитие экосистемы сервисов: перспективным представляется создание единой платформы кадастровых сервисов с возможностью интеграции смежных услуг (например, градостроительных, налоговых);

3. Исследовательские задачи: требуют дальнейшей проработки вопросы:

- оптимизации межведомственного взаимодействия, разработки специализированных метрик качества услуг;

- создания адаптивных SLA для различных категорий пользователей.

Предложенный подход открывает новые возможности для повышения эффективности кадастровой системы. Однако его реализация требует комплексного учета организационных, технологических и нормативных факторов. Дальнейшие исследования целесообразно направить на разработку конкретных механизмов внедрения и оценку их эффективности в реальных условиях [9–10].

Заключение

Исследование подтвердило эффективность применения ITSM-принципов для модернизации кадастровой системы. Разработанная модель "Кадастр как сервис" позволяет:

1. Основные преимущества:

- переход на клиентоориентированное обслуживание;

- стандартизацию и прозрачность процессов;

- повышение управляемости и контроля качества.

2. Ключевые результаты:

- адаптированные ITSM-процессы для кадастровой сферы;

- модели workflow обработки запросов;

- механизмы контроля SLA и качества услуг.

3. Перспективы внедрения:

- поэтапная реализация через пилотные проекты;

- интеграция с существующими информационными системами;

– развитие нормативной базы.

Проведенное исследование создает основу для цифровой трансформации кадастровой деятельности, сочетая проверенные ITSM-методологии со специфической земельно-имущественных процессов. Реализация предложенного подхода требует межведомственного взаимодействия и поэтапного внедрения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Агапов, Е. П. Информационные технологии управления земельно-имущественным комплексом / Е. П. Агапов, В. В. Курейчик. – М.: Финансы и статистика, 2008. – 320 с.
2. Белов, А. Н. ITIL 4. Основы IT Service Management / А. Н. Белов. – М.: ДМК Пресс, 2020. – 288 с.
3. Вендеров, А. М. CASE-технологии. Современные методы и средства проектирования информационных систем / А. М. Вендеров. – М.: Финансы и статистика, 2004. – 208 с.
4. Глухов, В. В. Управление земельными ресурсами: учебное пособие / В. В. Глухов, М. Д. Довдий. – СПб.: Лань, 2011. – 448 с.
5. Дейкстра, Э. Дисциплина программирования / Э. Дейкстра. – М.: Мир, 1978. – 275 с.
6. Землякова, Г. Л. Информационные системы и технологии в землеустройстве и кадастре / Г. Л. Землякова. – М.: КолосС, 2008. – 304 с.
7. Кендалл, К. Е. Современные методы управления земельными ресурсами / К. Е. Кендалл, Дж. Е. Кендалл. – М.: БИНОМ. Лаборатория знаний, 2007. – 592 с.
8. Литвинов, А. Ю. ITIL v3 для профессионалов. Практическое руководство / А. Ю. Литвинов. – М.: Альпина Паблишер, 2010. – 368 с.
9. Романов, В. П. Информационные технологии в экономике / В. П. Романов, Ю. Б. Рубин, В. И. Солдаткин. – М.: ЮНИТИ-ДАНА, 2000. – 400 с.
10. Скворцов, А. В. Управление ИТ-сервисами на основе ITIL / А. В. Скворцов. – М.: ИТ Пресс, 2007. – 288 с.

© П. А. Уфилин, Д. А. Аничев, 2025

Д. А. Шергин^{1✉}, Д. Е. Пешков¹

Разработка виртуального стенда для практического тестирования информационной безопасности Active Directory

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: shergindanil717@gmail.com

Аннотация. Статья посвящена разработке виртуального стенда для практического тестирования информационной безопасности Active Directory (AD), направленного на подготовку специалистов в области кибербезопасности. Актуальность исследования обусловлена широким распространением AD в корпоративных сетях и высокой частотой успешных атак из-за недостаточной защищенности ее компонентов. В работе использованы методы виртуализации (VMware Workstation 17 Pro) и моделирования корпоративной инфраструктуры, включающей виртуальные машины с различными операционными системами (Linux Ubuntu, Windows Server 2019, Windows 10). На стенде реализованы ключевые уязвимости AD, такие как слабая парольная политика, устаревшее ПО, некорректные настройки доступа и другие. Результатом исследования стал функциональный стенд, имитирующий реальную корпоративную сеть, который позволяет начинающим специалистам отрабатывать методы защиты и атаки в контролируемой среде. Стенд эффективно решает проблему нехватки практических навыков у начинающих специалистов.

Ключевые слова: информационная безопасность, безопасность инфраструктуры, Active Directory, виртуальный стенд

D. A. Shergin^{1✉}, D. E. Peshkov¹

Development of a virtual bench for practical testing of Active Directory information security

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: shergindanil717@gmail.com

Abstract. The article is devoted to the development of a virtual bench for practical testing of Active Directory (AD) information security aimed at training specialists in the field of cyber security. The relevance of the research is due to the widespread use of AD in corporate networks and the high frequency of successful attacks due to insufficient security of its components. The work uses virtualisation methods (VMware Workstation 17 Pro) and simulation of corporate infrastructure including virtual machines with different operating systems (Linux Ubuntu, Windows Server 2019, Windows 10). The stand implemented key AD vulnerabilities such as weak password policy, outdated software, incorrect access settings and others. The result of the research is a functional stand simulating a real corporate network, which allows novice specialists to practice defence and attack methods in a controlled environment. The stand effectively solves the problem of lack of practical skills among novice specialists.

Keywords: information security, infrastructure security, Active Directory, virtual bench

Введение

В мире стремительного роста и развития информационных систем и технологий все больше компаний старается наладить и выстроить все свои процессы, приведя их к единым стандартам и структуре. Компании активно внедряют Active Directory (далее – AD) для стандартизации процессов, так как эта технология удобна и популярна – ее используют 75 % крупнейших ИТ-компаний по всему миру. Однако управление привилегированным доступом в AD остается уязвимым местом: по данным Positive Technologies, в 64 % случаев злоумышленники могут получить доступ к конфиденциальной информации за 1–7 дней. Отсюда следует, что существует проблема в нехватке грамотных специалистов для оценки защищенности Active Directory и ее компонентов. Исходя из данной проблемы, было принято решение о разработке виртуального стенда для практического тестирования информационной безопасности Active Directory.

Актуальность

Active Directory – это служба каталогов, разработанная компанией Microsoft для Windows-доменных сетей. Она представляет собой централизованную и стандартизированную систему, которая автоматизирует управление пользовательскими данными, безопасностью и ресурсами сети.

Основные функции данной технологии:

- управление учетными записями пользователей;
- аутентификация и авторизация;
- групповые политики;
- управление ресурсами сети.

Active Directory является основой для управления большей части ресурсов организаций, использующих инфраструктуру Windows. Статистика, которую приводят Microsoft, показывает, что число организаций использующих данную технологию превысило 12,8 млн., а количество пользователей достигло более 950 млн., данные показатели выросли за последние 5 лет на 30 и 45 процентов соответственно, а из списка 500 крупнейших компаний по версии Fortune около 90 % из них используют AD [1].

Однако несмотря на достаточную защищенность данной технологии, многие компании не осуществляют надлежащей безопасной настройки данной технологии, что приводит к компрометации корпоративных ресурсов и активов компаний.

Так исходя из отчета РТ по итогам аудита информационной безопасности за 2023 год в 100 % проектов, в которых проводилось внутреннее тестирование на проникновение, удалось получить контроль над доменом.

В 81 % проектов общий уровень защищенности был определен как низкий.

Самое быстрое получение максимальных привилегий в домене Active Directory – 6,5 часов после начала проведения работ по внутреннему пентесту, в остальных этот показатель варьируется от 1 до 7 дней. В 64 % проектов злоумышленник мог бы получить несанкционированный доступ к важной конфи-

денциальной информации. В некоторых случаях эта информация являлась интеллектуальной собственностью или служебной перепиской сотрудников.

Количество шагов требуемых для получения максимальных привилегий в домене составило до 8 шагов в 40 % случаях, что является достаточно критичным показателем и ведет к быстрой компрометации корпоративной сети компании [2].

Вышеперечисленные тезисы показывают, что несмотря на удобство и популярность использования Active Directory многими компаниями, не каждая компания уделяет должное внимание безопасности этой технологии, что может привести к компрометации корпоративных ресурсов и активов компаний. Отсюда следует, что существует проблема в нехватке грамотных специалистов для оценки защищенности Active Directory и ее компонентов. Исходя из данной проблемы, было принято решение о разработке виртуального стенда для практического тестирования информационной безопасности Active Directory, который позволит студентам по направлению Информационная безопасность отработать свои знания и умения на практике и получить практический опыт оценки защищенности Active Directory, приближенный к реальным условиям [3].

Актуальные уязвимости Active Directory

Опираясь на результаты пентеста (аудита информационной безопасности) 2023 года от компании Positive Technologies, которые представляют собой собранную статистику за целый год и ее полный анализ, можно выделить ключевые уязвимости [2, 4]. Данные уязвимости встречаются во время тестирования на проникновение инфраструктуры организаций и Active Directory в частности:

- слабая парольная политика;
- устаревшее ПО и протоколы;
- небезопасная конфигурация;
- некорректная настройка политик доступа.

Данный перечень охватывает большее количество атак, которые можно реализовать в рамках данных уязвимостей, которые способны привести к несанкционированному доступу в корпоративную сеть. В частности, компрометация учетной записи администратора способна повлечь за собой полный контроль над критически важными системами, утечку конфиденциальных данных и даже саботирование бизнес-процессов.

Использование неподдерживаемых версий программного обеспечения и устаревших криптографических протоколов представляет серьезную угрозу информационной безопасности и делает систему открытой для известных атак. Злоумышленники могут воспользоваться публично доступными эксплоитами. Кроме того, слабые протоколы шифрования позволяют перехватывать и модифицировать передаваемые данные, что особенно опасно при обработке персональной информации или финансовых транзакций.

Некорректная настройка серверов, баз данных и сетевого оборудования значительно увеличивает поверхность атаки. Распространенные ошибки включают

использование стандартных учетных записей с привилегированным доступом, оставление открытых портов для удаленного управления (RDP, SSH без защиты) и отсутствие сегментации сети [5]. Подобные упущения позволяют злоумышленникам относительно легко проникать в систему, перемещаться внутри нее и внедрять вредоносное ПО. Например, недостаточная защита интерфейса управления базой данных может привести к утечке всей хранимой информации, а некорректные настройки межсетевого экрана – к несанкционированному доступу извне [6].

Отсутствие строгого контроля над правами пользователей и избыточные привилегии создают условия для внутренних угроз и горизонтального перемещения злоумышленников в случае компрометации. Если сотрудники имеют доступ к ресурсам, не требующимся для их работы, это нарушает принцип минимальных привилегий и увеличивает риск утечки или повреждения данных. В частности, недостаточная сегментация сети позволяет злоумышленнику, получившему доступ к одной системе, быстро распространять влияние на другие узлы.

Практическая часть исследования

На начальном этапе создания стенда была определена основная цепочка атаки, которая будет заложена в стенде (рис. 1).

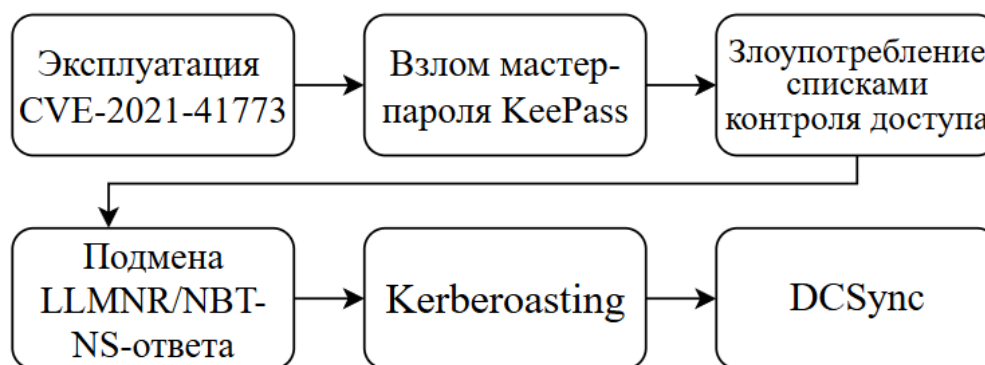


Рис. 1. Цепочка атаки

Для создания стенда было выбрано средство виртуализации VMware workstation 17 Pro. Данный инструмент позволяет запускать на одном физическом компьютере несколько виртуальных машин с различными операционными системами. В рамках стенда были настроены четыре виртуальные машины (далее – VM):

- VM №1 на базе операционной системы Linux Ubuntu 20.04;
- VM №2 на базе операционной системы Windows Server 2019;
- VM №3 на базе операционной системы Windows 10;
- VM №4 на базе операционной системы Windows 10.

В стенде было реализовано два ключевых этапа при которых атакующий должен сначала закрепиться внутри первой машины, а затем получить доступ в локальную сеть. Для этого на VM №1 было настроено два сетевых интерфейса, один из которых предоставляет выход в интернет, а второй позволяет взаимодействовать с машинами из локальной сети, которые в свою очередь не имеют выхода в интернет, находятся в одном домене и могут беспрепятственно взаимодействовать между собой. VM №2 выступает в роли контроллера домена (рис. 2).

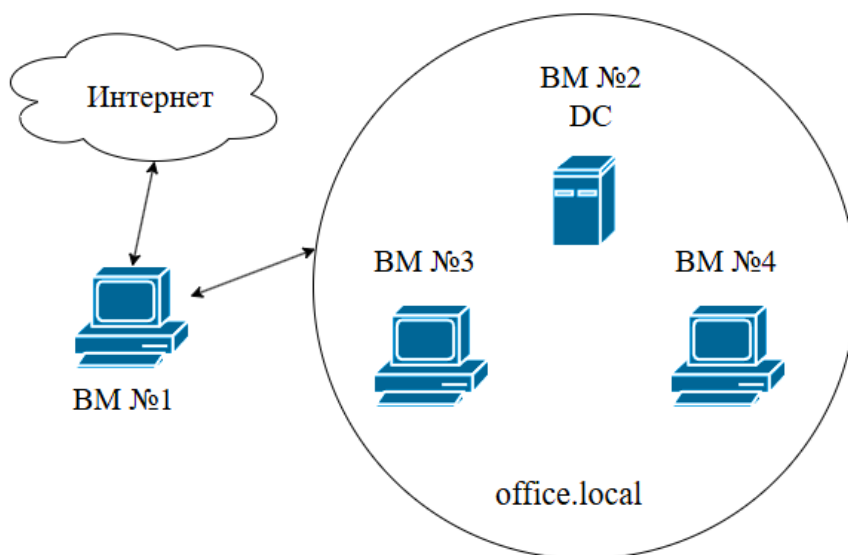


Рис. 2. Сетевое взаимодействие стенда

На VM1 было развернуто веб-приложение, использующее уязвимую версию веб-сервера Apache 2.4.49. А также был создан скрипт, который предоставляет информацию о сервере и использует протокол CGI. В дальнейшем это позволит проэксплуатировать уязвимость CVE-2021-41773 (рис. 3).

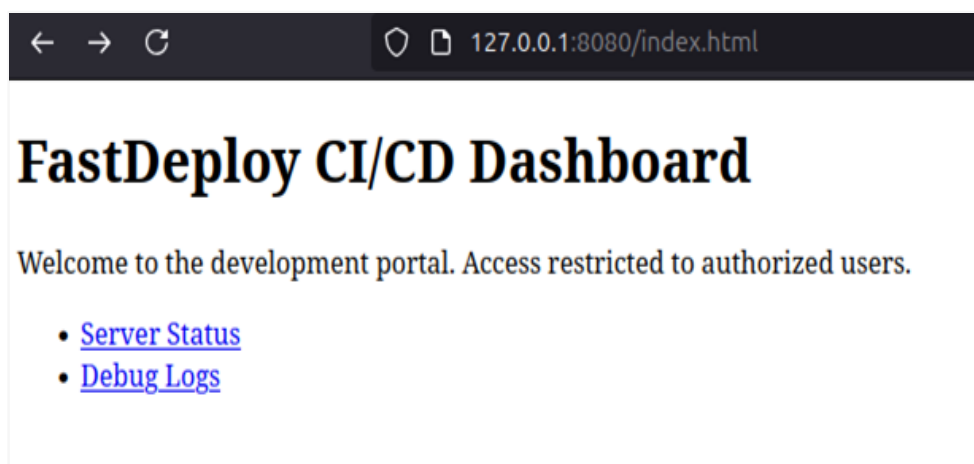


Рис. 3. Уязвимое веб-приложение

Также на VM1 был установлен менеджер паролей KeePass со слабым мастер-паролем, подверженным перебору в автономном режиме. Данный менеджер паролей хранит внутри себя учетные данные к удаленному рабочему столу пользователя на VM3 (рис. 4).

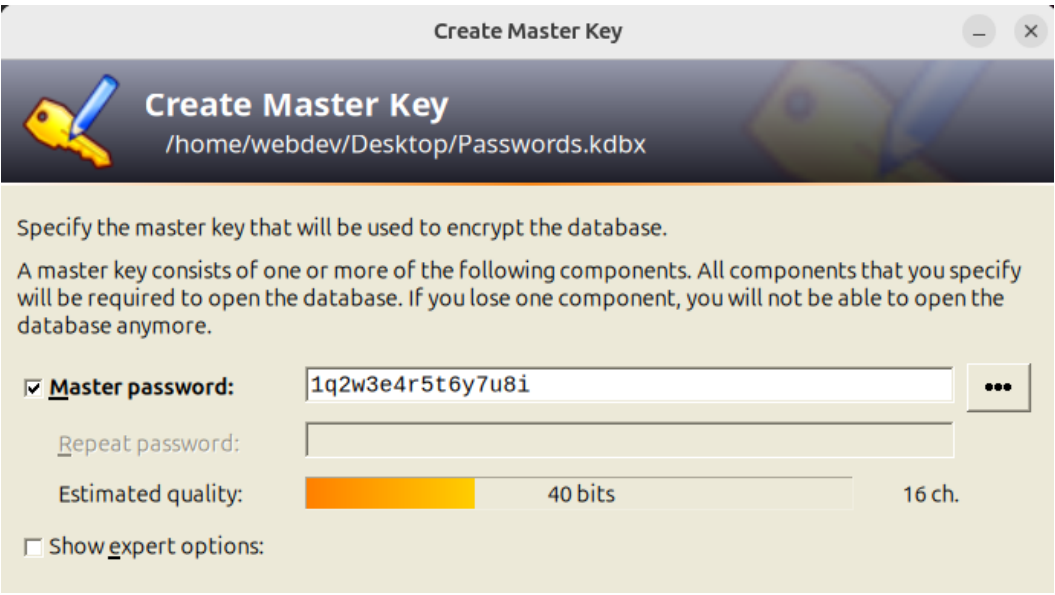


Рис. 4. Сетевое взаимодействие стенда

В домене office.local были созданы группы и соответствующие им пользователи. Данные группы имитируют разные отделы в компании, для каждой группы настроены свои политики доступа, некоторые из которых специально настроены некорректно что позволит повысить свои привилегии как вертикально, так и горизонтально табл. 1.

Таблица 1

Группы и пользователи в домене office.local

Название группы в домене	Имя пользователя
SupportTeam	Vlad_Support
	Victor_Support
Sellers	Petr_Seller
	Max_Seller
ExternalContractors	Iskra_manager
IT_Managers	Roman_IT_Manager
NetAdmins	Yra_SysAdmin
DataCenter	Alex_DataCenter
SeverOps	Vlad_Support
	Ivan_Support

В рамках домена была настроена общая сетевая папка, доступная всем пользователям по протоколу SMB. Внутри нее созданы дополнительные папки с различными уровнями доступа, которые в дальнейшем будут использоваться для задуманных атак [7].

Заключение

В результате был разработан виртуальный стенд, который представляет из себя некую корпоративную инфраструктуру вымышленной компании. Данный стенд можно использовать в качестве практической отработки навыков начинающих специалистов в области тестирования на проникновения Active Directory.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. IT-Lite. Обзор возможностей Active Directory: фундамент для инфраструктуры. – Текст : электронный // IT-Lite : [сайт]. – URL: <https://www.it-lite.ru/blog/iaas/obzor-vozmozhnostey-active-directory/> – (дата обращения: 29.04.2025).
2. Итоги пентестов 2023. – Текст : электронный // Positive Technologies : [сайт]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2023/> – (дата обращения: 29.04.2025).
3. ADMINVPS. Что такое Active Directory в Windows. – Текст : электронный // ADMINVPS : [сайт]. – URL: <https://adminvps.ru/blog/chto-takoe-active-directory-v-windows/> (дата обращения 12.05.2025).
4. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. – Текст : электронный // Positive Technologies : [сайт]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/> – (дата обращения: 22.04.2025).
5. J. Neumeier, A.L. Zelezinskii, O.V. Arhipova. Management of security of information in companies // Экономический вектор. 2023. №2. С.38-41.
6. Методика оценки угроз безопасности информации. – Текст : электронный // Федеральная служба по техническому и экспортному контролю : [сайт]. – URL: <https://fstec.ru/component/attachments/download/2919> (дата обращения: 20.12.2023).
7. Скоропупов И. О., Бубнова А. А., Карманов И. Н. Методы проведения атак для получения прав администратора домена в Active Directory // Интерэкспо Гео-Сибирь. – Новосибирск: 2019. – Т. 6. – №. 1. – С. 187-192.

© Д. А. Шергин, Д. Е. Пешков, 2025

Ю. О. Якович¹✉, А. Н. Поликанин¹

СКУД "Орион": Реализация на практическом примере

¹Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: yakovich.yury@yandex.ru

Аннотация. В статье рассматривается процесс внедрения системы контроля и управления доступом (СКУД) «Орион» на примере завода строительных материалов. Описываются особенности проектирования, этапы реализации и результаты эксплуатации системы, а также ее влияние на повышение уровня информационной и физической безопасности предприятия. Особое внимание уделяется интеграции СКУД с другими системами безопасности, обеспечению режима коммерческой тайны и контролю доступа к критически важным объектам. Проведен анализ эффективности внедренных технических мер, выявлены преимущества и проблемы, а также даны рекомендации по дальнейшему развитию системы. Практический опыт предприятия демонстрирует, что применение модульной и масштабируемой архитектуры СКУД «Орион» позволяет гибко адаптироваться к изменяющимся требованиям безопасности и способствует устойчивому развитию производства. Исследование включает количественный анализ инцидентов безопасности до и после внедрения системы, а также оценку экономической эффективности проекта.

Ключевые слова: СКУД, Орион, контроль доступа, безопасность, коммерческая тайна, завод строительных материалов, интеграция систем

Y. O. Yakovich¹✉, A. N. Polikanin¹

SKUD "Orion": implementation using a practical example

¹Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: yakovich.yury@yandex.ru

Abstract. The article discusses the process of implementing the Orion access control and management system using the example of a building materials plant. The features of the design, the stages of implementation and the results of operation of the system are described, as well as its impact on increasing the level of information and physical security of the enterprise. Particular attention is paid to the integration of ACMS with other security systems, ensuring trade secrets and access control to critical facilities. An analysis of the effectiveness of the implemented technical measures has been carried out, advantages and problems have been identified, and recommendations for further development of the system have been given. The company's practical experience demonstrates that the use of Orion's modular and scalable ACS architecture allows for flexible adaptation to changing safety requirements and contributes to the sustainable development of production. The study includes a quantitative analysis of security incidents before and after the implementation of the system, as well as an assessment of the economic effectiveness of the project.

Keywords: ACMS, Orion, access control, security, trade secret, building materials plant, system integration

Введение

Современные промышленные предприятия сталкиваются с необходимостью комплексной защиты информации и материальных ресурсов. Особое значение приобретает обеспечение режима коммерческой тайны, а также предотвращение несанкционированного доступа к объектам и помещениям [1]. В этой связи внедрение систем контроля и управления доступом (СКУД) становится одним из ключевых направлений повышения уровня безопасности [2]. СКУД «Орион» представляет собой интегрированное решение, позволяющее централизованно управлять доступом, контролировать перемещение сотрудников и обеспечивать защиту критически важных зон [3].

Актуальность данной темы обусловлена несколькими факторами. Во-первых, в условиях высокой конкуренции на рынке строительных материалов защита коммерческой тайны и интеллектуальной собственности становится критически важной для сохранения конкурентных преимуществ [1]. Во-вторых, требования законодательства, в частности Федерального закона №98-ФЗ «О коммерческой тайне», обязывают предприятия принимать меры по защите конфиденциальной информации [1]. В-третьих, современные угрозы безопасности, включая промышленный шпионаж, кражи и саботаж, требуют комплексного подхода к обеспечению безопасности предприятия [4, 5].

Целью данной работы является описание практического опыта внедрения СКУД «Орион» на заводе строительных материалов, а также исследование эффективности реализованных технических мер в обеспечении информационной и физической безопасности. В статье рассматриваются этапы проектирования системы, особенности настройки уровней доступа, интеграция с другими средствами безопасности и анализ результатов эксплуатации [6].

Научная новизна исследования заключается в разработке методики оценки эффективности СКУД на промышленном предприятии с учетом специфики производства строительных материалов, а также в создании модели интеграции системы контроля доступа с другими элементами комплексной системы безопасности [7].

Методы и методики

Проектирование и внедрение СКУД «Орион» на предприятии осуществлялось с учетом требований Федерального закона №98-ФЗ «О коммерческой тайне» [1], а также отраслевых стандартов информационной безопасности [8]. В качестве основы использовалась модульная архитектура комплекса, включающая программное обеспечение АРМ «Орион Про» [3], контроллеры доступа, считыватели ключей-меток и системы видеонаблюдения.

Теоретической базой исследования послужили работы отечественных и зарубежных авторов в области информационной безопасности и контроля доступа. В частности, были использованы методики оценки рисков информационной безопасности, предложенные в работах Астахова А. М. [9], Малюка А. А. [5], а так-

же международные стандарты ISO/IEC 27001 и ISO/IEC 27002, регламентирующие требования к системам управления информационной безопасностью [8].

Проектирование СКУД «Орион» на заводе строительных материалов осуществлялось в несколько этапов:

1. Анализ объекта защиты, включающий изучение территории предприятия, расположения зданий и помещений, определение критически важных зон и оценку существующих мер безопасности [10];
2. Разработка концепции системы контроля доступа, определение требований к функциональности, надежности и масштабируемости системы [11];
3. Выбор технических средств и программного обеспечения, соответствующих требованиям концепции [12];
4. Проектирование архитектуры системы, включая схемы размещения оборудования, кабельные трассы и точки подключения к инженерным системам;
5. Разработка алгоритмов работы системы, включая определение уровней доступа, временных зон и сценариев реакции на события.

Для определения уровней доступа была проведена классификация сотрудников по функциональным группам: высшее руководство, бухгалтерия, информационный отдел, руководители отделов и рядовые сотрудники. Каждой группе был назначен соответствующий набор прав доступа, что позволило ограничить доступ к конфиденциальной информации и критически важным помещениям [13].

Для оценки эффективности внедренной системы контроля доступа были использованы следующие методы:

1. Статистический анализ инцидентов безопасности до и после внедрения СКУД, включая несанкционированный доступ, кражи и утечки информации;
2. Анкетирование сотрудников предприятия для оценки удобства использования системы и ее влияния на рабочие процессы [6];
3. Аудит журналов доступа для выявления аномалий и потенциальных угроз;
4. Экономический анализ затрат на внедрение и эксплуатацию системы в сравнении с предотвращенными потерями;
5. Внедрение системы сопровождалось разработкой локальных нормативных документов, регламентирующих порядок работы с системой, выдачи и учета ключей, а также контроля доступа [14].

Результаты

В результате проектирования и внедрения на заводе строительных материалов была реализована комплексная система контроля и управления доступом на базе СКУД «Орион» [3]. Архитектура системы включает следующие основные компоненты:

1. Центральный сервер с установленным программным обеспечением АРМ «Орион Про», обеспечивающий централизованное управление системой, хранение базы данных пользователей и журналов событий [3];
2. Рабочие станции операторов системы, расположенные в помещении службы безопасности и на проходной предприятия;

3. Контроллеры доступа С2000-2, установленные на каждой точке прохода и объединенные в единую сеть по интерфейсу RS-485;

4. Считыватели ключей-меток, установленные на входах в здания, помещения и другие контролируемые зоны;

5. Электромагнитные замки и турникеты, управляемые контроллерами доступа;

6. Система видеонаблюдения, интегрированная с СКУД для обеспечения визуального контроля точек прохода [7].

Всего на предприятии было установлено 42 точки контроля доступа, охватывающие все критически важные зоны, включая входы на территорию, производственные цеха, склады, административные помещения, серверные и помещения с конфиденциальной информацией.

Одним из ключевых элементов внедренной системы стала разработка и реализация многоуровневой модели доступа, учитывающей организационную структуру предприятия и требования к защите информации [13]. Были определены следующие уровни доступа:

Высшее руководство (генеральный директор, заместители директора) – доступ во все зоны предприятия, включая общие зоны, бухгалтерию, серверную, личные кабинеты, отделы и зоны руководства.

Бухгалтерия – доступ в общие зоны и помещения бухгалтерии.

Информационный отдел – доступ в общие зоны, серверную, личный кабинет и, при необходимости, в бухгалтерию.

Руководители отделов – доступ в общие зоны, свой отдел и личный кабинет начальника отдела.

Рядовые сотрудники – доступ в общие зоны и свой отдел или производственное помещение.

Для каждого уровня доступа были определены временные зоны, в которые разрешен доступ в соответствующие помещения. Например, рядовые сотрудники имеют доступ в рабочие помещения только в рабочее время, в то время как руководство и служба безопасности – круглосуточно.

Внедрение СКУД «Орион» стало важным элементом обеспечения режима коммерческой тайны на предприятии в соответствии с требованиями Федерального закона №98-ФЗ [1]. Система позволила реализовать следующие меры защиты:

1. Ограничение доступа к информации, составляющей коммерческую тайну, путем контроля физического доступа в помещения, где хранится или обрабатывается такая информация [1];

2. Учет лиц, получивших доступ к коммерческой тайне, через систему журналирования событий доступа [13];

3. Регулирование отношений по использованию информации, составляющей коммерческую тайну, путем разграничения прав доступа и контроля за их соблюдением [15];

4. Контроль за соблюдением режима коммерческой тайны через мониторинг событий доступа и анализ журналов системы.

Обсуждение

Практический опыт внедрения СКУД «Орион» на предприятии показал, что использование комплексных технических решений является эффективным инструментом защиты коммерческой тайны и обеспечения физической безопасности [6]. Гибкость системы позволяет адаптировать уровни доступа под изменяющиеся требования бизнеса и законодательства [11].

Важным аспектом эффективности системы является ее влияние на трудовую дисциплину. Автоматический учет времени прихода и ухода сотрудников, а также контроль их перемещений по территории предприятия способствуют повышению дисциплины и производительности труда [14].

Однако в процессе эксплуатации выявлены и некоторые проблемы, связанные с необходимостью регулярного обновления программного обеспечения, обучением персонала и поддержанием оборудования в технически исправном состоянии [3].

Одной из проблем стала необходимость адаптации сотрудников к новой системе контроля доступа. Некоторые работники испытывали трудности с использованием электронных ключей, особенно в первые недели после внедрения. Для решения этой проблемы были проведены дополнительные тренинги и разработаны наглядные инструкции по использованию системы [6].

Другой проблемой стала необходимость обеспечения бесперебойной работы системы в условиях производственной среды. Пыль, влажность и перепады температур, характерные для производства строительных материалов, могут негативно влиять на работу электронного оборудования. Для решения этой проблемы были использованы специальные защитные корпуса для контроллеров и считывателей, а также проводится регулярное техническое обслуживание системы [10].

Заключение

Внедрение системы контроля и управления доступом «Орион» на заводе строительных материалов позволило существенно повысить уровень безопасности предприятия, обеспечить соблюдение режима коммерческой тайны и оптимизировать процессы контроля доступа [1, 3]. Практический пример демонстрирует, что комплексный подход к защите информации и физическому контролю является залогом устойчивого развития и конкурентоспособности производства [7].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (ред. от 14.07.2022) // КонсультантПлюс. URL : http://www.consultant.ru/document/cons_doc_LAW_48-186/ (дата обращения: 03.05.2025).
2. Что такое система контроля и управления доступом (СКУД)? // Delta. 2022. URL: <https://www.delta.ru/blog/cto-takoe-skud/> (дата обращения: 03.05.2025).
3. Руководство пользователя АРМ «Орион Про». ООО «Орион». URL: <https://orion.ru/products/orion-pro/> (дата обращения: 03.05.2025).
4. Петров В.Р. Информационная безопасность в системах контроля и управления доступом // Вестник МГТУ им. Н.Э. Баумана. 2023. № 4. С. 45–53.

5. Малюк А.А. Информационная безопасность: концептуальные основы защиты информации. М.: Горячая линия-Телеком, 2021. 256 с.
6. Кузнецова М.В. Практические аспекты внедрения систем контроля доступа // Материалы конференции «Инновации в безопасности». 2024. С. 78–85.
7. Сидоров Ю.С. Интеграция систем безопасности на промышленных предприятиях. Новосибирск: СГУТиТ, 2024. 98 с.
8. ГОСТ Р 57580.1-2017. Информационная безопасность. Термины и определения. – М.: Стандартинформ, 2017. – 24 с.
9. Астахов А.М. Методы оценки рисков информационной безопасности // Информационные технологии и безопасность. 2022. № 3. С. 34–42.
10. Техническая защита информации: средства и методы // SpectrumData. 2024. URL: <https://spectrumdata.ru/blog/proverka-soiskatelya/kak-obespechit-tekhnikeskuyu-zashchitu-informatsii-na-predpriyatii/> (дата обращения: 03.05.2025).
11. Иванов И.И., Петров П.П. Современные системы контроля доступа в промышленности // Информационная безопасность. 2023. № 6. С. 12–19.
12. Российские производители систем контроля и управления доступом // SecuTeck. URL: <https://www.secuteck.ru/rossijskie-proizvoditeli-sistem-kontrolya-i-upravleniya-dostupom> (дата обращения: 03.05.2025).
13. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 01.03.2024) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 03.05.2025).
14. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 14.07.2022) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 03.05.2025).
15. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 14.07.2022) // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 03.05.2025).

© Ю. О. Якович, А. Н. Поликанин, 2025

СОДЕРЖАНИЕ

1. В. Ю. Сапегин. Метод обнаружения маскировки сетевого трафика	3
2. А. Е. Софронов. Автоматизированный стенд для сравнения производительности инструментов пассивного анализа сетевого трафика.....	12
3. А. С. Труш, Е. Ю. Воронкин. Разработка системы интеллектуального анализа деловой речи для автоматизированного создания статей.....	21
4. А. И. Удалов, А. А. Шарапов. Разработка программного модуля «Определения спелости овощей для промышленных теплиц с помощью машинного зрения»	27
5. Н. С. Федотов, Д. Ю. Смирнов. Адаптация пользовательской конфигурации «1С: Предприятие 8.2» для организации учебного процесса в вузе под версию «1С: Предприятие 8.3».....	34
6. А. Д. Филькова, А. А. Шарапов. Разработка системы автономного управления дроном с использованием компьютерного зрения для непрерывного слежения за объектом	40
7. А. А. Цыганков. Виртуальный стенд для проведения экспериментального сравнительного исследования методов активного анализа информационных систем.....	45
8. А. В. Челнокова. Система автоматизированного развертывания и технологического сопровождения инфраструктуры предприятия	52
9. А. С. Чулкова, Я. А. Карташов, А. А. Шарапов. Разработка системы мониторинга состояния дорожного покрытия для анализа и принятия решения о дальнейшей эксплуатации	61
10. С. А. Чунарева, Н. С. Головачев. Разработка интерактивной информационно-справочной трехмерной модели номерного фонда базы отдыха средствами Unreal Engine	71
11. О. А. Шведова, Е. Ю. Воронкин. Разработка программного обеспечения для генерации характеристик дизайна персонажей для видеоигр	78
12. Е. А. Шевченко, Е. Ю. Воронкин. Разработка расширения браузера для создания коллекции образцов элементов веб-страницы с использованием JavaScript	86
13. К. Г. Щербинина, А. А. Шарапов. Совершенствование системы автоматического контроля доступа на парковку СГУГиТ с использованием нейронной сети	91
14. М. Е. Арапова, В. А. Васильева, Е. Ю. Кутенкова. Анализ изменений в стандартах ЕСКД.....	96
15. А. М. Бахтиярова, Е. Д. Моисеева, Д. В. Климова, Д. М. Никулин. Использование новых термозащитных покрытий в беспилотных авиационных системах.....	101

16. Н. В. Белоконь, С. А. Горбач, А. А. Балаганский, Д. Н. Титов. Разработка камеры, совмещенной с инфракрасным датчиком движения на базе ESP32	107
17. П. Ф. Бжицких, А. А. Шрамков, В. П. Цыплаков, Е. Ю. Кутенкова. Сравнение инструментов искусственного интеллекта с российской системой по оптимизации оформления дипломной работы	111
18. Н. Р. Воронина, А. А. Киселев, В. М. Белов. Нейросетевая модель классификатора объектов КИИ.....	115
19. Н. И. Егоренко, М. П. Егоренко. Анализ качества аппроксимации выборки EMNIST-букв моделью CNN	122
20. Д. В. Железных, Д. Д. Сизиков, Н. М. Дорохова, Ю. М. Карлина. Разработка сайта интернет-магазина	129
21. М. С. Исмаилова, С. А. Арбузов. Исследование возможности применения недорогих MEMS инерциальных датчиков для реализации технологии захвата движения	133
22. И. С. Кажикин, М. И. Сидельников, П. Л. Солеева. Анализ требований к обработке информации в автоматизированных информационных системах	141
23. Д. А. Кондрашин, Г. А. Казанцев, Е. В. Рыжкова. Универсальный аудит безопасности обработки персональных данных	148
24. В. Р. Костылева, А. М. Бахтиярова, М. С. Исмаилова, И. В. Парко. Новые горизонты космоса: российские корабли нового поколения.....	155
25. А. Д. Крюков, Е. М. Попырин, Б. Н. Примин, Н. М. Дорохова. Перспективы внедрения электрического транспорта на примере города Новосибирска.....	161
26. А. А. Кутенков. Искусственный интеллект в генерации кода	165
27. Е. А. Лебедев, И. В. Парко. Конструктивные особенности лобовых стекол легковых автомобилей.....	171
28. К. А. Литягин, С. А. Солмин, Н. В. Сафонова Н. М. Дорохова. Резонатор Гельмгольца	176
29. Р. А. Ложков, И. В. Парко. Сверхлегкая оптика для наноспутника	179
30. Р. А. Ложков, Д. А. Учаев, И. В. Парко. Танковая оптика	184
31. С. А. Лысенко, К. С. Юшков, Е. В. Рыжкова. Чат-бот как средство повышения киберграмотности учащихся посредством интерактивных заданий	188
32. Е. А. Малёж, Г. В. Симонова. Входной контроль средств допускного контроля на соответствие установленным требованиям	195
33. А. Ф. Миннимухаметова, Е. В. Рыжкова. Статический и динамический анализ: два инструмента для идеального кода.....	199
34. П. Н. Миронов, Д. А. Аничев. Автоматизация учета геодезического оборудования и обработки заявок в GLPI: практическое руководство для инженеров.....	206

35. А. Н. Патрин, А. И. Петров, Д. Н. Титов. Автоматизированная система сигнализования несанкционированного физического доступа к объекту защиты	213
36. А. Ю. Песков, В. И. Ковынев, Е. Ю. Кутенкова. Анализ операций резьбонарезания.....	219
37. А. В. Попиль, Р. П. Пак, О. В. Грицкевич. Виртуальный проектный офис: преимущества и недостатки	225
38. В. А. Сафонова, Д. А. Железных, Н. М. Дорохова. Перспективы развития водородного транспорта в России.....	233
39. П. А. Уфилин, Д. А. Аничев. Кадастр как сервис: адаптация ITSM- принципов в управлении земельно-имущественными процессами.....	237
40. Д. А. Шергин, Д. Е. Пешков. Разработка виртуального стенда для практического тестирования информационной безопасности Active Directory	242
41. Ю. О. Якович, А. Н. Поликанин. СКУД "Орион": Реализация на практическом примере	249

CONTENTS

1. V. Yu. Sapegin. Method for detecting network traffic obfuscation	3
2. A. E. Sofronov. Automated test bench for performance comparison of passive network traffic analysis tools	12
3. A. S. Trush, E. Y. Voronkin. Development of an intelligent business speech analysis system for automated article creation.....	21
4. A. I. Udalov, A. A. Sharapov. Development of the software module "Determining the ripeness of vegetables for industrial greenhouses using machine vision"	27
5. N. S. Fedotov, D. Yu. Smirnov. Adaptation of the custom configuration "1C: Enterprise 8.2" for educational process at university under the version "1C: Enterprise 8.3"	34
6. A. D. Filkova, A. A. Sharapov. Development of an autonomous drone control system using computer vision for continuous object tracking.....	40
7. A. A. Tsygankov. Virtual stand for experimental comparative study of active analysis methods for information systems	45
8. A. V. Chelnokova. System of automated deployment and technological support of enterprise infrastructure	52
9. A. S. Chulkova, Y. A. Kartashov, A. A. Sharapov. Development of a road surface condition monitoring system for analysis and decision-making on further operation.....	61
10. S. A. Chunareva, N. S. Golovachev. Development of an interactive information and reference three-dimensional model of the number of rooms of the recreation center using Unreal Engine	71
11. O. A. Shvedova, E. Yu. Voronkin. Software development for generating character design characteristics for video games	78
12. E. A. Shevchenko, E. Yu. Vononkin. Developing a browser extension to create a collection of sample web page elements using JavaScript	86
13. K. G. Scherbinina, A. A. Sharapov. Improvement of the automatic parking SSUGT access control system using a neural network.....	91
14. M. E. Arapova, V. A. Vasilyeva, E. Yu. Kutenkova. Analysis of changes in the ESKD standards.....	96
15. A. M. Bakhtiyarova, E. D. Moiseeva, D. V. Klimova, D. M. Nikulin. Use of new thermal protective coatings in unmanned aircraft systems	101
16. N. V. Belokon, S. A. Gorbach, A. A. Balagansky, D. N. Titov. Development of a camera integrated with a PIR motion sensor based on ESP32	107
17. P. F. Brzickih, V. P. Tsyplakov, A. A. Shramkov, E. U. Kutenkova. Comparison of artificial intelligence tools with the russian system for optimizing the design of thesis papers.....	111

18. N. R. Voronina, A. A. Kiselyov, V. M. Belov. Neural network model of the CII object classifier.....	115
19. N. I. Egorenko, M. P. Egorenko. Analysis of approximation quality of EMNIST letter samples using a CNN model.....	122
20. D. V. Zheleznykh, D. D. Sizikov, N. M. Dorokhova, Yu. M. Karlina. Development of an online store website	129
21. M. S. Ismailova, S. A. Arbuzov. Exploring the possibility of using inexpensive MEMS inertial sensors to implement motion capture technology	133
22. I. S. Kazhikin, M. I. Sidelnikov, P. L. Soleeva. Analysis of information processing requirements in automated information systems	141
23. D. A. Kondrashin, G. A. Kazantsev, E. V. Ryzhkova. Universal audit of personal data processing security	148
24. V. R. Kostyleva, A. M. Bakhtiyarova, M. S. Ismailova, I. V. Parko. New horizons of space: russian spaceships of the new generation	155
25. A. D. Kryukov, E. M. Popyrin, B. N. Primin, N. M. Dorokhova. Prospects for the introduction of electric transport using the example of the city of Novosibirsk	161
26. A. A. Kutenkov. Artificial intelligence in code generation	165
27. E. A. Lebedev, I. V. Parko. Design features of windshields of passenger cars.....	171
28. K. A. Lityagin, S. A. Solmin, N. V. Safonova, N. M. Dorokhova. Helmholtz Resonator	176
29. R. A. Lozhkov, I. V. Parko. Ultralight optics for nanosatellite	179
30. R. A. Lozhkov, D. A. Ychaev, I. V. Parko. Tank optics	184
31. S. A. Lysenko, K. S. Yushkov, E. V. Ryzhkova. Chatbot as a means of increasing students' cyber literacy through interactive tasks	188
32. E. A. Malezh, G. V. Simonova. Input control of access control equipment for compliance with established requirements.....	195
33. A. F. Minnimuhametova, E. V. Ryzhkova. Static and dynamic analysis: two tools for perfect code	199
34. P. A. Mironov, D. A. Anichev. Automation of geodetic equipment accounting and application processing at GLPI: a practical guide for engineers	206
35. A. N. Patrin, A. I. Petrov, D. N. Titov. Automated alarm system for unauthorized physical access to a security facility	213
36. A. Yu. Peskov, V. I. Kovynev, E. Yu. Kutenkova. Analysis of thread cutting operations	219
37. A. V. Popil, R. P. Pak, O. V. Gritskevich. Virtual project office: advantages and disadvantages	225
38. V. A. Safonova, D. A. Zheleznykh, N. M. Dorokhova. Prospects for the development of hydrogen transport in Russia.....	233
39. P. A. Ufillin, D. A. Anichev. Cadastre as a service: adaptation of ITSM-principles in the management of land and property processes.....	237
40. D. A. Shergin, D. E. Peshkov. Development of a virtual bench for practical testing of Active Directory information security	242

41. Y. O. Yakovich, A. N. Polikanin. SKUD "Orion": implementation using a practical example..... 249

Научное издание

ИНТЕРЭКСПО ГЕО-СИБИРЬ

XXI Международный научный конгресс

Сборник материалов в 8 т.

Т. 7

**Научно-технологическая конференция
молодых ученых**

«МОЛОДЕЖЬ. ИННОВАЦИИ. ТЕХНОЛОГИИ»

№ 3

Материалы публикуются в авторской редакции

Компьютерная верстка *А. П. Бочарникова*

Изд. лиц. ЛР № 020461 от 04.03.1997.

Подписано в печать 25.09.2025. Формат 60 × 84 1/16.

Усл. печ. л. 15,17. Тираж 34 экз. Заказ 116.

Гигиеническое заключение

№ 54.НК.05.953.П.000147.12.02. от 10.12.2002.

Редакционно-издательский отдел СГУГиТ
630108, Новосибирск, ул. Плеханова, 10.

Отпечатано в картопечатной лаборатории СГУГиТ
630108, Новосибирск, ул. Плеханова, 8.